p-adic Galois representations and (φ, Γ)-modules

by

Dávid Szabó

Master's Thesis

Supervisor: Gergely Zábrádi
Department of Algebra and Number Theory

Eötvös Loránd University
Faculty of Sciences

Budapest, June 2015

Acknowledgement

I would like to express my appreciation to my supervisor Gergely Zábrádi for introducing me to the topic and giving me the readings. I am grateful for his help, for the discussions we had as well as for his patience.

I am truly grateful for the constant support of my parents Elemér Szabó and Katalin Rózsa. I would also like to thank Áron Szabó for his comments on the draft.

Papa emlékére

Contents

Introduction and overview

Algebraic number fields are finite extensions of the field $\mathbb{Q}$ of the rational numbers. Every number field can be embedded to a finite Galois extension of $\mathbb{Q}$. Studying the corresponding Galois groups is a central topic in algebraic number theory. Consider an algebraic closure $\mathbb{Q}^{\text{alg}}$ of $\mathbb{Q}$. Then $\mathbb{Q}^{\text{alg}}/\mathbb{Q}$ is an (infinite) Galois extension. By the Fundamental Theorem of Galois Theory, the Galois group of this extension contains the Galois group of every finite Galois extension of $\mathbb{Q}$ as a quotient. So we can study all finite Galois extension at once by investigating the so called absolute Galois group $G_{\mathbb{Q}} := \text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$ of $\mathbb{Q}$. However, this group is far from being completely understood.

One approach is to study $G_{\mathbb{Q}}$ via the field $\mathbb{Q}_p$ of p-adic numbers for a prime number p. Let $G_{\mathbb{Q}_p} := \text{Gal}(\mathbb{Q}_p^{\text{alg}}/\mathbb{Q}_p)$ be the absolute Galois group of $\mathbb{Q}_p$. $\mathbb{Q}$ embeds to $\mathbb{Q}_p$, and any injection $\mathbb{Q}^{\text{alg}} \hookrightarrow \mathbb{Q}_p^{\text{alg}}$ gives rise to an embedding $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$. In this way $G_{\mathbb{Q}_p}$ can be identified with a (closed) subgroup of $G_{\mathbb{Q}}$ for any p which motivates studying the group $G_{\mathbb{Q}_p}$. It is a general technique to study this group via its linear B-representations, i.e. identifying $G_{\mathbb{Q}_p}$ with a subgroup of automorphism group of finitely generated B-modules. Such representations are called Galois representations of $\mathbb{Q}_p$. Jean-Marc Fontaine developed a theory ([FO] or [Fon90]) amongst other for various cases for B: the finite field $\mathbb{F}_p$ of order p (mod p representations), the ring $\mathbb{Z}_p$ of p-adic integers, or $\mathbb{Q}_p$ (p-adic representations) where p is the same prime that we fixed at the beginning of this paragraph. Fontaine defined the category of (φ, Γ)-modules which is equivalent to the category of B-representations of $G_{\mathbb{Q}_p}$. This new category is better understood and the calculations in this category are simpler. The goal of this thesis to give an introduction to Fontaine's theory for those having the knowledge of standard abstract algebra at MSc level.

In the first chapter, we review some topics that are necessary to understand the theory.

In the second chapter we study the absolute Galois group of an arbitrary field E of characteristic $p > 0$. Interestingly, this theory needs to be developed in order to study our goal. Here we introduce the category of φ-modules.

In the first section, we first study the $\mathbb{F}_p$-representations. The main result is that the category of $\mathbb{F}_p$-representation of E is equivalent to the category of the so called φ-modules over E, which we will define. This section contains most of the ideas needed for later sections and chapter so we give a very detailed proof of the equivalence building only

on standard undergraduate knowledge.
In the following section, we prove a similar result for $\mathbb{Z}_p$ and $\mathbb{Q}_p$-representations. These categories are also equivalent to a category of φ-modules, but this time over a more complicated ring, called the Cohen ring. The main difficulty of the proof lies in the construction of the Cohen ring.

In the third and final chapter, we present out original goal, the representations of $G_{\mathbb{Q}}$. In fact, more generally, we investigate the representations of the absolute Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ of a general p-adic field K, i.e. a finite extension of $\mathbb{Q}_p$. The main result of this chapter is Fonatine's fundamental theorem: $K_\infty/K \cong \mathrm{Gal}(E_K^{\mathrm{alg}^{\mathrm{alg}}}/E_K)$ for some intermediate $\mathbb{Z}_p$-extension $K^{\mathrm{sep}}/K_\infty/K$ and for some field E_K of characteristic p. This verifies the necessity of studying the Galois representations of fields of characteristic p. The remaining action of $\Gamma_K = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ describes the full absolute Galois group of K. With this, theory of φ-modules is extended to the theory of (φ, Γ)-modules to which the category is of Galois representations is equivalent.
In the final section, we demonstrate how to use this theory to calculate certain p-cohomological dimensions, a result due to Laurent Herr. Although it is an important fact that statement of this theorem is independent of the theory of (φ, Γ)-modules, this theory can be used to prove the theorem.

Chapter 1

Preliminaries

1.1 Category of B-representations

Definition 1.1.1 (Topological group, ring, module)**.** G is a *topological group*, if $(G, \cdot)$ is a group and a topological space such that the following maps are continuous:

$$G \to G \qquad g \mapsto g^{-1}, \qquad\qquad G \times G \to G \qquad (g_1, g_2) \mapsto g_1 \cdot g_2,$$

B is a *topological ring*, if $(B, +, \cdot)$ is a ring and a topological space such that the following maps are continuous:

$$B \times B \to B \quad (\lambda_1, \lambda_2) \mapsto \lambda_1 + \lambda_2, \qquad\qquad B \times B \to B \quad (\lambda_1, \lambda_2) \mapsto \lambda_1 \cdot \lambda_2,$$

X is a *topological B-module*, if B is a topological ring, X is a B-module and a topological space such that the following maps are continuous:

$$X \times X \to X \quad (x_1, x_2) \mapsto x_1 + x_2, \qquad\qquad B \times X \to X \qquad (\lambda, x) \mapsto \lambda x.$$

The product spaces above are all endowed with the product topology.

Definition 1.1.2 (B-representation)**.** X is called a *B-representation of G* if G is topological group, B be a commutative topological ring and X be a finitely generated topological B-module with continuous G actions on B and on X such that for all $g \in G, \lambda, \lambda_1, \lambda_2 \in B, x, x_1, x_2 \in X$

$$\begin{aligned} g(\lambda_1 + \lambda_2) &= g(\lambda_1) + g(\lambda_2), & g(\lambda_1 \lambda_2) &= g(\lambda_1) g(\lambda_2), \\ g(x_1 + x_2) &= g(x_1) + g(x_2), & g(\lambda x) &= g(\lambda) g(x). \end{aligned}$$

We shall refer the bottom line as *G-semi-linearity*. When no natural topology is given, we usually take the discrete topology to ensure continuity. When B is a field and the G-action on B is trivial (i.e. $g(\lambda) = \lambda$), this notion gives the usual linear group representation.

Definition 1.1.3 (Category of B-representations of G)**.** Fix topological group G which acts continuously on a fixed commutative topological ring B. We can define the category $\mathbf{Rep}_B(G)$, where the objects are the B-representations of G and the morphisms are the B-module homomorphisms commuting with the action, i.e.

$$\mathrm{Mor}_{\mathbf{Rep}_B(G)}(X, X') := \{\theta \in \mathrm{Mor}_{B-\mathrm{mod}}(X, X) : \forall g \in G \quad \theta \circ g = g \circ \theta\}.$$

Definition 1.1.4. Given $V_1, V_2 \in \mathrm{Obj}(\mathbf{Rep}_B(G))$, $V_1 \otimes_B V_2 \in \mathrm{Obj}(\mathbf{Rep}_B(G))$ where for $g \in G$ the action is defined as

$$g\left(\sum_{i=1}^{r} v_i \otimes v_i'\right) := \sum_{i=1}^{r} g(v_i) \otimes g(v_i').$$

Definition 1.1.5 (Abelian category)**.** A category is said to be *abelian*, if it has a zero object, has all binary products and coproducts, has all kernels and cokernels, and every monomorphism is the kernel of some morphism and every epimorphism is the cokernel of some morphism.

Lemma 1.1.6. $\mathbf{Rep}_B(G)$ *is abelian.*

Note. Any module category is abelian.

1.2 Infinite Galois theory, Galois representations

Definition 1.2.1 (Inverse system, inverse limit, profinite topology)**.** Let $\mathcal{C}$ be a category with infinite products. Let I be a directed set (i.e. a partially ordered set where any two elements have a common upper bound). $\{A_i \in \mathrm{Obj}(\mathcal{C}) : i \in I\}$ and the transition maps $\{f_{ji} \in \mathrm{Mor}_{\mathcal{C}}(A_j, A_i) : i \leq j \in I\}$ form an *inverse system* if $f_{ii} = \mathrm{Id}_{A_i}$ and $f_{ji} \circ f_{kj} = f_{ki}$ for any $i \leq j \leq k \in I$.
In this setup we define the *inverse (or projective) limit* as follows

$$\varprojlim_{i \in I} A_i := \left\{ (a_i)_{i \in I} \in \prod_{i \in I} A_i : \forall i \leq j \in I \quad f_{ji}(a_j) = a_i \right\} \in \mathrm{Obj}(\mathcal{C}).$$

For the category of topological spaces/groups/rings $\varprojlim_{i \in I} A_i$ is endowed with the subspace topology of the product topology. When no topology is given, we usually take the discrete topology on each A_i. When each A_i is a finite group with discrete topology, then the induced topology on $\varprojlim_{i \in I} A_i$ is called the *profinite topology* and this group is called a profinite group.

Definition 1.2.2 (Direct system, direct limit)**.** Let $\mathcal{C}$. A I be a directed set with $\{A_i \in \mathrm{Obj}(\mathcal{C}) : i \in I\}$ and transition maps $\{f_{ij} \in \mathrm{Mor}_{\mathcal{C}}(A_i, A_j) : i \leq j \in I\}$ form a *direct system* if $f_{ii} = \mathrm{Id}_{A_i}$ and $f_{jk} \circ f_{ij} = f_{ik}$ for any $i \leq j \leq k \in I$.
In this setup we define the *direct (or inductive) limit* as

$$\varinjlim_{i \in I} A_i := \bigsqcup_{i \in I} A_i \,/_{\sim} \in \mathrm{Obj}(\mathcal{C}),$$

a quotient of the disjoint union where $A_i \ni a_i \sim a_j \in A_j \iff \exists i, j \leq k \in I \quad f_{ik}(a_i) = f_{jk}(a_j)$.

Definition 1.2.3 (Normal, separable, Galois extension)**.** Let L/K be a (possibly infinite) algebraic extension, $\alpha \in L$ with minimal polynomial $m_\alpha \in L[X]$ over K.
L/K is *normal*, if $\forall \alpha \in L$, m_α splits into linear factors in $L[X]$ (i.e. all conjugates of α lie in L).
L/K is *separable*, if $\forall \alpha \in L$ is separable, i.e. m_α is separable, i.e. $\gcd(m_\alpha, m'_\alpha) = 1$ where m'_α denotes the formal derivative of m_α.
L/K is *Galois*, if it is normal and separable, i.e. if $\forall \alpha \in L$, m_α has $\deg m_\alpha$ many distinct roots in L. For such an extension, its *Galois group* is defined to be $\mathrm{Gal}(L/K) := \{g \in \mathrm{Aut}(L) : g\big|_K = \mathrm{Id}\}$.

Lemma 1.2.4 (Artin)**.** *Let L be an arbitrary field with subgroup $G \leq \mathrm{Aut}(L)$ of order $n < \infty$ and let $K := L^G := \{\alpha \in L : \forall g \in G \quad g(\alpha) = \alpha\}$. Then L/K is a Galois extension of order n with Galois group G.*

Proof. Pick $\alpha \in L$. Choose $\mathrm{Id} \in S \subseteq G$ maximal (with respect to containment) such that $|\{s(\alpha) : s \in S\}| = |S|$. Let $f(X) := \prod_{s \in S}(X - s(\alpha)) \in L[X]$, a separable polynomial having α as its root with $\deg f = |S| \leq |G| = n$. Let $g \in G$ be arbitrary. Then for all $s \in S$, there is an $s' \in S$ such that $gs(\alpha) = s'\alpha$ by the maximality of S. Thus some permutation takes $(gs(\alpha))_{s \in S}$ into $(s(\alpha))_{s \in S}$, so $f(X)$ is invariant under the action of G, i.e. in fact $f(X) \in L^G[X] = K[X]$. Then α is a solution of a separable polynomial of degree at most n that is splitting into distinct factors over K, meaning that L/K is Galois with $[L : K] \leq n$. But from $G \leq \mathrm{Gal}(L/K)$, $n = |G| \leq \mathrm{Gal}(L/K) = [L : K] \leq n$, thus equality holds everywhere meaning that $G = \mathrm{Gal}(L/K)$. □

Lemma 1.2.5 (Dedekind)**.** *If L/K is a finite Galois extension of degree n, $\mathrm{Gal}(L/K) = \{g_i : 1 \leq i \leq n\}$ be its Galois group, $\{\alpha_j \in L : 1 \leq j \leq n\}$ is a K-basis for L, then the matrix $(g_i(\alpha_j))_{1 \leq i,j \leq n}$ is invertible over L.*

Proof. This is a special case of [Mil14, Corollary 5.16]. □

Example 1.2.6 (Finite Galois extensions form an inverse system)**.** Let L/K be a Galois extension of fields and let $\mathcal{E} := \{E \subseteq L : E/K \text{ finite Galois}\}$. $\mathcal{E}$ is made a partially ordered set by inclusion. Note that this is also a directed set, since for $E_1, E_2 \in \mathcal{E}$, $E_1, E_2 \subseteq E_1E_2 \in \mathcal{E}$ is a common upper bound. For $E_1 \subseteq E_2 \in \mathcal{E}$ define the transition maps as the restrictions $\mathrm{Gal}(E_2/K) \to \mathrm{Gal}(E_1/K), \quad g \mapsto g\big|_{E_1}$. These maps are indeed well defined.

Lemma 1.2.7. *In the setup of Example 1.2.6, we have the following natural isomorphism of groups.*

$$\mathrm{Gal}(L/K) \to \varprojlim_{E \in \mathcal{E}} \mathrm{Gal}(E/K), \qquad g \mapsto \left(g\big|_E\right)_{E \in \mathcal{E}}$$

Proof. Since every element $\alpha \in L$ is in a finite Galois extension, namely the splitting field of the minimal polynomial of α over K, $\bigcup \mathcal{E} = L$, so defining the Galois action over all this subfield defines the action completely, so this is indeed an injection.

On the other hand, for $(\gamma_E)_{E\in\mathcal{E}} \in \varprojlim_{E\in\mathcal{E}} \mathrm{Gal}(E/K)$, we can find its preimage $g \in \mathrm{Gal}(L/K)$ defined by $g(\alpha) = \gamma_E(\alpha)$ where $\alpha \in L = \bigcup \mathcal{E}$ and E is any field such that $\alpha \in E \in \mathcal{E}$. This is well defined, since for any choice of such fields E_1, E_2, the compatibility of the transition maps implies $\gamma_{E_1}(\alpha) = (\gamma_{E_1E_2})\big|_{E_1}(\alpha) = \gamma_{E_1E_2}(\alpha) = (\gamma_{E_1E_2})\big|_{E_2}(\alpha) = \gamma_{E_2}(\alpha)$. □

Definition 1.2.8 (Krull topology)**.** Let L/K is a Galois extension. The topology on $\mathrm{Gal}(L/K)$ induced by isomorphism of Lemma 1.2.7 is called the *Krull topology* where $\varprojlim_{E\in\mathcal{E}} \mathrm{Gal}(E/K)$ is endowed with the profinite topology.

Remark 1.2.9. The Krull topology is compatible with the group operations, so $\mathrm{Gal}(L/K)$ is a topological group. Then the isomorphism of Lemma 1.2.7 is also a homeomorphism of the topological spaces. With the Krull topology, $\mathrm{Gal}(L/K)$ has the following neighbourhood basis at $g \in \mathrm{Gal}(L/K)$:

$$\Big\{\{g' \in \mathrm{Gal}(L/K) : g'\big|_E = g\big|_E\} : E \in \mathcal{E}\Big\}.$$

$\mathrm{Gal}(L/K)$ is a Hausdorff, compact, and totally disconnected topological group, in fact these properties characterise profinite groups.

Theorem 1.2.10 (Fundamental Theorem of Galois Theory, [Mil14, Thm. 7.12])**.** *Let L/K be a Galois extension. Then the following maps are inverses of each other*

$$\begin{aligned}\{H \le \mathrm{Gal}(L/K) \text{ closed subgroup}\} &\leftrightarrow \{F : L/F/K \text{ intermediate field}\}\\ H &\mapsto L^H := \{\alpha \in L : \forall h \in H \quad h(\alpha) = \alpha\}\\ \mathrm{Gal}(L/F) &\hookleftarrow F\end{aligned}$$

Furthermore

$$\begin{aligned}\mathrm{Gal}(L/F) \le \mathrm{Gal}(L/K) \text{ is open} &\iff F/K \text{ is finite}\\ &\implies |\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)| = [F : K]\end{aligned}$$

and

$$\begin{aligned}\mathrm{Gal}(L/F) \le \mathrm{Gal}(L/K) \text{ is normal} &\iff F/K \text{ is Galois}\\ &\implies \mathrm{Gal}(L/K) \Big/ \mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K)\end{aligned}$$

Definition 1.2.11 (Perfect field)**.** A field k is *perfect*, if all irreducible polynomials in $k[X]$ are separable.

Lemma 1.2.12. *k is perfect if and only if* $\mathrm{char}\, k = 0$ *or the Frobenius $\sigma : x \mapsto x^p$ is an isomorphism for* $0 < p := \mathrm{char}\, k$.

Proof. See [Mil14, proposition 2.16]. □

Example 1.2.13. Finite fields and fields of characteristic 0, such as $\mathbb{Q}$ and $\mathbb{Q}_p$, are perfect.

By Zorn's lemma, every field K has an *algebraic closure*, i.e. an algebraic extension of K which is also algebraically closed. We denote one algebraic closure by K^{alg}. Algebraic closures are typically not unique, but all algebraic closures are isomorphic.

Definition 1.2.14 (Separable closure)**.** The *separable closure* of a K field is defined to be

$$K^{\text{sep}} := \{\alpha \in K^{\text{alg}} : \alpha \text{ is separable over } K\}$$

where K^{alg} is a fixed algebraic closure.

Note that K^{sep}/K is indeed a field extension which is separable by definition and it is also normal since K^{alg} is algebraically closed. Note that by definition if K is perfect, then $K^{\text{sep}} = K^{\text{alg}}$.

By the definitions, we have the following observation.

Lemma 1.2.15. *If $f \in K^{\text{sep}}[X]$ is separable (i.e. if $\gcd(f, f') = 1$), then f has $\deg f$ many distinc roots in K^{sep}.*

Since every element of K^{sep} lies in a finite Galois extension of K (namely in th Galois closure of $K(\alpha)$, and K^{sep}/K contains every finite Galois extension of K.

Definition 1.2.16 (Absolute Galois group, Galois representation)**.** Define the *absolute Galois group* of an arbitrary field K by $G_K := \text{Gal}(K^{\text{sep}}/K)$.
A B-representation of $\text{Gal}(K^{\text{sep}}/K)$ is called the *Galois B-representation* of K.

We see that to study finite Galois extensions of K, it is enough to study its absolute Galois group, because every Galois group of a finite finite Galois extension of K is a quotient of the absolute Galois group. In this sense, K^{sep}/K is the largest Galois extension. From Lemma 1.2.7 we see the following.

Lemma 1.2.17.

$$\text{Gal}(K^{\text{sep}}/K) \cong \varprojlim_{\substack{E/K \\ \textit{finite Galois}}} \text{Gal}(E/K)$$

1.3 Semi-linear maps

Let B be a ring with 1, M be a B-module and $\sigma : B \to B$ be a ring homomorphism.

Definition 1.3.1 (σ-semi-linearity)**.** We say a map $\varphi : M \to M$ is *σ-semi-linear* if for all $\lambda \in B, x, x_1, x_2 \in M$

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

We can define a module over B similar to the tensor product with which the φ map becomes linear.

Definition 1.3.2. Let $B \otimes_\sigma M := M_\sigma := {}^{F(B\times M)}/_{\sim}$ be the quotient of free B-module where the equivalence relation is defined by

$$\begin{aligned} &(\lambda_1+\lambda_2,x)\sim(\lambda_1,x)+(\lambda_2,x), && (\lambda_1\lambda_2,x)\sim\lambda_1(\lambda_2,x),\\ &(\lambda,x_1+x_2)\sim(\lambda,x_1)+(\lambda,x_2), && (\lambda_1,\lambda_2x)\sim(\lambda_1\sigma(\lambda_2),x) \end{aligned}$$

for $\lambda,\lambda_1,\lambda_2\in B, x,x_1,x_2\in M$. The equivalence class of (λ,x) is denoted by $\lambda\otimes_\sigma x$.

Lemma 1.3.3. *The following maps are mutually inverses of each other.*

$$\begin{aligned} \{\varphi : M\to M \quad \sigma\text{-semi-linear}\} &\leftrightarrow \{\Phi : M_\sigma \to M \quad B\text{-linear}\}\\ \Phi_{(\cdot)} : \varphi &\mapsto \left(\Phi_\varphi : \sum_{i=1}^r \lambda_i\otimes_\sigma x_i \mapsto \sum_{i=1}^r \lambda_i\varphi(x_i)\right)\\ (\varphi_\Phi : x\mapsto \Phi(1\otimes_\sigma x)) &\mapsfrom \Phi : \varphi_{(\cdot)} \end{aligned}$$

Proof. Suppose $\varphi : M\to M$ is a σ-semi-linear map. Then by definitions we have

$$\Phi_\varphi\left(\sum_{i=1}^r \lambda_i\otimes\lambda_i'x_i\right) = \sum_{i=1}^r \lambda_i\varphi(\lambda_i'x_i) = \sum_{i=1}^r \lambda_i\sigma(\lambda_i')\varphi(x_i) = \Phi_\varphi\left(\sum_{i=1}^r \lambda_i\sigma(\lambda_i')\otimes x_i\right)$$

i.e. Φ_φ does not depend on the choice of the representative. By the definition of scalar multiplication, Φ_φ is B-indeed linear. On the other hand, if $\Phi : M_\sigma\to M$ is B-linear, then $\varphi_\Phi(\lambda x) = \Phi(1\otimes_\sigma\lambda x) = \Phi(\sigma(\lambda)\otimes_\sigma x) = \sigma(\lambda)\Phi(1\otimes_\sigma x) = \sigma(\lambda)\varphi(x)$, so φ_Φ is indeed σ-semi-linear. Finally $\varphi_{\Phi_\varphi}(x) = \Phi_\varphi(1\otimes_\sigma x) = \varphi(x)$ and

$$\Phi_{\varphi_\Phi}\left(\sum_{i=1}^r \lambda_i\otimes_\sigma x_i\right) = \sum_{i=1}^r \lambda_i\varphi_\Phi(x_i) = \sum_{i=1}^r \lambda_i\Phi(1\otimes_\sigma x_i) = \Phi\left(\sum_{i=1}^r \lambda_i\otimes_\sigma x_i\right)$$

shows that the maps are inverses of each other. □

Definition 1.3.4. Let M be a free B-module of rank $d<\infty$ with an E-basis $\{e_i : 1\le i\le d\}$ and $\varphi : M\to M$ be a σ-semi-linear map. Define the corresponding matrix

$$\mathsf{A}_M := (a_{ij})$$

by $\varphi(e_i) = \sum_{j=1}^d a_{ij}e_j$ for $1\le i\le d$.

Lemma 1.3.5. *In the setup of Definition 1.3.4*

$$\Phi_\varphi \text{ is an isomorphism} \iff \sum_{x\in M} B\varphi(x) = M \iff \mathsf{A}_M\in \mathrm{GL}_d(E).$$

Proof. First note that $\{1\otimes_\sigma e_i : 1\le i\le d\}$ is a basis for M_σ, thus M_σ is also a free B-module of rank d.

If Φ_φ is an isomorphism, Φ_φ is surjective, so there are $a'_{ij} \in E$ for $1 \leq i, j \leq d$ such that $\Phi_\varphi\left(\sum_{j=1}^d a'_{ij} \otimes e_j\right) = \sum_{j=1}^d a'_{ij}\varphi(e_j) = e_i$ which means that $(a'_{ij}) = \mathsf{A}_M^{-1}$ and that $\varphi[M]$ spans M. On the other hand, if A_M is invertible and $\mathsf{A}_M^{-1} = (a'_{ij})$, then since Φ_φ maps $\sum_{j=1}^d \left(\sum_{i=1}^d \lambda_i a'_{ij}\right) \otimes e_j$ to $\sum_{j=1}^d \lambda_i e_i$, an arbitrary element of M, so Φ_φ is surjective and $\varphi[M]$ spans M. Since $\dim_E M = \dim_E M_\sigma$ is finite by assumption, Φ_φ is injective, so it is an isomorphism. □

1.4 Completion of a ring with respect to a filtration

This subsection is based on [Ati69, Chapter 10] and [Mat80, Chapter 9]. Let A be a commutative ring with 1.

Definition 1.4.1 (Decreasing filtration, associated topology)**.** $\{I_n : n \in \mathbb{N}\}$ is a *decreasing filtration of* A if $I_n \leq A$ is an ideal for all n, $I_0 = A$, $I_n \supseteq I_{n+1}$ for all $n \in \mathbb{N}$ and $I_n I_k \subseteq I_{n+k}$ for all $n, k \in \mathbb{N}$.
The *topology associated to the decreasing filtration* is defined by letting $\{r + I_n : n \in \mathbb{N}\}$ be a neighbourhood basis at $r \in A$. This makes A into a topological ring.

We can define convergence on A with respect to this topology as follows.

Definition 1.4.2 (Convergence, Cauchy sequences, completeness)**.** Let $\{I_n : n \in \mathbb{N}\}$ be a decreasing filtration of A and $(r_n)_{n\in\mathbb{N}}$ be a sequence in A.
$(r_n)_{n\in\mathbb{N}}$ *converges to* $r \in A$, if $(\forall n \in \mathbb{N})(\exists K \in \mathbb{N})(\forall k \geq K)(r_k - r \in I_n)$.
$(r_n)_{n\in\mathbb{N}}$ is *Cauchy*, if $(\forall n \in \mathbb{N})(\exists N_n \in \mathbb{N})(\forall k, m \geq N_n)(r_k - r_m \in I_n)$.
A is *complete* (with respect to the filtration) if every Cauchy sequence converges in A.

Intuitively, having a difference in I_n for big n means the two elements are close to each other.

Definition 1.4.3 (Completion)**.** We define the completion of A with respect to the decreasing filtration as

$$\widehat{A} := \{(r_n)_{n\in\mathbb{N}} : (r_n)_{n\in\mathbb{N}} \text{ is Cauchy in } A\} \,/_\sim$$

where $(r_n)_{i\in\mathbb{N}} \sim (r'_n)_{n\in\mathbb{N}}$ if and only if $(r_n - r'_n)_{n\in\mathbb{N}}$ converges to 0. Addition and multiplication are defined point-wise.

Lemma 1.4.4. *The following map is an isomorphism of topological rings*

$$\theta : \widehat{A} \to \varprojlim_{n\in\mathbb{N}} A/I_n, \qquad [(r_n)_{n\in\mathbb{N}}] \mapsto (r_{N_n} + I_n)_{n\in\mathbb{N}}.$$

where N_n is an index from Definition 1.4.2 of a Cauchy sequence.

Proof. If $(r'_n)_{n\in\mathbb{N}} \sim (r_n)_{n\in\mathbb{N}}$, then $r_{N_n} + I_n = r_k + I_n = r'_k + I_n = r'_{N'_n} + I_n$ for $k = \max\{N_n, N'_n, K\}$ where N_n, N'_n are from the Cauchy sequences and K is from the

convergence of the difference, so θ does not depend on the choice of the representative. $\mathbb{N}$ has the usual ordering, the transition map is ${}^{A}/_{I_m} \to {}^{A}/_{I_n}, r + I_m \mapsto r + I_n$, which is well defined since $I_n \supseteq I_m$ for $n \leq m$. We see that $r_{N_m} + I_n = r_k + I_n = r_{N_n} + I_n$ for $k = \max\{N_m, N_n\}$ by the definition of a Cauchy sequence, thus the image under θ is compatible with the transition maps. This shows that θ is well-defined. We also see that θ is a homomorphism.

Let $(r_n)_{n\in\mathbb{N}} \in \ker\theta$. Then $r_{N_n} - 0 = r_{N_n} \in I_n$ for all n which means that $(r_n)_{n\in\mathbb{N}} \sim (0)_{n\in\mathbb{N}}$ thus the kernel is trivial, so θ is injective.

Let $(r_n + I_n)_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} {}^{A}/_{I_n}$. Then from the compatibility of the transition maps, $r_m - r_n \in I_n$ for $m \geq n$, thus $N_n = n$ makes $(r_n)_{n\in\mathbb{N}}$ a Cauchy sequence. So $\theta([(r_n + I_n)_{n\in\mathbb{N}}]) = (r_n + I_n)_{n\in\mathbb{N}}$, thus θ is surjective. □

Note. The ring $\widehat{A}$ is complete by definition and contains A since $A \hookrightarrow \widehat{A}, r \mapsto (r)_{n\in\mathbb{N}}$. Note that A is complete if and only if $A \cong \varprojlim_{n\in\mathbb{N}} {}^{A}/_{I_n}$. Note that the kernel of $A \to \varprojlim_{n\in\mathbb{N}} {}^{A}/_{I_n}$ is $\bigcap_{n\in\mathbb{N}} I_n$, so $\bigcap_{n\in\mathbb{N}} I_n = \{0\}$ (meaning that the topology is Hausdorff) is a necessary condition of the completeness.

Definition 1.4.5 (I-adic completion)**.** When the filtration is given by $I_n = I^n$, the powers of some proper ideal $I \lneq A$, then the corresponding completion, denoted by $\widehat{A_I}$, is called the *I-adic completion*.

1.5 Non-Archimedean fields, extension of valuations

Let K be a field. Recall that a map $v : K \to \mathbb{R} \cup \{\infty\}$ is called a *non-Archimedean valuation*, if for all $x, y \in K$

$$v(x) = \infty \iff v = 0, \quad v(xy) = v(x) + v(y), \quad v(x + y) \geq \min\{v(x), x(y)\}. \tag{1.1}$$

A valuation is *discrete* if $v(K) \subseteq \mathbb{Z} \cup \{\infty\}$. Similarly a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is called a *non-Archimedean absolue value* if

$$|x| = 0 \iff v = 0, \qquad |xy| = |x||y|, \qquad |x + y| \leq \max\{|x|, |y|\}.$$

One can get an absolute value from a valuation by letting $|x| := b^{-v(x)}$ for a fixed real number $b > 1$ and vice versa by $v(x) := -\log_b(|x|)$. We can define a metric on K by $d(x, y) := |x - y|$.

Let K be a field with a non-Archimedean valuation v (which is called a *non-Archimedean field*). In this case $\mathcal{O}_K := \{x \in K : v(x) \geq 0\}$ is the *ring of integers* of K which is a local ring with maximal ideal $\mathfrak{m}_K := \{x \in K : v(x) > 0\}$. The usual completion of $\mathcal{O}_K$ with respect to the metric is isomorphic (as topological rings) to the $\mathfrak{m}_K$-adic completion of $\mathcal{O}_K$, i.e. to $\varprojlim_{n\in\mathbb{N}} \mathcal{O}_K \Big/ \mathfrak{m}_K^n$.

In this completion, for $0 \neq [(r_n)_{n\in\mathbb{N}}]$, the limit $\lim_{n\to\infty} v(r_n)$ exists in $\mathbb{R}$ and is independent of the choice of the representative from the definition of a Cauchy sequence,

so we can define a valuation $\widehat{v}$ on $\widehat{\mathcal{O}_K}$ by

$$\widehat{v}([(r_n)]) := \begin{cases} \lim_{n\to\infty} v(r_n), & [(r_n)] = 0 \\ \infty, & [(r_n)] \neq 0 \end{cases} \tag{1.2}$$

which extends the original valuation v. This can be extended further to $\operatorname{Frac}\widehat{\mathcal{O}_K}$ in the natural way. Also note the that formula in Equation (1.2) defines a valuation on the completion $\widehat{K}$ of the field K, here completions means the usual metric completion defined by the valuation. $\operatorname{Frac}\widehat{\mathcal{O}_K} = \widehat{K}$ and the two valuations on them coincide.

Example 1.5.1 (p-adic integers)**.** As a special case, for some prime number p, the $p\mathbb{Z}$-adic completion of $\mathbb{Z}$ is exactly the completion of $\mathbb{Z}$ with respect to the p-adic absolute value, i.e. $\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$, the p-adic integers.

For the rest of the section, fix a discrete non-Archimedean valuation $v : \mathbb{Q}_p \to \mathbb{Z}\cup\{\infty\}$ normalised such that $v(p) = 1$, fix an algebraic closure $\mathbb{Q}_p^{\text{alg}}$ of $\mathbb{Q}_p$ and let $K/\mathbb{Q}_p$ be a finite extension in $\mathbb{Q}_p^{\text{alg}}$.

Definition 1.5.2. We can define a valuation v_K on K by

$$v_K(x) := \begin{cases} \frac{1}{[K:\mathbb{Q}_p]} v(\mathrm{N}_{K/\mathbb{Q}_p}(x)), & x \neq 0 \\ \infty, & x = 0 \end{cases}$$

where $\mathrm{N}_{K/\mathbb{Q}_p} : K \to \mathbb{Q}_p$ is the norm of the extension $K/\mathbb{Q}_p$ defined by $\mathrm{N}_{K/\mathbb{Q}_p}(x) = \det(K \to K, y \mapsto xy)$. This is the extension of v, i.e. $v_K\big|_{\mathbb{Q}_p} = v$. K is complete because the valuation v_K is discrete. In fact, this is the only way to extend the valuation v. (The key ingredient to this fact is Hensel's lemma, see [Záb14, Section 4.4].) Let

$$\mathcal{O}_K := \{x \in K : v_K(x) \geq 0\}$$

be the *ring if integers*, which is a local with the unique maximal ideal given by

$$\mathfrak{m}_K := \{x \in K : v_K(x) > 0\}.$$

In fact, $\mathfrak{m}_K$ is a principal ideal and each generator is called a *uniformising parameter* or *uniformiser*. Define the *residue field* k_K by

$$k_K := \mathcal{O}_K/\mathfrak{m}_K.$$

Note that k_K is indeed as field as $\mathfrak{m}_K \leq \mathcal{O}_K$ is a maximal ideal. Moreover, k_K is a finite extension of $k_{\mathbb{Q}_p}$ and its degree

$$f_K := [k_K : k_{\mathbb{Q}_p}]$$

is defined to be the *residue degree*. Pick any uniformiser π_K and define the *ramification degree* e_K by

$$e_K := \frac{1}{v_K(\pi_K)}.$$

Note. For $K = \mathbb{Q}_p$ we have $v_{\mathbb{Q}_p} = v$, $v[\mathbb{Q}_p^\times] = \mathbb{Z}$, $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$, $\pi_{\mathbb{Q}_p} = p$, $\mathfrak{m}_{\mathbb{Q}_p} = p\mathbb{Z}_p$ and $k_{\mathbb{Q}_p} = \mathbb{F}_p$. Also $v_K[K^\times] = \frac{1}{e_K}\mathbb{Z}$, and $\mathcal{O}_K = k_K[[\pi_K]]$, $K = k_K((\pi_K))$.

Let L/K be finite extensions of $\mathbb{Q}_p$ in $\mathbb{Q}_p^{\text{alg}}$. Then we see that $v_L\big|_K = v_K$, i.e. that the extensions of the valuation are compatible. Also $\mathfrak{m}_K = \mathfrak{m}_L \cap \mathcal{O}_K$, so k_L is a finite extension of k_K where $f_{L/K} := \frac{f_L}{f_K} = [k_L : k_K]$ by the Tower Rule. Also $v_K(K^\times) \leq v_L(L^\times)$ is a subring of finite index, and this index is $e_{L/K} := \frac{e_L}{e_K} = [v_L(L^\times) : v_K(K^\times)]$. An important fact is that

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

Definition 1.5.3 (Ramified, unramified extension)**.** L/K is *completely unramified*, if the following equivalent conditions hold

$$e_{L/K} = 1 \iff v_L(\pi_L) = v_L(\pi_K) \iff \pi_K\mathcal{O}_L = \mathfrak{m}_L \iff [L : K] = [k_L : k_K].$$

L/K is *totally ramified*, if the following equivalent conditions hold

$$f_{L/K} = 1 \iff k_L \cong k_K \iff v_L(\pi_K) = [L : K]v_L(\pi_L) \iff e_{L/K} = [L : K].$$

For more details, see [Záb14].

1.6 Galois cohomology

Definition 1.6.1 (G-module category)**.** X is a *G-module* if $(X, +)$ is an abelian group on which G acts additively, i.e. such that $g(x_1+x_2) = g(x_1)+g(x_2)$ for all $g \in G, x_1, x_2 \in X$. A *morphism* between two G-modules X and X' is defined to be a group homomorphism commuting with the action of G, i.e. a group homomorphism $\theta : X \to X'$ such that $\theta(g(x)) = g(\theta(x))$ for all $g \in G, x \in X$.

Note that category of G-modules is equivalent to the category of modules over the ring $\mathbb{Z}[G]$. In particular, it is abelian and *has enough injectives*, i.e. every G-module can be embedded into an injective G-module. Recall, a G-module I is *injective* it satisfies any of the following equivalent conditions (for all X, Y G-modules).

$$\text{Hom}(-, I) \text{ is exact} \iff 0 \to I \to X \to Y \to 0 \text{ splits} \iff \begin{array}{ccccc} 0 & \longrightarrow & X & \longrightarrow & Y \\ & & \downarrow & \swarrow_{\exists} & \\ & & I & & \end{array}$$

Let X be a G-module. $\mathtt{F}(X) := X^G := \{x \in X : \forall g \in G, \quad g(x) = x\}$ is an abelian group, and so $\mathtt{F}$ is a functor from the category of G-modules to the category of abelian groups, moreover it is left exact. Then we can form an *injective resolution of X*, i.e. a long exact sequence $0 \to X \to I^0 \to I^1 \to I^2 \to \ldots$ with I^n being an injective G-module for all $n \geq 0$. Apply the functor $\mathtt{F}$ to this sequence and delete the first term to get the not necessarily exact sequence $0 \to (I^0)^G \to (I^1)^G \to (I^2)^G \to \ldots$.

Definition 1.6.2 (Cohomology)**.** Define the *nth cohomology*

$$H^n(G, X)$$

of X to for $n \geq 0$ to be the *homology* at the nth spot, i.e. the kernel of the map from $(I^n)^G$ modulo the image of the map to $(I^n)^G$. H^n is also called the *nth right derived functor* of $\mathtt{F}$ and is denoted by $R^n\,\mathtt{F}(X)$.

Note that different injective resolutions yield isomorphic cohomology groups. Moreover

$$H^0(G, X) = \mathtt{F}(X) = X^G$$

from left exactness of the functor $\mathtt{F}$.

Lemma 1.6.3. *If X_i are G-modules for $i \in I$, then $\prod_{i\in I} X_i$ is also a G-module by $g((x_i)_{i\in I}) := (g(x_i))_{i\in I}$. Further $H^n(G, \prod_{i\in I} X_i) \cong \prod_{i\in I} H^n(G, X_i)$.*

Proof. See [Mil13, Proposition 1.25] □

Lemma 1.6.4. *A short exact sequence $0 \to X \to Y \to Z \to 0$ gives rise to a long exact sequence of homologies*

$$0 \to X^G \to Y^G \to Z^G \to H^1(G, X) \to H^1(G, Y) \to H^1(G, Z) \to H^2(G, X) \to \dots$$

Proof. The connecting morphisms are provided by the Snake Lemma. For details, see [Mil13, Proposition A.11]. □

Definition 1.6.5 (Galois cohomology)**.** An important case is when $G = \mathrm{Gal}(L/K)$ for some Galois extension L/K in which case $(L, +)$ is a G-module. The *nth Galois cohomology group* is then defined to be $H^n(G, (L, +))$.

Theorem 1.6.6 (Additive Hilbert 90)**.** *For any Galois extension L/K we have*

$$H^n(\mathrm{Gal}(L/K), (L, +)) = 0$$

for $n > 0$.

Proof. This follows from the existence of a normal basis which is based on Dedekind's lemma. For details, see [Mil13, Poposition 1.24]. □

Note that this theorem show that $(L, +)$ is an injective $\mathrm{Gal}(L/K)$-module. Compare this theorem with Corollary 2.1.10, the (multiplicative) Hilbert 90. For more details on this section, see [Mil13, Chapter II].

Chapter 2

Galois Representations over fields of characteristic $p > 0$

In this chapter let E be a field of characteristic $p > 0$. Fix an algebraic closure E^{alg} of E and the separable closure $E^{\text{sep}} \subseteq E^{\text{alg}}$ of E. In this section we set $G := \text{Gal}(E^{\text{sep}}/E)$ to be the absolute Galois group of E, however, some definitions are valid for general groups.

2.1 $\mathbb{F}_p$-representations

In this section we shall investigate $\mathbb{F}_p$-representations with $\mathbb{F}_p$ having the discrete topology on which G acts trivially (so the representation is linear). These representations are usually called *mod p representations*, but we shall refer to them as $\mathbb{F}_p$-representations. Since E is of characteristic $p > 0$, $\mathbb{F}_p \subseteq E$, thus the action of G on $\mathbb{F}_p$ is trivial, thus the $\mathbb{F}_p$-representations of G are all linear. Denote the Frobenius map $E^{\text{sep}} \to E^{\text{sep}}, \lambda \mapsto \lambda^p$ by σ.

2.1.1 The category $\mathbf{M}_{\varphi}^{\text{ét}}(E)$ of étale φ-modules

Definition 2.1.1 ((étale) φ-module)**.** A *φ-module over E* is an E-vector space M together with a σ-semi-linear map $\varphi : M \to M$ called the *Frobenius*. Equivalently by Lemma 1.3.3, a φ-module M with a linear map $\Phi_\varphi : M_\sigma \to M$.
If further Φ_φ is an isomorphism and $\dim_E M < \infty$, then M is said to be an *étale φ-module*.

Note. We always denote the Frobenius map on a φ-module by φ.

Example 2.1.2. E is an étale φ-module by the Frobenius on E, i.e. $\varphi := \sigma = (\lambda \mapsto \lambda^p)$. In fact, this shows why φ is called a Frobenius map.

Definition 2.1.3 (Dual étale φ-module)**.** Let M be étale, $\{e_i^* : 1 \leq i \leq d\}$ be the dual basis for M^* and $(a'_{ij}) := (\mathsf{A}_M)^{-1}$ (which exists by Lemma 1.3.5). Then M^* is also an

étale φ-module via

$$\varphi\left(\sum_{i=1}^{d}\lambda_i e_i^*\right) := \sum_{i=1}^{d}\sigma(\lambda_i)\sum_{j=1}^{d}a'_{ji}e_j^* = \sum_{i=1}^{d}\lambda_i^p\sum_{j=1}^{d}a'_{ji}e_j^*$$

Note. $(\mathsf{A}_{M^*})^T = (\mathsf{A}_M)^{-1}$.

Lemma 2.1.4. *For étale φ-modules M and M', $M\otimes_E M'$ is also an étale φ-module via*

$$\varphi\left(\sum_{i=1}^{r}x_i\otimes x'_i\right) := \sum_{i=1}^{r}\varphi(x_i)\otimes\varphi(x'_i).$$

Proof. It is easy to check that the map φ on the tensor product is well–defined and is σ-semi-linear, i.e. $M\otimes_E M$ is a φ-module. Also note that from properties of tensor product, we have $\det(\mathsf{A}_{M\otimes_E M'}) = (\det\mathsf{A}_M)^{\dim_E M'}(\det\mathsf{A}_{M'})^{\dim_E M} \neq 0$, so from Lemma 1.3.5 $M\otimes_E M'$ is étale. □

There is also a purely module theoretic way of defining φ-modules. For an indeterminate $\varphi\notin E$, let $I := \sum_{\lambda\in E}E\langle\varphi\rangle(\varphi\lambda-\sigma(\lambda)\varphi)E\langle\varphi\rangle$ be the two-sided ideal of the non-commutative $E\langle\varphi\rangle$ generated by E and φ (where elements of E still commute with each other but not with powers of φ). Define the quotient $E_\varphi := {}^{E\langle\varphi\rangle}/_I$, which is called a *skew polynomial ring*. Then a φ-module over E can be considered as a left E_φ-module where the Frobenius map becomes scalar multiplication by $\varphi+I\in E_\varphi$. A homomorphism $\xi: M\to M'$ of E_φ-modules is characterised by

$$\xi(x_1+x_2)=\xi(x_1)+\xi(x_2),\quad \xi((\lambda+I)x)=(\lambda+I)\xi(x),\quad \xi((\varphi+I)x)=(\varphi+I)\xi(x)$$

for $\lambda\in E, x, x_1, x_2\in M$. The first two relations mean that ξ is E-linear when viewed as map between φ-modules. The last relation means that the Frobenius maps on M and M' commute with ξ. This motivates the following definition.

Definition 2.1.5 (Category of étale φ-modules)**.** We define the *category* $\mathbf{M}_\varphi^{ét}(E)$ *of étale φ-modules over E* . The objects are the étale φ-modules over E and the morphisms are E-linear maps commuting with the corresponding Frobenius, i.e.

$$\mathrm{Mor}_{\mathbf{M}_\varphi^{ét}(E)}(M,M') := \{\xi: M\to M' : \xi \text{ is } E\text{-linear}, \xi\circ\varphi=\varphi\circ\xi\}$$

Theorem 2.1.6. $\mathbf{M}_\varphi^{ét}(E)$ *is abelian.*

Proof. The category of φ-modules is abelian, since it is equivalent to the category of left E_φ-modules. The zero object is étale and so are the product and coproduct of étale objects by definition. Now we show that the kernel exist in this category. Let $\xi: M\to M'$ a morphism of étale φ-modules. Since Φ_φ is an isomorphism, we can define $\xi^{\Phi_\varphi} := \Phi_\varphi\circ\xi\circ\Phi_\varphi^{-1}: M_\sigma\to M'_\sigma$. Now for $x\in\ker\xi^{\Phi_\varphi}$, $0=\Phi_\varphi(\xi^{\Phi_\varphi}(x))=\xi^{\Phi_\varphi}(\Phi_\varphi(x))$, so $\Phi_\varphi\big|_{\ker\xi^{\Phi_\varphi}}$ maps to $\ker\xi$. This map is E-linear, injective and $\dim_E\ker\xi^{\Phi_\varphi}=\dim_E\ker\xi$, so it is in fact bijective, i.e. an isomorphism. So $\Phi_\varphi\big|_{\ker\xi^{\Phi_\varphi}}:\ker\xi^{\Phi_\varphi}=(\ker\xi)_\sigma\to\ker\xi$, the kernel of ξ, is an étale φ-module. The dual argument shows that cokernel also exists. The rest of the statement is a consequence of these existences. □

2.1.2 The additive functor $\mathtt{M} : \mathbf{Rep}_{\mathbb{F}_p}(\mathrm{Gal}(E^{\mathrm{sep}}/E)) \to \mathbf{M}_{\varphi}^{\text{ét}}(E)$

Let $\mathbf{Rep}_{\mathbb{F}_p}(G)$ be the category of finite dimensional $\mathbb{F}_p$-representations of G. Let V be an $\mathbb{F}_p$-representation of G. Set

$$U := E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} V.$$

We shall give several structures on this abelian group U. For $\sum_{i=1}^r \mu_i \otimes v_i \in U, \mu \in E^{\mathrm{sep}}, g \in G$ define an E^{sep}-vector space structure and a G-action on U by

$$\mu\left(\sum_{i=1}^r \mu_i \otimes v_i\right) := \sum_{i=1}^r (\mu\mu_i) \otimes v_i \qquad g\left(\sum_{i=1}^r \mu_i \otimes v_i\right) := \sum_{i=1}^r g(\mu_i) \otimes g(v_i). \tag{2.1}$$

It is easy to see that both maps are well-defined, i.e. independent of the choice of representatives. We see that $g(\mu u) = g(\mu)g(u)$ for $g \in G, \mu \in E^{\mathrm{sep}}, u \in U$. Let $U^G := \{x \in U : \forall g \in G \quad g(x) = x\}$ the set of elements fixed by G under the above action. This is an E-vector space, since for $\lambda \in E, x \in U^G, g \in G$, by above $g(\lambda x) = g(\lambda)g(x) = \lambda x$. By the procedure above (the so called *extension of scalars*) $E^{\mathrm{sep}} \otimes_E U^G$ can be given an E^{sep}-vector space structure.

Lemma 2.1.7. *The Frobenius φ on U^G defined by*

$$\varphi\left(\sum_{i=1}^r \mu_i \otimes v_i\right) := \sum_{i=1}^r \sigma(\mu_i) \otimes v_i = \sum_{i=1}^r \mu_i^p \otimes v_i \tag{2.2}$$

makes U^G an étale φ-module over E.

Proof. Let $x = \sum_{i=1}^r \mu_i \otimes v_i \in U^G$. For $g \in G$, $g(\varphi(x)) = \sum_{i=1}^r g(\mu_i^p) \otimes g(v_i) = \sum_{i=1}^r g(\mu_i)^p \otimes g(v_i) = \varphi(g(x)) = \varphi(x)$ hence $\varphi(x) \in U^G$, so φ indeed maps to U^G. We also see that $\varphi(\lambda x) = \sum_{i=1}^r \sigma(\mu)\sigma(\mu_i) \otimes v_i = \sigma(\lambda)\varphi(x)$ for $\lambda \in E$, i.e. that φ is σ-semi-linear. This show that U^G is a φ-module over E. In fact, we have show that the formula in Equation (2.2) makes U a φ-module over E^{sep} on which $g \circ \varphi = \varphi \circ g$ for all $g \in G$.

Now prove that U^G is étale. Notice that U^G is finite dimensional, since $\dim_E U^G = \dim_{E^{\mathrm{sep}}} E^{\mathrm{sep}} \otimes_E U^G = \dim_{E^{\mathrm{sep}}} U = \dim_{E^{\mathrm{sep}}} E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} V = \dim_{\mathbb{F}_p} V =: d$ where in the middle we used Proposition 2.1.9. Let $\{v_i : 1 \le i \le d\}$ be an $\mathbb{F}_p$-basis for V and let $\{e_i : 1 \le i \le d\}$ be an E-basis for U^G. Then $\{1 \otimes e_i : 1 \le i \le d\}$ is E^{sep}-basis for $E^{\mathrm{sep}} \otimes_E U^G$. Let $B = (b_{ij})_{i,j} \in \mathrm{GL}_d(E^{\mathrm{sep}})$ be the invertible matrix over E^{sep} for α_V from Proposition 2.1.9, i.e. $\alpha_V(1 \otimes e_i) = e_i = \sum_{j=1}^d b_{ij}(1 \otimes v_j)$. Then for $B^{-1} = (b'_{ij})_{i,j}$, $1 \otimes v_j = \sum_{k=1}^d b'_{jk} e_k$. By definition

$$\varphi(e_i) = \sum_{j=1}^d b_{ij}^p \otimes v_j = \sum_{j=1}^d b_{ij}^p \sum_{k=1}^d b'_{jk} e_k,$$

so the matrix corresponding to φ in this basis is $\mathsf{A}_{U^G} = \left(\sum_{j=1}^d b_{ij}^p b'_{jk}\right)_{i,k} = \sigma[B]B^{-1}$. Since $\mathrm{char}(E^{\mathrm{sep}}) = p$, we have $\det \mathsf{A}_{U^G} = \det(\sigma[B]) \det(B^{-1}) = \frac{\det(B)^p}{\det B} \neq 0$, thus U^G is étale by Lemma 1.3.5. □

Lemma 2.1.8. *For any $u \in U$ there exists a finite Galois extension F/E such that $\mathrm{Gal}(E^{\mathrm{sep}}/F)$ acts identically on u.*

Proof. Let $u := \sum_{i=1}^{r} \mu_i \otimes v_i$. Let $\mathrm{Stab}_G(\{v_i : 1 \leq i \leq r\})$ be the stabiliser under the action of G on V. Note that $\mathrm{Stab}_G(\{v_i : 1 \leq i \leq r\}) = \bigcap_{i=1}^{n}(G \to V, g \mapsto g(v_i) - v_i)^{-1}[\{0\}]$, a finite intersection of inverse images under continuous maps. Since V has the discrete topology, $\{0\} \subseteq V$ is open, hence so is $\mathrm{Stab}_G(\{v_i : 1 \leq i \leq r\})$. Any open subgroup of a profinite group is also closed, so by the Fundamental Theorem of Galois Theory (Theorem 1.2.10) there is an intermediate field L such that $\mathrm{Gal}(E^{\mathrm{sep}}/L) = \mathrm{Stab}_G(\{v_i : 1 \leq i \leq r\})$ where L/E is a finite extension.

Let F be the Galois closure of the field generated by L and $E(\{\mu_i : 1 \leq i \leq r\})$. The field extension $E(\{\mu_i : 1 \leq i \leq r\})/E$ is finite as $\mu_i \in E^{\mathrm{sep}}$ are algebraic over E, also L/E is finite. Thus F/E is a finite Galois extension and $\mathrm{Gal}(E^{\mathrm{sep}}/F) \leq \mathrm{Gal}(E^{\mathrm{sep}}/L) = \mathrm{Stab}_G(\{v_i : 1 \leq i \leq r\})$. So every element of $\mathrm{Gal}(E^{\mathrm{sep}}/F)$ fixes all μ_i and v_i, hence fixes u. Hence F is as required. □

Proposition 2.1.9. *We have the following isomorphism of E^{sep}-vector spaces*

$$\alpha_V : E^{\mathrm{sep}} \otimes_E U^G \to U, \quad \sum_{i=1}^{r} \mu_i \otimes x_i \mapsto \sum_{i=1}^{r} \mu_i x_i$$

Proof. Since α_V is an E^{sep}-linear map, we need to show that it is injective and surjective.

Injectivity It is enough to show that $\ker \alpha_V$ is trivial. Let $\{1 \otimes e_i : 1 \leq i \leq d\}$ be a basis for $E^{\mathrm{sep}} \otimes_E U^G$. For $y := \sum_{i=1}^{d} \mu_i \otimes e_i \in E^{\mathrm{sep}} \otimes_e U^G$ let $I_y := \{i : \mu_i \neq 0\}$. Assume that the kernel is not trivial and choose one $y \in \ker \alpha_V \setminus \{0\}$ such that I_y is minimal with respect to containment. Then $I_y \neq \emptyset$ and without loss of generality we may assume that $1 \in I_y$ and $\mu_1 = 1$ by reindexing and considering $\frac{y}{\mu_1}$. Then for all $g \in G$, we have

$$0 = g(\alpha_V(y)) - \alpha_V(y) = \sum_{i=1}^{d} g(\mu_i)g(e_i) - \sum_{i=1}^{d} \mu_i e_i = \sum_{i=1}^{d} (g(\mu_i) - \mu_i)e_i$$

So for $y' := \sum_{i=1}^{d}(g(\mu_i) - \mu_i) \otimes e_i$, $y' \in \ker \alpha_V$ and $I_{y'} \subseteq I_y \setminus \{1\}$. The minimality of I_y implies that $y' = 0$, i.e. for all i, $g(\mu_i) - \mu_i = 0$, thus $\mu_i \in (E^{\mathrm{sep}})^G = E$. But then $0 \neq y = \sum_{i=1}^{d} 1 \otimes \mu_i e_i = 1 \otimes \alpha_V(y) = 0$, a contradiction. So the kernel is indeed trivial finishing the proof of the injectivity.

Surjectivity This part is based on [Ber10, Lemma III.8.21]. Pick an arbitrary $u \in U$. We will construct a preimage of u explicitly. Let F/E be the finite Galois extension of degree, say, n such that $H := \mathrm{Gal}(E^{\mathrm{sep}}/F)$ fixes u by Lemma 2.1.8. Now $|G : H| = [F : E] = n$ and for each left coset of H in G, fix a representative $g_i \in G$ for $1 \leq i \leq n$ with g_1 being the identity. Since ${}^{G}/_{H} \cong \mathrm{Gal}(F/E)$, the restrictions of the representatives gives the Galois group $\mathrm{Gal}(F/E) = \{g_i\big|_F : 1 \leq i \leq n\}$. Let $\{\lambda_1, \ldots, \lambda_n\}$ be an E-basis

of F. From Dedekind's Lemma (Lemma 1.2.5), the $n \times n$ matrix $A = (g_i\big|_F(\lambda_j))_{1\leq i,j\leq n}$ is invertible, denote its inverse by $A^{-1} = (a'_{ij})$. Then

$$u = g_1(u) = \sum_{i=1}^{n} g_i(u) \sum_{j=1}^{n} g_i\big|_F(\lambda_j) a'_{j,1} = \sum_{j=1}^{n} a'_{j,1} \sum_{i=1}^{n} g_i(\lambda_j u).$$

Let $u_j := \sum_{i=1}^{n} g_i(\lambda_j u) \in U$. If $\sum_{j=1}^{n} a'_{j,1} \otimes u_j$ is in the domain of α_V, then we just showed that $\alpha_V\left(\sum_{j=1}^{n} a'_{j,1} \otimes u_j\right) = u$. Since $a'_{i,j} \in F \subseteq E^{\text{sep}}$, it suffices to show that $u_j \in U^G$.

Pick an arbitrary $g \in G$. Multiplication on the left by g permutes the left cosets: $gg_iH = g_{k(i)}H$ where $k \in S_n$ is a permutation, so for some $h_i \in H$, $gg_i = g_{k(i)}h_i$. Now by construction of F, H acts identically on u, likewise the action of H is identical on $\lambda_i \in F$ by definition. Thus

$$g(u_j) = \sum_{i=1}^{n} gg_i(\lambda_j u) = \sum_{j=1}^{n} g_{k(i)}\Big(h_i(\lambda_j)h_i(u)\Big) = \sum_{j=1}^{n} g_{k(i)}(\lambda_j u) = u_j$$

since k is a permutation, thus $u_i \in U^G$ as required. This finishes the proof of surjectivity. □

In fact, we proved the following statement.

Corollary 2.1.10 (Hilbert's 90)**.** *Let U be an E^{sep}-representation of G of dimension d. Then the map in Proposition 2.1.9 is an isomorphism, i.e. U has an a E^{sep}-basis which is fixed pointwise by G, i.e. $U \cong (E^{\text{sep}})^d$ as E^{sep}-representations, were G acts on $(E^{\text{sep}})^d$ in the natural way, i.e. by $g : (\mu_i)_{i=1}^d \mapsto (g(\mu_i))_{i=1}^d$. Moreover*

$$H^1(G, \mathrm{GL}_d(L)) = 0$$

and in particular $H^1(G, (L \setminus \{0\}, \cdot)) = 0$.

Theorem 2.1.11. *Let E be a field of characteristic $p > 0$, let $G = \mathrm{Gal}(E^{\text{sep}}/E)$. On $E^{\text{sep}} \otimes_{\mathbb{F}_p} V$ the G-action and the vector space structure is defined in Equation (2.1), the Frobenius in Equation (2.2) where V is an $\mathbb{F}_p$ representation of G. The categories are given in definitions 1.1.3 and 2.1.5. Then*

$$\begin{aligned} \mathtt{M} : \mathbf{Rep}_{\mathbb{F}_p}(G) &\to \mathbf{M}_{\varphi}^{\acute{e}t}(E) \\ \mathrm{Obj}(\mathbf{Rep}_{\mathbb{F}_p}(G)) \ni V &\mapsto (E^{\text{sep}} \otimes_{\mathbb{F}_p} V)^G \\ \mathrm{Mor}_{\mathbf{Rep}_{\mathbb{F}_p}(G)}(V_1, V_2) \ni \theta &\mapsto \left(\sum_{i=1}^{r} \mu_i \otimes v_i \mapsto \sum_{i=1}^{r} \mu_i \otimes \theta(v_i)\right) \end{aligned} \tag{2.3}$$

is an additive functor. Moreover $\dim_{\mathbb{F}_p} V = \dim_E \mathtt{M}(V)$, and $\mathtt{M}(V) \otimes_E \mathtt{M}(V') \cong \mathtt{M}(V \otimes_{\mathbb{F}_p} V')$, $\mathtt{M}(\mathbb{F}_p) \cong E$ as étale φ-modules.

Proof. From Lemma 2.1.7, we have $\mathtt{M}(V) \in \mathrm{Obj}(\mathbf{M}_{\varphi}^{\text{ét}}(E))$, so we need to show only the morphism part of the functoriality.

First we check that $\mathtt{M}(\theta)$ from Equation (2.3) is well defined. We show that $g \circ \mathtt{M}(\theta) = \mathtt{M}(\theta) \circ g$ on $\mathtt{M}(V_1)$. Indeed, for $g \in G$, $x_1 = \sum_{i=1}^{r} \mu_i \otimes \theta(v_i) \in \mathtt{M}(V_1)$ then $g(\mathtt{M}(\theta)(x_1)) = \sum_{i=1}^{r} g(\mu_i) \otimes g(\theta(v_i)) = \sum_{i=1}^{r} g(\mu_i) \otimes \theta(g(v_i)) = \mathtt{M}(\theta)(g(x_1)) = \mathtt{M}(\theta)(x_1)$ since θ commutes with the action of G on V_i by Definition 1.1.3. Thus $\mathrm{Im}(\mathtt{M}(\theta)) \subseteq \mathtt{M}(\mathrm{Im}(\theta))$. From the definitions $\varphi(\mathtt{M}(\theta(x_1))) = \sum_{i=1}^{r} \varphi(\mu_i) \otimes \theta(v_i) = \mathtt{M}(\theta)(\varphi(x_1))$, i.e. $\varphi \circ \mathtt{M}(\theta) = \mathtt{M}(\theta) \circ \varphi$ on $\mathtt{M}(V_1)$, thus by Definition 2.1.5, $\mathtt{M}(\theta)$ is indeed a morphism between the appropriate objects.

It is clear that $\mathtt{M}(\mathrm{Id}_V) = \mathrm{Id}_{\mathtt{M}(V)}$, and that $\mathtt{M}(\theta_2 \circ \theta_1) = \mathtt{M}(\theta_2) \circ \mathtt{M}(\theta_1)$ for $\theta_1 \in \mathrm{Mor}(V_1, V_2), \theta_2 \in \mathrm{Mor}(V_2, V_3)$. Additivity of $\mathtt{M}$ follows from bilinearity of the tensor product.

Invariance of the dimensions was proved in Proposition 2.1.9.

Let $V, V' \in \mathbf{Rep}_{\mathbb{F}_p}(G)$ with bases $\{e_i : 1 \le i \le d\}$ and $\{e'_j : 1 \le i \le d'\}$, respectively. Define the an E-linear map $\tau : \mathtt{M}(V) \otimes_E \mathtt{M}(V') \to \mathtt{M}(V \otimes_{\mathbb{F}_p} V')$ by

$$x \otimes x' := \sum_{i=1}^{d} \mu_i \otimes e_i \otimes \sum_{j=1}^{d'} \mu'_j \otimes e'_j \mapsto \sum_{i=1}^{d} \sum_{j=1}^{d'} \mu_i \mu'_j \otimes e_i \otimes e'_j.$$

We see that τ commutes with the action of G, so $g(\tau(x \otimes x')) = \tau(g(x \otimes x')) = \tau(g(x) \otimes g(x')) = \tau(x \otimes x')$, i.e. indeed $\mathrm{Im}(\tau) \subseteq \mathtt{M}(V \otimes_{\mathbb{F}_p} V')$. Also from the definitions $\tau \circ \varphi = \varphi \circ \tau$, showing that $\tau \in \mathrm{Mor}_{\mathbf{Rep}_{\mathbb{F}_p}(G)}(V, V')$. τ is injective, since $\tau(x \otimes x') = 0$ implies that $\forall i, \mu_i = 0$ or $\forall j, \mu'_j = 0$, i.e. that $x \otimes x' = 0$. Then τ is an isomorphism since $\dim_E(\mathtt{M}(V) \otimes_E \mathtt{M}(V')) = \dim_{\mathbb{F}_p} V \cdot \dim_{\mathbb{F}_p} V' = \dim_E \mathtt{M}(V \otimes_{\mathbb{F}_p} V')$ is finite.

The last part follows from the natural isomorphism of $E^{\text{sep}} \otimes_{\mathbb{F}_p} \mathbb{F}_p \cong E^{\text{sep}}$, . □

2.1.3 The additive functor $\mathtt{V} : \mathbf{M}_{\varphi}^{\text{ét}}(E) \to \mathbf{Rep}_{\mathbb{F}_p}(\mathrm{Gal}(E^{\text{sep}}/E))$

In a similar manner as in Theorem 2.1.11, we want to define a functor from $\mathbf{M}_{\varphi}^{\text{ét}}(E)$ to $\mathbf{Rep}_{\mathbb{F}_p}(\mathrm{Gal}(E^{\text{sep}}/E))$. The definitions and the calculations follow a very similar pattern as in the previous subsection, therefore will not be present in full details.

Let M be an étale φ-module over E. Let $N := E^{\text{sep}} \otimes_E M$ and define the σ-semi-linear map φ on N as

$$\varphi\left(\sum_{i=1}^{r} \mu_i \otimes x_i\right) := \sum_{i=1}^{r} \sigma(\mu_i) \otimes \varphi(x_i) = \sum_{i=1}^{r} \mu_i^p \otimes \varphi(x_i) \tag{2.4}$$

making N a φ-module over E^{sep}. N is also étale by Lemma 1.3.5, because from $\langle \varphi[M] \rangle_E = M$ we see that $\langle \varphi[N] \rangle_{E^{\text{sep}}} = N$. Let $N^{\varphi} := \{v \in N : \varphi(v) = v\}$. This is an $\mathbb{F}_p$-vector space since $\mathbb{F}_p$ is fixed by σ and the map φ defined above is σ-semi-linear. Define a G-action on N^{φ} as

$$g\left(\sum_{i=1}^{r} \mu_i \otimes x_i\right) := \sum_{i=1}^{r} g(\mu_i) \otimes x_i. \tag{2.5}$$

(In fact this defines an action on N but we will not need this.) The action of G on E^{sep} commutes with σ, which implies that φ and the action of G on N^φ (and in fact on N) commute, hence $\varphi(g(v)) = g(\varphi(v)) = g(v)$ for $v \in N^\varphi$. Thus the above definition is indeed an action of N^φ. Moreover one can see from Definition 1.1.2 that N^φ is an $\mathbb{F}_p$-representation of G.

Proposition 2.1.12.

$$\alpha_M : E^{\text{sep}} \otimes_{\mathbb{F}_p} N^\varphi \to N \qquad \sum_{i=1}^{r} \mu_i \otimes v_i \mapsto \sum_{i=1}^{r} \mu_i v_i$$

is an isomorphism of E^{sep}-vector spaces.

Proof. The map α_M is E^{sep}-linear, so we need to show only the injectivity and surjectivity.

Injectivity This proof is similar to the injectivity part of the proof of Proposition 2.1.9. We will basically show that in N^φ, $\mathbb{F}_p$-linear independence implies E^{sep}-linear independence.

It is enough to show that $\ker \alpha_M$ is trivial. Let $\{1 \otimes e_i : 1 \le i \le d\}$ be a basis for $E^{\text{sep}} \otimes_{\mathbb{F}_p} N^G$. Let $v := \sum_{i=1}^{d} \mu_i \otimes e_i$ and define $I_v := \{i : \mu_i \neq 0\}$. Assume on the contrary that $\ker \alpha_M \neq \{0\}$ and chose one $v \in \ker \alpha_V \setminus \{0\}$ such that I_v is minimal with respect to containment. By reindexing and considering $\frac{v}{\mu_1}$ we may assume without loss of generality that $\mu_1 = 1$. Then $0 = \varphi(\alpha_M(v)) - \alpha_M(v) = \sum_{i=1}^{d} (\sigma(\mu_i) - \mu_i) e_i$. So for $v' := \sum_{i=1}^{d} (\sigma(\mu_i) - \mu_i) \otimes e_i$, $v' \in \ker \alpha_V$ and $I_{v'} \subseteq I_v \setminus \{1\}$, thus minimality of I_y implies $y' = 0$. This means that $\sigma(\mu_i) = \mu_i$, i.e. $\mu_i \in \mathbb{F}_p$ for all i. But then $0 \neq v = \sum_{i=1}^{d} 1 \otimes \mu_i e_i = 1 \otimes \alpha_M(v) = 0$, a contradiction.

Surjectivity This part is based on [Sch07, Satz 2.1]. Note that it is enough to show that $\dim_{E^{\text{sep}}} E^{\text{sep}} \otimes_{\mathbb{F}_p} N^\varphi \ge \dim_{E^{\text{sep}}} N =: d$. We will do so by proving that there exists an E^{sep}-basis for N contained in N^φ which is $\mathbb{F}_p$-linearly independent in N^φ. We proceed by induction on d The statement is obvious for $d = 0$.

Now let $d = 1$. Pick $u_0 \in N \setminus \{0\}$. Let $u_i := \varphi^i(u_0)$ and chose r minimal such that $\{v_i : 0 \le i \le r\}$ is E^{sep}-linearly dependent. The fact that $v \neq 0$ means $r \ge 1$. By E^{sep}-linear dependence there exists $(a_i)_{i=0}^{r} \in (E^{\text{sep}})^{r+1}$ such that $\sum_{i=0}^{r} a_i u_i = 0$. By E^{sep}-linear independence of $\{v_i : 0 \le i \le r-1\}$, this $(a_i)_{i=0}^{r}$ vector is unique up to a factor of $\mu \in E^{\text{sep}}$ and $a_r \neq 0$. We want to find non-zero vector $v \in N^\varphi$ from the E^{sep}-linear span of the φ-orbit of u_0, that is, $v = \sum_{i=0}^{r-1} \mu_i u_i$ for some $\mu_i \in E^{\text{sep}}$. Now $v \in N^\varphi$ means that

$$0 = \varphi(v) - v = \sum_{i=0}^{r-1} \mu_i^p u_{i+1} - \sum_{i=0}^{r-1} \mu_i u_i = -\mu_0 u_0 + \left(\sum_{i=1}^{r-1} (\mu_{i-1}^p - \mu_i) u_i \right) + \mu_{r-1}^p u_r.$$

This is another E^{sep}-linear combination of $\{v_i : 0 \le i \le r\}$ yielding 0, so there is a $\mu \in E^{\text{sep}}$ such that $-\mu_0 = \mu a_0$, $\mu_{i-1}^p - \mu_i = \mu a_i$ (for $1 \le i \le r-1$) and $\mu_{r-1}^p = \mu a_r$.

Substituting every equation to the following one, we see that μ is a root of the polynomial $F := \sum_{i=0}^{r} a_{r-i}^{p^i} X^{p^i} \in E^{\mathrm{sep}}[X]$. Reversely, any $0 \neq \mu$ root of F yields $q \neq v \in N^{\varphi}$, i.e. a non-zero $1 \otimes v \in E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} N^{\varphi}$. Then $\{v\}$ is a basis as claimed. So it is enough to find one such root μ.

Now we determine $\deg F$. By minimality of r, $\{v_i : 0 \leq i \leq m-1\}$ is E^{sep}-linearly independent, so we can extend it to an E^{sep} basis B of N. N is étale, so by Lemma 1.3.5, we have $\langle \varphi[B] \rangle_{E^{\mathrm{sep}}} = \langle \varphi[N] \rangle_{E^{\mathrm{sep}}} = N$, thus $\varphi[B]$ is also a basis of N, in particular $\varphi[\{v_i : 0 \leq i \leq m-1\}] = \{v_i : 1 \leq i \leq m\}$ is E^{sep}-linearly independent. Thus $a_0 \neq 0$, so $\deg F = p^r$. Also the derivative is $F' = a_r \neq 0$ since $\operatorname{char} E^{\mathrm{sep}} = p$, thus $\gcd(F, F') = 1$, i.e. F is separable. Then from Lemma 1.2.15, F has $\deg F = p^r \geq p \geq 2$ many distinct roots in E^{sep}, one of which is non-zero.

Now assume $d > 1$. Let $0 \neq v_1 \in N^{\varphi}$. Then the quotient space $N' := {}^{N}\!/_{E^{\mathrm{sep}} v_1}$ is also an (étale) φ-module of dimension $d-1$ via $u + E^{\mathrm{sep}} v_1 \mapsto \varphi(u) + E^{\mathrm{sep}} v_1$. By induction $\{v_i' + E^{\mathrm{sep}} v_1 : 2 \leq i \leq d\}$ is an E^{sep} basis for N' contained in $(N')^{\varphi}$ which is $\mathbb{F}_p$-linearly independent in $(N')^{\varphi}$. So $\varphi(v_i') = v_i' + \mu_i v_1$ for some $\mu_i \in E^{\mathrm{sep}}$. Note that $X^p - X + \mu_i \in E^{\mathrm{sep}}[X]$ is a separable polynomial, so it has a root a_i. Define $v_i := v_i' + a_i v_1$ for $2 \leq i \leq d$. Then

$$\varphi(v_i) = \varphi(v_i') + a_i^p v_1 = (v_i' + \mu_i v_1) + a_i^p v_1 = v_i' + a_i v_1 = v_i$$

so v_i is a lifting of $v_i' + E^{\mathrm{sep}} v_1$ contained in N^{φ}. Thus $\{v_i : 1 \leq i \leq d\}$ is an E^{sep} basis for N contained in N^{φ} where $\mathbb{F}_p$-linear independence in N^{φ} is inherited from the induction hypothesis. This finishes the proof. □

Note. It is the theory of étale algebras that lies underneath the proof. For the dual étale φ-module M^* there is a corresponding étale algebra over E. To finish the surjectivity part of the proof this way, see [FO, Theorem 2.21]. The main step of the proof is the equivalent description of étale algebras using Kähler differentials and on the other hand using Cartesian product of separable extensions. For details of the theory, see [Mor13, Section 2].

Later we will see that being a φ-module over a general ring is a unified notion (actually it is a module over the ring with a semi-linear map on it). However, the definition of being étale depends on the base ring, cf. definitions 2.1.1, 2.2.16 and 2.3.1. The root of these definition is the corresponding étale algebra. In general, the φ-module is étale if and only if the corresponding algebra is étale (which is defined using étale morphisms), and when this definition is translated to the language of φ-modules, it takes different forms depending on the actual ring.

Theorem 2.1.13. *Let E be a field of characteristic $p > 0$, let $G = \mathrm{Gal}(E^{\mathrm{sep}}/E)$. On $E^{\mathrm{sep}} \otimes_E M$ the G-action is defined in Equation* (2.5)*, the Frobenius in* (2.4) *where M is*

an étale φ-module over E. The categories are given in definitions 1.1.3 and 2.1.5. Then

$$\begin{aligned} \mathtt{V} : \mathbf{M}_{\varphi}^{ét}(E) &\to \mathbf{Rep}_{\mathbb{F}_p}(G) \\ \mathrm{Obj}(\mathbf{M}_{\varphi}^{ét}(E)) \ni M &\mapsto (E^{\mathrm{sep}} \otimes_E M)^{\varphi} \\ \mathrm{Mor}_{\mathbf{M}_{\varphi}^{ét}(E)}(M_1, M_2) \ni \xi &\mapsto \left(\sum_{i=1}^{r} \mu_i \otimes x_i \mapsto \sum_{i=1}^{r} \mu_i \otimes \xi(x_i) \right) \end{aligned}$$

is an additive functor. Moreover $\dim_{\mathbb{F}_p} \mathtt{V}(M) = \dim_E M$ *and* $\mathtt{V}(M) \otimes_{\mathbb{F}_p} \mathtt{V}(M') \cong \mathtt{V}(M \otimes_E M')$, $\mathtt{V}(E) \cong \mathbb{F}_p$ *as $\mathbb{F}_p$-representations of G.*

Proof. We have seen that $\mathtt{V}(M)$ is an $\mathbb{F}_p$-representation of G. It is easy to check from the definitions that $\varphi \circ \mathtt{V}(\xi) = \mathtt{V}(\xi) \circ \varphi$ since the Frobenius maps on M_1, M_2 commute with the morphism ξ, thus $\mathrm{Im}(\mathtt{V}(\xi)) \subseteq \mathtt{V}(\mathrm{Im}(\xi))$. Also $g \circ \mathtt{V}(\xi) = \mathtt{V}(\xi) \circ g$ for any $g \in G$, i.e. $\mathtt{V}(\xi)$ is a morphism of $\mathbb{F}_p$-representations. From Proposition 2.1.12,

$$\dim_{\mathbb{F}_p} \mathtt{V}(M) = \dim_{E^{\mathrm{sep}}} E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} \mathtt{V}(M) = \dim_{E^{\mathrm{sep}}} E^{\mathrm{sep}} \otimes_E M = \dim_E M.$$

The rest of the statement follows a similar argument as the proof of Theorem 2.1.11. □

2.1.4 Categorical equivalence

In this subsection we prove the main result of the section, namely the categorical equivalence of étale φ-modules and the $\mathbb{F}_p$-representations.

Theorem 2.1.14. $\mathbf{Rep}_{\mathbb{F}_p}(\mathrm{Gal}(E^{\mathrm{sep}}/E))$ *is categorically equivalent to* $\mathbf{M}_{\varphi}^{ét}(E)$ *via*

$$\mathtt{M} : \mathbf{Rep}_{\mathbb{F}_p}(\mathrm{Gal}(E^{\mathrm{sep}}/E)) \to \mathbf{M}_{\varphi}^{ét}(E), \qquad \mathtt{V} : \mathbf{M}_{\varphi}^{ét}(E) \to \mathbf{Rep}_{\mathbb{F}_p}(\mathrm{Gal}(E^{\mathrm{sep}}/E))$$

Proof. We have shown in Theorems 2.1.11 and 2.1.13 functoriality of $\mathtt{M}$ and $\mathtt{V}$. We need to show that $\mathtt{MV}$ and $\mathtt{VM}$ are naturally isomorphic to the corresponding identity functors.

Pick a $V \in \mathrm{Obj}(\mathbf{Rep}_{\mathbb{F}_p}(G))$. We will construct an isomorphism $\mathtt{VM}(V) \to V$. Let $\{e_i : 1 \le i \le d\}$ be an $\mathbb{F}_p$-basis of V. Let $w := \sum_{i=1}^{d} \sum_{j=1}^{r_i} \mu'_{ij} \otimes \mu_{ij} \otimes e_i \in \mathtt{VM}(V_1)$. By definition

$$\begin{aligned} \mathtt{VM}(V) &= \left\{ w \in E^{\mathrm{sep}} \otimes_E (E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} V)^G : \sum_{i=1}^{d} \sum_{j=1}^{r_i} \sigma(\mu'_{ij}) \otimes \sigma(\mu_{ij}) \otimes e_i = w \right\} \\ &= \left\{ w \in E^{\mathrm{sep}} \otimes_E (E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} V)^G : 1 \le i \le d, \sigma \left(\sum_{j=1}^{r_i} \mu'_{ij}\mu_{ij} \right) = \sum_{j=1}^{r_i} \mu'_{ij}\mu_{ij} \right\} \\ &= \left\{ w \in E^{\mathrm{sep}} \otimes_E (E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} V)^G : 1 \le i \le d, \sum_{j=1}^{r_i} \mu'_{ij}\mu_{ij} \in \mathbb{F}_p \right\} \end{aligned}$$

since $(E^{\mathrm{sep}})^{\varphi} := \{\mu \in E^{\mathrm{sep}} : \sigma(\mu) = \mu^p = \mu\} = \mathbb{F}_p$. Then this means that in fact $\alpha_V\big|_{\mathtt{VM}(V)} : \mathtt{VM}(V) \to \mathbb{F}_p \otimes_{\mathbb{F}_p} V$ where α_V is the isomorphism from Proposition 2.1.9. By

Theorems 2.1.11 and 2.1.13, $\dim_{\mathbb{F}_P} \mathtt{VM}(V) = \dim_E \mathtt{M}(V) = \dim_{\mathbb{F}_p} V = \dim_{\mathbb{F}_p} \mathbb{F}_p \otimes_{\mathbb{F}_p} V$ thus $\alpha_V\big|_{\mathtt{VM}(V)}$ is remains an isomorphism. Denote the natural isomorphism by

$$\beta_V : \mathbb{F}_p \otimes_{\mathbb{F}_p} V \to V, \qquad \sum_{i=1}^{r} \kappa_i \otimes v_i \mapsto \sum_{i=1}^{r} \kappa_i v_i$$

and define $\eta_V := \beta_V \circ \alpha_V\big|_{\mathtt{VM}(V)} : \mathtt{VM}(V) \to V$. Being the composition of two isomorphisms, η_V is an isomorphism.

Now let $\theta \in \mathrm{Mor}_{\mathbf{Rep}_{\mathbb{F}_p}(G)}(V_1, V_2)$ be a morphism between étale φ-modules. Let $w \in \mathtt{VM}(V_1)$ as above. Then $\mu'_{ij}\mu_{ij} \in \mathbb{F}_p \subseteq E$ on which the action of G is trivial, so

$$\begin{aligned}
\eta_{V_2}(\mathtt{VM}(\theta)(w)) &= \eta_{V_2}\left(\sum_{i=1}^{d}\sum_{j=1}^{r_i} \mu'_{ij} \otimes \mathtt{M}(\theta)(\mu_{ij} \otimes e_i)\right) \\
&= \eta_{V_2}\left(\sum_{i=1}^{d}\sum_{j=1}^{r_i} \mu'_{ij} \otimes \mu_{ij} \otimes \theta(e_i)\right) = \sum_{i=1}^{d}\sum_{j=1}^{r_i} \mu'_{ij}\mu_{ij}\theta(e_i) \\
&= \theta\left(\sum_{i=1}^{d}\sum_{j=1}^{r_i} \mu'_{ij}\mu_{ij} e_i\right) = \mathrm{Id}_{\mathbf{Rep}_{\mathbb{F}_p}(G)}(\theta)(\eta_{V_1}(w)).
\end{aligned}$$

This means that $\eta_{V_2} \circ \mathtt{VM}(\theta) = \mathrm{Id}_{\mathbf{Rep}_{\mathbb{F}_p}(G)}(\theta) \circ \eta_{V_1}$ for any θ, i.e. $\mathtt{VM}$ is naturally isomorphic to the identity functor $\mathrm{Id}_{\mathbf{Rep}_{\mathbb{F}_p}(G)}$.

It remains to show that $\mathtt{MV}$ is naturally isomorphic to the identity functor $\mathrm{Id}_{\mathbf{M}_\varphi^{\text{ét}}(E)}$. This is formally the same as the above natural equivalence after interchanging the roles of φ and $g \in G$. Let $M \in \mathbf{M}_\varphi^{\text{ét}}(E)$ with basis $\{b_i : 1 \le i \le d\}$ and pick an arbitrary $y := \sum_{i=1}^{d}\sum_{j=1}^{r_i} \mu'_{ij} \otimes \mu_{ij} \otimes b_i \in \mathtt{MV}(M)$. Then

$$\mathtt{MV}(M) = \left\{ y \in E^{\text{sep}} \otimes_{\mathbb{F}_p} (E^{\text{sep}} \otimes_E M)^{\varphi} : 1 \le i \le d \quad \sum_{j=1}^{r_i} \mu'_{ij}\mu_{ij} \in E = (E^{\text{sep}})^G \right\}$$

so $\alpha_M\big|_{\mathtt{MV}(M)} : \mathtt{MV}(M) \to E \otimes_E M$ where α_M is the isomorphism from Proposition 2.1.12. Let $\beta_M : E \otimes_E M \to M, \quad \sum_{i=1}^{r} \lambda_i \otimes x_i \mapsto \sum_{i=1}^{r} \lambda_i x_i$ and let $\eta_M := \beta_M \circ \alpha_M\big|_{\mathtt{MV}(M)} : \mathtt{MV}(M) \to M$, which is an isomorphism. Then $\eta_{M_2} \circ \mathtt{MV}(\theta) = \mathrm{Id}_{\mathbf{M}_\varphi^{\text{ét}}(E)}(\xi) \circ \eta_{M_1}$ for any $\xi \in \mathrm{Mor}_{\mathbf{M}_\varphi^{\text{ét}}(E)}(M_1, M_2)$. □

Theorem 2.1.15. *For any $A \in \mathrm{GL}_d(E)$, define an étale φ-module $M_A := E^d$, the standard d dimensional vector space over E with basis $\{e_i : 1 \le i \le d\}$ and let $\varphi : M_A \to M_A, \quad \sum_{i=1}^{d} \lambda_i e_i \mapsto \sum_{i=1}^{d} \lambda_i^p \sum_{j=1}^{d} a_{ij} e_j$. Then the following maps are mutually inverses of each other*

$$\left\{ [V] : \begin{array}{c} V \in \mathrm{Obj}\,\mathbf{Rep}_{\mathbb{F}_p}(\mathrm{Gal}(E^{\text{sep}}/E)), \\ \dim_{\mathbb{F}_p} V = d \end{array} \right\} \leftrightarrow \mathrm{GL}_d(E) \Big/ \sigma[Q]^{-1} A Q \sim A$$

$$[V] \mapsto [\mathsf{A}_{\mathtt{M}(V)}]$$

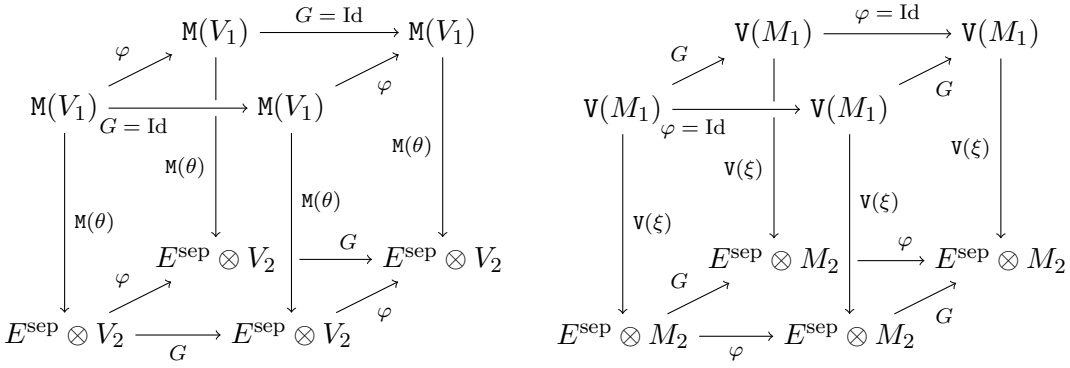
$$[\mathtt{V}(M_A)] \leftarrow\!\shortmid [A]$$

where $[V]$ denotes the isomorphism class of V.

Proof. By Theorem 2.1.14, two representations are isomorphic if and only if the corresponding étale φ-modules are isomorphic. Two étale φ-modules are isomorphic if and only if in suitable bases the matrices corresponding to them are the same. If $M \in \mathrm{Obj}(\mathbf{M}_{\varphi}^{\text{ét}}(E))$ has matrix A_M in a basis $\{e_i : 1 \leq i \leq d\}$ of M, then in another basis $\{f_j : 1 \leq j \leq d\}$ where $e_i = \sum_{j=1}^{d} q_{ij} f_j$ for $Q := (q_{ij})_{1 \leq i,j \leq d} \in \mathrm{GL}_d(E)$, the corresponding matrix is $\sigma[Q]^{-1}\mathsf{A}_M Q$. Note that $[A] = [\mathsf{A}_{M_A}]$ and $M \cong M_{\mathsf{A}_M}$ by definition. Thus $[V] = [V'] \iff \mathtt{M}(V) \cong \mathtt{M}(V') \iff [\mathsf{A}_{\mathtt{M}(V)}] = [\mathsf{A}_{\mathtt{M}(V)}]$ and also $[A] = [A'] \iff [\mathsf{A}_{M_A}] = [\mathsf{A}_{M_{A'}}] \iff M_A \cong M_{A'} \iff [\mathtt{V}(M_A)] = [\mathtt{V}(M_{A'})]$ so the maps are well-defined.

Finally note that $\mathtt{V}(M_{\mathsf{A}_{\mathtt{M}(V)}}) \cong \mathtt{V}(\mathtt{M}(V)) \cong V$ and $[\mathsf{A}_{\mathtt{M}(\mathtt{V}(M_A))}] = [\mathsf{A}_{M_A}] = [A]$ to finish the proof. □

2.1.5 Overview



(a) The functor $\mathtt{M}$ (b) The functor $\mathtt{V}$

Figure 2.1: Commutative diagrams representing the constructions of the functors $\mathtt{M}$ and $\mathtt{V}$ where $\theta \in \mathrm{Mor}_{\mathbf{Rep}_{\mathbb{F}_p}(G)}(V_1, V_2)$ and $\xi \in \mathrm{Mor}_{\mathbf{M}_{\varphi}^{\text{ét}}(E)}(M_1, M_2)$. For simplicity, consider these diagrams as edges of cubes.

First review the key steps of the constructions of the functors $\mathtt{M}$ and $\mathtt{V}$. Consider the diagrams in Figure 2.1. At the previous subsections we have shown that every part of these diagrams commute. Commutativity of the top and bottom faces implied that φ on $\mathtt{M}(V)$, and respectively the action of G on $\mathtt{V}(M)$, are well defined, i.e. the image lies in the domain. Commutativity of the front and back faces showed that $\mathtt{M}(\theta)$ and $\mathtt{V}(\xi)$ map to the correct object, while commutativity of the left and right faces meant that $\mathtt{M}(\theta)$ and $\mathtt{V}(\xi)$ are indeed morphisms of the corresponding category. Note the similarity of the commutative diagrams and how φ and the action of G interchange their roles. This suggests a common underlying structure beneath these categories. Commutativity was clear when the functions acted on different side of the tensor product, which is one of the reasons of defining the G-action and φ as above. Another key point was that the the morphisms of the two categories commute with the corresponding maps. Lastly, and

most importantly, the rest of the commutative diagrams relied on the fact that G and φ commutes on E^{sep}.

Summarising these observations and the key points of the proof of Theorem 2.1.14, we have the following remark.

Remark 2.1.16. Let S be a topological ring on which a group G acts continuously and let $\sigma : S \to S$ be a continuous homomorphism. Suppose further that

1. G commutes with φ on S,
2. $\alpha_V : S \otimes_{S^G} \mathtt{M}(V) \to S \otimes_{S^\sigma} V$ is an isomorphism (Proposition 2.1.9) and
3. $\alpha_M : S \otimes_{S^\sigma} \mathtt{V}(M) \to S \otimes_{S^G} M$ is an isomorphism (Proposition 2.1.12).

Then the categories $\mathbf{Rep}_{S^\sigma}(G)$ and $\mathbf{M}_\varphi^{\text{ét}}(S^G)$ are equivalent.

2.2 $\mathbb{Z}_p$-representations

Recall that E denotes an arbitrary field of characteristic $p > 0$ and $G = \text{Gal}(E^{\text{sep}}/E)$ its absolute Galois group. Endow $\mathbb{Z}_p$ with the p-adic topology and let G act trivially on $\mathbb{Z}_p$, i.e. consider a linear representation of G. In this section we study these representations, and we describe the $\mathbb{Z}_p$-representations of G by giving a categorical equivalence as in Theorem 2.1.14. From Remark 2.1.16, we only need to construct a ring S such that $S^\sigma = \mathbb{Z}_p$ and satisfying all the other hypotheses. The ideas used in this section are the same as in Section 2.1, however, there are more technical details. For example in Section 2.1, the trivial choice $S = E^{\text{sep}}$ suffices, in this section, for construction of S, we will use the Cohen rings, which are introduced below.

2.2.1 Witt vectors and Cohen rings

This section is based on [FO, Section A.2] and [Haz09, Chapter Witt vector: Part 1]. We know that every p-adic integer can be uniquely written as series $\sum_{i=0}^{\infty} a_i p^i$ converging with respect to the p-adic absolute value, where $a_i \in \{0, 1, \ldots, p-1\} = \mathbb{F}_p$ for $i \in \mathbb{N}$. Addition and multiplication are not easy in this form because thy involves carry-overs. To describe these operations, we need to introduce the notion of Witt vectors in definition 2.2.3. The construction happens to be useful not only when the underlying field is $\mathbb{F}_p$ but also for a general commutative ring.

The ring of Witt vectors

Let A be a commutative ring and p be a prime number.

Lemma 2.2.1. $\forall \Phi \in \mathbb{Z}[X, Y] \quad \exists! \{\Phi_i \in \mathbb{Z}[X_0, \ldots, X_i, Y_0, \ldots, Y_i] : i \in \mathbb{N}\} \quad \forall n \in \mathbb{N}$

$$\Phi\left(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\right) = \sum_{i=0}^{n} p^i \Phi_i(X_0, \ldots, X_i, Y_0, \ldots, Y_i)^{p^{n-i}}$$

Proof. Induction on n. □

Definition 2.2.2 (Witt vectors of length n)**.** For $\Phi = X + Y$ set $S_i := \Phi_i$ from Lemma 2.2.1 and for $\Phi = XY$ set $P_i = \Phi_i$ for $i \in \mathbb{N}$. For $n \geq 1$,

$$W_n(A) := \prod_{i=0}^{n-1} A$$

is the *ring of Witt vectors of length n over A* where the ring operations are defined by

$$(a_i)_{i=0}^{n-1} + (b_i)_{i=0}^{n-1} := \big(S_i(a_0, \dots, a_{i-1}, b_0, \dots, b_{i-1})\big)_{i=0}^{n-1}$$
$$(a_i)_{i=0}^{n-1} \cdot (b_i)_{i=0}^{n-1} := \big(P_i(a_0, \dots, a_{i-1}, b_0, \dots, b_{i-1})\big)_{i=0}^{n-1}$$

with $0_{W_n(A)} = (0, 0, 0, \dots, 0) \in W_n(A)$ and $1_{W_n(A)} = (1, 0, 0, \dots, 0) \in W_n(A)$ being the additive and multiplicative identities, respectively. $W_n(A)$ is a topological ring with the discrete topology.

Definition 2.2.3 (Witt vectors)**.** Consider $\mathbb{Z}_{>0}$ with the usual ordering. We can define the transition maps $W_n(A) \to W_k(A), \quad (a_i)_{i=0}^{n-1} \mapsto (a_i)_{i=0}^{k-1}$ for $n \geq k > 0$. Then

$$W(A) := \varprojlim_{n \in \mathbb{Z}_{>0}} W_n(A)$$

is the topological ring of *Witt vectors over A*.

Example 2.2.4. It is an important case when $A = \mathbb{F}_p$. Then $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$ and $W(\mathbb{F}_p) = \mathbb{Z}_p$, the p-adic integers. In fact this motivated the definition of Witt vectors in the general setup.

$$\theta : W_n(A) \to \prod_{i=0}^{n-1} A, \qquad (a_i)_{i=0}^{n-1} \mapsto \Big(\sum_{j=0}^{i} p^i a_j^{p^{i-j}}\Big)_{i=0}^{n-1}$$

is a ring homomorphism. Likewise $W(A) \to \varprojlim_{n \in \mathbb{Z}_{>0}} \prod_{i=0}^{n-1} A = \prod_{i=0}^{\infty} A$ is a homomorphism.
This W (and similarly W_n for all n) is actually functorial, i.e. for a morphism $\theta : A \to A'$ of commutative rings, the map $W(\theta) : W(A) \to W(A'), \quad (a_i)_{i=0}^{\infty} \mapsto (\theta(a_i))_{i=0}^{\infty}$ is a ring homomorphism.
We can define the right shift map $\nu : W(A) \to W(A), \quad (a_i)_{i=0}^{\infty} \mapsto (0, a_0, a_1, a_2, \dots)$. With this, we have an isomorphism $W_k(A) \cong W(A)\big/\nu^k[W(A)]$. In particular $A \cong W_1(A) \cong W(A)\big/\nu[W(A)]$.

Definition 2.2.5 (Frobenius on $W(E)$)**.** When $A = E$ is of characteristic p, then Frobenius homomorphism $E \to E, \quad \lambda \mapsto \lambda^p$ gives rise to a so called *Frobenius map on $W(E)$*:

$$\sigma : W(E) \to W(E) \qquad (\lambda_i)_{i=0}^{\infty} \mapsto (\lambda_i^p)_{i=0}^{\infty}.$$

Now let $A = k$ be a perfect field of characteristic p. Then $W(k)$ has a unique maximal ideal $\mathfrak{m} := \nu[W(k)]$, which is a principal ideal generated by $p = (0, 1, 0, 0, \dots)$. We can then define the corresponding valuation v on $W(k)$ as

$$v : W(k) \to \mathbb{N} \cup \{\infty\}, \qquad (a_i)_{i=0}^{\infty} \mapsto \inf\{i : a_i \neq 0\}$$

where we use the convention $\inf \emptyset = \infty$ with which $\mathfrak{m} = pW(k) = \{a \in W(k) : v(a) \geq 1\}$, cf. Section 1.5. Note that on $W(k)$, multiplication by p^n is given by $\nu^n \sigma^n$.

Theorem 2.2.6. *For every perfect field k of characteristic $p > 0$ there exists a unique (up to isomorphism) complete discrete valuation ring of characteristic 0 which is completely unramified and whose residue field is k and this ring is $W(k)$, the ring of Witt vectors, i.e.* $\operatorname{char} W(k) = 0$, $\mathfrak{m}_{W(k)} = pW(k)$, $W(k) \cong \varprojlim_{n\in\mathbb{N}} W(k) \Big/ p^n W(k)$, $k \cong W(k) \Big/ \mathfrak{m}_{W(k)}$.

The Cohen ring

We want to generalise Theorem 2.2.6 for any arbitrary (not necessarily perfect) field. Let E be a field of characteristic p.

Definition 2.2.7. Let $E^p := \sigma[E] = \{\lambda^p \in E : \lambda \in E\}$. A *$p$-basis* of E is a set $\mathcal{B} \subseteq E$ such that the following extensions of E satisfy $E^p(\mathcal{B}) = E$ and $[E^p(B) : E^p] = p^{|B|}$ for all finite subset $B \subseteq \mathcal{B}$.

Lemma 2.2.8. *Any field E of characteristic p has a p-basis.*

Proof. Note that E is perfect if and only if $E^p = E$ by Lemma 1.2.12, so $p^{|B|} = 1$ for any finite subset of the p-basis, hence for perfect fields the only p-basis is $\mathcal{B} = \emptyset$.

If E is not perfect, then the Frobenius map is not surjective again by Lemma 1.2.12, so in this case there exists $b \in E$ which is not a pth power. Then $\{b\}$ satisfies the degree condition of being a p-basis. Since the all p-bases are contained in E, there is a maximal $\mathcal{B} \subseteq E$ satisfying the degree condition by Zorn's lemma. For this $\mathcal{B}$, $E^p(\mathcal{B}) = E$, otherwise we could extend $\mathcal{B}$ by non-pth power. Thus $\emptyset \neq \mathcal{B}$ is a p-basis for E by the Tower Rule of extensions. □

Remark 2.2.9. If $\mathcal{B}$ is a p-basis for E, then

$$\left\{ \prod_{b\in B} b^{n_b} : B \subseteq \mathcal{B}, |B| < \infty, \forall b \in B \quad n_b \in \{0, 1, \dots, p^n - 1\} \right\}$$

is an E-basis for E^{p^n}.

Definition 2.2.10 (Cohen ring)**.** Let $\mathcal{B}$ be a p-basis of E. For $n \geq 1$ let

$$C_n(E) := \left\langle W_n(E^{p^{n-1}}) \cup \{(b, 0, \dots, 0) \in W_n(E) : b \in \mathcal{B}\} \right\rangle \leq W_n(E)$$

be the generated subring of $W_n(E)$. The restriction of the transition maps $W_n(E) \to W_k(E)$ in fact induces a map $C_n(E) \to C_k(E)$ for $n \geq k > 0$ and the *Cohen ring of* E is defined to be

$$C(E) := \varprojlim_{n \in \mathbb{Z}_{>0}} C_n(E).$$

Remark 2.2.11. By construction and Lemma 2.2.8, we see that for a perfect field k, $C(k) = W(k)$ and more generally $W(E_{\mathrm{p}}) \leq C(E) \leq W(E)$ where $E_{\mathrm{p}} := \bigcap_{n=0}^{\infty} E^{p^n} \leq E$ is the maximal perfect subfield of E by Lemma 1.2.12.

Lemma 2.2.12. *Similarly to the ring of Witt vectors, C_n and C are functional. In particular C also has a Frobenius, the restriction of that on the Witt vectors at Definition 2.2.5.*

Now we can state a generalisation of Theorem 2.2.6 for arbitrary fields of positive characteristic.

Theorem 2.2.13. *For every field E of characteristic $p > 0$ there exists a unique (up to isomorphism) complete discrete valuation ring of characteristic* 0 *which is completely unramified and whose residue field is E and this ring is $C(E)$, the Cohen ring, i.e. we have* $\operatorname{char} C(E) = 0$, $\mathfrak{m}_{C(E)} = pC(E)$, $C(E) \cong \varprojlim_{n \in \mathbb{N}} C(E) \Big/ p^n C(E)$ *and* $E \cong C(E) \Big/ \mathfrak{m}_{C(E)}$.

2.2.2 Categorical equivalence

The construction to be presented is very similar to that in Section 2.1. For the detailed arguments, see that section.

Let $\mathcal{O}_{\mathcal{E}} := \mathcal{O}_{\mathcal{E}_E} := C(E)$ the Cohen ring of E and let $\mathcal{E} := \mathcal{E}_E := \operatorname{Frac} \mathcal{O}_{\mathcal{E}} = \mathcal{O}_{\mathcal{E}}[\frac{1}{p}]$ be its field of fractions. Let F/E be a finite Galois extension. From functionality of the Cohen rings, we see that an automorphism of F fixing E can be lifted to an automorphism of $C(F)$ fixing $\mathcal{O}_{\mathcal{E}}$ and hence to an automorphism of $\operatorname{Frac} C(F)$ fixing $\mathcal{E}$. Different automorphisms give different liftings, so we see that $\operatorname{Frac} C(F)/\mathcal{E}$ is Galois with $\operatorname{Gal}(\operatorname{Frac} C(F)/\mathcal{E}) \cong \operatorname{Gal}(F/E)$. For Galois extensions $L/F/E$ of E, we have $\operatorname{Frac} C(L)/\operatorname{Frac} C(F)$, so we can define

$$\mathcal{E}^{\mathrm{unr}} := \mathcal{E}_E^{\mathrm{unr}} := \bigcup_{\substack{F/E \\ \text{finite Galois}}} \operatorname{Frac} C(F) \tag{2.6}$$

the union of unramified extension. This makes $\mathcal{E}^{\mathrm{unr}}/\mathcal{E}$ a Galois extension. From Lemmas 1.2.7 and 1.2.17, we see that

$$\operatorname{Gal}(\mathcal{E}^{\mathrm{unr}}/\mathcal{E}) \cong \varprojlim_{\substack{F/E \\ \text{finite Galois}}} \operatorname{Gal}(\operatorname{Frac} C(F)/\mathcal{E}) \cong \varprojlim_{\substack{F/E \\ \text{finite Galois}}} \operatorname{Gal}(F/E) \cong G$$

By Lemma 2.2.12, there is a Frobenius map on each $\operatorname{Frac} C(F)$ whose restriction to F is $x \mapsto x^p$. These maps are are compatible, so they define a Frobenius map on $\mathcal{E}^{\mathrm{unr}}$ which we denoted by σ. Since the usual Frobenius $x \mapsto x^p$ commutes with the action $\mathrm{Gal}(F/E)$, the liftings also commute, i.e. σ and the G-action commute on $\mathcal{E}^{\mathrm{unr}}$. Let

$$\widehat{\mathcal{E}^{\mathrm{unr}}} := \widehat{\mathcal{E}_E^{\mathrm{unr}}} \tag{2.7}$$

be the completion of $\mathcal{E}^{\mathrm{unr}}$ with respect to the valuation and denote its ring of integers by

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} := \mathcal{O}_{\widehat{\mathcal{E}_E^{\mathrm{unr}}}}. \tag{2.8}$$

The G-action and σ are both defined on these object by continuous extensions.

The next few statements are based on the seminar notes [Böc08].

Lemma 2.2.14. $(\mathcal{O}_{\widehat{\mathcal{E}^{unr}}})^\sigma = \mathbb{Z}_p$

Proof. The usual Frobenius $x \mapsto x^p$ on $\mathbb{F}_p$ acts identically, so its lifting to $C(\mathbb{F}_p) = W(\mathbb{F}_p) = \mathbb{Z}_p$ is also the identity. This shows that $(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^\sigma \supseteq \mathbb{Z}_p$. For the other direction, note that $(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^\sigma \subseteq (W(E^{\mathrm{sep}}))^\varphi = W(\mathbb{F}_p) = \mathbb{Z}_p$. □

Lemma 2.2.15. $(\mathcal{O}_{\widehat{\mathcal{E}^{unr}}})^G = \mathcal{O}_\mathcal{E}$

Proof. By construction $(\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}})^G = \mathcal{O}_\mathcal{E}$, which shows that $(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^G \supseteq \mathcal{O}_\mathcal{E}$. For the other direction, consider the following exact commutative diagram.

$$\begin{array}{ccccccc}
0 & \longrightarrow & p^n(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^G & \longrightarrow & (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^G & \longrightarrow & \left(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \Big/ (p^n)\right)^G \\
 & & \uparrow & & \uparrow & & \uparrow = \\
0 & \longrightarrow & p^n(\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}})^G & \longrightarrow & (\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}})^G & \longrightarrow & \left(\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}} \Big/ (p^n)\right)^G \to H^1(G, \mathcal{O}_{\mathcal{E}^{\mathrm{unr}}}) \\
 & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & &
\end{array}$$

Equality at the right column follows from the fact that the completion of a ring is complete. From Theorem 1.6.6, $H^1(G, \mathcal{O}_{\mathcal{E}^{\mathrm{unr}}}) = 0$, so the second row is short exact, thus $\left(\mathcal{O}_{\mathcal{E}^{\mathrm{unr}}} \Big/ (p^n)\right)^G \cong \mathcal{O}_\mathcal{E} \Big/ (p^n)$. Then from the first row we see that $(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^G \Big/ (p^n) \leq \left(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \Big/ (p^n)\right)^G \cong \mathcal{O}_\mathcal{E} \Big/ (p^n)$. Complete these ring (p)-adically, i.e. apply $\varprojlim_{n\in\mathbb{N}}$ to both sides. Since the action of G is continuous, the ring $(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^G$ is (p)-adically complete. But the Cohen ring $\mathcal{O}_\mathcal{E}$ is complete by Theorem 2.2.13, so we see that $(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^G = \widehat{(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}})^G} \leq \widehat{\mathcal{O}_\mathcal{E}} = \mathcal{O}_\mathcal{E}$ to complete the proof. □

Now in order to describe the $\mathbb{Z}_p$-representations, we consider étale φ-modules over $\mathcal{O}_\mathcal{E}$ by Remark 2.1.16.

Definition 2.2.16 ((étale) φ-modules over $\mathcal{O}_\mathcal{E}$)**.** A *φ-module M over $\mathcal{O}_\mathcal{E}$* is an $\mathcal{O}_\mathcal{E}$-module M together with a σ-semi-linear map $\varphi : M \to M$ which is called a *Frobenius*. Such a module is said to be *étale*, if it is finitely generated and $\Phi_\varphi : M_\sigma \to M$ is an $\mathcal{O}_\mathcal{E}$-module isomorphism.

The category of (étale) φ-modules is abelian, cf. Theorem 2.1.6. Now we define the functors $\mathtt{M}$ and $\mathtt{V}$ between these categories similarly as before.

Definition 2.2.17 (Functors $\mathtt{M}$, $\mathtt{V}$)**.** Let V be a $\mathbb{Z}_p$-representation of G. First define a Frobenius and a G-action on $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathbb{Z}_p} V$ by

$$\varphi\left(\sum_{i=1}^{r} \mu_i \otimes v_i\right) := \sum_{i=1}^{r} \sigma(\mu_i) \otimes v_i, \qquad g\left(\sum_{i=1}^{r} \mu_i \otimes v_i\right) := \sum_{i=1}^{r} g(\mu_i) \otimes g(v_i),$$

then define $\mathtt{M}(V) := (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathbb{Z}_p} V)^G$, the fixed elements of the defined G-action, which is an étale φ-module over $\mathcal{O}_\mathcal{E}$.
Now let M be an étale φ-module over $\mathcal{O}_\mathcal{E}$. First define a G-action on and a Frobenius on $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} M$ by

$$g\left(\sum_{i=1}^{r} \mu_i \otimes x_i\right) := \sum_{i=1}^{r} g(\mu_i) \otimes x_i, \qquad \varphi\left(\sum_{i=1}^{r} \mu_i \otimes x_i\right) := \sum_{i=1}^{r} \sigma(\mu_i) \otimes \varphi(x_i),$$

then define $\mathtt{V}(M) := (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} M)^\varphi$, the fixed elements of the defined φ-action which, is a $\mathbb{Z}_p$-representation of G.

Remark 2.2.18. With a slight abuse of notation, as a shorthand, we denote these actions by $\sigma \otimes \mathrm{Id}$, $G \otimes G$, $G \otimes \mathrm{Id}$ and $\sigma \otimes \varphi$, respectively.

Proposition 2.2.19. *For any $\mathbb{Z}_p$-representation V of G the following map is an isomorphism.*

$$\alpha_V : \mathcal{O}_{\widehat{\mathcal{E}^{unr}}} \otimes_{\mathcal{O}_\mathcal{E}} \mathtt{M}(V) \to \mathcal{O}_{\widehat{\mathcal{E}^{unr}}} \otimes_{\mathbb{Z}_p} V, \qquad \sum_{i=1}^{r} \mu_i \otimes x_i \mapsto \sum_{i=1}^{r} \mu_i x_i$$

Proof. Let $U := \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathbb{Z}_p} V$, an $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}}$-module with a G-action defined above. Note that $U^G = \mathtt{M}(V)$. We want to prove $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} U^G \cong U$. We first prove this statement for $U = X$ when X is an $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}}$-module with a G-action annihilated by p^n (i.e. $p^n X = 0$). Note that such an X is naturally isomorphic to a module over $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \Big/ p^n \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}}$ in which case the tensor product is taken over $\mathcal{O}_E \Big/ p^n \mathcal{O}_E$. We proceed by induction on n.

For $n = 1$, we know that $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \Big/ p^n \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \cong E^{\mathrm{sep}}$ and $\mathcal{O}_\mathcal{E} \Big/ p\mathcal{O}_\mathcal{E} \cong E$. So by Corollary 2.1.10, the statement is true.

Suppose $n > 1$ and that X is annihilated by p^n. Let $X' := \{x \in X : px = 0\}$ and $X'' := X \Big/ X'$. Since X' is annihilated by p, similarly to the $n = 1$ case we see that $X' \cong (E^{\mathrm{sep}})^d$ as G-representations for some d. From the short exact sequence $0 \to X' \to X \to X''$ by Lemma 1.6.4 we get a long exact sequence $0 \to (X')^G \to$

$X^G \to (X'')^G \to H^1(G, X') = \prod_{i=1}^d H^1(G, E^{\text{sep}}) \cong 0$ which happens to be a short exact sequence by using Lemma 1.6.3 and Theorem 1.6.6 to the last term. Since $\mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}}$ is a free $\mathcal{O}_\mathcal{E}$-module, it is flat in particular, so by definition the functor $\mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} -$ is exact, so applying this functor to the short exact sequence, we get the first row of the a the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} (X')^G & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} X^G & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} (X'')^G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle \alpha_{n-1}} & & \\ 0 & \longrightarrow & X' & \longrightarrow & X & \longrightarrow & X'' & \longrightarrow & 0 \end{array}$$

Since X is annihilated by p^n, X'' is annihilated by p^{n-1}. From the $n = 1$ case applied to X', and by applying the induction step for X'', we see that α_1 and α_{n-1} are isomorphisms. Them from the Snake lemma, we get a long exact sequence $0 \to \ker \alpha_1 = 0 \to \ker \alpha_n \to \ker \alpha_{n-1} = 0 \to \operatorname{coker} \alpha_1 = 0 \to \operatorname{coker} \alpha_n \to \operatorname{coker} \alpha_{n-1} = 0 \to 0$. From this long exact sequence, we see that $\ker \alpha_n = 0$ and $\operatorname{coker} \alpha_n = 0$ since they are between two the trivial module, i.e. α_n is an injection and a surjection, hence an isomorphism finishing the inductive step.

Let us turn out attention to the original statement. We claim the following isomorphisms to finish the proof of the statement.

$$\begin{aligned} \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} U^G &\cong \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} \left(\varprojlim_{n \in \mathbb{Z}_{>0}} U \big/ p^n U \right)^G \cong \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} \varprojlim_{n \in \mathbb{Z}_{>0}} \left(U \big/ p^n U \right)^G \\ &\cong \varprojlim_{n \in \mathbb{Z}_{>0}} \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} \left(U \big/ p^n U \right)^G \cong \varprojlim_{n \in \mathbb{Z}_{>0}} U \big/ p^n U \cong U \end{aligned}$$

For the first and last isomorphisms, notice that as the completion is complete, $\mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \cong \varprojlim_{n \in \mathbb{N}} \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \Big/ p^n \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}}$ which implies that $U \cong \varprojlim_{n \in \mathbb{N}} U \big/ p^n U$ as U is a finitely generated $\mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}}$-module on which the structure theorem can be applied.

The second isomorphism holds, as G acts component-wise on the inverse limit, so its action can be interchanged with taking the inverse limit.

For the penultimate isomorphism, note that $X = U \big/ p^n U$ is annihilated by p^n, in which case we proved the statement.

Consider the third isomorphism, namely that the functors $\mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} -$ and $\varprojlim_{n \in \mathbb{N}}$ commute. Define

$$\begin{aligned} T := \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} \varprojlim_{n \in \mathbb{Z}_{>0}} \left(U \big/ p^n U \right)^G &\to \varprojlim_{n \in \mathbb{Z}_{>0}} \mathcal{O}_{\widehat{\mathcal{E}^{\text{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} \left(U \big/ p^n U \right)^G := L \\ \sum_{i=1}^r \mu_i \otimes \left(u_i^{(n)} \right)_n &\mapsto \left(\sum_{i=1}^r \mu_i \otimes u_i^{(n)} \right)_n \end{aligned}$$

which is a well-defined homomorphism. To prove that this map is injective, we may assume that $\{\mu_i : 1 \le i \le r\}$ is $\mathcal{O}_\mathcal{E}$-linearly independent. Then for an element of the kernel, we have then $\sum_{i=1}^r \mu_i \otimes u_i^{(n)} = 0$ for all $n \in \mathbb{Z}_{>0}$, i.e. $u_i^{(n)} = 0$.

$T \cong \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}} \otimes_{\mathcal{O}_\mathcal{E}} U^G$ and $L \cong U$ finitely generated $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{unr}}}}$-modules and consider $T \leq L$ by the above injection. ${}^{T}/_{pT} \cong {}^{L}/_{pL}$, ${}^{L}/_{T} \Big/ {}^{pL}/_{T} \cong 0$, so ${}^{L}/_{T} \cong {}^{pL}/_{T}$. But ${}^{pL}/_{T}$ is the Jacobson radical of ${}^{L}/_{T}$, so by Nakayama's lemma, ${}^{L}/_{T} \cong 0$, i.e. $L \cong T$ as required. □

Proposition 2.2.20. *For any étale φ-module M over $\mathcal{O}_\mathcal{E}$ the following map is an isomorphism.*

$$\alpha_M : \mathcal{O}_{\widehat{\mathcal{E}^{unr}}} \otimes_{\mathbb{Z}_p} \mathtt{V}(M) \to \mathcal{O}_{\widehat{\mathcal{E}^{unr}}} \otimes_{\mathcal{O}_\mathcal{E}} M$$
$$\sum_{i=1}^{r} \mu_i \otimes v_i \mapsto \sum_{i=1}^{r} \mu_i v_i$$

Proof. The proof is similar to the proof of Proposition 2.2.19 but here for the base case we use Proposition 2.1.12. □

We arrived to the main statement of this section.

Theorem 2.2.21. *The category* $\mathbf{Rep}_{\mathbb{Z}_p}(\mathrm{Gal}(E^{\mathrm{sep}}/E))$ *is categorically equivalent to the category* $\mathbf{M}_\varphi^{ét}(C(E))$ *of étale φ-modules over the Cohen ring of E via* M *and* V *defined in Definition 2.2.17.*

Proof. This is a straightforward consequence of Remark 2.1.16, Lemmas 2.2.14 and 2.2.15, and Propositions 2.2.20 and 2.2.19. □

Note. This categorical equivalence gives a completely analogous description of the $\mathbb{Z}_p$-representations of $\mathrm{Gal}(E^{\mathrm{sep}}/E)$ of dimension d using the very same definition of equivalence on the matrix group $\mathrm{GL}_d(C(E))$ as in Theorem 2.1.15.

2.3 $\mathbb{Q}_p$-representations

In this section we study $\mathbb{Q}_p$-representation of the absolute Galois group $G = \mathrm{Gal}(E^{\mathrm{sep}}/E)$ of the filed E of characteristic $p > 0$. These representations are also called *p-adic representations*. The theory and the proofs in this section is practically the same as for the $\mathbb{Z}_p$-representations so here we just present the key statements without proof. For details and notations, see the Section 2.2 on the $\mathbb{Z}_p$-representations.

Definition 2.3.1 ((étale) φ-modules over $\mathcal{E}$)**.** An $\mathcal{E}$-vector space D with a σ-semi-linear map $\varphi : D \to D$ is called an *φ-module over $\mathcal{E}$*.
If further $\dim_\mathcal{E} D$ is finite and there is an $\mathcal{O}_\mathcal{E}$-submodule M of D (regarded as an $\mathcal{O}_\mathcal{E}$-module) which is stable under the the action of φ, then we D is an *étale φ-module over $\mathcal{E}$*.

Lemma 2.3.2. $(\widehat{\mathcal{E}^{unr}})^\sigma = \mathbb{Q}_p$ *and* $(\widehat{\mathcal{E}^{unr}})^G = \mathcal{E}$

Proof. Same as the proof of Lemmas 2.2.14 and 2.2.15. □

Define the functors $\mathtt{M} : \mathbf{Rep}_{\mathbb{Q}_p}(G) \to \mathbf{M}_{\varphi}^{\text{ét}}(\mathcal{E})$ and $\mathtt{V} : \mathbf{M}_{\varphi}^{\text{ét}}(\mathcal{E}) \to \mathbf{Rep}_{\mathbb{Q}_p}(G)$ completely analogously as in Definition 2.2.17. Note that we need the submodule condition in the definition of étale φ-modules over $\mathcal{E}$ to have these functors well-defined.

Proposition 2.3.3. *For any $\mathbb{Q}_p$-representation V of G the following map is an isomorphism.*

$$\alpha_V : \widehat{\mathcal{E}^{unr}} \otimes_{\mathcal{E}} \mathtt{M}(V) \to \widehat{\mathcal{E}^{unr}} \otimes_{\mathbb{Q}_p} V, \qquad \sum_{i=1}^{r} \mu_i \otimes x_i \mapsto \sum_{i=1}^{r} \mu_i x_i$$

For any étale φ-module M over $\mathcal{E}$ the following map is an isomorphism.

$$\alpha_M : \widehat{\mathcal{E}^{unr}} \otimes_{\mathbb{Q}_p} \mathtt{V}(M) \to \widehat{\mathcal{E}^{unr}} \otimes_{\mathcal{E}} M, \qquad \sum_{i=1}^{r} \mu_i \otimes v_i \mapsto \sum_{i=1}^{r} \mu_i v_i$$

Proof. Same as the proof of Propositions 2.2.19 and 2.2.20. □

Theorem 2.3.4. *The category $\mathbf{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}(E^{\mathrm{sep}}/E))$ of p-adic representations is categorically equivalent to the category $\mathbf{M}_{\varphi}^{\acute{e}t}(\mathrm{Frac}\, C(E))$ of étale φ-modules over the field of fractions of the Witt vectors of E via $\mathtt{M}$ and $\mathtt{V}$. This equivalence classifies all the representations using square matrices over $\mathrm{Frac}\, C(E)$.*

Chapter 3

Galois Representations of p-adic fields

Let p be a prime number. A p-adic field K is a finite extension of $\mathbb{Q}_p$. In this chapter, we study the Galois representations of K.

3.1 Cyclotomic and $\mathbb{Z}_p$-extensions, $R(\bar{A})$

Let F be a finite extension of $\mathbb{Q}_p$. For $n \in \mathbb{N}$, let $\mu_{p^n} := \{a \in \mathbb{Q}_p^{\text{alg}} : a^{p^n} = 1\} = \langle \zeta_n \rangle$ be the cyclic group of p^nth roots of unity generated by a primitive root ζ_n, let $\mu_{p^\infty} := \bigcup_{n\in\mathbb{N}} \mu_{p^n}$, and let $F^{\text{cyc}} := F(\mu_{p^\infty})$, which is a Galois extension over F. For $g \in \text{Gal}(F^{\text{cyc}}/F)$, $g(\zeta_n)^{p^n} = g(\zeta_n^{p^n}) = g(1) = 1$, so $g(\zeta_n) \in \mu_{p^n} = \langle \zeta_n \rangle$, thus $g(\zeta_n) = \zeta_n^{u_n}$ for some $u_n \in \mathbb{Z}$, which is uniquely defined modulo p^n. For $N \geq n$, $\zeta_n \in \mu_{p^N} = \langle \zeta_N \rangle$, so for some k, $\zeta_n = \zeta_N^k$, thus $g(\zeta_n) = g(\zeta_N^k) = g(\zeta_N)^k = \zeta_N^{u_N k} = \zeta_n^{u_N}$, i.e. $u_n - u_N \in p^n\mathbb{Z}$. Since $\ker g = \{1\}$, $1 \neq g(\zeta_1) = \zeta_1^{u_1}$, so $u_1 \notin p\mathbb{Z}$. This means that

$$\begin{aligned} \chi : \text{Gal}(F^{\text{cyc}}/F) \to \left(\varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}\right)^\times = \mathbb{Z}_p^\times \cong \mathbb{Z}_p \times \mathbb{Z}\Big/\max\{2, p-1\}\mathbb{Z} \\ g \mapsto (u_n + p^n\mathbb{Z})_{n\in\mathbb{Z}_{>0}} \end{aligned}$$

is a well-defined homomorphism called the *p-adic cyclotomic character*. We see that $\ker \chi = \{\text{Id}\}$, so χ is injective. (Note that for $F = \mathbb{Q}_p$, the p-adic cyclotomic character χ is an isomorphisms, i.e. $\text{Gal}(\mathbb{Q}_p^{\text{cyc}}/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$.) The group $\chi[\text{Gal}(F^{\text{cyc}}/F)]$ is a closed infinite subgroup of $\mathbb{Z}_p^\times$. The closed subgroups of $\mathbb{Z}_p$ are $\{0\}$ and $p^n\mathbb{Z}_p \cong \mathbb{Z}_p$ for $n \in \mathbb{N}$. Thus for some finite group Δ_F we have

$$\text{Gal}(F^{\text{cyc}}/F) \cong \Delta_F \times \mathbb{Z}_p,$$

thus $\text{Gal}(F^{\text{cyc}}/F)$ has a quotient isomorphic to $\mathbb{Z}_p$, so by the Fundamental Theorem of Galois Theory (Theorem 1.2.10), there is unique a Galois extension F_∞/F in F^{cyc} with $\text{Gal}(F_\infty/F) \cong \mathbb{Z}_p$.

Definition 3.1.1 ($\mathbb{Z}_p$-extension)**.** A $\mathbb{Z}_p$-*extension* is a Galois extension whose Galois group is isomorphic to $\mathbb{Z}_p$.

The above discussion shows that there is a unique $\mathbb{Z}_p$-extension of F contained in F^{cyc}, which we denoted by F_∞. The closed subgroups of $\mathbb{Z}_p$ are discussed above, and so the quotients of with these are isomorphic to $\mathbb{Z}_p$ or $\mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$. So again by the Fundamental Theorem of Galois Theory, all Galois subextensions of F_∞/F are F_n for $n \in \mathbb{N} \cup \{\infty\}$ where $F_0 = F$, $F_n \subsetneq F_N$ for $n < N \in \mathbb{N}$ and $\text{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$. Observe that $F_\infty = \bigcup_{n\in\mathbb{N}} F_n$ and by Lemma 1.2.7

$$\text{Gal}(F_\infty/F) \cong \varprojlim_{n\in\mathbb{N}} \text{Gal}(F_n/F) \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$$

Now we prove a lemma that will be used throughout the chapter.

Lemma 3.1.2. *Let A be a commutative ring that is separated and complete with respect to the pA-adic metric, i.e. $A \cong \varprojlim_{n\in\mathbb{N}} A/p^nA$, cf. section 1.4. Then*

$$S(A) := \left\{(x^{(n)})_n \in A^{\mathbb{N}} : \forall n \in \mathbb{N} \quad x^{(n)} = (x^{(n+1)})^p\right\}$$

with $(xy)^{(n)} := x^{(n)}y^{(n)}$ and $(x+y)^{(n)} := \left(\lim_{m\to\infty}\left(x^{(n+m)} + y^{(n+m)}\right)^{p^m}\right)_n$ define a ring.

Proof. Let $\bar{A} := A/pA$, a ring of characteristic $p > 0$ and let

$$R(\bar{A}) := \left\{(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} : \bar{A} : \forall n \in \mathbb{N} \quad x_n = x_{n+1}^p\right\}$$

be a ring where the operations are defined component-wise. In other words,

$$R(\bar{A}) = \varprojlim_{n\in\mathbb{N}} \bar{A}_n,$$

where $\bar{A}_n = \bar{A}$, the ordering on $\mathbb{N}$ is the usual one and the transition maps $\bar{A}_n \to \bar{A}_k$ are σ^{n-k} for $k \leq n$. We will construct a bijection between $R(\bar{A})$ and (A).

Pick $(x_n)_n \in R(\bar{A})$ and choose and arbitrary lifting $\hat{x}_n \in A$ for each $n \in \mathbb{N}$, i.e. choose $\hat{x}_n \in A$ so that $x_n = \hat{x}_n + pA$. Then by definition $\hat{x}_{n+1}^p - \hat{x}_n \in pA$. From the binomial theorem, $(\hat{x}_{n+1}^p - \hat{x}_n)^p = \hat{x}_{n+1}^{p^2} - \hat{x}_n^p - p(\hat{x}_{n+1}^p - \hat{x}_n)f(\hat{x}_{n+1}, \hat{x}_n)$ for some polynomial $f(x, y)$, so $\hat{x}_{n+1}^{p^2} - \hat{x}_n^p \in p^2A$ and we see inductively that for all $m \in \mathbb{N}$, $\hat{x}_{n+1}^{p^{m+1}} - \hat{x}_n^{p^m} \in p^{m+1}A$. Then by a telescopic sum, we see that $\hat{x}_{n+m+1}^{p^{m+1}} - \hat{x}_n^{p^m} \in p^{m+1}A$. Again by a telescopic sum, we see that $\hat{x}_{n+M}^{p^M} - \hat{x}_{n+m}^{p^m} \in p^{m+1}$ for $M \geq m$, i.e. the sequence $\left(\hat{x}_{n+m}^{p^m}\right)_m$ is a Cauchy sequence with respect to the pA-adic filtration. By assumption, A is complete, i.e. this sequence converges to some $x^{(n)} \in A$. Define the map

$$R(\bar{A}) \to S(A), \qquad (x_n)_n \mapsto (x^{(n)})_n$$

from the construction above.

We see that $x^{(n)} = (x^{(n+1)})^p$, and that $x^{(n)}$ does not depend on the choice of the liftings $\hat{x}_n$, i.e. the map is well-defined. Also this map is a bijection and the pullback of the ring structure of $R(\bar{A})$ under this map to $S(A)$ coincides with the ring structure in the statement. □

Note. For the rest of this chapter we identify the ring $R(\bar{A})$ with $S(A)$ via the above isomorphism. Write lower indices for elements of $R(\bar{A})$ and upper indices for the elements of $S(A)$. Denote the natural projection to the mth coordinate by

$$\theta_m : R(\bar{A}) = \varprojlim_{n\in\mathbb{N}} \bar{A}_n \to A_n, \qquad (a_n)_{n\in NN} \mapsto a_m.$$

3.2 Setup for the rest of the chapter

Let K be a p-adic field for a fixed prime p, i.e. a finite extension of the field $\mathbb{Q}_p$ of the p-adic numbers. Fix an algebraic closure K^{alg} of K. Note that $K^{\mathrm{alg}} \cong \mathbb{Q}^{\mathrm{alg}}$. Let v be the valuation on $\mathbb{Q}_p$ such that $v(p) = 1$. This valuation extends to a valuation v_K of K by Definition 1.5.2. With the same formula, the valuation of $\mathbb{Q}_p$ can be extended uniquely to any finite extension of K. Since K^{alg} is the union of finite extension of $\mathbb{Q}_p$ contained in K^{alg} and the extensions of the valuation v are compatible, then there is a unique way to extend v to a valuation $v_{K^{\mathrm{alg}}}$ of K^{alg}. Note that $v_{K^{\mathrm{alg}}}[(K^{\mathrm{alg}})^\times] = \mathbb{Q}$, so K^{alg} is not complete anymore as opposed to the finite extensions. Let

$$C := \widehat{K^{\mathrm{alg}}}$$

be the completion of K^{alg} with respect to $v_{K^{\mathrm{alg}}}$. C is algebraically closed by Krasner's lemma. By Equation (1.2) the valuation $v_{K^{\mathrm{alg}}}$ extends continuously to a valuation

$$v := v_C$$

on C, the restriction of which gives the valuation of any subfield of C. Note that any extension of $\mathbb{Q}_p$ is of characteristic 0, so by Example 1.2.13 it is a perfect field in which case the separable closure is simply the algebraic closure. Fix

$$k := k_K,$$

the residue field of K. Since $K/\mathbb{Q}_p$ is finite, $k/k_{\mathbb{Q}_p}$ is also finite and $k_{\mathbb{Q}_p} = \mathbb{F}_p$, so k is a finite field of characteristic p, in particular it is perfect by Example 1.2.13. Let

$$K_0 := \operatorname{Frac} W(k)$$

be the fraction field of the ring of the Witt vectors over k. Since $k_{K_0} = k = k_K$, the extension K/K_0 is totally ramified. $\{\pi_K^i : 0 \le i \le e_K - 1\}$ is an $\mathcal{O}_{K_0}$-basis of $\mathcal{O}_K$ as well as a K_0-basis for K.

For an arbitrary intermediate extension $K^{\mathrm{alg}}/L/K_0$ denote the corresponding absolute Galois group by

$$G_L := \mathrm{Gal}(K^{\mathrm{alg}}/L).$$

Let

$$R_L := R\left(\mathcal{O}_L \big/ p\mathcal{O}_L\right).$$

From the fact that the completion of $\widehat{L}$ is itself, we obtain $R_{\widehat{L}} = \varprojlim_{n\in\mathbb{N}} \mathcal{O}_{\widehat{L}} \Big/ p\mathcal{O}_{\widehat{L}} = \varprojlim_{n\in\mathbb{N}} \mathcal{O}_L \big/ p\mathcal{O}_L = R_L$. In particular let

$$R := R_C = R_{K^{\mathrm{alg}}}.$$

Let

$$1 \neq \varepsilon := (\varepsilon^{(n)})_{n\in\mathbb{N}} := (\varepsilon_n)_{n\in\mathbb{N}} \in R \tag{3.1}$$

be a sequence of compatible primitive p^nth roots of unity, i.e. $\varepsilon^{(0)} = 1$, $\varepsilon^{(0)} \neq 1$ and $\varepsilon^{(n)} = (\varepsilon^{(n+1)})^p$ for $n \in \mathbb{N}$. Let

$$K_0^{\mathrm{cyc}} := \bigcup_{n\in\mathbb{N}} K_0(\varepsilon^{(n)}), \qquad\qquad K^{\mathrm{cyc}} := \bigcup_{n\in\mathbb{N}} K(\varepsilon^{(n)})$$

be the cyclotomics extension of K_0 and K, respectively with the unique $\mathbb{Z}_p$ extensions

$$(K_0)_\infty, \qquad\qquad K_\infty,$$

respectively. Let

$$\Gamma_K := \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p, \qquad \Delta_K := \mathrm{Gal}(K^{\mathrm{cyc}}/K_\infty),$$

where $K^{\mathrm{cyc}}/K_\infty$ is a finite ramified Galois extension. Let

$$\pi := (\pi_n)_n := (\pi^{(n)})_n := \varepsilon - 1 = (\varepsilon^{(n)} - 1)_{n\in\mathbb{N}} \in R_{K_0^{\mathrm{cyc}}}. \tag{3.2}$$

Now $v_R(\pi) = v_{\mathbb{C}_K}(\pi^{(0)}) = v_{\mathbb{C}_K}\left(\lim_{m\to\infty}(\varepsilon^{(n)} - 1)^{p^m}\right) = \lim_{m\to\infty} p^m \frac{1}{p^{m-1}(p-1)} = 1 + \frac{1}{p-1} > 1$ showing that $\varepsilon \in R_{K_0^{\mathrm{cyc}}}$ is a unit.

For a summary see the left side of Figure 3.1 on page 46.

3.3 Fontaine's fundamental theorem

This section follows the ideas of Fontaine from [FO, Chapter 4].

Proposition 3.3.1. *$R = R_{K^{\mathrm{alg}}}$ defined above is a perfect, complete valuation ring of characteristic p with residue field isomorphic to $k^{\mathrm{alg}} \cong \mathbb{F}_p^{\mathrm{alg}}$ where the valuation is given by*

$$v_R((x^{(n)})_n) := v_{\mathbb{C}_K}(x^{(0)})$$

Moreover

$$\mathrm{Frac}\, R = \left\{(x^{(n)})_n \in {\mathbb{C}_K}^{\mathbb{N}} : \forall n \in \mathbb{N} \quad x^{(n)} = (x^{(n+1)})^p\right\} = S(\mathbb{C}_K)$$

is an algebraically closed field.

Proof. By definition $\operatorname{char} R = 0$. If $x = (x_n)_{n\in\mathbb{N}} \in R$, then $x = (x_{n+1})^p_{n\in\mathbb{N}}$, so the Frobenius is surjective. Also if $x^p = 0$, then $x_n = 0$ for all n, i.e. it is injective as well. So by Lemma 1.2.12 R is perfect.

Now we turn to prove that v_R is a valuation on R, i.e. that it satisfies the Equation (1.1). First, not that $\infty = v_R(x) \iff \infty = v_{\mathbb{C}_K}(x^{(0)}) \iff x^{(0)} = 0 \iff x = 0$ and that $v_R(xy) = v_{\mathbb{C}_K}((xy)^{(0)}) = v_{\mathbb{C}_K}(x^{(0)}y^{(0)}) = v_{\mathbb{C}_K}(x^{(0)})+v_{\mathbb{C}_K}(y^{(0)}) = v_R(x)+v_R(y)$ from the definitions. Finally note that from $v_{\mathbb{C}_K}(x^{(0)}) = p^n v_{\mathbb{C}_K}(x^{(n)})$,

$$\begin{aligned} v_R(x+y) &= v_R\left(\lim_{m\to\infty}(x^{(n+m)}+y^{(n+m)})^{p^m}\right) = v_{\mathbb{C}_K}\left(\lim_{m\to\infty}(x^{(m)}+y^{(m)})^{p^m}\right) \\ &= \lim_{m\to\infty} p^m v_{\mathbb{C}_K}(x^{(m)}+y^{(m)}) \geq \lim_{m\to\infty} p^m \min\{v_{\mathbb{C}_K}(x^{(m)}), v_{\mathbb{C}_K}(y^{(m)})\} \\ &\geq \lim_{m\to\infty} \min\{v_{\mathbb{C}_K}(x^{(0)}), v_{\mathbb{C}_K}(y^{(0)})\} \geq \min\{v_{\mathbb{C}_K}(x^{(0)}), v_{\mathbb{C}_K}(y^{(0)})\} \\ &= \min\{v_R(x), v_R(y)\} \end{aligned}$$

By definition $v_R(x) \geq p^n \iff v_{\mathbb{C}_K}(x^{(n)}) \geq 1 \iff x_n = 0$, thus $\{x \in R : v_R(x) \geq p^n\}$ coincides with the kernel of the projection $R \to \mathcal{O}_{\mathbb{C}_K} \Big/ p\mathcal{O}_{\mathbb{C}_K}$ to the nth coordinate, which is a neighbourhood basis for $n \in \mathbb{N}$. This means that the topology of the inverse limit (with the discrete topology for each term) coincides with the topology defined by the valuation. But then from the discreteness of $R \to \mathcal{O}_{\mathbb{C}_K} \Big/ p\mathcal{O}_{\mathbb{C}_K}$, every Cauchy sequence in R becomes stationary for big enough indices, so converges in R, i.e. R is complete to the valuation v_R.

For the proof that $\operatorname{Frac} R$ is algebraically closed, see [FO, Poroposition 4.8]. □

Note. Note that $v_R[R^\times] \cong \mathbb{Q}_{\geq 0}$. Let $\tau : R \xrightarrow{\theta_0} \mathcal{O}_{K^{\mathrm{alg}}} \Big/ p\mathcal{O}_{K^{\mathrm{alg}}} \to \mathcal{O}_{K^{\mathrm{alg}}} \Big/ \pi_{K^{\mathrm{alg}}}\mathcal{O}_{K^{\mathrm{alg}}} = k$. This τ map has a uniqe section (right inverse) $s : k^{\mathrm{alg}} \to R$.

For an intermediate extension $K^{\mathrm{sep}}/L/K_0$, G_L acts on R coordinate-wise, i.e. $g(x) := (g(x^{(n)}))_{n\in\mathbb{N}}$, and on $\operatorname{Frac} R$ by $g\left(\frac{x}{y}\right) := \frac{g(x)}{g(y)}$.

Lemma 3.3.2. *$R^{G_L} = R_L$, $(\operatorname{Frac} R)^{G_L} = \operatorname{Frac} R_L$ and $k_{\operatorname{Frac} R_L} = k_L = (k^{\mathrm{alg}})^{G_L}$. Furthermore if $v_{\mathbb{C}_K}[L^\times] \cong \mathbb{Z}$, then $R_L = k_L$.*

Proof. The action is coordinate-wise on $R = R_{\mathbb{C}_K}$, so $x \in R^{G_L}$ if and only if $x^{(n)} \in (\mathcal{O}_{\mathbb{C}_K})^{G_L}$ for all $n \in \mathbb{N}$, but $(\mathcal{O}_{\mathbb{C}_K})^{G_L} = \mathcal{O}_{\mathbb{C}_K{}^{G_L}} = \mathcal{O}_{\mathbb{C}_K{}^{G_L}} = \mathcal{O}_{\widehat{(K^{\mathrm{alg}})}^{G_L}} = \mathcal{O}_{\widehat{(K^{\mathrm{alg}})^{G_L}}} = \mathcal{O}_{\widehat{L}} = \varprojlim_{n\in\mathbb{N}} \mathcal{O}_{\widehat{L}} \Big/ p\mathcal{O}_{\widehat{L}} = \varprojlim_{n\in\mathbb{N}} \mathcal{O}_L \Big/ p\mathcal{O}_L$ from the idempotence of completion, so $R^{G_L} = R_L$ indeed. The proof of $(\operatorname{Frac} R)^{G_L} = \operatorname{Frac} R_L$ is similar.

We have $\mathrm{Id}_{k^{\mathrm{alg}}} : k^{\mathrm{alg}} \overset{s}{\hookrightarrow} R \overset{\tau}{\twoheadrightarrow} k^{\mathrm{alg}}$. Taking the G_L-invariants of this map, we get the $k_L \hookrightarrow R^{G_L} \twoheadrightarrow k_L$ identity map. Hence $k_{\operatorname{Frac} R^{G_L}} = k_L$.

For the last part, note that it is enough to show that $x \in R^{G_L}$ with $v_R(x) > 0$ is only possible for $x = 0$. For any n, we have $v_{\mathbb{C}_K}(x^{(n)}) = p^{-n} v_{\mathbb{C}_K}(x^{(0)})$. But note that $v[\widehat{L}\times] = v[L\times]$ is discrete by assumption, so $v_{\mathbb{C}_K}(x^{(0)}) = \infty$ and we are done. □

Remark 3.3.3. K has discrete valuation, so the previous lemma, we see that $R^{G_K} \cong k$.

Denote the formal Laurent series with coefficients in k with formal variable π from Equation (3.2) by

$$E_0 := R^{G_K}((\pi)) \subseteq \operatorname{Frac} R \tag{3.3}$$

which plays a crucial role in the theory. Note that from the previous remark, $E_0 \cong k((\pi))$.

Since $\operatorname{Frac} R$ is algebraically closed by Proposition 3.3.1, let E_0^{sep} be the unique separable closure of $E_0 \subseteq \operatorname{Frac} R$ contained in $\operatorname{Frac} R$.

Theorem 3.3.4 (Fontaine's fundamental theorem)**.** *$H := G_{K_0^{cyc}}$ acts on $\operatorname{Frac} R \supseteq E_0^{\text{sep}} \supseteq E_0$ coordinate-wise. The restriction*

$$\operatorname{Gal}(K^{\text{alg}}/K_0^{cyc}) \to \operatorname{Gal}(E_0^{\text{sep}}/E_0), \qquad g \mapsto g\big|_{E_0^{\text{sep}}}$$

gives an isomorphism of the Galois groups.

Proof. First shows that the map is well-defined. Let $x \in E_0^{\text{sep}}$ and let $\sum_{i=0}^r \mu_i X^i =: P(X) \in E_0[X]$ be its (separable) minimal polynomial over E_0. Pick $g \in H$. Then $g(x)$ is a root of $g(P)(X) := \sum_{i=0}^r g(\mu_i)X^i$. Let $\mu_i := \sum_j \lambda_{i,j}\pi^j \in k((\pi)) = E_0$, then $g(\mu_i) = \sum_j \lambda_{i,j} g(\pi^j)$ as H acts trivially on $k \cong R^{G_{K_0}}$. Note that $g(\varepsilon) = \varepsilon^{\chi(g)}$ for $\chi(g) \in \mathbb{N}$ by the definitions of the cyclotomic character, so $g(\pi) = (\pi+1)^{\chi(g)} - 1 \in k((\pi)) = E_0$ as $\varepsilon = \pi + 1$ by definition. This shows that $g(P)(X) \in E_0[X]$, i.e. that $g(x)$ is separable over E_0, thus $g(x) \in E_0^{\text{sep}}$. We have shown that $H[E_0^{\text{sep}}] \subseteq E_0$.

Now we show that the map is injective. Pick g from the kernel, i.e. $g(x) = x$ for all $x \in E_0^{\text{sep}}$. Let $y^{(0)} \in \mathbb{C}_K$ be arbitrary. As $\mathbb{C}_K$ is algebraically closed, for all $n > 0$ there is $y^{(n)}$ such that $y^{(n)} = (y^{(n+1)})^p$, i.e. $y := (y^{(n)})_n \in \operatorname{Frac} R$. By [FO, Theorem 4.16] E_0^{sep} is dense in $\operatorname{Frac} R$, so $g(y) = y$ as the action defined coordinate-wise is continuous. Then $g(y^{(0)}) = y^{(0)}$, i.e. g acts identically on an arbitrary element of $\mathbb{C}_K$. But $K^{\text{alg}} \subseteq \mathbb{C}_K$, so g acts identically on K^{alg} which means that $g \in H$ is the identity element.

Finally we prove the surjectivity. Since the map is injective, we can identify $H \leq \operatorname{Gal}(E_0^{\text{sep}}/E_0)$ as a closed subgroup. So by Theorem 1.2.10 for $F := (E_0^{\text{sep}})^H$, E_0^{sep}/F is Galois with Galois group isomorphic to H.

Recall that for $S \subseteq \mathbb{C}_K$, $S^{\text{rad}} := \{x \in \mathbb{C}_K : \exists n \in \mathbb{N} \;\; x^{p^n} \in S\}$. We claim that $(\operatorname{Frac} R)^H \subseteq \widehat{E_0^{\text{rad}}}$. (In fact according to [FO, Theorem 4.15], equality holds but we don't need that.) Note that it is enough to show that E_0^{rad} is dense in $R_{K_0^{\text{cyc}}} = \varprojlim_{n\in\mathbb{N}} \mathcal{O}_{K_0^{\text{cyc}}} \Big/ p\mathcal{O}_{K_0^{\text{cyc}}}$. Denote by $\theta_m : R \to \mathcal{O}_{K^{\text{alg}}} \Big/ p\mathcal{O}_{K^{\text{alg}}}$ the projection map to the mth coordinate. We need to prove that $\theta_m[\mathcal{O}_{E_0^{\text{rad}}}] \supseteq \mathcal{O}_{K_0^{\text{cyc}}} \Big/ p\mathcal{O}_{K_0^{\text{cyc}}}$ for all $m \in \mathbb{N}$. Since $\mathcal{O}_{K_0}[\varepsilon(n)] = \mathcal{O}_{K_0}[\pi(n)]$ and $K_0^{\text{cyc}} = \bigcup_{n\in\mathbb{N}} \mathcal{O}_{K_0}(\varepsilon(n))$, $\mathcal{O}_{K_0^{\text{cyc}}} = \bigcup_{n\in\mathbb{N}} \mathcal{O}_{K_0}[\pi^{(n)}]$. The k-algebra $\mathcal{O}_{K_0^{\text{cyc}}} \Big/ p\mathcal{O}_{K_0^{\text{cyc}}}$ is generated by $\{\pi_n : n \in \mathbb{N}\}$ and $k \subseteq \mathcal{O}_{E_0}$, so it is enough to show that $\pi_n \in \theta(\mathcal{O}_{E_0^{\text{rad}}})$ for all $n, m \in \mathbb{N}$. But for all $s \in \mathbb{Z}$, $\pi^{p^{-s}} \in E_0^{\text{rad}} = k[[\pi]]^{\text{rad}}$ by definition, and by letting $\varepsilon^{(k)} := 0$ for $k < 0$ we see that $\pi^{p^{-s}} = \varepsilon^{p^{-s}} - 1 = (\varepsilon^{(n+s)}) - 1 = (\varepsilon^{(n+s)} - 1) = (\pi_{n+s})$ where for the last equality we assumed $n + s \geq 0$. So setting

$s = n - m$ we have $\pi_n = \varepsilon_n - 1 = \theta_m(\pi^{p^{m-n}})$ as required to complete the proof of the claim.

Now we have $E_0 \subseteq F = (E_0^{\mathrm{sep}})^H \subseteq (\operatorname{Frac} R)^H \subseteq \widehat{E_0^{\mathrm{rad}}}$. F/E_0 is Galois, in particular separable, so let $\{g_i : 1 \leq i \leq d\}$ denote the distinct E_0-embeddings of F to E_0^{sep} where $d = [F : E_0]$. We can extend these embeddings to $F^{\mathrm{rad}} = (E_0)^{\mathrm{rad}}$ by $g_i(x) := (g_i(x^{p^n}))^{p^{-n}}$ where n is such that $x^{p^n} \in F$. We can extend this map continuously to $\widehat{E_0^{\mathrm{rad}}} \to \widehat{E_0^{\mathrm{alg}}}$. But g_i acts identically on E_0, so the extended maps are still the identity on $\widehat{E_0^{\mathrm{rad}}}$, i.e. g_i is the identity. This means that $1 = d = [F : E_0]$, hence $E_0 = F = (E_0^{\mathrm{sep}})^H$, H must be the full Galois group by Theorem 1.2.10, i.e. $H \cong \mathrm{Gal}(E_0^{\mathrm{sep}}/E_0)$ to finish the proof. □

The importance of this theorem is that it reduces the theory to the known $p > 0$ characteristic case. The theorem describes the Galois group $G_{K_0^{\mathrm{cyc}}}$, but we are interested in the Galois groups over K. For this, note that from $K_0^{\mathrm{cyc}} \subseteq K_0^{\mathrm{cyc}}$, $G_{K^{\mathrm{cyc}}} \leq G_{K_0^{\mathrm{cyc}}}$ and let

$$E'_K := (E_0)^{G_{K^{\mathrm{cyc}}}}$$

be the corresponding fixed field from Theorem 1.2.10 with which E_0^{sep}/E'_K is Galois with Galois group isomorphic to. Further, define

$$E_K := (E'_K)^{\Delta_K} \tag{3.4}$$

As Δ_K is finite from Artin's theorem (Lemma 1.2.4) we know that E'_K/E_K is a Galois extension with coresponding Galois isomorphic to Δ_K. Since the extensions E'/E_0 and E'/E_K are both totally ramified, we see that

$$E_K \cong k((X)).$$

More importantly, by definition and using Theorem 1.2.10 $\Delta_K \cong G_{K_\infty} \big/ G_{K^{\mathrm{cyc}}}$ (when acting of subfields of K^{alg}), so for the absolute Galois group $\mathrm{Gal}(E_K^{\mathrm{sep}}/E_K) \cong G_{K\infty}$.

For a summary see the middle part of Figure 3.1 on page 46.

3.4 $\mathbb{F}_p$, $\mathbb{Z}_p$ and $\mathbb{Q}_p$-representations and (φ,Γ)-modules

Fix a prime number p. Let

$$B \in \Big\{\mathbb{F}_p, \qquad \mathbb{Z}_p, \qquad \mathbb{Q}_p\Big\}.$$

Recall that K is a finite extension of $\mathbb{Q}_p$. In this section we describe the Galois B-representations of K. We use the notations from the previous sections. At Theorem 3.3.4, we proved that $G_{K_\infty} = \mathrm{Gal}(K^{\mathrm{alg}}/K_\infty) \cong \mathrm{Gal}(E_K^{\mathrm{sep}}/E_K)$ for a field E_K of characteristic p. Recall that $G_{K_\infty} \leq G_K = \mathrm{Gal}(K^{\mathrm{alg}}/K)$ and $\mathbb{Z}_p \cong \mathrm{Gal}(K_\infty/K) = \Gamma_K \cong G_K \Big/ G_{K_\infty}$. Recalling Equations (2.8) and (2.7) let

$$S_K \in \Big\{E_K^{\mathrm{sep}}, \qquad \mathcal{O}_{\widehat{\mathcal{E}_{E_K}^{\mathrm{unr}}}}, \qquad \widehat{\mathcal{E}_{E_K}^{\mathrm{unr}}}\Big\}$$

corresponding to B. Let σ be the absolute Frobenius map on S_K in all cases. Further recalling the Cohen rings, let

$$T_K \in \left\{ E_K, \qquad C(E_K), \qquad \operatorname{Frac} C(E_K) \right\}$$

corresponding to B. See Remark 2.1.16 and the right side of Figure 3.1 on page 46. G_K acts on the field $\operatorname{Frac} R = \widehat{E_K^{\mathrm{sep}}}$. E_K^{sep} is stable under this action, so we can restrict the this to a G_K-action of E_K^{sep}. By the functoriality of the Cohen ring C, we see that G_K acts on S_K. We saw at Chapter 2 that $(S_K)^{\sigma} = B$, $(S_K)^{G_{K_\infty}} = T_K$. For $g \in G_K$, the restricted action $g\big|_{T_K}$ is an element of $\Gamma_K = \mathrm{Gal}(K_\infty/K)$, i.e. on T_K, G_K acts via Γ_K because G_{K_∞} fixes T_K.

Also we saw that $\mathtt{M}(V) = (S_K \otimes_B V)^{G_{K_\infty} \otimes G_{K_\infty}}$ is an étale φ-module over T_K for any B-representation V of G_K (cf. Remark 2.2.18). On $\mathtt{M}(V)$ we can define an action of Γ_K. For an element $gG_{K_\infty} \in {}^{G_K}\big/_{G_{K_\infty}} \cong \Gamma_K$ define the action as $gh \otimes gh$ for an arbitrary representative $gh \in gG_{K_\infty}$. This does not depend on the choice of h, as $\mathtt{M}(V)$ is fixed point-wise by all $h \in G_{K_\infty}$ by definition. On $\mathtt{M}(V)$ the action of Γ_K and σ commutes, because Γ_K commutes with the Frobenius σ. This motivates the following definition.

Definition 3.4.1 (Category of étale (φ,Γ)-modules over T_K)**.** A (φ,Γ)-*module over* T_K is an étale φ-module over T_K together with a continuous Γ_K-semi-linear action of Γ_K which commutes with φ.
The category of such modules is denoted by $\mathbf{M}^{\acute{e}t}_{(\varphi,\Gamma)}(T_K)$ where the objects are the (φ,Γ)-modules and the morphisms are T_K-linear maps commuting with φ and the action of Γ_K. This is an abelian category.

By above for any B-representation V, $\mathtt{M}(V)$ is an étale (φ,Γ)-modules over T_K. As before, we can define a quasi-inverse functor $\mathtt{V}$. Let $M \in \operatorname{Obj} \mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(T_K)$. As before let $\mathtt{V}(M) := (S_K \otimes_{T_K} M)^{\sigma\otimes\varphi}$ and define a G_K-action on it by $g\left(\sum_{i=1}^r \mu_i \otimes x\right) := \sum_{i=1}^r g(\mu_i) \otimes (gG_{K_\infty})(x)$ for any $g \in G_K$ where $gG_{K_\infty} \in {}^{G_K}\big/_{G_{K_\infty}} \cong \Gamma_K$. Checking the definitions shows that $\mathtt{V}(M) \in \mathbf{Rep}_B(G_K)$.

We arrived to the main theorem of this chapter.

Theorem 3.4.2. *For a finite extension K of $\mathbb{Q}_p$ the functors* $\mathtt{M}$ *and* $\mathtt{V}$ *defined above give an equivalence of the following categories that preserves the rank and the tensor product*

$$\begin{aligned}
\mathbf{Rep}_{\mathbb{F}_p}(\mathrm{Gal}(K^{\mathrm{alg}}/K)) &\sim \mathbf{M}^{\acute{e}t}_{(\varphi,\Gamma)}(E_K)\\
\mathbf{Rep}_{\mathbb{Z}_p}(\mathrm{Gal}(K^{\mathrm{alg}}/K)) &\sim \mathbf{M}^{\acute{e}t}_{(\varphi,\Gamma)}(C(E_K))\\
\mathbf{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}(K^{\mathrm{alg}}/K)) &\sim \mathbf{M}^{\acute{e}t}_{(\varphi,\Gamma)}(\operatorname{Frac} C(E_K))
\end{aligned}$$

where E_K is defined at Equation (3.4) *and the Cohen ring at Definition 2.2.10.*

Proof. This is a consequence of the above discussion and the categorical equivalences at Theorems 2.1.14, 2.2.21 and 2.3.4. □

Remark 3.4.3. $E_K \cong k_K((X))$, the formal Laurent series over the residue field k_K of K, so we could take that instead of E_K at the theorem. In particular, for $K = \mathbb{Q}_p$, we need to consider $\mathbb{F}_p((X))$.

We call $\gamma \in \Gamma_K$ *a topological generator of* Γ_K if $\langle\gamma\rangle = \{\gamma^n : n \in \mathbb{Z}\}$ is a dense subgroup of $\mathbb{Z}_p$ (with respect to the p-adic topology). Note that since $\Gamma_K \cong (\mathbb{Z}_p, +)$, any $\gamma \in \mathbb{Z}_p^\times$ is a topological generator. This means that the action of Γ_K is uniquely described by defining the action of the single element $\gamma \in \Gamma_K$. This is why we introduced the $\mathbb{Z}_p$-extension K_∞ instead of K^{cyc}, although in the latter case a similar categorical equivalence is true. Let $D \in \mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(T_K)$ and let $\{e_i : 1 \le i \le d\}$ be a T_K-basis for D. Let $\mathsf{A} := (a_{ij}), \mathsf{B} := (b_{ij}) \in \mathrm{GL}_d(T_K)$ defined by $\varphi(e_i) = \sum_{j=1}^d a_{ij}e_j$ and $\gamma(e_i) = \sum_{j=1}^d b_{ij}e_j$ for all $1 \le i \le d$. Then the fact that Γ_K commutes with φ can be simply expressed as

$$\gamma[\mathsf{A}]\mathsf{B} = \sigma[\mathsf{B}]\mathsf{A},$$

where γ is the action on T_K defined earlier. This means that a (φ,Γ)-module (and hence a B-representation of K) can be given by two matrices A and B satisfying the above criteria. We can fix a topological generator γ for all (φ,Γ)-modules, say $\gamma = 1$. Then we can describe the equivalent B-representation of G_K similarly to Theorem 2.1.15.

$$\left\{ [V] : \begin{matrix} V \in \operatorname{Obj}\mathbf{Rep}_B(G_K), \\ \dim_B V = d \end{matrix} \right\} \leftrightarrow \left\{ [(\mathsf{A},\mathsf{B})] : \begin{matrix} (\mathsf{A},\mathsf{B}) \in (\mathrm{GL}_d(T_K))^2, \\ \gamma[\mathsf{A}]\mathsf{B} = \sigma[\mathsf{B}]\mathsf{A} \end{matrix} \right\}$$

where $(A,B) \sim (A',B')$ if and only if there exists $Q \in \mathrm{GL}_d(T_K)$ such that $\sigma[Q]^{-1}AQ = A$ and $\gamma[Q]^{-1}BQ = B$.

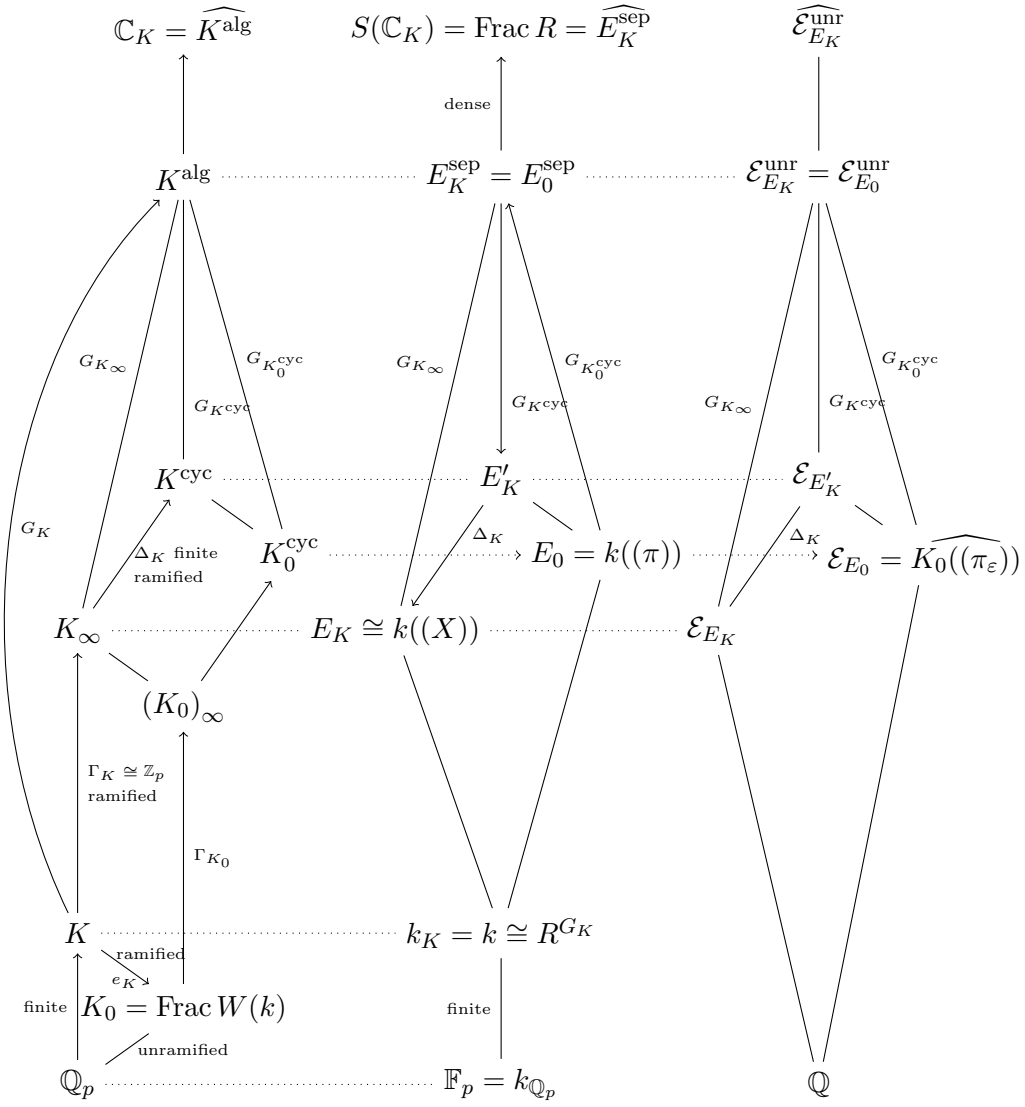


Figure 3.1: Summary of the Galois extensions of non-Archimedean fields. The arrows roughly indicate the order of the definition of the fields. Dotted lines are not field extensions, they only indicate analogies. The left side represents extensions of K which is in our main interest. The extensions at the middle are from Fontaine's fundamental theorem (Theorem 3.3.4) building a similar Galois group structure but over a fields (the residue field of K) of characteristic p. Finally the right side represents the Cohen rings constructions for the description of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ representations.

3.5 An application for determining the p-cohomological dimension

In this section, the theorem of L. Herr about cohomologcal dimension is presented from [Her98]. Let K be a finite extension of $\mathbb{Q}_p$ as in the previous section. Recall that $G_K = \mathrm{Gal}(K^{\mathrm{alg}}/K)$ and choose a topological generator γ for $\Gamma_K = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Recall $\mathcal{O}_{\mathcal{E}_{E_K}} = C(E_K)$ the Cohen ring of E_K from Equation (3.4).

Definition 3.5.1 (p-torsion representation)**.** $V \in \mathrm{Obj}\,\mathbf{Rep}_{\mathbb{Z}_p}(G_K)$ is *p-torsion*, if there exists $\exists n \in \mathbb{N}$ such that $p^n V = 0$. The subcategory of p-torsion $\mathbb{Z}_p$-representations is denoted by $\mathbf{Rep}_{\mathbb{Z}_p}^{p-tor}$.

Definition 3.5.2 (Length of a module)**.** The *length of a module* M is defined to be $\sup\{n : (\forall 0 \leq i \leq n)(\exists M_i \leq M)(\forall 0 \leq i < j \leq n)(M_i \subsetneq M_j)\}$ and M is of *finite length* if the length of M is finite.

Definition 3.5.3 (p-torsion étale (φ,Γ)-module)**.** Similarly $M \in \mathrm{Obj}\,\mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ is *p-torsion*, if M is of finite length as an $\mathcal{O}_{\mathcal{E}_E}$-module. The subcategory such modules is denoted by $\mathbf{M}^{\acute{e}t,p-tor}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$.

Theorem 3.5.4. *The functor* $\mathtt{M} : \mathbf{Rep}_{\mathbb{Z}_p}^{p-tor}(G_K) \to \mathbf{M}^{\acute{e}t,p-tor}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ *gives an equivalence of categories.*

Proof. This follows from Theorem 3.4.2. □

We now start the preparation of proving the Herr's theorem (Theorem 3.5.14) by giving the following auxiliary definition.

Definition 3.5.5 (X-lattice)**.** Let X be an indeterminate and let N be a $W((X))$-module of finite length. A finitely generated $W[[X]]$-submodule Λ of N (when regarded as a $W[[X]]$-module) is an *X-lattice* if Λ generates N as a $W((X))$-module.

Recall the field E_0 from Equation (3.3) and denote the field of fractions of the Cohen ring of E_0 by $\mathcal{E}_{E_0} := \mathrm{Frac}\, C(E_0)$. We now give its ring of integers $\mathcal{O}_{\mathcal{E}_{E_0}}$ explicitly. Recall $\varepsilon \in R$ from Equation (3.1). Let $[\varepsilon] := (\varepsilon, 0, 0, \dots) \in W(R)$ be the Teichmüller representative and let $\pi_\varepsilon := [\varepsilon] - 1 \in W(R)$. Then $\mathcal{O}_{\mathcal{E}_{E_0}} = \{\sum_{n\in\mathbb{Z}} \lambda_n \pi_\varepsilon^n : \lambda_n \in W, \lim_{n\to-\infty} = 0\}$, for details see [FO, subsection 4.3.2]. Then $\mathcal{E}_{E_0} = \widehat{K_0((\pi_\varepsilon))}$. For a graphical summary, see the right side of Figure 3.1 on page 46. Set

$$\tau := \gamma - \mathrm{Id}, \qquad \rho := \varphi - \mathrm{Id}$$

and $W := W(k) = \mathcal{O}_{K_0}$, the Witt vectors over $k = k_K$ from Definition 2.2.3.

Lemma 3.5.6. *Let* $M \in \mathbf{M}^{\acute{e}t}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_0}})$ *of finite length as an* $\mathcal{O}_{\mathcal{E}_{E_0}}$*-module. Then* M *contains a* π_ε*-lattice* Λ' *stable under* φ *and the action of* Γ_K *on which* ρ *is bijective.*

Proof. We will construct first a π_ε-lattice Λ which is stable under φ on which ρ is bijective. Then we take its closure Λ' with respect to the action of Γ_K and show that these properties remain true, i.e. that Λ' is as required.

Fix a generating system $\{e_i : 1 \leq i \leq d\}$ of M over $W((\pi_\varepsilon))$, in other words $M = \sum_{i=1}^d e_i W((\pi_\varepsilon))$ and let $(a_{ij} \in W((\pi_\varepsilon))^{d\times d}$ be defined by $\varphi(e_i) = \sum_{i=1}^d a_{ij}e_j$. Since by assumption M is of finite length, there is an $n \in \mathbb{N}$ (e.g. its length) such that M is annihilated by p^n, we may assume $n \geq 1$. Let $f_i := \pi_\varepsilon^{rp^{n-1}} e_i$ for $1 \leq i \leq d$ where $r \in \mathbb{N}$ is to be determined. We want to calculate $\varphi(f_i)$. Note that for the Frobenius σ on $\mathcal{E}_{E_0}$ we have $\sigma(\pi_\varepsilon) \equiv \pi_\varepsilon \mod p^n W((\pi_\varepsilon))$ and thus inductively $\sigma(\pi_\varepsilon^{p^{n-1}}) \equiv \pi_\varepsilon^{p^n} \mod p^n W((\pi_\varepsilon))$. So by the σ-semi-linearly of φ,

$$\varphi(f_i) = \sum_{j=1}^d \sigma(\pi_\varepsilon^{rp^{n-1}})a_{ij}e_j = \sum_{j=1}^d \pi_\varepsilon^{rp^n} a_{ij}e_j = \sum_{j=1}^d \pi_\varepsilon^{r(p-1)p^{n-1}} a_{ij}f_j$$

Since there are finitely many $a_{ij} \in W((\pi_\varepsilon))$, we can find an $s \in \mathbb{N}$ such that for all i and j, $\pi_\varepsilon^s a_{ij} \in \left(\pi_\varepsilon^{p^{n-1}} W[[\pi_\varepsilon]]\right) + p^n W((\pi_\varepsilon))$. But then choosing r in the definition of f_i such that $r(p-1)p^{n-1} \geq s$ we see that the submodule

$$\Lambda := \sum_{i=1}^d W[[\pi_\varepsilon]]f_i$$

of M (as a $W[[\pi_\varepsilon]]$-module) is stable under φ. By construction, Λ generates M as $W((\pi_\varepsilon))$-module.

Now we show that $\rho = \varphi - \mathrm{Id}$ is bijective on Λ. Pick $x := \sum_{i=1}^d x_i f_i \in \Lambda$. Note that it is enough to show that $\lim_{r\to\infty} \varphi^r(x) = 0$, because this means that the first non-zero coefficient of formal power series $\varphi^r(x) \in W[[\pi_\varepsilon]]$ grows beyond all bounds, i.e. for any $m \in \mathbb{N}$ the coefficient π_ε^m of $\varphi^r(x)$ will be non-zero for only for finitely many values of r, thus $-\sum_{r=0}^\infty \varphi^r(x)$ is meaningful and equals $(\varphi - \mathrm{Id})^{-1}(x) = \rho^{-1}(x)$. Now

$$\varphi(x) = \sum_{i=1}^d \sigma(x_i)\varphi(f_i) = \sum_{i=1}^d \sigma(x_i) \sum_{j=1}^d \pi_\varepsilon^{r(p-1)p^{n-1}} a_{ij}f_j \in \pi_\varepsilon^{p^{n-1}}\Lambda$$

and similarly $y \in \pi_\varepsilon^{tp^{n-1}}\Lambda \implies \varphi(y) \in \pi_\varepsilon^{tp^n}\varphi[\Lambda] \subseteq \pi_\varepsilon^{(1+tp)p^{n-1}}\Lambda$ for any $t \in \mathbb{N}$, hence $\lim_{r\to\infty} \varphi^r(x) = 0$.

Let $x \in \Lambda$. By definition, Γ_K acts continuously on M, so $\lim_{r\to\infty}(\gamma^{p^r}(x) - x) = 0$. Note that Λ is an open neighbourhood of $0 \in M$ since M is a $W((\pi_\varepsilon))$-module of finite length. Then there exists $t_x \in \mathbb{N}$ such that $\gamma^{p^n}(x) - x, \gamma^{p^n}(x) \in \Lambda$ for all $r \geq t_x$. Let $t := \max\{t_{f_i} : 1 \leq i \leq d\}$. Recall that $W[[\pi_\varepsilon]]$ is stable under the action of Γ_K. Then for arbitrary $y \in \Lambda$, $\gamma^{p^t}(y) \in \Lambda$, so

$$\Lambda' := \sum_{i=0}^{p^t-1} \gamma^i[\Lambda]$$

is stable under Γ_K. Moreover, Λ' is also a π_ε-lattice because it is finitely generated, and Λ' is stable under φ. Also $\lim_{r\to\infty} \varphi^r(x) = 0$ remains true for $x \in \Lambda'$ so by a similar argument, ρ is bijective on Λ'. □

Corollary 3.5.7. *For all $x \in M \in \mathbf{M}^{\acute{e}t}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_0}})$ there exists $r \in \mathbb{N}$ and $t_0 \in M$ such that $\tau^r(x) = \rho(t_0)$.*

Proof. $\lim_{r\to\infty} \tau^r(x) = 0$ from continuity of the action of Γ_K on M. Let Λ' be the π_ε-lattice provided by the previous lemma. Then Λ' is an open neighbourhood of $0 \in M$ on which ρ is a invertible. So for some $r \in \mathbb{N}$, $\tau^r(x) \in \Lambda'$ whose image under ρ^{-1} is say, t_0, thus $\tau^r(x) = \rho(t_0)$, as stated. □

Proposition 3.5.8. *For all $M \in \mathbf{M}^{\acute{e}t,p-tor}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ and for all $y \in M$, there exists $N_y \in \mathbf{M}^{\acute{e}t,p-tor}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ into which M can be embedded and $\exists x \in N_y$ such that $y = \rho(x)$.*

Proof. $\mathcal{O}_{\mathcal{E}_{E_K}}$ is a finitely generated $\mathcal{O}_{\mathcal{E}_{E_0}}$-module and $\Gamma_{K_0} := \mathrm{Gal}((K_0)_\infty/K_0) \leq \Gamma_K$. So we can consider M as an element of $\mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_0}})$.

We construct N_y and x explicitly. Let $r \in \mathbb{N}$ and $t_0 \in M$ be provided by the previous corollary, so $\tau^r(x) = \rho(t_0) = \varphi(t_0) - t_0$. If $r = 0$, then $N_y := M$, $x := t_0$ and we are done.

Suppose $r \geq 1$. Let $n \in \mathbb{N}$ be such that $p^n M = 0$, which exists by the definition of p-torsion. For indeterminates t_i let

$$N_y := M \oplus \sum_{i=1}^{r} \left(\mathcal{O}_{\mathcal{E}_{E_K}} \Big/ p^n \mathcal{O}_{\mathcal{E}_{E_K}} \right) t_i$$

be the direct sum of M and a free $\mathcal{O}_{\mathcal{E}_{E_K}} \Big/ p^n \mathcal{O}_{\mathcal{E}_{E_K}}$-module of rank r. N_y is annihilated by p^n. Define the action φ and γ by

$$\varphi(t_i) := t_i + \tau^{r-i}(y), \qquad \gamma(t_i) := t_i + t_{i-1}$$

for $1 \leq i \leq r$ and extend these maps semi-linearly together with the original maps on M. Note that by the choice of t_0, the equation of φ is satisfied for $i = 0$ as well. Using this with $0 \leq i \leq r$ and the equation for γ with $1 \leq i \leq r$ we see that

$$\begin{aligned}\varphi(\gamma(t_i)) &= \varphi(t_i + t_{i-1}) = \varphi(t_i) + (t_{i-1}) = \left(t_i + \tau^{r-i}(y)\right) + \left(t_{i-1} + \tau^{r-i+1}(y)\right) \\ &= (t_i + t_{i-1}) + (\mathrm{Id} + \tau) \circ (\tau^{r-i})(y) = \gamma(t_i) + \gamma(\tau^{r-i}(y)) = \gamma(t_i + \tau^{r-i}(y)) \\ &= \gamma(\varphi(t_i))\end{aligned}$$

for $1 \leq i \leq r$. From the semi-linearity of φ and γ, we see that

$$\begin{aligned}\varphi\left(\gamma\left(z + \sum_{i=1}^{r} \lambda_i t_i\right)\right) &= \varphi(\gamma(z)) + \sum_{i=1}^{r} \sigma(\gamma(\lambda_i)\varphi(\gamma(t_i)) = \gamma(\varphi(z)) + \sum_{i=1}^{r} \gamma(\sigma(\lambda_i)\gamma(\varphi(t_i)) \\ &= \gamma\left(\varphi\left(z + \sum_{i=1}^{r} \lambda_i t_i\right)\right)\end{aligned}$$

for an arbitrary element $z + \sum_{i=1}^{r} \lambda_i t_i \in N_y$, because the φ and γ commute on M moreover σ and γ commute on $\mathcal{O}_{\mathcal{E}_{E_K}}$. Then $N_y \in \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ and $M \subseteq N_y$. Finally note that for $x := t_r$, $\varphi(x) = x + \tau^0(x)$ by definition of the action φ, so $\rho(x) = y$. □

Definition 3.5.9 (Effaceable functor)**.** A functor $\mathtt{F} : \mathcal{C} \to \mathcal{C}'$ between abelian categories is *effaceable* if for all $M \in \mathrm{Obj}(\mathcal{C})$ and for all $x \in \mathtt{F}(M)$ there is a monomorphism $u : M \to N$ in $\mathcal{C}$ such that $\mathtt{F}(u)(x) = 0 \in \mathtt{F}(N)$.

Definition 3.5.10 (δ-functor)**.** Let $\mathcal{C}$ and $\mathcal{C}'$ be abelian categories. A *δ-functor* from $\mathcal{C}$ to $\mathcal{C}'$ is a collection of functors $(\mathtt{T}^n : \mathcal{C} \to \mathcal{C}')_{n\in\mathbb{N}}$ with morphisms $\delta^n : \mathtt{T}^n(A'') \to \mathtt{T}^{n+1}(A')$ for each exact sequence $0 \to A' \to A \to A'' \to 0$ in $\mathcal{C}$ such that

$$0 \to \mathtt{T}^0(A') \to \mathtt{T}^0(A) \to \mathtt{T}^0(A'') \xrightarrow{\delta^0} \mathtt{T}^1(A') \to \mathtt{T}^1(A) \to \mathtt{T}^1(A'') \xrightarrow{\delta^1} \mathtt{T}^1(A') \to \dots$$

is exact and for every morphism of the above short exact sequence to the short exact sequence $0 \to B' \to B \to B'' \to 0$ the following diagram is commutative.

$$\begin{array}{ccc} \mathtt{T}^n(A'') & \xrightarrow{\delta^n} & \mathtt{T}^{n+1}(A') \\ \downarrow & & \downarrow \\ \mathtt{T}^n(B'') & \xrightarrow{\delta^n} & \mathtt{T}^{n+1}(B') \end{array}$$

Proposition 3.5.11 (Grothendieck)**.** *Let $\mathcal{C}$ and $\mathcal{C}'$ be abelian categories with $\mathcal{C}$ having enough injectives. Let $(\mathtt{T}^n)_{n\in\mathbb{N}}$ be a δ-functor from $\mathcal{C}$ to $\mathcal{C}'$ such that $\mathtt{T}^n$ is effaceable for every $n > 0$. Then $\mathtt{T}^0$ is left exact and $\mathtt{T}^n$ is isomorphic to the nth right derived functor $R^n\,\mathtt{T}^0$ of $\mathtt{T}^0$ for all $n \in \mathbb{N}$.*

Proof. This is Theorem 1.3A and Corollary 1.4 from [Har77, p. 206]. The proof is based on Grothendieck's Tôhoku paper and the notion of universal δ-functors. □

We want to use Proposition 3.5.11 but the problem is that $\mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ does not have enough injectives. So instead, let us consider the category

$$\varinjlim \mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$$

whose objects are injective limits of objects of $\mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$. This category has enough injectives and it is abelian.

Definition 3.5.12 (Herr-complex)**.** For $M \in \varinjlim \mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$, let

$$C_{(\varphi,\Gamma)}(M) : 0 \to M \xrightarrow{f_0 : x \mapsto (\rho(x), \tau(x))} M \oplus M \xrightarrow{f_1 : (y,z) \mapsto \tau(y) - \rho(z)} M \to 0 \to 0 \to \dots$$

be the *Herr-complex* whose second term, i.e. M, has index 0. Since φ and γ commute on $\mathtt{M}$, so do ρ and τ, thus indeed $f_2 \circ f_1 = 0$. Denote the nth homology by $\mathtt{H}^n(M)$. Then $(\mathtt{H}^n)_{n\in\mathbb{N}}$ is a δ-functor (with the connecting δ-morphisms provided by the Snake Lemma) from $\varinjlim \mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ to the category of abelian groups.

Lemma 3.5.13. *$\mathtt{H}^n$ is effaceable for $n > 0$.*

Proof. We prove the statement using Proposition 3.5.8.

Let $n = 1$ and consider $\mathtt{H}^1$. Pick an arbitrary $M \in \varinjlim \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ and pick $y, z \in M$ such that

$$\tau(y) = \rho(z) \tag{3.5}$$

i.e. $(y, z) \in \ker f_1$. Then by definition, $M = \varinjlim_{i\in I} M_i$ for some $M_i \in \mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ for $i \in I$, and $y = ([y_i])_{i\in I}$ where $y_i \in M_i$. By Proposition 3.5.8, we have $x_i \in N_{y,i} \in \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ with $M_i \subseteq N_{y,i}$ such that $y_i = \rho(x_i)$ for each $\forall i \in I$. Then let $N_y := \varinjlim_{i\in U} N_{y,i} \in \varinjlim \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ and $x := ([x])_{i\in I} \in N_y$. Now by construction, $M \subseteq N_y \ni x$ and

$$\rho(x) = y. \tag{3.6}$$

Both M and N_y are of finite length by definition, so they are annihilated by a power of p, so let $s \in \mathbb{N}$ be such that $p^s x = p^s z = 0$. Similarly to the proof Proposition 3.5.8, let

$$N_{(y,z)} := N_y \oplus \left(\mathcal{O}_{\mathcal{E}_{E_K}} \Big/ p^s \mathcal{O}_{\mathcal{E}_{E_K}}\right) v$$

be the direct sum of N_y and a free $\mathcal{O}_{\mathcal{E}_{E_K}} \Big/ p^s \mathcal{O}_{\mathcal{E}_{E_K}}$-module of rank 1 generated by v. Denote the natural embedding by $u : M \hookrightarrow N_{(y,z)}$. Define an action of φ and γ on $N_{(y,z)}$ by letting

$$\varphi(v) := v, \qquad \gamma(v) := v + \tau(u(x)) - u(z).$$

Then by Equations (3.5) and (3.6) we see that

$$\begin{aligned}
\varphi(\gamma(v)) &= v + \varphi(\tau(u(x))) - \varphi(u(z)) = v + \tau(\varphi(u(x))) - \varphi(u(z)) \\
&\overset{(3.6)}{=} v + \tau(u(x) + u(y)) - \varphi(u(z)) \overset{(3.5)}{=} v + \tau(u(x)) + \rho(u(z)) - \varphi(u(z)) \\
&= v + \tau(u(x)) - u(z) = \gamma(v) = \gamma(\varphi(v)).
\end{aligned}$$

The semi-linearly extended action of φ and Γ commute on $N_{(y,z)}$. This shows that $N_{(y,z)} \in \varinjlim \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$. Note that $\rho(u(x)-v) = \rho(u(x))-\rho(v) \overset{(3.6)}{=} u(y)-0 = u(y)$ and that $\tau(u(x)-v) = \tau(u(x))-\tau(v) = \tau(u(x))-(\tau(u(x))-u(z)) = u(z)$. This means that $f_{1,N_{(y,z)}}((u(x)-v)) = (u(y), u(z))$, so

$$\mathtt{H}^1(u)((y, z) + \operatorname{Im} f_{1,M}) = (u(y), u(z)) + \operatorname{Im} f_{1,N_{(y,z)}} = \operatorname{Im} f_{1,N_{(y,z)}}.$$

To summarise, we have shown that for an arbitrary $(y, z) + \operatorname{Im} f_0 \in \mathtt{H}^1(M)$ there is a monomorphism $u : M \to N_{(y,z)}$ in $\varinjlim \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ such that $\mathtt{H}^1(u)((y, z)+\operatorname{Im} f_0) = 0 \in \mathtt{H}^1(N_{(y,z)})$, i.e. that $\mathtt{H}^1$ is effaceable.

Now let $n = 2$, we want to show that the functor $\mathtt{H}^2$ is effaceable. Pick an arbitrary $y \in M \in \varinjlim \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ arbitrarily. In a manner similarly to the case $n = 1$, Proposition 3.5.8 implies that M embeds into $N_y \in \varinjlim \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$, and there is an $x \in N_y$ such that $y = \rho(x)$. Identify M via the embedding. Now $f_1((0, -x)) = \tau(0)-\rho(-x) = -x-\varphi(x) = -x+\sigma(-1)\varphi(x) = \varphi(x)-x = \rho(x) = y$ since the Frobenius

σ takes -1 to 1 in any characteristic. This shows that $y \in \operatorname{Im} f_1$, hence $\mathtt{H}^2$ is effaceable as at the $n = 1$ case.

$\mathtt{H}^n$ is effaceable for $n > 2$ because the occurring objects are trivial. □

Now we are ready to prove the theorem of Herr ([Her98, Théorème A]).

Theorem 3.5.14 (Herr)**.** *For any representation $V \in \mathbf{Rep}_{\mathbb{Z}_p}^{p-tor}(G_K)$, the cohomology group $H^n(G_K, V)$ is trivial for $n > 2$.*

Proof. Note by Theorem 3.5.4, $\mathtt{M}(V) \in \mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$. Note that this is a subcategory of $\varinjlim \mathbf{M}^{\text{ét}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ in the natural way so we can talk about the complex $C_{(\varphi,\Gamma)}(\mathtt{M}(V))$. From Lemma 3.5.13, we know that the homologies $\mathtt{H}^n$ of the complex $C_{(\varphi,\Gamma)}(\mathtt{M}(V))$ are effaceable for $n > 0$. Then by Proposition 3.5.11, $\mathtt{H}^n$ is isomorphic to $R^n\,\mathtt{H}^0$ for all $n \in \mathbb{N}$. Let $\mathtt{F}(V) := V^{G_K}$ as in Definition 1.6.2. Note that using the categorical equivalence of Theorem 3.5.4, the functor $\mathtt{F}$ acts on the category $\varinjlim \mathbf{M}^{\text{ét},p-\text{tor}}_{(\varphi,\Gamma)}(\mathcal{O}_{\mathcal{E}_{E_K}})$ as $\mathtt{M}(V) \mapsto \mathtt{M}(V)^{\{\varphi,\gamma\}} := \{x \in \mathtt{M}(V) : x = \varphi(x) = \gamma(x)\} = \ker f_0 = H^0(G_K, V)$. This means that $\mathtt{H}^0 \cong \mathtt{F}$, so taking the right derived functors, we still get isomorphic functors: $H^n = R^n\,\mathtt{F} \cong R^n\,\mathtt{H}^0 \cong \mathtt{H}^n$. But by definition of $C_{(\varphi,\Gamma)}(\mathtt{M}(V))$, we see that $\mathtt{H}^n = 0$ for $n > 2$ hence the statement holds. □

Remark 3.5.15. Note that the statement does not use the theory of (φ, Γ)-modules, but our proof heavily relied on this theory. Furthermore, it is clear from the proof that the homologies are determined by the Herr-complex and they can be calculated.

The *p-cohomological dimension of K* is defined to be the smallest $d \in \mathbb{N}$ such that $H^n(G_K, V) = 0$ for all p-torsion representation V and for all $n > d$. If no such d exists, then it is ∞. The theorem of Herr in fact implies that the p-cohomological dimension of any finite extension K of $\mathbb{Q}_p$ is at most 2. This is known to be true in a more general setup due to K. Morita.

Theorem 3.5.16 (Morita)**.** *Let K be a complete discrete valuation field of characteristic 0 with residue field k of characteristic $p > 0$. Assume further that $[k : k^p] = p^n < \infty$ and that K contains a primitive pth root of unity if $p \neq 2$ and a primitive 4th root of unity if $p = 2$. Then the p-cohomological dimension of K is exactly $n + 2$.*

Proof. See [Mor08]. The proof uses the theory of (φ, Γ)-modules with the same techniques as the presented proof of Herr's theorem, but now the complex $C_{(\varphi,\Gamma)}(M)$ is of length $n + 2$. □

Remark 3.5.17. When $K/\mathbb{Q}_p$ is a finite extension, then k_K is a finite extension of $k_{\mathbb{Q}_p} = \mathbb{F}_p$, so $k = k_K$ is a finite field, in particular perfect. In this case $k = k^p$, so $n = 0$ from the theorem and we get back Herr's theorem.

Bibliography

[Ati69] Michael Atiyah. *Introduction to commutative algebra*. Addison-Wesley, 1969. ISBN: 0201407515.

[Ber10] Grégory Berhuy. *An introduction to Galois cohomology and its applications*. Cambridge, UK: Cambridge University Press, 2010. ISBN: 9780521738668.

[Böc08] Gebhard Böckle. *p-adic Galois representations of G_E with* char $E = p > 0$ *and the ring R*. 2008. URL: `http://math.uni.lu/~wiese/pAdicGR/Boeckle.pdf` (visited on 05/25/2015).

[Fon90] Jean-Marc Fontaine. "Représentations p-adiques des corps locaux (1ère partie)". French. In: *The Grothendieck Festschrift*. Ed. by Pierre Cartier et al. Modern Birkhäuser Classics. Birkhäuser Boston, 1990, pp. 249–309. ISBN: 978-0-8176-4567-0. DOI: `10.1007/978-0-8176-4575-5_6`. URL: `http://dx.doi.org/10.1007/978-0-8176-4575-5_6` (visited on 05/25/2015).

[FO] Jean-Marc Fontaine and Yi Ouyang. *Theory of p-adic Galois Representations*. URL: `http://www.math.u-psud.fr/~fontaine/galoisrep.pdf` (visited on 05/25/2015).

[Har77] Robin Hartshorne. *Algebraic geometry*. New York: Springer-Verlag, 1977. ISBN: 0-387-90244-9.

[Haz09] Michiel Hazewinkel. *Handbook of Algebra*. Vol. 6. North Holland, 2009. ISBN: 9780444532572.

[Her98] Laurent Herr. "Sur la cohomologie galoisienne des corps p-adiques". French. In: *Bulletin de la Société mathématique de France* 126.4 (1998), pp. 563–600. URL: `http://smf4.emath.fr/Publications/Bulletin/126/pdf/smf_bull_126_563-600.pdf` (visited on 05/25/2015).

[Mat80] Hideyuki Matsumura. *Commutative algebra*. Benjamin/Cummings, 1980. ISBN: 0-8053-7026-9.

[Mil13] James S. Milne. *Class Field Theory (v4.02)*. 2013. URL: `http://www.jmilne.org/math/CourseNotes/CFT.pdf` (visited on 05/25/2015).

[Mil14] James S. Milne. *Fields and Galois Theory (v4.50)*. 2014. URL: `http://www.jmilne.org/math/CourseNotes/FT.pdf` (visited on 05/25/2015).

[Mor08] Kazuma Morita. "Galois cohomology of a p-adic field via (φ, Γ)-modules in the imperfect residue field case". In: *J. Math. Sci. Univ. Tokyo* 15.2 (2008), pp. 219–241. URL: http://www.ms.u-tokyo.ac.jp/journal/pdf/jms150202.pdf (visited on 05/25/2015).

[Mor13] Maxim Mornev. *Flat and étale morphisms*. 2013. URL: http://pub.math.leidenuniv.nl/~jinj/2013/efg/flatetale.pdf (visited on 05/25/2015).

[Sch07] Peter Schneider. *Die Theorie des Anstieges*. German. 2007. URL: http://wwwmath.uni-muenster.de/u/pschnei/publ/lectnotes/Theorie-des-Anstiegs.pdf (visited on 05/25/2015).

[Záb14] Gergely Zábrádi. *Algebrai számelmélet jegyzet*. Hungarian. 2014. URL: http://www.cs.elte.hu/~zger/Jegyzetek/algszamjegyzet.pdf (visited on 05/25/2015).