On the cohomological coprimality of Galois representations

ディマバヤオ, ジェローム トマガン

https://doi.org/10.15017/1500518

出版情報：九州大学, 2014, 博士（数理学）, 課程博士
バージョン：

On the cohomological coprimality of Galois representations

Jerome T. Dimabayao

A dissertation submitted to
Kyushu University
for the degree of
Doctor of Mathematics
February 2015

To my mother Salve and my love Issa.

Introduction

The vanishing of cohomology groups associated with p-adic Galois representations defined by elliptic curves is one of the useful results towards generalization of methods in Iwasawa theory to larger Galois extensions. Such vanishing enables the computation of Euler characteristics for discrete modules associated to p-adic Galois representations ([CSW01], [CS99]) and Selmer groups of elliptic curves over extensions containing all p-power roots of unity ([CH01], [CSS03]).

Let R be a topological commutative ring with unity and V be a topological R-module. Let G be a closed subgroup of the group $\mathrm{Aut}_R(V)$ of topological R-automorphisms of V endowed with the compact-open topology. We consider the continuous cohomology groups $H^m(G, V)$ of G with coefficients in V defined by continuous cochains.

Definition 1. We say that V has *vanishing G-cohomology* if the cohomology groups $H^m(G, V)$ are trivial for all $m = 0, 1, \ldots$.

Let p be a prime number. In [CSW01], Coates, Sujatha and Wintenberger computed the Euler characteristic of the discrete module associated to the p-adic representation of a p-adic field K given by the étale cohomology group of a proper smooth variety with potential good reduction over K. In order to do this, they proved the following

Theorem 2 ([CSW01], Theorems 1.1 and 1.5)**.** *Let X be a proper smooth variety defined over K with potential good reduction. Let $i \geq 0$ be an integer. Put $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ and consider the Galois representation $\rho : G_K \to \mathrm{GL}(V)$. Denote by $K(\mu_{p^\infty})$ the field extension of K obtained by adjoining to K all roots of unity whose order is a power of p. Let $G_V = \rho(G_K)$ and $H_V = \rho(G_{K(\mu_{p^\infty})})$. Then:*
(1) if i is nonzero, then V has vanishing G_V-cohomology;
(2) if i is odd, then V has vanishing H_V-cohomology.

In the above theorem, let $K(V)$ be the fixed subfield of $\overline{K}$ by the kernel of ρ. Observe that we may identify G_V with the Galois group $\mathrm{Gal}(K(V)/K)$. Similarly, H_V may be identified with $\mathrm{Gal}(K(V)/K(V) \cap K(\mu_{p^\infty}))$.

A result similar to Theorem 2 holds in the case where the variety X is defined over a number field.

Theorem 3 ([Su00], Theorem 2.7)**.** *Let X be a proper smooth variety over a number field F. Let p be a prime and $i \geq 0$ an integer. Put $V = H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_p)$ and consider the Galois representation $\rho : G_F \to \mathrm{GL}(V)$. Denote by $F(\mu_{p^\infty})$ the field extension of F obtained by adjoining to F all roots of unity whose order is a power of p. Let $G_V = \rho(G_F)$ and $H_V = \rho(G_{F(\mu_{p^\infty})})$. Then:*
(1) if i is nonzero, then V has vanishing G_V-cohomology;
(2) if i is odd, then V has vanishing H_V-cohomology.

These results provide a vast generalization of the following theorem due to Imai.

Theorem 4 ([Im75], Theorem 1)**.** *Let A be an abelian variety over a p-adic field K with potential good reduction and consider the representation $V = V_p(A)$ of G_K given by the Tate module of A. Then the group $A(K(\mu_{p^\infty}))[p^\infty]$ is finite.*

For a p-adic Galois representation V as in Theorems 2 and 3, let T be a $\mathbb{Z}_p$-lattice which is stable by the Galois action. To see why Theorem 4 follows from Theorem 2, we just note that the vanishing of $H^0(J_V, V)$ is equivalent to the finiteness of $H^0(J_V, V/T)$ via the following

Lemma 5 (cf. e.g. [KT13], Lemma 2.1)**.** *Let G be a group, $\psi : G \to \mathrm{GL}_{\mathbb{Q}_p}(V)$ be a $\mathbb{Q}_p$-linear representation of G, and T a G-stable $\mathbb{Z}_p$-lattice in V. Then the following conditions are equivalent:*

(i) $H^0(G, V) = 0$;

(ii) $H^0(G, V/T)$ *is a finite group.*

Our interest is to generalize Theorems 2 and 3. More precisely, we want to find the answer to the following

Problem 1. *Consider a Galois extension L of K (resp. F) and put $J_V = \rho(G_L)$. When does the representation V have vanishing J_V-cohomology?*

From the proof of Theorem 2, we may obtain a simple criterion that gives a partial answer to the above problem:

Theorem 6 (Theorem 7.2.7; [Di14-1], Theorem 1.2)**.** *Let X be a proper smooth variety over a p-adic field K with potential good reduction and i a positive odd integer. Put $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ and $K_{\infty,V} := K(V) \cap K(\mu_{p^\infty})$.*

Let L/K be any p-adic Lie extension such that $K(\mu_{p^\infty})$ is of finite degree over $K_{\infty,L} := L \cap K(\mu_{p^\infty})$. Assume that the Lie algebras

$$\mathrm{Lie}(\mathrm{Gal}(K(V)/K_{\infty,V})) \textit{ and } \mathrm{Lie}(\mathrm{Gal}(L/K_{\infty,L}))$$

have no common simple factor. Then V has vanishing J_V-cohomology, where $J_V = \rho(G_L)$.

For example, the above criterion implies the following vanishing result:

Corollary 7 (Theorem 7.2.17; [Di14-1], Theorem 4.8)**.** *Let X be a proper smooth variety over a p-adic field K with potential good ordinary reduction and let E/K be an elliptic curve with potential good supersingular reduction. Let i be a positive odd integer and we put $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ and $V' = V_p(E)$. We denote by ρ and ρ' the continuous homomorphisms giving the action of G_K on V and V' respectively. Then*
(i) if $L = K(V')$ and $J_V = \rho(G_L)$, then V has vanishing J_V-cohomology; and
(ii) if $L' = K(V)$ and $J_{V'} = \rho'(G_{L'})$, then V' has vanishing $J_{V'}$-cohomology.

The above corollary suggests another related problem. Suppose we take representations $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ and $V' = H^j_{\text{ét}}(Y_{\overline{K}}, \mathbb{Q}_p)$ as in Theorem 2 (or Theorem 3) and we take $L = K(V')$. Then does it follow in general that if X and Y are "different", then V has vanishing J_V-cohomology? Of course, this statement is vague because there is no general way to define the "difference" between general proper smooth varieties. As we will see later (see Chapter 2), in many situations where we can describe this "difference" we may obtain the vanishing of cohomology.

In some cases it is already helpful to determine whether the group $H^0(J_V, V)$ vanishes or not. Establishing the finiteness of $H^0(J_V, V/T)$ where J_V is given by an arbitrary p-adic Lie extension allows us to weaken hypotheses of many theorems in the Iwasawa theory of elliptic curves (cf. [KT13], Section 6). Let us recall some known related results. For the moment, we concentrate on the case where the base field is a p-adic field K. In [Oz09], Ozeki considered the case when the field L is obtained by adjoining to K the coordinates of p-power torsion points of an abelian variety. Suppose A/K is an abelian variety with potential good *ordinary* reduction and consider the representation $V = V_p(A)$ given by the Tate module of A. In this case Ozeki determined, under suitable conditions, a necessary and sufficient condition for the vanishing of $H^0(J_V, V)$. Let L be a Galois extension of K. Following *op. cit.*, we say that the residue field k_L of L is a *potential prime-to-p extension* if the p-part of the degree of k_L over k is finite. Then we have the following result:

Theorem 8 ([Oz09], Theorem 1.1 (2))**.** *Suppose A is an abelian variety with good ordinary reduction over K. Let L be a Galois extension of K with residue field k_L. Assume that L contains $K(\mu_{p^\infty})$ and the coordinates of the p-torsion points of A. Then $H^0(J_V, V)$ vanishes if and only if k_L is a potential prime-to-p extension of k.*

It turns out that the statement of the above theorem can be extended to include the vanishing of the higher-dimensional cohomology groups.

Theorem 9 (Corollary 7.2.15)**.** *Suppose A is an abelian variety with good ordinary reduction over K. Let L be a Galois extension of K with residue field k_L. Assume that L contains $K(\mu_{p^\infty})$ and the coordinates of the p-torsion points of A. Then V has vanishing J_V-cohomology if and only if k_L is a potential prime-to-p extension of k.*

Consider the case where $V = V_p(E)$ is given by an elliptic curve E/K with potential good reduction and $L = K(E'_{p^\infty})$ is the field extension obtained by adjoining to K the coordinates of p-power torsion points of another elliptic curve E'/K. By distinguishing the reduction types of E and E', Ozeki further proved the following

Theorem 10 ([Oz09], Theorem 1.2)**.** *The group $H^0(J_V, V)$ vanishes in the following cases:*

E	E'
ordinary	*supersingular*
	multiplicative
supersingular with FCM	*ordinary*
	*supersingular with FCM**
	supersingular without FCM
	multiplicative
supersingular without FCM	*ordinary*
	supersingular with FCM
	*supersingular without FCM**
	multiplicative

In the table above, FCM means formal complex multiplication (see Chapter 1 for the definition) and * means that the vanishing holds under some suitable condition as in Theorem 2.3 of Chapter 2.

In [KT13], Kubo and Taguchi studied the vanishing of $H^0(J_V, V)$ in the general setting where K is a complete discrete valuation field of mixed characteristic $(0, p)$. This includes the possibility that the residue field k of K is imperfect. For this setting, let M be the extension obtained by adjoining all p-power roots of all elements of $K^\times$.

Theorem 11 ([KT13], Theorem 1.2 (i))**.** *Let K be a complete discrete valuation field of mixed characteristic $(0,p)$. Assume X is a proper smooth variety over K with potential good reduction and i an odd integer ≥ 1. Put $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$. Then the group $H^0(J_V, V)$ vanishes for any subfield L of M.*

Although we were not able to do so in this thesis, it seems possible that Theorem 2 can be extended in this general setting.

The above theorem is just the p-part of the main result of Kubo and Taguchi. In fact, they also considered the ℓ-adic cohomologies (cf. *op.cit.* Theorem 1.2 (ii)). With the notation and hypothesis in the theorem above, assume in addition that the residue field k of K is an algebraic extension of finite separable degree over a purely transcendental extension of a prime field (*essentially of finite type* in the language of [KT13]). Let $\ell \neq p$ be a prime. Then they proved that for the $\mathbb{Q}_\ell$-vector space $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell)$, the group of G_L-fixed points $H^0(G_L, V)$ vanishes for any subfield L of M.

As observed in Corollary 7 and Theorems 8 and 10, we may consider Problem 1 with L taken to be a field extension of K which corresponds to the kernel of another representation V' of G_K. The problem in this scenario becomes symmetric as we may ask the same question to the representation V' and the field extension L' corresponding to the kernel of V. As such, the problem in this case becomes a problem of comparison, or "independence", between the representations V and V' from which we can derive some cohomological results. There can be several notions of "independence", the simplest being non-isomorphism. Another notion is the "independence" among representations in a given system of representations of a profinite group which was studied by Serre [Se13] (also see Chapter 6). In view of the above discussion we propose another notion of "independence" between representations.

Definition 12. Let G be a topological group and R and R' be topological rings. Let $\rho : G \to \mathrm{GL}_R(V)$ and $\rho' : G \to \mathrm{GL}_{R'}(V')$ be two continuous linear representations of G on a topological R-module V and a topological R'-module V', respectively. Put $\mathcal{G} = \rho(\operatorname{Ker}\rho')$ and $\mathcal{G}' = \rho'(\operatorname{Ker}\rho)$. We say that V and V' are *cohomologically coprime* if V has vanishing $\mathcal{G}$-cohomology and V' has vanishing $\mathcal{G}'$-cohomology.

Note that when $G = G_K$ is the absolute Galois group of a field K in the above definition, we have $\rho(\operatorname{Ker}\rho') = \rho(G_{K(V')}) \simeq \operatorname{Gal}(K(V)/K(V) \cap K(V'))$, and similarly $\rho'(\operatorname{Ker}\rho) = \rho'(G_{K(V)}) \simeq \operatorname{Gal}(K(V')/K(V) \cap K(V'))$. In view of the above definition, we have the following special case of Problem 1.

Problem 2. *Let G be the absolute Galois group of a p-adic field or a number field. Given continuous representations V and V' of G, when are V and V' cohomologically coprime?*

Using some (partial) answers to Problem 1 for the vanishing of cohomology groups, we may obtain partial answers to Problem 2 for some representations of G as above coming from geometry. For instance we see from Corollary 7 that the representations $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ and $V_p(E)$ of a p-adic field K are cohomologically coprime, for a proper smooth variety X/K with potential good ordinary reduction, a positive odd integer i and an elliptic curve E/K with potential good supersingular reduction.

Like Theorem 8, Theorem 10 can be extended to include the vanishing of higher-dimensional cohomology groups when both elliptic curves have potential good reduction. We state this in terms of cohomological coprimality.

Theorem 13 (Theorem 2.3; [Di14-1], Theorem 5.1)**.** *Let E and E' be elliptic curves with potential good reduction over a p-adic field K. Then $V_p(E)$ and $V_p(E')$ are cohomologically coprime in the following cases:*

E	E'
ordinary	supersingular
supersingular with FCM	ordinary
	supersingular with FCM*
	supersingular without FCM
supersingular without FCM	ordinary
	supersingular with FCM
	supersingular without FCM*

Here, "FCM" and * have the same meaning as those in Theorem 10.

In the global setting, we can say more. From the results on almost independence of systems of representations of a number field, we may extend Theorem 3 to systems of representations associated with a proper smooth variety over a number field indexed by a set of primes. This extension allows us to prove the following result.

Theorem 14 (Theorem 7.3.3)**.** *Let S and S' be sets of primes. Let X and X' be proper smooth varieties over a number field F and i, i' be positive integers. Put $V_S = \bigoplus_{\ell \in S} H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_\ell)$ and $V'_{S'} = \bigoplus_{\ell \in S'} H^{i'}_{\text{ét}}(X'_{\overline{F}}, \mathbb{Q}_\ell)$. If $S \cap S' = \emptyset$, then V_S and $V'_{S'}$ are cohomologically coprime.*

Interestingly, if we concentrate on the case of elliptic curves over a number field, we see that non-existence of isogeny implies the cohomological coprimality of the associated Galois representations. This is furnished by the following theorem.

Theorem 15 (Theorem 2.5; [Di14-2], Theorem 1.3)**.** *Let S and S' be sets of primes. Let E and E' be elliptic curves over a number field F. Put $V_S = \bigoplus_{\ell\in S} V_\ell(E)$ and $V'_{S'} = \bigoplus_{\ell\in S'} V_\ell(E')$ Assume that E and E' are not isogenous over $\overline{F}$. Then V_S and $V'_{S'}$ are cohomologically coprime.*

This implies the following corollary, which in some way is reminiscent of the Isogeny Theorem for elliptic curves (see Chapter 2).

Corollary 16 (Corollary 2.6; [Di14-2], Corollary 1.4)**.** *Let E and E' be elliptic curves over a number field F. The following statements are equivalent:*
(i) E and E' are not isogenous over $\overline{F}$;
(ii) $V_S|_{G_{F'}}$ and $V'_{S'}|_{G_{F'}}$ are cohomologically coprime for any S and S' and for every finite extension F' of F;
(iii) $V_\ell(E)|_{G_{F'}}$ and $V_\ell(E')|_{G_{F'}}$ are cohomologically coprime for some prime number ℓ and for every finite extension F' of F.

We now describe the organization of this thesis. We first define the notations and recall some terminologies which are used in this thesis in Chapter 1. In Chapter 2 we list our results regarding the cohomological coprimality of Galois representations over a p-adic field and over a number field. We recall the definitions of the cohomology of profinite groups and Lie algebras in Chapter 3. In Chapter 4, we give a background on p-adic Hodge theory. We discuss the main ideas and recall some important results which are used for the proof of Theorems 2 and 3. Since Theorems 2 and 3 are essential for the proof of our results, we give an exposition of their proofs in Chapter 5 as given by Coates, Sujatha and Wintenberger in [CSW01] and by Sujatha in [Su00], respectively. The proofs for the vanishing G_V-cohomology (and H_V-cohomology) follow the same line of thought. Using a theorem of Lazard, we identify the cohomology group $H^r(G_V, V)$ with a $\mathbb{Q}_p$-vector subspace of the Lie algebra cohomology group $H^r(\mathrm{Lie}(G_V), V)$ and show that the cohomology groups $H^r(\mathrm{Lie}(G_V), V)$ vanish. The proof of the latter uses a criterion for the vanishing of Lie algebra cohomology groups. This requires a special element of the Lie algebra whose eigenvalues satisfy a linear condition (see Chapter 5, §5.1). The complicated part is the construction of such special elements. We explain the construction of the desired elements in the Lie algebras of the images of Galois representations concerned. For this part we reproduce the arguments in [CSW01] and [Su00] in proving the said results. We also recall the analogue of Theorem 2 for ℓ-adic representations with $\ell \neq p$. In Chapter 6, we deal with the almost independence of systems of ℓ-adic representations. We recall its definition as given by Serre and prove some results that will be used for the proof of Theorems 14 and 15. Finally we give the proof of our results in Chapter 7 using the arguments in Chapters 5 and 6. We present some criteria (Theorem 7.2.7, Theorem 7.2.12 and Lemma 7.3.1) for the vanishing of J_V-cohomology that follow from the proofs of Theorems 2 and 3, thus obtaining partial answers to Problem 1. These criteria are used to prove our results (Chapter 2) on cohomological coprimality. Two appendices are included to provide a convenient reference to concepts and well-known results used in some of the proofs which are scattered in the literature.

Acknowledgements

It gives me great pleasure to express my sincerest gratitude to Yuichiro Taguchi, who suggested this topic of research and under whose supervision I completed this work. During the period of my research I received enlightenment, encouragement, and helpful advice through his guidance.

I am greatly indebted to Yoshiyasu Ozeki for discussing his work to me and for his enthusiasm for answering my questions. I also extend my gratitude to Yoshihiro Ochi for taking the time to read my work and point out some mistakes.

I would like to offer my appreciation to Professors Masato Kurihara, Makoto Matsumoto and Noriyuki Suwa for their insights, comments and suggestions while this work was in progress. Many of the improvements in this work are due to them.

Thanks are due to people with whom I had a chance to discuss when I presented parts of this work in meetings and workshops. I am especially thankful to Atsushi Yamagami, Tomoki Mihara and Shou Yoshikawa for their comments and questions that challenged my results, thus leading to improvements.

I am also grateful to the members of the Arithmetic Geometry Seminar at Kyushu University from whom I learned much of what I know about topics surrounding this thesis. I especially thank Shun'ichi Yokoyama, Yoshinori Mishiba, Megumi Takata, Shinya Okumura, Yasuhiro Ikematsu and Yu Takakura for helpful mathematical conversations and for helping me cope with the life in Japan.

My study in Kyushu University would not have been possible without the financial support from the Ministry of Education, Culture, Sports, Science and Technology of Japan. I also thank the Institute of Mathematics, University of the Philippines-Diliman for its support and for allowing me to take a leave to pursue higher education in Japan.

Special thanks to Fidel Nemenzo for sparking my interest in number theory and for introducing to me the challenging yet fulfilling world of numbers.

My mother has continually been a source of warm encouragement and love. Finally, I thank Issa for the love and inspiration. She has always been there for me, supporting throughout all my endeavours, even from 2310 kilometers away.

Contents

Chapter 1

Notations and Terminologies

Let ℓ be a prime number. The field of rational ℓ-adic numbers is denoted by $\mathbb{Q}_\ell$. Throughout this thesis, F denotes any field of characteristic 0. When $\ell = p$ is fixed and F is a p-adic field, we use K instead of F to distinguish the local setting from the global one. For a p-adic field K, we let $\mathcal{O}_K$ be the ring of integers of K. We denote by k the residue field of $\mathcal{O}_K$ (or of K, for brevity). We denote the cardinality of k by $q = p^f$. We also let K_0 denote the maximal unramified subextension in $K/\mathbb{Q}_p$.

For a field F, we fix a separable closure $\overline{F}$. For a positive integer m, let $F(\mu_{\ell^m})$ be the field extension obtained by adjoining to F all ℓ^mth roots of unity. We write $F(\mu_{\ell^\infty}) := \cup_{m\in\mathbb{Z}_{\geq 0}} F(\mu_{\ell^m})$. For a subextension L of $\overline{F}$ over F, we denote by G_L the Galois group $\mathrm{Gal}(\overline{F}/L)$. Endowing G_F with the Krull topology makes it into a *profinite group*; that is, a totally disconnected, compact, Hausdorff topological group. For a topological ring R, a *continuous representation* of G_F on a topological R-module M is a continuous homomorphism $\rho : G_F \to \mathrm{GL}_R(M)$. We denote by $F(M)$ the fixed subfield of $\overline{F}$ by the kernel of ρ. An *ℓ-adic representation* of the Galois group G_F will always refer to a continuous representation $\rho_\ell : G_F \to \mathrm{GL}_{\mathbb{Q}_\ell}(V)$, where V is a finite-dimensional vector space over $\mathbb{Q}_\ell$, made into a topological $\mathbb{Q}_\ell$-module by endowing it with the ℓ-adic topology. For such a continuous representation, we denote by G_ℓ the image group $\rho_\ell(G_F)$. When $\ell = p$ and $F = K$, we often suppress the subscript and simply write $\rho : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(V)$. In this case we put $G_V = \rho(G_K)$ and $H_V = \rho(G_{K(\mu_{p^\infty})})$. We write K^{nr} for the maximal unramified extension of K and I_K for the Galois group $G_{K^{\mathrm{nr}}}$; that is, the inertia subgroup of G_K. The image of I_K by a p-adic representation ρ of G_K as above is denoted by I_V.

In this thesis, $\chi : \mathcal{G} \to \mathbb{Z}_p^\times$ always denotes the *p-adic cyclotomic character*, that is, the continuous character such that $g(\zeta) = \zeta^{\chi(g)}$ for all $g \in \mathcal{G}$ and all

$\zeta \in \mu_{p^\infty}$, where μ_{p^∞} is the group of all p-power roots of unity in $\overline{F}$.

For any vector space W over $\mathbb{Q}_\ell$ and any field extension L of $\mathbb{Q}_\ell$, we write W_L for $W \otimes_{\mathbb{Q}_\ell} L$.

By a *variety* over a field F, we mean a separated scheme of finite type over F. For a variety X over F, we write $X_{\overline{F}} = X \otimes_F \overline{F}$. Given an integer $i \geq 0$, we can define the ith étale cohomology group $H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Z}/\ell^m\mathbb{Z})$. This is a finite abelian group killed by ℓ^m. The maps

$$H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Z}/\ell^{m+1}\mathbb{Z}) \to H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Z}/\ell^m\mathbb{Z})$$

given by reduction modulo ℓ^m make $(H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Z}/\ell^m\mathbb{Z}))_{m\in\mathbb{Z}_{\geq 1}}$ into a projective system and its inverse limit $\varprojlim H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Z}/\ell^m\mathbb{Z})$ is a $\mathbb{Z}_\ell$-module of finite type on which G_F acts continuously. Its extension of scalars

$$H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_\ell) := \varprojlim H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Z}/\ell^m\mathbb{Z}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

gives rise to an ℓ-adic representation

$$\rho : G_F \to \mathrm{GL}_{\mathbb{Q}_\ell}(V_\ell),$$

where we write $V_\ell = H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_\ell)$.

Let Λ be the set of all rational prime numbers. For a subset S of Λ, let $(\rho_\ell : G_F \to \mathrm{GL}_{\mathbb{Q}_\ell}(V_\ell))_{\ell\in S}$ be a system of (general) ℓ-adic representations indexed by S. In this case, we write $\rho_S = \prod_{\ell\in S} \rho_\ell : G_F \to \prod_{\ell\in S} \mathrm{GL}_{\mathbb{Q}_\ell}(V_\ell))$ and $V_S = \bigoplus_{\ell\in S} V_\ell$ for its representation space.

For a g-dimensional abelian variety A over F, we let $A[\ell^m]$ be the group of $\overline{F}$-rational points of A of order ℓ^m. The Tate module $T_\ell(A) := \varprojlim A[\ell^m]$ of A is a $\mathbb{Z}_\ell$-module of rank $2g$ with a continuous action of G_F. We denote by

$$\rho_A : G_F \longrightarrow \mathrm{GL}(T_\ell(A)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$$

the natural continuous representation associated with $T_\ell(A)$. We use the usual notation $V_\ell(A) = T_\ell(A)\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$. Let $\mathbb{Q}_\ell(r)$ denote the rth twist by the ℓ-adic cyclotomic character, where $r \in \mathbb{Z}$. The dual $V_\ell(A)^\vee = \mathrm{Hom}(V_\ell(A), \mathbb{Q}_\ell)$ is canonically isomorphic to $H^1_{\text{ét}}(A_{\overline{F}}, \mathbb{Q}_\ell)$. On the other hand, the Weil pairing allows us to identify $V_\ell(A)$ with $V_\ell(A^\vee)$ in a canonical way. Thus we may canonically identify $V_\ell(A)$ with $H^1_{\text{ét}}(A^\vee_{\overline{F}}, \mathbb{Q}_\ell(1))$. We also note that $F(V_\ell(A)) = F(A_{\ell^\infty})$, where $F(A_{\ell^\infty})$ is the extension of F generated by the coordinates of all the ℓ-power torsion points on the group of $\overline{F}$-valued points $A(\overline{F})$. By the Weil pairing, the field $F(A_{\ell^\infty})$ contains $F(\mu_{\ell^\infty})$.

Given a proper smooth variety X over K, we say that X has *good reduction* over K if there exists a proper smooth scheme $\mathcal{X}$ over $\mathrm{Spec}(\mathcal{O}_K)$ whose generic fiber $\mathcal{X} \times_{\mathcal{O}_K} K$ is isomorphic to X. Following Bloch-Kato [BK86],

X is said to have *good ordinary reduction* over K if there exists a proper smooth scheme $\mathcal{X}$ over $\mathrm{Spec}(\mathcal{O}_K)$ as above with special fiber $\mathcal{Y}$ such that the de Rham-Witt cohomology groups $H^r(\mathcal{Y}, d\Omega^s_{\mathcal{Y}})$ are trivial for all r and all s, where $d\Omega^s_{\mathcal{Y}}$ is the sheaf of exact differentials on $\mathcal{Y}$. When X is an abelian variety of dimension g, this definition coincides with the property that the group of $\bar{k}$-points of $\mathcal{Y}$ killed by p is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^g$, which is the the classical definition of an abelian variety with good ordinary reduction. Here, $\bar{k}$ denotes an algebraic closure of the residue field k of K. We say X has *potential good* (resp. *potential good ordinary*) reduction over K if there exists a finite extension K'/K such that X has good (resp. good ordinary) reduction over K'.

An elliptic curve (that is, a one-dimensional abelian variety) will always be denoted by E or E'. Consider an elliptic curve E over K. Choose a minimal Weierstrass model for E with coefficients in $\mathcal{O}_K$. If the curve $\tilde{E}$ obtained by reducing the coefficients of the chosen Weierstrass model for E over K has a node, we say that E has *multiplicative reduction* over K. Suppose E has good reduction over K. In this case, the $\bar{k}$-points of $\tilde{E}$ killed by p is either isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or is trivial. As mentioned above, the reduction is ordinary if the former holds. If the latter holds, we say that E has *good supersingular reduction*. We say that E has *potential good supersingular* (resp. *potential multiplicative* reduction over K if there exists a finite extension K'/K such that E has good supersingular (resp. multiplicative) reduction over K'.

An elliptic curve E over K with good supersingular reduction is said to have *formal complex multiplication over K* if the endomorphism ring of the p-divisible group $\mathcal{E}(p)$ associated with the Néron model $\mathcal{E}$ of E over $\mathcal{O}_K$ is a $\mathbb{Z}_p$-module of rank 2. We simply say E has *formal complex multiplication* if $E \times_K K'$ has formal complex multiplication for some algebraic extension K' of K. Then the quadratic field $\mathrm{End}_{\mathcal{O}_{K'}}(\mathcal{E}(p)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is called the *formal complex multiplication field* of E. We can take for K' a finite extension of K of degree at most 2.

If F is a field and F' is an algebraic extension of F, we say that F' is a *prime-to-p extension* of F if F' is a union of finite extensions over F of degree prime-to-p. If F' is a prime-to-p extension over some finite extension field of F, we say that F' is a *potential prime-to-p extension* of F. Clearly, if F' is a potential prime-to-p extension of F, then every intermediate field F'' (with $F \subseteq F'' \subseteq F'$) is a potential prime-to-p extension of F.

For a finite-dimensional $\mathbb{Q}_p$-vector space V and a subgroup J of $\mathrm{GL}(V)$ we write J^{alg} for its Zariski closure, that is, the intersection of all algebraic subgroups J' of $\mathrm{GL}(V)$ such that J' is defined over $\mathbb{Q}_p$ and $J'(\mathbb{Q}_p)$ contains J. For a p-adic Lie group or an algebraic group J, its Lie algebra is denoted by $\mathrm{Lie}(J)$.

A q-Weil number of weight $w \geq 0$ is an algebraic integer α such that $|\iota(\alpha)| = q^{\frac{w}{2}}$ for all field embeddings $\iota : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$.

Chapter 2

Cohomological Coprimality

We list our results on the cohomological coprimality of representations coming from geometry. We follow the notations as stated in Chapter 1. First, we consider the setting where the base field is a p-adic field K.

Theorem 2.1. *Let $\rho : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(V)$ and $\rho' : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(V')$ be potentially crystalline representations (cf. Chapter 4, Definition 4.2.1 (3)). Let K' be a finite extension of K such that $\rho|_{G_{K'}}$ and $\rho'|_{G_{K'}}$ are crystalline. Let Φ and Φ' denote the associated endomorphism of the filtered module associated to $\rho|_{G_{K'}}$ and $\rho'|_{G_{K'}}$, respectively. Suppose the following conditions are satisfied:*
(i) the eigenvalues of Φ and Φ' are q-Weil numbers of odd weight;
(ii) the determinant of Φ and Φ' are rational numbers;
(iii) there exists a filtration

$$0 = V_{-1} \subsetneq V_0 \subsetneq V_1 = V$$

of $G_{K'}$-stable subspaces such that $I_{K'}$ acts on V_0 by χ^a and $I_{K'}$ acts on V_1/V_0 by χ^b, where a and b are distinct integers;
(iv) the residue field of $K(V')$ is a potential prime-to-p extension of k;
(v) $V^{G_{L'}} = 0$ for every finite extension L' of $K(V')$ and $V'^{G_{L'}} = 0$ for every finite extension L' of $K(V)$.
Then V and V' are cohomologically coprime.

Although the above theorem already gives a nice consequence for abelian varieties, it should be possible to extend it to the case where the filtration has arbitrary length. Unfortunately, we were not able to obtain such an extension in this thesis. We leave this for now and hope to be able to prove this generalization in the future.

Theorem 2.2. *Let X be a proper smooth variety over K with potential good ordinary reduction and let E/K be an elliptic curve with potential good supersingular reduction. Let i be a positive odd integer and we put $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ and $V' = V_p(E)$. Then V and V' are cohomologically coprime.*

Suppose E and E' are elliptic curves over K. We prove some results on the cohomological coprimality of $V_p(E)$ and $V_p(E')$. As in Theorem 10 in the Introduction, this is done by distinguishing the reduction types of E and E'. As such, it provides an extension of the said theorem. This is summarized in the following

Theorem 2.3. *Let E and E' be elliptic curves over K. The cohomological coprimality of $V_p(E)$ and $V_p(E')$ is given by the following table:*

E	E'	*Cohomologically coprime*
ordinary	*ordinary*	*No*$^\sharp$
	supersingular	*Yes*
	multiplicative	*"No"*
supersingular with FCM	*supersingular with FCM*	*Yes**
	supersingular without FCM	*Yes*
	multiplicative	*"No"*
supersingular without FCM	*supersingular without FCM*	*Yes**
	multiplicative	*"No"*
multiplicative	*multiplicative*	*"No"*

Again, FCM in the above table means formal complex multiplication. The symbol * means conditional cohomological coprimality. The cohomological coprimality in this case holds under the additional assumption that the group $E(L')[p^\infty]$ of L'-rational points of E of p-power order is finite for every finite extension L' of $K(E'_{p^\infty})$. For $\sharp$, refer to Remark 7.2.18. For the case where one of the elliptic curves has multiplicative reduction, we refer to Remark 7.2.27. The rest is provided by Theorem 7.2.19 in §7.2.6.

We also consider ℓ-adic representations associated with proper smooth varieties as above. Let ℓ and ℓ' be primes. Let X and X' be proper smooth varieties with potential good reduction over K and i and i' be non-zero integers. We consider the ℓ-adic and ℓ'-adic representations of G_K given by $\rho_\ell : G_K \to \mathrm{GL}(V_\ell)$ and $\rho'_{\ell'} : G_K \to \mathrm{GL}(V'_{\ell'})$ where $V_\ell = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell)$ and $V'_{\ell'} = H^{i'}_{\text{ét}}(X'_{\overline{K}}, \mathbb{Q}_{\ell'})$, respectively. Then we have the following

Theorem 2.4. *Let ℓ and ℓ' be distinct primes. Assume the above situation. Then V_ℓ and $V'_{\ell'}$ are cohomologically coprime.*

We now consider the setting where the base field is a number field F. We let S and S' be subsets of Λ and suppose E and E' are elliptic curves over F. We consider the systems of ℓ-adic representations associated with E and E' indexed by S and S', respectively:

$$(\rho_\ell : G_F \to \mathrm{GL}(V_\ell(E)))_{\ell\in S}$$

and

$$(\rho'_\ell : G_F \to \mathrm{GL}(V_\ell(E')))_{\ell\in S'}.$$

Let $V_S = \bigoplus_{\ell\in S} V_\ell(E)$ and $V'_{S'} = \bigoplus_{\ell\in S'} V_\ell(E')$.

Theorem 2.5. *Let S and S' be sets of primes. Let E and E' be elliptic curves over F.*
(i) Assume that E and E' are not isogenous over $\overline{F}$. Then V_S and $V'_{S'}$ are cohomologically coprime.
(ii) If $S \cap S' = \emptyset$, then V_S and $V'_{S'}$ are cohomologically coprime.

The Isogeny Theorem due to Faltings ([Fa83], §5 Korollar 2) implies that

$$\begin{aligned} E \text{ and } E' \text{ are isogenous over } F &\Leftrightarrow V_\ell(E) \simeq V_\ell(E') \text{ as } G_F\text{-modules for some prime } \ell \\ &\Leftrightarrow V_\ell(E) \simeq V_\ell(E') \text{ as } G_F\text{-modules for all primes } \ell. \end{aligned}$$

We have the following

Corollary 2.6. *Let E and E' be elliptic curves over F. The following statements are equivalent:*
(i) E and E' are not isogenous over $\overline{F}$;
(ii) $V_S|_{G_{F'}}$ and $V'_{S'}|_{G_{F'}}$ are cohomologically coprime for any S and S' and for every finite extension F' of F;
(iii) $V_\ell(E)|_{G_{F'}}$ $(= V_{\{\ell\}}|_{G_{F'}})$ and $V_\ell(E')|_{G_{F'}}$ $(= V'_{\{\ell\}}|_{G_{F'}})$ are cohomologically coprime for some prime number ℓ and for every finite extension F' of F.

Proof. The implication $(i) \Rightarrow (ii)$ is given by Theorem 2.5-(i) and clearly $(ii) \Rightarrow (iii)$. We show $(iii) \Rightarrow (i)$. If E and E' are isogenous over $\overline{F}$, then they are isogenous over some finite extension F' of F. Then the Isogeny Theorem implies that $V_\ell(E)$ and $V_\ell(E')$ are isomorphic as $G_{F'}$-modules for some prime ℓ. Since kernels of isomorphic representations coincide, $V_\ell(E)$ and $V_\ell(E')$ are not cohomologically coprime over F'. □

Chapter 3

Cohomology of profinite groups and of Lie algebras

3.1 Cohomology of profinite groups

Let G be a profinite group. A *topological G-module M* is a topological group endowed with a continuous action of G, i.e., the map $G \times M \to M$ is continuous. For $n \in \mathbb{Z}_{>0}$, endow G^n with the product topology. We define the *nth group of continuous cochains* $C^n(G, M)$ as the group of continuous maps $G^n \to M$ for $n > 0$, and $C^n(G, M) := M$, for $n = 0$. We define the *nth coboundary map* $d_n : C^n(G, M) \to C^{n+1}(G, M)$ by the formula

$$\begin{aligned}(d_n\varphi)(g_1, \ldots, g_{n+1}) = {} & g_1\varphi(g_2, \ldots, g_{n+1}) \\ & + \sum_{i=1}^{n}(-1)^i\varphi(g_1, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots g_{n+1}) \\ & + (-1)^{n+1}\varphi(g_1, \ldots, g_n),\end{aligned}$$

for $\varphi \in C^n(G, M)$.

It can be verified that for any $n \geq 0$, we have $d_{n+1} \circ d_n = 0$ (cf. [NSW08], Proposition 1.2.1). Hence, the sequence $C^\bullet(G, M)$

$$C^0(G, A) \xrightarrow{d_0} C^1(G, A) \xrightarrow{d_1} C^2(G, A) \xrightarrow{d_2} \ldots \xrightarrow{d_{n-1}} C^n(G, A) \xrightarrow{d_n} \ldots \tag{3.1}$$

is a cochain complex. The kernel of d_n is the group of *continuous n-cocycles*, denoted by $Z^n(G, M)$. For $n \geq 1$ we define $B^n(G, M)$ to be the image of d_{n-1} and $B^0(G, M)$ to be the trivial group. The elements $B^n(G, M)$ are called the *continuous n-coboundaries*. Since $d_{n+1} \circ d_n = 0$, we see that $B^n(G, M) \subseteq Z^n(G, M)$ for all $n \geq 0$.

Definition 3.1.1. The *nth continuous cohomology group* of G with coefficients in M is

$$H^n(G,M) = Z^n(G,M)/B^n(G,M).$$

Note that the groups $Z^n(G,M)$, $B^n(G,M)$ and $H^n(G,M)$ are all abelian groups. We will often omit 'continuous' when we refer to the groups defined above. The cohomology groups measure how far the cochain complex $C^\bullet(G,M)$ is from being exact.

The cohomological functors $C^n(G,-)$ and $H^n(G,-)$ are functorial. If $\eta : M_1 \to M_2$ is a morphism of topological G-modules, then it induces a morphism of complexes $C^\bullet(G,M_1) \to C^\bullet(G,M_2)$, which then induces morphisms from $Z^n(G,M_1)$ (resp. $B^n(G,M_1)$ or $H^n(G,M_1)$) to $Z^n(G,M_2)$ (resp. $B^n(G,M_2)$ or $H^n(G,M_2)$).

The following proposition will be used later.

Proposition 3.1.2 ([Ko02], Theorem 3.6)**.** *Let G be a profinite group and M a G-module. Suppose M is a direct sum of G-modules M_i, $i \in I$. Then $H^n(G,M)$ is a direct sum of the abelian groups $H^n(G,M_i)$, $i \in I$.*

The Hochschild-Serre spectral sequence

A spectral sequence is an important tool in studying (co)homology groups. We recall below the spectral sequence due to G. Hochschild and J.-P. Serre.

Theorem 3.1.3 ([HS53], Chap. I, §7 Proposition 7)**.** *Let G be profinite group, H a closed normal subgroup and M a G-module. Then there exists a spectral sequence*

$$H^r(G/H, H^s(H,M)) \Rightarrow H^{r+s}(G,M).$$

As a consequence of the spectral sequence, we have the following

Corollary 3.1.4 ([HS53], Chap. III, §4 Theorem 2)**.** *Let $m \geq 1$ and assume that $H^r(H,M) = 0$ for $0 < r < m$. Then we have the following exact sequence*

$$\begin{aligned} 0 \to H^m(G/H, M^H) \to H^m(G,M) \to & H^m(H,M)^{G/H} \\ & \to H^{m+1}(G/H, M^H) \to H^{m+1}(G,M). \end{aligned}$$

Corollary 3.1.5 ([NSW08], Corollary 2.4.2)**.** *If $H^r(H,M) = 0$ for $r > 0$, then*

$$H^m(G/H, M^H) \simeq H^m(G,M) \qquad (m \geq 0).$$

Proof. This follows from Corollary 3.1.4 by induction on m. □

3.2 Lie Algebra Cohomology

Let $\mathfrak{g}$ be a Lie algebra over a field F and M be a $\mathfrak{g}$-module which is finite-dimensional as an F-vector space. We denote by $M^{\mathfrak{g}}$ the subspace of M consisting of all $m \in M$ with $\gamma \cdot m = 0$ for all $\gamma \in \mathfrak{g}$.

The *n-dimensional cochains* for $\mathfrak{g}$ in M are the n-linear alternating functions f on $\mathfrak{g}^n$ with values in M, that is, n-linear functions f such that $f(\gamma_1, \ldots, \gamma_n) = 0$ whenever $\gamma_i = \gamma_j$ for $1 \le i < j \le n$. The n-dimensional cochains form a vector space $C^n(\mathfrak{g}, M)$ over F. We identify $C^0(\mathfrak{g}, M)$ with M.

For $n \ge 0$ we define a linear map $d_n : C^n(\mathfrak{g}, M) \to C^{n+1}(\mathfrak{g}, M)$ by the formula

$$\begin{aligned}(d_n f)(\gamma_0, \ldots, \gamma_n) = &\sum_{i=0}^{n} (-1)^i \gamma_i \cdot f(\gamma_0, \ldots, \hat{\gamma_i}, \ldots, \gamma_n) \\ &+ \sum_{r<s} (-1)^{r+s} f([\gamma_r, \gamma_s], \gamma_0, \ldots, \hat{\gamma_r}, \ldots, \hat{\gamma_s}, \ldots, \gamma_n),\end{aligned}$$

where the symbol $\hat{}$ indicates that the argument below it must be omitted. We call d_n a *coboundary operator*. It can be shown that the coboundary operator satisfies the following properties (cf. [CE48], Chapter III §14):

(1) $d_{n+1} \circ d_n = 0$, for $n \ge 0$;

(2) $d_n(\gamma \cdot f) = \gamma \cdot (d_n f)$ for $\gamma \in \mathfrak{g}$ and $f \in C^n(\mathfrak{g}, M)$; and

(3) $(d_0 f)(\gamma) = \gamma \cdot f$ for $f \in C^0(\mathfrak{g}, M) = M$.

Having known property (1) above, we define the space $Z^n(\mathfrak{g}, M)$ of *n-cocycles* as the kernel of the transformation d_n, and the space $B^n(\mathfrak{g}, M)$ of *n-coboundaries* as the image of d_{n-1}. By definition, $B^0(\mathfrak{g}, M) = 0$.

Definition 3.2.1. The *nth cohomology group* $H^n(\mathfrak{g}, M)$ of $\mathfrak{g}$ with coefficients in M is defined as the quotient space

$$H^n(\mathfrak{g}, M) := Z^n(\mathfrak{g}, M)/B^n(\mathfrak{g}, M).$$

Chapter 4

Background from p-adic Hodge theory

Let K be a p-adic field and denote by $\mathrm{Rep}(G_K)$ the category of p-adic representations of G_K. In this chapter, we recall certain full Tannakian subcategories of $\mathrm{Rep}(G_K)$. This means that these categories contain the unit representation and are stable by the "usual" operations of linear algebra; that is, taking sub-objects, quotients, direct sum, tensor product and dual. These are:

- the category $\mathrm{Rep}_{\mathrm{HT}}(G_K)$ of Hodge-Tate representations,
- the category $\mathrm{Rep}_{\mathrm{dR}}(G_K)$ of de-Rham representations,
- the category $\mathrm{Rep}_{\mathrm{st}}(G_K)$ of semi-stable representations,
- the category $\mathrm{Rep}_{\mathrm{cris}}(G_K)$ of crystalline representations,
- the category $\mathrm{Rep}_{\mathrm{pst}}(G_K)$ of potentially semi-stable representations,
- the category $\mathrm{Rep}_{\mathrm{pcris}}(G_K)$ of potentially crystalline representations, and
- the category $\mathrm{Rep}_{\mathrm{nr}}(G_K)$ of unramified representations.

We have the following hierarchy of these categories:

$$
\begin{array}{ccccccccc}
 & & \mathrm{Rep}_{\mathrm{pcris}}(G_K) & \subset & \mathrm{Rep}_{\mathrm{pst}}(G_K) & \subset & \mathrm{Rep}_{\mathrm{dR}}(G_K) & \subset & \mathrm{Rep}_{\mathrm{HT}}(G_K) \\
 & & \cup & & \cup & & & & \cap \\
\mathrm{Rep}_{\mathrm{nr}}(G_K) & \subset & \mathrm{Rep}_{\mathrm{cris}}(G_K) & \subset & \mathrm{Rep}_{\mathrm{st}}(G_K) & & & & \mathrm{Rep}(G_K)
\end{array}
$$

In fact we have $\mathrm{Rep}_{\mathrm{pst}}(G_K) = \mathrm{Rep}_{\mathrm{dR}}(G_K)$, but note that the other inclusions are strict.

4.1 Hodge-Tate representations

Let K be a p-adic field and $\mathbb{C}_p$ be the completion of the algebraic closure of $\overline{\mathbb{Q}_p}$. Let $\rho : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(V)$ be a p-adic representation of G_K. We may extend the action of G_F on V to the $\mathbb{C}_p$-vector space $V_{\mathbb{C}_p} = V \otimes_{\mathbb{Q}_p} \mathbb{C}_p$ by

$$\sigma(\sum_i (v_i \otimes c_i)) = \sum_i \sigma(v_i) \otimes \sigma(c_i),$$

for $v_i \in V$, $c_i \in \mathbb{C}_p$ and $\sigma \in G_K$. For $m \in \mathbb{Z}$, we consider the K-vector space

$$V_{\mathbb{C}_p}\{m\} := \{v \in V_{\mathbb{C}_p} | \sigma(v) = \chi(\sigma)^m v \text{ for all } \sigma \in G_K\}$$

where $\chi : G_K \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character. The inclusion $V_{\mathbb{C}_p}\{m\} \subseteq V_{\mathbb{C}_p}$ extends to a $\mathbb{C}_p$-linear injective map

$$\xi_V : \bigoplus_{m\in\mathbb{Z}} (V_{\mathbb{C}_p}\{m\} \otimes_K \mathbb{C}_p) \to V_{\mathbb{C}_p}.$$

This particularly implies that the K-vector spaces $V_{\mathbb{C}_p}\{m\}$ are finite-dimensional and trivial for almost all $m \in \mathbb{Z}$.

Definition 4.1.1. A p-adic representation V of G_K is said to be *Hodge-Tate* if the homomorphism ξ_V is an isomorphism.

Put

$$t_m = \dim_K V_{\mathbb{C}_p}\{m\} = \dim_{\mathbb{C}_p}(V_{\mathbb{C}_p}\{m\} \otimes_K \mathbb{C}_p).$$

Clearly, V is Hodge-Tate if and only if $\sum_m t_m = \dim_{\mathbb{Q}_p} V$.

Definition 4.1.2. Let V be a Hodge-Tate representation of G_K. The nonzero integers m which occur in the decomposition $V_{\mathbb{C}_p} \simeq \bigoplus_{m\in\mathbb{Z}}(V_{\mathbb{C}_p}\{m\} \otimes_K \mathbb{C}_p)$ are called the *Hodge-Tate weights* of V and t_m is the *multiplicity* of a weight m.

Example 4.1.3 ([Fa88], §1.b, [Fa02])**.** Let X be a proper smooth variety over a p-adic field K and $i \in \mathbb{Z}$. There is a canonical isomorphism which is compatible with the action of G_K,

$$H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \mathbb{C}_p = \bigoplus_{0\le r\le i} H^{r,i-r}(X_K) \otimes_K \mathbb{C}_p(-r).$$

Here $H^{r,s}(X_K) = H^s\left(X_K, \Omega^r_{X_K/K}\right)$ and $\Omega^r_{X_K/K}$ is the sheaf of r-differentials. Thus $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is a Hodge-Tate representation with Hodge-Tate weights $0, -1, \ldots, -i$. Further, the Hodge symmetry shows that $t_i = t_{-(i-j)}$.

Consider a Hodge-Tate representation $\rho : G_K \to \mathrm{GL}(V)$ of G_K. The *operator of Sen* is the element $\Psi \in \mathrm{End}_{\mathbb{C}_p}(V_{\mathbb{C}_p})$ such that

$$\Psi v = mv, \qquad \text{for } m \in \mathbb{Z}, \quad v \in V_{\mathbb{C}_p}\{m\} \otimes_K \mathbb{C}_p\,.$$

Let I_V be the image of I_K under ρ and we write I_V^{alg} for its Zariski closure.

Theorem 4.1.4 ([Sen73], §4, Theorem 1)**.** *The Lie algebra* $\mathfrak{i} = \mathrm{Lie}(I_V)$ *is the smallest* $\mathbb{Q}_p$*-subspace of* $\mathrm{End}_{\mathbb{Q}_p} V$ *such that* $\mathfrak{i} \otimes_{\mathbb{Q}_p} \mathbb{C}_p$ *contains* Ψ*.*

Theorem 4.1.5 ([Sen73], §6, Theorem 2)**.** *The Lie algebra* $\mathrm{Lie}(I_V) \subseteq \mathrm{End}_{\mathbb{Q}_p}(V)$ *is algebraic. That is,*

$$\mathrm{Lie}(I_V) = \mathrm{Lie}(I_V^{\mathrm{alg}}).$$

4.2 de Rham, semistable and crystalline representations

In order to understand and sub-categorise the category $\mathrm{Rep}(G_K)$, Fontaine constructed some *rings of periods* B_*. These are topological $\mathbb{Q}_p$-algebras with a continuous and linear action of G_K together with some additional structures which are compatible with the action of G_K such that $K_* = \mathrm{B}_*^{G_K}$ is a field and the K_*-vector space $D_{\mathrm{B}_*}(V) = (V \otimes_{\mathbb{Q}_p} \mathrm{B}_*)^{G_K}$ is an interesting invariant of an object V of $\mathrm{Rep}(G_K)$ that inherits the additional structures of V. For such rings B_*, it can be shown that

$$\dim_{K_*}(V \otimes_{\mathbb{Q}_p} \mathrm{B}_*)^{G_K} \leq \dim_{\mathbb{Q}_p} V.$$

We briefly recall the the period rings B_{dR}, B_{st} and $\mathrm{B}_{\mathrm{cris}}$.

Roughly speaking, the ring B_{dR} is a complete discrete valuation field, with residue field isomorphic to $\mathbb{C}_p$ having the following properties:

- $\mathrm{B}_{\mathrm{dR}}^{G_K} = K$,
- B_{dR} has a uniformizer t such that $\sigma(t) = \chi(\sigma)t$, for all $\sigma \in G_K$, and
- B_{dR} has filtration $\mathrm{B}_{\mathrm{dR}}^r = \{b \in \mathrm{B}_{\mathrm{dR}} | \mathrm{ord}_t(b) \geq r\}$.

The rings B_{st} and $\mathrm{B}_{\mathrm{cris}}$ are subrings of B_{dR} such that

$$\mathbb{Q}_p \subset \mathrm{B}_{\mathrm{cris}} \subset \mathrm{B}_{\mathrm{st}} \subset \mathrm{B}_{\mathrm{dR}}$$

and ${\mathrm{B}_{\mathrm{cris}}}^{G_K} = {\mathrm{B}_{\mathrm{st}}}^{G_K} = K_0$, the maximal unramified subextension in $K/\mathbb{Q}_p$. The ring B_{st} comes equipped with two operators: the "Frobenius" $\varphi : \mathrm{B}_{\mathrm{st}} \to \mathrm{B}_{\mathrm{st}}$ and the "monodromy operator" $N : \mathrm{B}_{\mathrm{st}} \to \mathrm{B}_{\mathrm{st}}$ which commute with the G_{K_0}-action and such that $N\varphi = p\varphi N$. Furthermore, $\mathrm{B}_{\mathrm{cris}} = \{b \in \mathrm{B}_{\mathrm{st}} | Nb = 0\}$.

Definition 4.2.1. (1) A p-adic representation $\rho : G_K \to \mathrm{GL}(V)$ of G_K is said to be *de Rham* if

$$\dim_K (V \otimes_{\mathbb{Q}_p} \mathrm{B}_{\mathrm{dR}})^{G_K} = \dim_{\mathbb{Q}_p} V.$$

(2) A p-adic representation V of G_K is said to be *semi-stable* if

$$\dim_{K_0} (V \otimes_{\mathbb{Q}_p} \mathrm{B}_{\mathrm{st}})^{G_K} = \dim_{\mathbb{Q}_p} V.$$

A p-adic representation V of G_K is said to be *potentially semi-stable* if there exists a finite extension K' of K such that $V|_{G_{K'}}$ is semi-stable.

(3) A p-adic representation V of G_K is said to be *crystalline* if

$$\dim_{K_0} (V \otimes_{\mathbb{Q}_p} \mathrm{B}_{\mathrm{cris}})^{G_K} = \dim_{\mathbb{Q}_p} V.$$

A p-adic representation V of G_K is said to be *potentially crystalline* if there exists a finite extension K' of K such that $V|_{G_{K'}}$ is crystalline.

Potentially semi-stable representations are de Rham. As mentioned earlier, we have $\mathrm{Rep}_{\mathrm{dR}}(G_K) = \mathrm{Rep}_{\mathrm{pst}}(G_K)$. This follows from the following result.

Theorem 4.2.2 ([Ber02], Théorème 0.7)**.** *If V is a de Rham representation, then V is potentially semi-stable.*

Definition 4.2.3. A *filtered* (φ, N)*-module* is a quadruple $(\mathcal{D}, \varphi, N, \mathrm{Fil}^\bullet \mathcal{D}_K)$ where

- $\mathcal{D}$ is a finite-dimensional K_0-vector space,
- $\varphi : \mathcal{D} \to \mathcal{D}$, is an automorphism which is semi-linear with respect to the absolute Frobenius σ on K_0
- $N : \mathcal{D} \to \mathcal{D}$ is a K_0-linear endomorphism such that $N\varphi = p\varphi N$, and
- $\mathrm{Fil}^\bullet \mathcal{D}_K$ is a filtration on the K-vector space $\mathcal{D}_K := \mathcal{D} \otimes_{K_0} K$ that is decreasing ($\mathrm{Fil}^j \mathcal{D}_K \supseteq \mathrm{Fil}^{j+1} \mathcal{D}_K$), separated ($\cap_{j\in\mathbb{Z}} \mathrm{Fil}^j \mathcal{D}_K = 0$) and exhaustive ($\cup_{j\in\mathbb{Z}} \mathrm{Fil}^j \mathcal{D}_K = \mathcal{D}_K$).

To each filtered (φ, N)-module $\mathcal{D}$, we associate two polygons: the Hodge polygon $P_H(\mathcal{D})$ coming from the filtration and the Newton polygon $P_N(\mathcal{D})$ coming from the "slopes" of φ.

Definition 4.2.4. A filtered (φ, N)-module $\mathcal{D}$ over K is said to be *admissible* if for every subobject $\mathcal{D}'$ of $\mathcal{D}$, $P_H(\mathcal{D}')$ lies below $P_N(\mathcal{D}')$ and their endpoints are the same. We denote the category of admissible filtered (φ, N)-modules over K by $\mathrm{MF}^{\varphi,\mathrm{N}}_{\mathrm{adm}}$.

It can be shown that for every semistable representation V of G_K, the K_0-vector space $\mathrm{D}_{\mathrm{st}}(V) := (V \otimes_{\mathbb{Q}_p} \mathrm{B}_{\mathrm{st}})^{G_K}$ is an admissible filtered (φ, N)-module. In this case, the fth iterate $\Phi = \varphi^f$ of φ is a K_0-linear automorphism of $\mathrm{D}_{\mathrm{st}}(V)$. Similarly, for every crystalline representation V of G_K, the K_0-vector space $\mathrm{D}_{\mathrm{cris}}(V) := (V \otimes_{\mathbb{Q}_p} \mathrm{B}_{\mathrm{st}})^{G_K}$ is an admissible filtered (φ, N)-module with $N = 0$. In fact, we have the following

Proposition 4.2.5. *(1) The functor* $\mathrm{D}_{\mathrm{st}} : \mathrm{Rep}_{\mathrm{st}}(G_K) \to \mathrm{MF}^{\varphi,\mathrm{N}}_{\mathrm{adm}}$ *induces an equivalence of tensor categories.*

(2) The functor $\mathrm{D}_{\mathrm{cris}} : \mathrm{Rep}_{\mathrm{cris}}(G_K) \to \mathrm{MF}^{\varphi,\mathrm{N}=0}_{\mathrm{adm}}$ *induces an equivalence of tensor categories.*

Example 4.2.6. (1) Let X be a proper smooth variety with good (resp. semi-stable, potential good, potential semi-stable) reduction over K and i an integer. Then $H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is a crystalline (resp. semistable, potentially crystalline, potentially semi-stable) representation of G_K (cf. [Fa02], [Ts99]).
(2) If X has potential good reduction over K, then the eigenvalues of the K_0-linear automorphism Φ acting on $\mathrm{D}_{\mathrm{cris}}(H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p))$ are q-Weil numbers of weight i (cf. [CS99]).

4.3 Unramified representations

Definition 4.3.1. A p-adic representation $\rho : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(W)$ is said to be *unramified* if $\rho(I_K) = \{0\}$.

Let $\rho : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(W)$ be an unramified representation of G_K. Let $\mathbb{Q}_p^{\mathrm{nr}}$ be the maximal unramified extension of $\mathbb{Q}_p$ and $\widehat{\mathbb{Q}_p^{\mathrm{nr}}}$ its completion. The action of G_K on W extends to $W \otimes_{\mathbb{Q}_p} \widehat{\mathbb{Q}_p^{\mathrm{nr}}}$ by $\sigma(\sum_i (w_i \otimes c_i)) = \sum_i \sigma(w_i) \otimes \sigma(c_i)$, for $w_i \in W$, $c_i \in \widehat{\mathbb{Q}_p^{\mathrm{nr}}}$ and $\sigma \in G_K$.

Proposition 4.3.2 ([CSW01], Lemma 3.4)**.** *Assume that* $\rho : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(W)$ *is an unramified representation of* G_K*. Consider the* K_0*-subspace* $U = (W \otimes_{\mathbb{Q}_p} \widehat{\mathbb{Q}_p^{\mathrm{nr}}})^{G_K}$ *of* $W \otimes_{\mathbb{Q}_p} \widehat{\mathbb{Q}_p^{\mathrm{nr}}}$*. Then* W *is crystalline and* $\mathrm{D}_{\mathrm{cris}}(W) = U$*. Moreover, the* K_0*-automorphism* $\Phi_W = \varphi_W^f$ *of* $\mathrm{D}_{\mathrm{cris}}(W)$ *is given by*

$$\beta \circ \Phi_W \circ \beta^{-1} = \rho(\mathrm{Frob}^{-1}),$$

where Frob *is the arithmetic Frobenius in* G_K/I_K *and* $\beta : U \otimes_{K_0} \widehat{\mathbb{Q}_p^{\mathrm{nr}}} \simeq W \otimes_{\mathbb{Q}_p} \widehat{\mathbb{Q}_p^{\mathrm{nr}}}$ *is the isomorphism obtained by extending scalars on the* K_0*-subspace* U *of* W*.*

Chapter 5

The vanishing of G_V- and H_V-cohomologies

5.1 The strong Serre criterion

Let F be a field of characteristic zero. Fix an algebraic closure $\overline{F}$ of F. Let W be a finite-dimensional vector space over F and $\mathfrak{g}$ a finite-dimensional Lie algebra over F. Let

$$\tau : \mathfrak{g} \longrightarrow \mathrm{End}(W)$$

be a faithful Lie algebra homomorphism. We consider the Lie algebra cohomology groups of $\mathfrak{g}$ having coefficients in W.

Definition 5.1.1. We say that W has vanishing $\mathfrak{g}$-cohomology if $H^r(\mathfrak{g}, W) = 0$ for all $r \geq 0$.

For $x \in \mathfrak{g}$, we write $\mathbb{e}(x)$ for the set of distinct eigenvalues in $\overline{F}$ of $\tau(x)$. Following [CSW01], we make the following

Definition 5.1.2. We say that τ satisfies the *strong Serre criterion* if there exists $x \in \mathfrak{g}$ such that, for every integer $k \geq 0$, and for each choice $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_k, \beta_{k+1}$ of $2k+1$ elements of $\mathbb{e}(x)$ (not necessarily distinct), we have

$$\alpha_1 + \ldots + \alpha_k \neq \beta_1 + \ldots + \beta_k + \beta_{k+1}.$$

When $k = 0$, this should be interpreted as $\beta \neq 0$ for all $\beta \in \mathbb{e}(x)$.

Lemma 5.1.3. *If τ is faithful and satisfies the strong Serre criterion, then W has vanishing $\mathfrak{g}$-cohomology.*

Proof. This follows from [Se71], Théorème 1. $\square$

We now consider a continuous representation $\rho : G \to \mathrm{GL}_{\mathbb{Q}_p}(V)$ of a profinite group G on a finite-dimensional $\mathbb{Q}_p$-vector space V. Let G_V be the p-adic Lie group $\rho(G)$. The relation between the cohomology groups of G_V and $\mathrm{Lie}(G_V)$ is well-understood, thanks to the following

Proposition 5.1.4 ([La65], Chap. V, Théorème 2.4.10)**.** *Let U be a p-adic Lie group. The cohomology group $H^m(U, V)$ can be identified with a $\mathbb{Q}_p$-vector subspace of the Lie algebra cohomology group $H^m(\mathrm{Lie}(U), V)$ for all $m \geq 0$.*

From the representation ρ we have a faithful representation $G_V \hookrightarrow \mathrm{GL}(V)$. Considering the corresponding homomorphism of Lie algebras and extending scalars, we obtain a faithful Lie algebra representation $\mathrm{Lie}(G_V)_{\mathbb{C}_p} \hookrightarrow \mathrm{End}(V_{\mathbb{C}_p})$.

Proposition 5.1.5 ([CSW01], Proposition 2.3)**.** *Assume that* $\mathrm{Lie}(G_V)_{\mathbb{C}_p} \hookrightarrow \mathrm{End}(V_{\mathbb{C}_p})$ *satisfies the strong Serre criterion. Then for any open subgroup U of G_V, V has vanishing U-cohomology.*

Proof. Since Lie algebra cohomology is compatible with scalar extensions, we have

$$H^m(\mathrm{Lie}(G_V)_{\mathbb{C}_p}, V_{\mathbb{C}_p}) = H^m(\mathrm{Lie}(G_V), V)_{\mathbb{C}_p} \qquad (m \geq 0).$$

Hence the hypothesis and Lemma 5.1.3 imply that V has vanishing $\mathrm{Lie}(G_V)$-cohomology. If U is an open subgroup of G_V, then $\mathrm{Lie}(U) = \mathrm{Lie}(G_V)$ and it follows from Proposition 5.1.4 that V has vanishing U-cohomology. □

5.2 Local setting

5.2.1 p-adic Logarithms

We recall the extension of the p-adic logarithm to the multiplicative group of $\overline{\mathbb{Q}_p}$. Denote by $\overline{\mathcal{O}}$ the ring of integers of $\overline{\mathbb{Q}_p}$, by $\overline{\mathcal{O}}^\times$ the unit group of $\overline{\mathcal{O}}$, and by $\overline{\mathfrak{m}}$ the maximal ideal of $\overline{\mathcal{O}}$. The usual series

$$\log_p(z) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(z-1)^n$$

converges if and only if $z - 1 \in \overline{\mathfrak{m}}$. Let $\mu := \{z \in \overline{\mathbb{Q}_p} : z^m = 1, (p, m) = 1\}$. Then $\overline{\mathcal{O}}^\times = \mu \times (1 + \overline{\mathfrak{m}})$. We extend $\log_p$ to $\overline{\mathcal{O}}^\times$ by defining $\log_p(z) = 0$ for $z \in \mu$. Fix $\pi \in \overline{\mathbb{Q}_p}$ whose p-adic absolute value is less than one.

Definition 5.2.1. Let $x \in \overline{\mathbb{Q}_p}^{\times}$. Write $x = \pi^a y$, where $a \in \mathbb{Q}$ and $y \in \overline{\mathcal{O}}^{\times}$. Define

$$\log_\pi(x) := \log_p(y).$$

Let W be a finite-dimensional vector space over $\mathbb{Q}_p$. Take $\theta \in \mathrm{GL}_{\mathbb{Q}_p}(W)$. Write $\theta = su$, where s is semisimple and u is unipotent. Thus the series

$$\log(u) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(u-1)^n$$

converges. Write $W_{\overline{\mathbb{Q}_p}} = \bigoplus W_i$, where W_i is the eigenspace of W corresponding to an eigenvalue α_i of s. Define $\log_\pi(s)$ to be the endomorphism of $W_{\overline{\mathbb{Q}_p}}$ which acts on W_i by $\log_\pi(\alpha_i)$.

Definition 5.2.2. For $\theta = su \in \mathrm{GL}_{\mathbb{Q}_p}(W)$, we define

$$\log_\pi(\theta) := \log_\pi(s) + \log(u).$$

Let $m = \dim_{\mathbb{Q}_p}(W)$ and r the cardinality of $\mathrm{GL}_m(k)$. Assume $\theta \in \mathrm{GL}_{\mathbb{Q}_p}(W)$ topologically generates a compact subgroup of $\mathrm{GL}_{\mathbb{Q}_p}(W)$. Then θ stabilizes a lattice in W. Choosing a $\mathbb{Q}_p$-basis of W relative to this lattice implies that the matrix A of θ^r satisfies $A \equiv 1 \pmod p$. We can define

$$\log(\theta) = \frac{1}{r}\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(A-1)^n$$

Proposition 5.2.3 ([Bo08-1], Chap. III, §7.6 Propositions 10 and 13)**.** *Let W be a finite-dimensional vector space over $\mathbb{Q}_p$, and $\theta \in \mathrm{GL}_{\mathbb{Q}_p}(W)$. If θ topologically generates a compact subgroup of $\mathrm{GL}_{\mathbb{Q}_p}(W)$, then $\log_\pi(\theta) = \log(\theta)$. If J is an algebraic subgroup of GL_W and θ lies in $J(\mathbb{Q}_p)$, then $\log_\pi(\theta)$ lies in* $\mathrm{Lie}(J)$.

5.2.2 Proof of Theorem 2

In this section, we give an account of the proof of Theorem 2. In view of Example 4.2.6, we see that the theorem is a special case of the following result.

Proposition 5.2.4 ([CSW01], Propositions 4.1 and 4.2)**.** *Let $\rho : G_K \to \mathrm{GL}(V)$ be a potentially crystalline Galois representation of dimension n. Let K' be a finite extension of K such that $\rho|_{G_{K'}}$ is crystalline. Let $\Phi = \varphi^f$ denote the associated endomorphism of the filtered module associated to $\rho|_{G_{K'}}$.*

Assume that the eigenvalues of Φ *are* q*-Weil numbers of weight* w*. We also let* δ *be the determinant of the endomorphism* $\Phi = \varphi^f$*. Then*
(a) if w *is nonzero, then* V *has vanishing* G_V*-cohomology;*
(b) if w *is odd and* δ *is a rational number, then* V *has vanishing* H_V*-cohomology.*

Before proving this proposition, we list some results that we will need for the proof.

Lemma 5.2.5 ([CSW01], Lemma 3.5)**.** *Suppose* $\rho : G_K \to \mathrm{GL}(V)$ *is an* n*-dimensional semistable representation of* G_K *and let* $\det \rho : G_K \to \mathbb{Z}_p^\times$ *be its determinant character. Let* $m_1, \ldots, m_n$ *denote the Hodge-Tate weights of* V*, counting multiplicities, and put* $t = \sum_{j=1}^n m_j$*. Then the following statements are equivalent:*
(i) The map $\det \rho$ *coincides on an open subgroup of* G_K *with* χ^t*.*
(ii) If δ *denotes the determinant of the endomorphism* $\Phi = \varphi^f$ *of* $\mathrm{D}_{\mathrm{st}}(V)$*, then*

$$\log_\pi(\delta) = \log_\pi(q^{-t}). \tag{5.1}$$

In particular, when $t \neq 0$*, these equivalent assertions imply that the image of* $\det \rho$ *is infinite.*

In the crystalline case, the equivalent assertions of this lemma immediately hold under the hypothesis of Proposition 5.2.4. The following result is actually embedded in the proof of one of the main results of Coates, Sujatha and Wintenberger (see [CSW01], Proposition 4.2; also cf. [Se89], Chapter III Appendix A5).

Lemma 5.2.6. *Assume the hypothesis of Proposition 5.2.4. Let* $m_1, \ldots, m_n$ *be the Hodge-Tate weights of* V*, counting multiplicities. Then the determinant character* $\det \rho : G_K \to \mathbb{Z}_p^\times$ *coincides on an open subgroup of* G_K *with* χ^t*, where* χ *is the* p*-adic cyclotomic character and* $t = \frac{nw}{2} = \sum_{j=1}^n m_j$*.*

Remark 5.2.7. This lemma implies that if $\Delta_V = G_V \cap \mathrm{SL}(V)$, then $\mathrm{Lie}(\Delta_V) = \mathrm{Lie}(H_V)$. In particular, $K(\mu_{p^\infty})$ is a finite extension of $K(V) \cap K(\mu_{p^\infty})$.

Proof. The result is trivial if $n = 0$ so we assume that $n > 0$. We may also assume that $K = K'$. The hypothesis implies that δ is a rational number which is a product of q-Weil numbers of weight w. Thus, δ has archimedean absolute values equal to $q^{\frac{nw}{2}}$. On the other hand, by p-adic Hodge theory the p-adic absolute value of δ is q^{-t}, where t is the sum of the Hodge-Tate weights of V. Hence, we must have $t = \frac{nw}{2}$ and $\delta = \pm q^t$. Consider the one-dimensional p-adic representation $\det \rho \otimes \chi^{-t}$ of G_K, with representation space $W = (\bigwedge^d V)(-t)$. Since $\det \rho$ is crystalline, the restriction of the character $\det\rho$ to I_K is equal to χ^t (cf. [Fo94], Proposition 5.4.1). Thus W is unramified, and is in fact crystalline. We have $D_{\mathrm{cris}}(W) = Z[t]$, where $Z = \bigwedge^d D_{\mathrm{cris}}(V)$ and $Z[t]$ means that the automorphism Φ_Z of Z is replaced by the automorphism $q^t\Phi_Z$. Thus, the automorphism $\Phi_W = \varphi_W^f$ of W is multiplication by $\delta \cdot q^t = \pm 1$. Now as W is one-dimensional, Lemma 4.3.2 implies that Φ_W is equal to $(\det\rho \otimes \chi^{-t})(\mathrm{Frob}^{-1})$, where $\mathrm{Frob} \in G_K/I_K$ denotes the arithmetic Frobenius. Therefore Frob acts on W via multiplication by ± 1. From this we see that $\det\rho$ coincides with χ^t on an open subgroup of G_K. □

Theorem 5.2.8 ([CSW01], Theorem 3.1)**.** *Assume that $\rho : G_K \to \mathrm{GL}(V)$ is an n-dimensional semistable representation, and let $\Phi = \varphi^f$ denote the endomorphism acting on the filtered (φ, N)-module $\mathrm{D}_{\mathrm{st}}(V)$. Let $\lambda_1, \ldots, \lambda_n$ denote the eigenvalues in $\overline{\mathbb{Q}_p}$ of Φ. Consider the faithful representation $\mathrm{Lie}(G_V)_{\overline{\mathbb{Q}_p}} \hookrightarrow \mathrm{End}(V_{\overline{\mathbb{Q}_p}})$. Then there exists an element B in the Lie algebra $\mathrm{Lie}(G_V)_{\overline{\mathbb{Q}_p}}$ whose eigenvalues are*

$$\log_\pi(\lambda_1), \ldots, \log_\pi(\lambda_n).$$

Theorem 5.2.9 ([CSW01], Theorem 3.2)**.** *Assume that $\rho : G_K \to \mathrm{GL}(V)$ is an n-dimensional semistable representation, and that its determinant character $\det\rho : G_K \to \mathbb{Z}_p^\times$ coincides on an open subgroup of G_K with χ^t, where χ is the p-adic cyclotomic character and t is the sum of the Hodge-Tate weights of V. Let $\Phi = \varphi^f$ denote the endomorphism acting on the filtered (φ, N)-module $\mathrm{D}_{\mathrm{st}}(V)$ and $\lambda_1, \ldots, \lambda_n$ denote the eigenvalues in $\overline{\mathbb{Q}_p}$ of Φ. Consider the faithful representation $\mathrm{Lie}(\Delta_V)_{\overline{\mathbb{Q}_p}} \hookrightarrow \mathrm{End}(V_{\overline{\mathbb{Q}_p}})$, where $\Delta_V = G_V \cap \mathrm{SL}(V)$. Then there exists an element B' in the Lie algebra $\mathrm{Lie}(\Delta)_{\overline{\mathbb{Q}_p}}$ such that for a suitable ordering of $\lambda_1, \ldots, \lambda_n$, the eigenvalues of B' are*

$$\log_\pi(\lambda_1 q^{m_1}), \ldots, \log_\pi(\lambda_n q^{m_n}),$$

where $m_1, \ldots, m_n$ are the Hodge-Tate weights of V, counting multiplicities.

Admitting Theorems 5.2.8 and 5.2.9, we may proceed to prove Proposition 5.2.4 as follows.

Proof of Proposition 5.2.4. We assume that $n > 0$ as the case $n = 0$ is trivial. Choose π used to define $\log_\pi$ such that $\pi \notin \overline{\mathbb{Q}}$. This implies that $\log_\pi(z) \neq 0$ for every $z \in \overline{\mathbb{Q}_p}$ which is algebraic over $\mathbb{Q}$ but is not a root of unity. We may also assume that $K = K'$ so that V is crystalline.
(i) If $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of Φ, then Theorem 5.2.8 shows that there

is an element B in $\mathrm{Lie}(G_V)_{\overline{\mathbb{Q}_p}}$ whose eigenvalues are $\log_\pi(\lambda_1), \ldots, \log_\pi(\lambda_n)$. Let r be a non-negative integer and

$$\{\log_\pi(\xi_1), \ldots, \log_\pi(\xi_r), \log_\pi(\mu_1), \ldots, \log_\pi(\mu_{r+1})\}$$

be a multiset of $2r+1$ eigenvalues of B. We claim that

$$\sum_{j=1}^{r} \log_\pi(\xi_j) \neq \sum_{j=1}^{r+1} \log_\pi(\mu_j).$$

This is equivalent to showing that

$$\log_\pi(\kappa) \neq 0,$$

where

$$\kappa = \mu_{m+1} \prod_{j=1}^{r} \xi_j^{-1} \mu_j.$$

By hypothesis, κ is a q-Weil number of weight $w \neq 0$. Thus κ is an algebraic number which is not a root of unity. Therefore $\log_\pi(\kappa) \neq 0$ as claimed. This shows that the representation $\mathrm{Lie}(G_V)_{\overline{\mathbb{Q}_p}} \hookrightarrow \mathrm{End}(V_{\overline{\mathbb{Q}_p}})$ satisfies the strong Serre criterion. We conclude that V has vanishing G_V-cohomology from Proposition 5.1.5.
(ii) Lemma 5.2.6 implies that $\det \rho = \chi^t$ on an open subgroup of G_K where $t = \sum_{j=1}^{n} m_j = \frac{nw}{2} \neq 0$, as w is odd. By Theorem 5.2.9, there exists an element $B' \in \mathrm{Lie}(H_V)_{\overline{\mathbb{Q}_p}}$ whose eigenvalues are $\log_\pi(\lambda_1 q^{-m_1}), \ldots, \log_\pi(\lambda_n q^{-m_n})$. Let r be a non-negative integer and

$$\{\log_\pi(\xi_1 q^{-a_1}), \ldots, \log_\pi(\xi_r q^{-a_r}), \log_\pi(\mu_1 q^{-b_1}), \ldots, \log_\pi(\mu_1 q^{-b_{r+1}})\}$$

be a multiset of $2r+1$ eigenvalues of B'. Then

$$\sum_{j=1}^{r} \log_\pi(\xi_j q^{-a_j}) - \sum_{l=1}^{r+1} \log_\pi(\mu_j q^{-b_j}) = \log_\pi(\kappa),$$

where

$$\kappa = \mu_{r+1}^{-1} q^{b_{r+1}} \prod_{j=1}^{r} \xi_j \mu_j^{-1} q^{-a_j+b_j}.$$

Since the ξ_j's and the μ_j's are q-Weil numbers of weight w, it follows that κ has archimedean absolute value equal to $q^{\frac{s}{2}}$ where $s = w + 2(b_{r+1} + \sum_{j=1}^{r}(b_j - a_j))$. Since w is odd, we see that κ is a q-Weil number of odd weight s. In particular, $\log_\pi(\kappa) \neq 0$. Therefore the strong Serre criterion holds for the representation $\mathrm{Lie}(H_V)_{\overline{\mathbb{Q}_p}} \to \mathrm{End}(V_{\overline{\mathbb{Q}_p}})$. Again, we conclude from Proposition 5.1.5 that V has vanishing H_V-cohomology. $\square$

5.2.3 Construction of the elements B and B'

We now give the proof of Theorems 5.2.8 and 5.2.9. Throughout this section, $\rho : G_K \to \mathrm{GL}(V)$ is a finite-dimensional semistable representation of G_K over $\mathbb{Q}_p$. As in the previous subsection, $G_V = \rho(G_K)$, $\Delta_V = G_V \cap \mathrm{SL}(V)$. Also, $I_V = \rho(I_K)$. By definition, we have $G_V \subset G_V^{\mathrm{alg}}(\mathbb{Q}_p)$. For each representation $\alpha : G_V^{\mathrm{alg}} \to \mathrm{GL}(V_\alpha)$ in $\mathrm{Rep}_{\mathbb{Q}_p}(G_V^{\mathrm{alg}})$, we obtain a new representation of G_K

$$\rho_\alpha : G_K \xrightarrow{\rho} G_V \subset G_V^{\mathrm{alg}} \xrightarrow{\alpha} \mathrm{GL}(V_\alpha).$$

We write $G_{V_\alpha} = \rho_\alpha(G_K)$.

Proof of Theorem 5.2.8. The proof consists of two steps: the construction of an element of $\mathrm{Lie}(G_V^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}}$ with the desired set of eigenvalues and showing that this element actually belongs to $\mathrm{Lie}(G_V)_{\overline{\mathbb{Q}_p}}$.

<u>Step 1</u>: Let $\alpha : G_V^{\mathrm{alg}} \to \mathrm{GL}(V_\alpha)$ be a representation of G_V^{alg}. Then α gives rise to a homomorphism of algebraic groups $G_V^{\mathrm{alg}} \to G_{V_\alpha}^{\mathrm{alg}}$. Thus, we may identify $\mathrm{Rep}(G_{V_\alpha}^{\mathrm{alg}})$ with a Tannakian sub-category of $\mathrm{Rep}(G_V^{\mathrm{alg}})$. We have two fiber functors over K_0:

$$\begin{aligned} \omega_G : \mathrm{Rep}(G_V^{\mathrm{alg}}) &\longrightarrow \mathrm{Vec}_{K_0} \\ V_\alpha &\longmapsto V_\alpha \otimes_{\mathbb{Q}_p} K_0 \end{aligned}$$

and

$$\begin{aligned} \omega_D : \mathrm{Rep}(G_V^{\mathrm{alg}}) &\longrightarrow \mathrm{Vec}_{K_0} \\ V_\alpha &\longmapsto \mathrm{D}_{\mathrm{st}}(V_\alpha) = (V_\alpha \otimes_{\mathbb{Q}_p} \mathrm{B}_{\mathrm{st}})^{G_K}. \end{aligned}$$

We have an isomorphism $G_{V_\alpha}^{\mathrm{alg}} \simeq \underline{\mathrm{Aut}}^{\otimes}(\omega_G|\,\mathrm{Rep}(G_{V_\alpha}^{\mathrm{alg}}))$ of algebraic groups over K_0, where $\omega_G|\,\mathrm{Rep}(G_{V_\alpha}^{\mathrm{alg}})$ means the restriction of the functor ω_G to the subcategory $\mathrm{Rep}(G_{V_\alpha}^{\mathrm{alg}})$ (cf. Appendix A, Proposition A.4). We define the algebraic groups

$$\begin{aligned} G_D^{\mathrm{alg}} &:= \underline{\mathrm{Aut}}^{\otimes}(\omega_D) \\ G_{D_\alpha}^{\mathrm{alg}} &:= \underline{\mathrm{Aut}}^{\otimes}(\omega_D|\,\mathrm{Rep}(G_{V_\alpha}^{\mathrm{alg}})). \end{aligned}$$

Note that G_D^{alg} and $G_{D_\alpha}^{\mathrm{alg}}$ are both defined over K_0 and $G_{D_\alpha}^{\mathrm{alg}}$ is the image of G_D^{alg} in $\mathrm{GL}(\mathrm{D}_{\mathrm{st}}(V_\alpha))$.

We also define the affine algebraic varieties

$$\begin{aligned} \mathfrak{Is} &:= \underline{\mathrm{Isom}}^{\otimes}(\omega_D, \omega_G), \quad \text{and} \\ \mathfrak{Is}_\alpha &:= \underline{\mathrm{Isom}}^{\otimes}(\omega_D|\,\mathrm{Rep}(G_{V_\alpha}^{\mathrm{alg}}), \omega_G|\,\mathrm{Rep}(G_{V_\alpha}^{\mathrm{alg}})) \end{aligned}$$

Note that $\mathfrak{Is}_\alpha$ is a right torsor under $G^{\mathrm{alg}}_{D_\alpha}$ and a left torsor under $G^{\mathrm{alg}}_{V_\alpha}$.

Each $i = (\eta_{i,X})_{X\in \mathrm{Obj}(\mathrm{Rep}(G^{\mathrm{alg}}_V))} \in \mathfrak{Is}(\overline{\mathbb{Q}_p})$ gives a point $i_\alpha = (\eta_{i_\alpha,X})_{X\in \mathrm{Obj}(\mathrm{Rep}(G^{\mathrm{alg}}_{V_\alpha}))} \in \mathfrak{Is}_\alpha(\overline{\mathbb{Q}_p})$ by restriction to the sub-category $\mathrm{Rep}(G^{\mathrm{alg}}_{V_\alpha})$. In particular, we obtain from the family i_α an isomorphism

$$\eta_{i_\alpha} : \mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \xrightarrow{\simeq} (V_\alpha)_{\overline{\mathbb{Q}_p}} = (V_\alpha \otimes_{\mathbb{Q}_p} K_0) \otimes_{K_0} \overline{\mathbb{Q}_p}. \tag{5.2}$$

If $\xi = (\xi_X)_{X\in \mathrm{Obj}(\mathrm{Rep}(G^{\mathrm{alg}}_V))}$ is a family which lies in $G^{\mathrm{alg}}_{D_\alpha}(\overline{\mathbb{Q}_p})$, then there exists a family $\varsigma = (\varsigma_X)_{X\in \mathrm{Obj}(\mathrm{Rep}(G^{\mathrm{alg}}_V))}$ in $G^{\mathrm{alg}}_{V_\alpha}(\overline{\mathbb{Q}_p})$ such that the following diagram

$$\begin{tikzcd}
\mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \arrow[r, "\eta_{i_\alpha}"] \arrow[d, "\xi_{V_\alpha}"] & (V_\alpha)_{\overline{\mathbb{Q}_p}} \arrow[d, "\varsigma_{V_\alpha}"] \\
\mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \arrow[r, "\eta_{i_\alpha}"] & (V_\alpha)_{\overline{\mathbb{Q}_p}}
\end{tikzcd}$$

is commutative. Hence we see that the isomorphism (5.2) induces an isomorphism of algebraic groups

$$G^{\mathrm{alg}}_{D_\alpha} \times_{K_0} \overline{\mathbb{Q}_p} \underset{f}{\simeq} G^{\mathrm{alg}}_{V_\alpha} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p} \tag{5.3}$$

and an isomorphism of Lie algebras

$$\mathrm{Lie}(G^{\mathrm{alg}}_{D_\alpha}) \otimes_{K_0} \overline{\mathbb{Q}_p} \underset{\mathrm{Lie}(f)}{\simeq} \mathrm{Lie}(G^{\mathrm{alg}}_{V_\alpha}) \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}.$$

If we choose another point i' in $\mathfrak{Is}(\overline{\mathbb{Q}_p})$ so that we have another isomorphism $\eta_{i'_\alpha} : \mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \simeq (V_\alpha)_{\overline{\mathbb{Q}_p}}$, then we obtain a commutative diagram

$$\begin{tikzcd}
 & \mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \arrow[rr, "\eta_{i_\alpha}"] \arrow[dl, "\xi_{V_\alpha}"'] \arrow[dd, "\tau"] & & (V_\alpha)_{\overline{\mathbb{Q}_p}} \arrow[dl, "\varsigma_{V_\alpha}"'] \arrow[dd, "\sigma"] \\
\mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \arrow[rr, crossing over, "\eta_{i_\alpha}" near end] \arrow[dd, "\tau"] & & (V_\alpha)_{\overline{\mathbb{Q}_p}} & \\
 & \mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \arrow[rr, "\eta_{i'_\alpha}" near end] \arrow[dl, "\xi'_{V_\alpha}"'] & & (V_\alpha)_{\overline{\mathbb{Q}_p}} \arrow[dl, "\varsigma'_{V_\alpha}"'] \\
\mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \arrow[rr, "\eta_{i'_\alpha}"] & & (V_\alpha)_{\overline{\mathbb{Q}_p}} \arrow[from=uu, crossing over, "\sigma" near start] &
\end{tikzcd}$$

where all the arrows are isomorphisms. Here σ and ξ'_{V_α} are automorphisms of $(V_\alpha)_{\overline{\mathbb{Q}_p}}$, while τ and ς'_{V_α} are automorphisms of $\mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p}$. From the above diagram, we see that

$$\eta_{i'_\alpha} = \sigma \circ \eta_{i_\alpha} \circ \tau^{-1} \tag{5.4}$$

and that another choice of point i' changes the family ξ or ς by a conjugate. In turn, the isomorphism of algebraic groups $f' : G^{\mathrm{alg}}_{D_\alpha} \otimes_{K_0} \overline{\mathbb{Q}_p} \simeq G^{\mathrm{alg}}_{V_\alpha} \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ is obtained by taking an inner automorphism of $G^{\mathrm{alg}}_{D_\alpha}(\overline{\mathbb{Q}_p})$ or an inner automorphism of $G^{\mathrm{alg}}_{V_\alpha}(\overline{\mathbb{Q}_p})$. The same holds for the isomorphism $\mathrm{Lie}(f')$ of Lie algebras defined by f'.

Since V_α is semistable for each representation α of G^{alg}_V, the filtered (φ, N)-module $\mathrm{D}_{\mathrm{st}}(V_\alpha)$ has the K_0-automorphism $\Phi_\alpha = \varphi^f_\alpha$. Thus, the family $(\Phi_\alpha)_{\alpha \in \mathrm{Obj}(\mathrm{Rep}(G^{\mathrm{alg}}_V))}$ lies in $\underline{\mathrm{Aut}}^{\otimes}(\omega_D)$. So we obtain a canonical element of $G^{\mathrm{alg}}_D(K_0)$, which we will also denote by Φ. Then $\log_\pi(\Phi) \in \mathrm{Lie}(G^{\mathrm{alg}}_D)$. We now fix a point $i \in \mathfrak{Is}(\overline{\mathbb{Q}_p})$ and take α to be the tautological representation $\alpha : G^{\mathrm{alg}}_V \hookrightarrow \mathrm{GL}(V)$. Let $\eta_{i_\alpha} : \mathrm{D}_{\mathrm{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \simeq (V_\alpha \otimes_{\mathbb{Q}_p} K_0) \otimes_{K_0} \overline{\mathbb{Q}_p}$ denote the isomorphism as in (5.2). From this isomorphism we may identify $\mathrm{Lie}(G^{\mathrm{alg}}_D)_{\overline{\mathbb{Q}_p}}$ with a subspace of $\mathrm{End}(V_{\overline{\mathbb{Q}_p}})$. We now define

$$B_i := \eta_{i_\alpha} \circ \log_\pi(\Phi) \circ \eta^{-1}_{i_\alpha}. \tag{5.5}$$

The element B_i lies in $\mathrm{Lie}(G^{\mathrm{alg}}_D)_{\overline{\mathbb{Q}_p}}$ since $\log_\pi(\Phi)$ lies in $\mathrm{Lie}(G^{\mathrm{alg}}_D)$. Therefore B_i belongs to $\mathrm{End}(V_{\overline{\mathbb{Q}_p}})$. By definition, B_i and $\log_\pi(\Phi)$ have the same set of eigenvalues counting multiplicities. If $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of Φ counting multiplicities, then $\log_\pi(\lambda_1), \ldots, \log_\pi(\lambda_n)$ are the eigenvalues of $\log_\pi(\Phi)$ (hence of B_i), counting multiplicities. This completes the first step of the proof.

Step 2: We claim that $B_i \in \mathrm{Lie}(G_V)_{\overline{\mathbb{Q}_p}}$. Let $\bar{\alpha} : G^{\mathrm{alg}}_V \to \mathrm{GL}(V_{\bar{\alpha}})$ be the representation of G^{alg}_V such that $\mathrm{Ker}\,\bar{\alpha} = I^{\mathrm{alg}}_V$. Such a representation exists because I^{alg}_V is a normal subgroup of G^{alg}_V. Then $\rho_{\bar{\alpha}}$ is unramified. We write $\Phi_{\bar{\alpha}} = \varphi^f_{\bar{\alpha}}$ for the K_0-linear endomorphism of the filtered (φ, N)-module $\mathrm{D}_{\mathrm{st}}(V_{\bar{\alpha}})$. The image group $G_{V_{\bar{\alpha}}}$ is topologically generated by the image $\rho_{\bar{\alpha}}(\mathrm{Frob})$ of Frobenius $\mathrm{Frob} \in G_K/I_K$. Moreover, $G^{\mathrm{alg}}_{V_{\bar{\alpha}}}$ is the smallest algebraic subgroup of $\mathrm{GL}(V_{\bar{\alpha}})$ which contains $\rho_{\bar{\alpha}}(\mathrm{Frob})$ and is abelian. Since $\rho_{\bar{\alpha}}(\mathrm{Frob})$ generates a compact subgroup, Proposition 5.2.3 shows that the logarithm $\log(\rho_{\bar{\alpha}}(\mathrm{Frob}))$ is defined and generates the Lie algebra $\mathrm{Lie}(G_{V_{\bar{\alpha}}})$. Now, Theorem 4.1.5 implies that we have $\mathrm{Lie}(I_V) = \mathrm{Lie}(I^{\mathrm{alg}}_V)$. Thus, if $\Pi : \mathrm{Lie}(G^{\mathrm{alg}}_V) \to \mathrm{Lie}(G^{\mathrm{alg}}_{V_{\bar{\alpha}}})$ denotes the natural surjection, then we have

$$\mathrm{Lie}(G_V) = \Pi^{-1}(\mathrm{Lie}(G_{V_{\bar{\alpha}}})). \tag{5.6}$$

Let $\mathrm{Lie}(\bar{\alpha}) : \mathrm{Lie}(G_V^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}} \to \mathrm{Lie}(\mathrm{GL}(V_{\bar{\alpha}}))_{\overline{\mathbb{Q}_p}} = \mathrm{End}(V_{\bar{\alpha}})_{\overline{\mathbb{Q}_p}}$ be the Lie algebra homomorphism induced by $\bar{\alpha}$. It suffices to show that

$$\mathrm{Lie}(\bar{\alpha})(B_i) \in \mathrm{Lie}(G_{V_{\bar{\alpha}}})_{\overline{\mathbb{Q}_p}}. \tag{5.7}$$

Recall from Step 1 that the chosen point $i \in \mathfrak{Is}(\overline{\mathbb{Q}_p})$ gives a point $i_{\bar{\alpha}}$ in $\mathfrak{Is}_{\bar{\alpha}}(\overline{\mathbb{Q}_p})$. Then

$$\mathrm{Lie}(\bar{\alpha})(B_i) = \eta_{i_{\bar{\alpha}}} \circ \log_\pi(\Phi_{\bar{\alpha}}) \circ \eta_{i_{\bar{\alpha}}}^{-1}. \tag{5.8}$$

Let us first show that the right-hand side of (5.8) is the same for any choice of π and any choice of i. Since $\rho_{\bar{\alpha}}$ is unramified, the endomorphism $\Phi_{\bar{\alpha}}$ fixes a lattice. Thus, $\Phi_{\bar{\alpha}}$ generates a compact subgroup of $\mathrm{GL}_{K_0}(\mathrm{D_{st}}(V_{\bar{\alpha}}))$. By Proposition 5.2.3, $\log_\pi(\Phi_{\bar{\alpha}}) = \log(\Phi_{\bar{\alpha}})$ is independent of the choice of π. As $G_{V_{\bar{\alpha}}}^{\mathrm{alg}}$ is abelian, it follows from the isomorphism as in (5.3) that $G_{D_{\bar{\alpha}}}^{\mathrm{alg}} \times_{K_0} \overline{\mathbb{Q}_p}$ is also abelian. Let i' be another choice of point in $\mathfrak{Is}(\overline{\mathbb{Q}_p})$. In view of equation (5.4), for some $\sigma \in \mathrm{Aut}((V_\alpha)_{\overline{\mathbb{Q}_p}})$ and some $\tau \in \mathrm{Aut}(\mathrm{D_{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p})$ we have

$$\begin{aligned}
\eta_{i'_{\bar{\alpha}}} \circ \log(\Phi_{\bar{\alpha}}) \circ \eta_{i'_{\bar{\alpha}}}^{-1} &= \sigma \circ \eta_{i_{\bar{\alpha}}} \circ \tau^{-1} \circ \log(\Phi_{\bar{\alpha}}) \circ \tau \circ \eta_{i_{\bar{\alpha}}}^{-1} \circ \sigma^{-1} \\
&= \sigma \circ \eta_{i_{\bar{\alpha}}} \circ \log(\Phi_{\bar{\alpha}}) \circ \eta_{i_{\bar{\alpha}}}^{-1} \circ \sigma^{-1} \\
&= \eta_{i_{\bar{\alpha}}} \circ \log(\Phi_{\bar{\alpha}}) \circ \eta_{i_{\bar{\alpha}}}^{-1}.
\end{aligned}$$

Thus, the right-hand side of (5.8) is independent of the choice of i. In particular, we see that it is independent of the choice of $i_{\bar{\alpha}}$ in $\mathfrak{Is}_{\bar{\alpha}}(M)$ for any extension M of K_0. We now make a suitable choice of $i_{\bar{\alpha}}$ and M. On applying Proposition 4.3.2 to the unramified representation $\rho_{\bar{\alpha}}$ of G_K in $V_{\bar{\alpha}}$, we have the isomorphism

$$\beta_{\bar{\alpha}} : \mathrm{D_{st}}(V_{\bar{\alpha}}) \otimes_{K_0} \widehat{\mathbb{Q}_p^{\mathrm{nr}}} \simeq V_{\bar{\alpha}} \otimes_{\mathbb{Q}_p} \widehat{\mathbb{Q}_p^{\mathrm{nr}}}$$

and the analogous isomorphisms for all the unramified representations in the Tannakian category generated by $\rho_{\bar{\alpha}}$. We take the point $i_{\bar{\alpha}}$ in $\mathfrak{Is}_{\bar{\alpha}}(\widehat{\mathbb{Q}_p^{\mathrm{nr}}})$ to be the family defined by these isomorphisms and M to be $\widehat{\mathbb{Q}_p^{\mathrm{nr}}}$. Moreover, we know from the said proposition that the K_0-linear endomorphism of $\mathrm{D_{st}}(V_{\bar{\alpha}})$ and the image of Frob under $\rho_{\bar{\alpha}}$ are related via the equation

$$\beta_{\bar{\alpha}} \circ \Phi_{\bar{\alpha}} \circ \beta_{\bar{\alpha}}^{-1} = \rho_{\bar{\alpha}}(\mathrm{Frob}^{-1}). \tag{5.9}$$

Note that $\beta_{\bar{\alpha}}$ also defines an isomorphism $\mathrm{D_{st}}(V_\alpha) \otimes_{K_0} \overline{\mathbb{Q}_p} \simeq (V_\alpha)_{\overline{\mathbb{Q}_p}}$. Taking the logarithm of both sides of (5.9), we obtain from (5.8) that

$$\mathrm{Lie}(\bar{\alpha})(B_i) = \log(\rho_{\bar{\alpha}}(\mathrm{Frob}^{-1})), \tag{5.10}$$

which clearly belongs to $\mathrm{Lie}(G_{V_{\bar{\alpha}}})$. This completes the proof of Theorem 5.2.8. □

Proof of Theorem 5.2.9. Assume that the hypotheses of Theorem 5.2.9 hold for V. Since V is semistable, it is Hodge-Tate. Let $m_1, \ldots, m_n$ denote the Hodge-Tate weights of V. Thus we have a direct sum decomposition

$$V_{\mathbb{C}_p} = \bigoplus_{j=1}^{n} \mathbb{C}_p(m_j). \tag{5.11}$$

This allows us to define a homomorphism of algebraic groups over $\mathbb{C}_p$

$$\mu : \mathbb{G}_m \to I_V^{\mathrm{alg}} \times_{\mathbb{Q}_p} \mathbb{C}_p, \tag{5.12}$$

where, for $c \in \mathbb{C}_p^{\times}$, $\mu(c)$ is the automorphism of $V_{\mathbb{C}_p}$ given by

$$\mu(c)(x) = c^{m_j} x \qquad \text{for all } x \in \mathbb{C}_p(m_j)$$

as j runs over the set $\{1, \ldots, n\}$. Let us fix a point i in $\mathfrak{Is}(\overline{\mathbb{Q}_p})$ and take α again to be the tautological representation $\alpha : G_V^{\mathrm{alg}} \hookrightarrow \mathrm{GL}(V)$. We put

$$\Omega = \eta_{i_\alpha} \circ \Phi \circ \eta_{i_\alpha}^{-1} \in \mathrm{Aut}(V_{\overline{\mathbb{Q}_p}}). \tag{5.13}$$

Clearly, $\Omega \in G_V^{\mathrm{alg}}(\overline{\mathbb{Q}_p})$. We write Ω as a product $\Omega = su = us$, where $s, u \in G_V^{\mathrm{alg}}(\overline{\mathbb{Q}_p})$ such that s is semi-simple and u is unipotent. Let Θ be the smallest algebraic subgroup over $\overline{\mathbb{Q}_p}$ which contains s. It is a multiplicative group since s is semisimple. Replacing K by a finite extension, we may assume that Θ is a torus. Indeed, $\Theta = \Theta^0 \times P$, where Θ^0 is the connected component of Θ and P is a finite group. Then we may replace K by a finite extension K' such that the degree of the residue field extension $k'/\mathbb{F}_p$ is a multiple of the order of P. Let T be the maximal torus of $G_V^{\mathrm{alg}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ containing the torus Θ. We choose a maximal torus in $G_V^{\mathrm{alg}} \times_{\mathbb{Q}_p} \mathbb{C}_p$ containing the image of μ. Since all maximal tori in $G_V^{\mathrm{alg}} \times_{\mathbb{Q}_p} \mathbb{C}_p$ are conjugate, we find an element $g \in G_V^{\mathrm{alg}}(\mathbb{C}_p)$ such that $\mu' = g\mu g^{-1}$ has image in T. Note that the induced map $\mu' : \mathbb{G}_m \to T$ is defined over $\overline{\mathbb{Q}_p}$, so that $\mu'(q) \in T(\overline{\mathbb{Q}_p})$. We use once again the representation $\bar{\alpha} : G_V^{\mathrm{alg}} \to \mathrm{GL}(V_{\bar{\alpha}})$ whose kernel is I_V^{alg}. We have the exact sequence of algebraic groups

$$0 \to I_V^{\mathrm{alg}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p} \to G_V^{\mathrm{alg}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p} \to G_{V_{\bar{\alpha}}}^{\mathrm{alg}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p} \to 0.$$

The torus T acts on $G_V^{\mathrm{alg}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ and its normal subgroup $I_V^{\mathrm{alg}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ by inner automorphisms. Thus it also acts on the quotient $G_{V_{\bar{\alpha}}^{\mathrm{alg}}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ by inner automorphisms. But we saw earlier that $G_{V_{\bar{\alpha}}^{\mathrm{alg}}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ is abelian. Thus, the action of T on $G_{V_{\bar{\alpha}}^{\mathrm{alg}}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ and on its Lie algebra is trivial. Given an algebraic group J over $\overline{\mathbb{Q}_p}$, we write J_u for its unipotent radical and $\mathrm{Lie}(J)_u$ for the corresponding Lie algebra. We have the exact sequence of Lie algebras over $\overline{\mathbb{Q}_p}$

$$0 \to \mathrm{Lie}((I_V^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u \to \mathrm{Lie}((G_V^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u \to \mathrm{Lie}((G_{V_{\bar{\alpha}}}^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u \to 0.$$

The action by inner automorphisms of the torus T on the algebraic groups induces the adjoint action of T on the Lie algebras. As representations of a torus are semisimple and T acts trivially on $\mathrm{Lie}((G_{V_{\bar{\alpha}}}^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u$, we have the exact sequence

$$0 \to H^0(T, \mathrm{Lie}((I_V^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u) \to H^0(T, \mathrm{Lie}((G_V^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u) \to \mathrm{Lie}((G_{V_{\bar{\alpha}}}^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u \to 0.$$

Let u_0 be the image of u in $G_{V_{\bar{\alpha}}}^{\mathrm{alg}} \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ and n' be a lift of $\log(u_0)$ in $H^0(T, \mathrm{Lie}((G_V^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u)$. Put $u' = \exp(n') \in (G_V^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}})_u$. It is clear that u' commutes with the elements of T, particularly with s and $\mu'(q)$. We now take

$$B' := \log_\pi(s \cdot \mu'(q) \cdot u'). \tag{5.14}$$

Since u' is unipotent, the eigenvalues of s are precisely the eigenvalues $\lambda_1, \dots, \lambda_n$ of Φ and the eigenvalues of $\mu'(q)$ are the Hodge-Tate weights $m_1, \dots, m_n$ of V, it follows that the eigenvalues of B' are

$$\log_\pi(\lambda_1 q^{m_1}), \dots, \log_\pi(\lambda_n q^{m_n})$$

for a suitable ordering of $\lambda_1, \dots, \lambda_n$. Since B and B' have the same image in $\mathrm{Lie}(G_{V_{\bar{\alpha}}}^{\mathrm{alg}})_{\overline{\mathbb{Q}_p}}$, Theorem 5.2.8 and (5.7) implies that B' lies in $\mathrm{Lie}(G_{V_{\bar{\alpha}}})_{\overline{\mathbb{Q}_p}}$. Letting $\delta = \det \Phi = \prod_{j=1}^n \lambda_j$ and $t = \sum_{j=1^n} m_j$, we see that the trace of B' is

$$\begin{aligned}\mathrm{tr}(B') &= \sum_{j=1}^n \log_\pi(\lambda_j q^{m_j}) = \log_\pi(\prod_{j=1}^n \lambda_j q^{m_j}) \\ &= \log_\pi(\delta q^t) = \log_\pi(\delta) - \log_\pi(q^{-t}) = 0\end{aligned}$$

where the last equality follows from Lemma 5.2.5. Therefore B' lies in $\mathrm{Lie}(\Delta_V)_{\overline{\mathbb{Q}_p}}$ as desired. □

5.3 ℓ-adic case

Let ℓ be a prime not equal to p.

Definition 5.3.1. Let w be an integer. An ℓ-adic representation $\rho_\ell : G_K \to \mathrm{GL}_{\mathbb{Q}_\ell}(W)$ is said to be *pure of weight* w if the characteristic polynomial of $\rho_\ell(\mathrm{Frob})$ has coefficients in $\mathbb{Q}$ and the eigenvalues of $\rho_\ell(\mathrm{Frob})$ are q-Weil numbers of weight w.

Consider a proper smooth variety X over K with potential good reduction and the ℓ-adic representation $\rho_\ell : G_K \to \mathrm{GL}(V_\ell)$ of G_K given by the ith ℓ-adic étale cohomology group $V_\ell = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell)$. Replacing K by a finite extension, we may assume that X has good reduction over K. Then X has a proper smooth model $\mathcal{X} \to \mathrm{Spec}(\mathcal{O}_K)$. Let $\mathcal{Y} = \mathcal{X} \otimes_{\mathcal{O}_K} k$ and $\mathcal{Y}_{\overline{k}} = \mathcal{Y} \otimes_k \overline{k}$. Then we have the following (cf. [Ja10], §4)

Proposition 5.3.2. *For any prime $\ell \neq p$, we have a canonical isomorphism*

$$H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell) \simeq H^i_{\text{ét}}(\mathcal{Y}_{\overline{k}}, \mathbb{Q}_\ell)$$

which is compatible with the actions of G_K and $G_k := \mathrm{Gal}(\overline{k}/k)$.

Since $G_k \simeq G_K/I_K$, the above proposition shows that for any $\ell \neq p$, the representation V_ℓ is unramified after a finite extension.

Corollary 5.3.3. *For any prime $\ell \neq p$, the representation V_ℓ is pure of weight i.*

Proof. The Weil conjectures (cf. [De74], [De80]) imply that the characteristic polynomial of the image of Frobenius in G_k acting on $H^i_{\text{ét}}(\mathcal{Y}_{\overline{k}}, \mathbb{Q}_\ell)$ has coefficients in $\mathbb{Q}$ and its eigenvalues are q-Weil numbers of weight i, whence the corollary. $\square$

Theorem 5.3.4. *Let X be a proper smooth variety with potential good reduction over K. Let i be a positive integer. Then for any $\ell \neq p$, $V_\ell = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell)$ has vanishing G_ℓ-cohomology.*

Proof. Since V_ℓ is unramified, G_ℓ is topologically generated by the image $\rho_\ell(\mathrm{Frob})$ of Frobenius $\mathrm{Frob} \in G_K/I_K$. As $\rho_\ell(\mathrm{Frob})$ generates a compact subgroup of $\mathrm{GL}(V_\ell)$, Proposition 5.2.3 shows that the logarithm $\log(\rho_\ell(\mathrm{Frob}))$ is defined and it belongs to $\mathrm{Lie}(G_\ell)$. Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of $\rho_\ell(\mathrm{Frob})$, where $n = \dim_{\mathbb{Q}_\ell} V_\ell$. These are q-Weil numbers of weight i. Then the eigenvalues of $\log(\rho_\ell(\mathrm{Frob}))$ are

$$\log(\lambda_1), \ldots, \log(\lambda_n).$$

Let $r \in \mathbb{Z}_{\geq 1}$ and take a multiset $\{\log(\xi_1), \ldots, \log(\xi_r), \log(\mu_1), \ldots, \log(\mu_{r+1})\}$ of $2r+1$ eigenvalues of $\log(\rho_\ell(\mathrm{Frob}))$. Then

$$\sum_{j=1}^{r+1} \log(\mu_j) - \sum_{j=1}^{r} \log(\xi_j) = \log\left(\prod_{j=1}^{r+1} \mu_j\right) - \log\left(\prod_{j=1}^{r} \xi_j\right) = \log(\kappa).$$

where $\kappa = \prod_{j=1}^{r} \xi^{-1}\mu_j\mu_{r+1}$. Since κ is a q-Weil number of positive weight i, $\log(\kappa) \neq 0$. Thus the representation $\mathrm{Lie}(G_\ell)_{\overline{\mathbb{Q}_\ell}} \to \mathrm{End}(V_\ell)_{\overline{\mathbb{Q}_\ell}}$ satisfies the strong Serre criterion and the result follows from Proposition 5.1.5. □

5.4 Global setting

We give the proof of Theorem 3. Its proof uses the following result by Bogomolov.

Proposition 5.4.1 ([Bo80], Corollaire of Théorème 1). *Let $\rho : G_F \to \mathrm{GL}(V)$ be a p-adic representation of G_F. Assume that for every place v of F lying above p, the restriction $\rho_v : \mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{GL}(V)$ of ρ to the decomposition subgroup $\mathrm{Gal}(\overline{F}_v/F_v)$ of a place $\overline{v}$ of $\overline{F}$ lying above v is a Hodge-Tate representation. Then $\mathrm{Lie}(G_V) = \mathrm{Lie}(G_V^{\mathrm{alg}})$.*

Consequently, we have the following

Proposition 5.4.2 ([Su00], Proposition 2.8). *Let X be a proper smooth variety over a number field F. Let i be an integer. Put $V = H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_p)$ and consider the Galois representation $\rho : G_F \to \mathrm{GL}(V)$. Let $G_V \subseteq \mathrm{GL}(V)$ be the image of ρ. Then the Lie algebra $\mathrm{Lie}(G_V)$ of G_V contains the homotheties.*

Proof. As discussed in Example 4.1.3, the representation V satisifies the hypothesis of Proposition 5.4.1. On the other hand, $\mathrm{Lie}(G_V^{\mathrm{alg}})$ contains the homotheties by a remark of Deligne (cf. [Se76], §2.3). This proves the proposition. □

Proposition 5.4.3 ([OT14], Proposition 2.5). *Let X be a proper smooth variety over a number field F. Let i be an integer. Let V be the $\mathbb{Q}_p$-linear dual of $H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_p)$ and put $n = \dim_{\mathbb{Q}_p} V$. Then $\det(V)$ is isomorphic to the twist of $\mathbb{Q}_p(in/2)$ by a character ε of order at most 2. If i is odd, then $\varepsilon = 1$.*

This is a global version of Lemma 5.2.6 for the étale cohomology group of a proper smooth variety. As in Remark 5.2.7, Proposition 5.4.3 implies that $\mathrm{Lie}(H_V) = \mathrm{Lie}(G_V \cap \mathrm{SL}(V))$. It also implies that the field extension $F(\mu_{p^\infty})$ is of finite degree over $F(V) \cap F(\mu_{p^\infty})$.

Proof of Theorem 3. Fix a place v of F which lies above p. Let $n = \dim_{\mathbb{Q}_p} V = \dim_{\mathbb{C}_p} V_{\mathbb{C}_p}$ and $t_0, t_{-1}, \dots, t_{-i}$ be the multiplicities of the Hodge-Tate weights $0, -1, \dots, -i$, respectively of the representation $\rho_v : G_{F_v} \to \mathrm{GL}(V)$ obtained by restriction to the decomposition subgroup of v. Let I_V be the image under ρ_v of the inertia subgroup of $G_{\overline{F}_v}$. We fix a basis of V over $\mathbb{Q}_p$. Theorem 4.1.4 provides an element $\Psi \in \mathrm{Lie}(I_V) \otimes_{\mathbb{Q}_p} \mathbb{C}_p \subseteq \mathrm{Lie}(G_V) \otimes_{\mathbb{Q}_p} \mathbb{C}_p$ which, when viewed as an element of $\mathrm{End}(V_{\mathbb{C}_p})$, is an $n \times n$-matrix with square diagonal submatrices along the diagonal of the following shape:

$$\Psi = \begin{pmatrix} \begin{bmatrix} 0 & & \\ & \ddots & \\ & & 0 \end{bmatrix} & & & & \\ & \begin{bmatrix} -1 & & \\ & \ddots & \\ & & -1 \end{bmatrix} & & & \\ & & \ddots & & \\ & & & \begin{bmatrix} -i+1 & & \\ & \ddots & \\ & & -i+1 \end{bmatrix} & \\ & & & & \begin{bmatrix} -i & & \\ & \ddots & \\ & & -i \end{bmatrix} \end{pmatrix}. \tag{5.15}$$

Here the square submatrix $\begin{bmatrix} -j & & \\ & \ddots & \\ & & -j \end{bmatrix}$ is of size t_{-j}, for $j = 0, 1, \ldots, i$.

The set of eigenvalues of Ψ is

$$\mathbb{e}(\Psi) = \{-j | 0 \leq j \leq i\}.$$

Moreover, an integer $-j$ occurs t_{-j} times in $\mathbb{e}(\Psi)$.

Let I_n be the $n \times n$ identity matrix and let t be an element of $\mathbb{Q}_p$ that is not a rational number. Consider the $n \times n$ diagonal matrix

$$A = tI_n$$

Proposition 5.4.2 implies that A belongs to $\mathrm{Lie}(G_V)$ and thus to $\mathrm{Lie}(G_V) \otimes_{\mathbb{Q}_p} \mathbb{C}_p$. Put $B = \Psi + A$. This clearly belongs to $\mathrm{Lie}(G_V) \otimes_{\mathbb{Q}_p} \mathbb{C}_p$. The set of eigenvalues of B is

$$\mathbb{e}(B) = \{-j + t | 0 \leq j \leq i\}.$$

We now verify that the strong Serre criterion is satisfied for $\mathrm{Lie}(G_V)_{\mathbb{C}_p} \to \mathrm{End}(V_{\mathbb{C}_p})$. Let r be a non-negative integer and choose $2r+1$ eigenvalues of B. We must show that

$$(-j_1 + t) + \ldots + (-j_r + t) \neq (-k_1 + t) + \ldots + (-k_{r+1} + t),$$

where $j_1, \ldots, j_r, k_1, \ldots, k_{r+1}$ are non-negative integers less than or equal to i and $t \in \mathbb{Q}_p \setminus \mathbb{Q}$. But this is equivalent to showing that

$$t \neq \sum_{s=1}^{r+1} k_s - \sum_{s=1}^{r} j_s,$$

which clearly holds as the right-hand side is a rational integer but the left-hand side is not. It follows from Proposition 5.1.5 that V has vanishing G_V-cohomology.

We now restrict to the case where i is odd. We claim that B belongs to $\mathrm{Lie}(\Delta_V) \otimes_{\mathbb{Q}_p} \mathbb{C}_p$, where $\Delta_V = G_V \cap \mathrm{SL}(V)$. Note that $\mathrm{Lie}(\Delta_V) = \mathrm{Lie}(H_V)$ by Proposition 5.4.3. Note that $t_{-j} = t_{-(i-j)}$, for $j = 0, \ldots, i$ (cf. Example 4.1.3), and that $\sum_{j=0}^{i} t_{-j} = n$. Since i is odd, we have

$$2\left(t_0 + t_{-1} + \ldots + t_{-\frac{i-1}{2}}\right) = n.$$

The trace of the matrix Ψ is

$$\begin{aligned}
\mathrm{tr}(\Psi) &= -\sum_{0 \leq j \leq i} j t_{-j} \\
&= -\left(t_0(0+i) + t_{-1}(1+(i-1)) + \ldots + t_{-\frac{i-1}{2}}\left(\frac{i-1}{2} + \frac{i+1}{2}\right)\right) \\
&= -i\left(t_0 + t_{-1} + \ldots + t_{-\frac{i-1}{2}}\right) \\
&= -\frac{in}{2}
\end{aligned}$$

Therefore

$$\mathrm{tr}(B) = \mathrm{tr}(\Psi) + \mathrm{tr}(A) = -\frac{in}{2} + n\left(\frac{i}{2}\right) = 0,$$

which proves the claim. Therefore V has vanishing H_V-cohomology. □

Chapter 6

Almost independence of systems of representations

6.1 Goursat's Lemma and some of its consequences

Let $\varphi_1 : G \to G_1$ and $\varphi_2 : G \to G_2$ be continuous representations of a profinite group G into locally compact groups G_1 and G_2, respectively. Consider the continuous homomorphism $\varphi = (\varphi_1, \varphi_2) : G \to \varphi_1(G) \times \varphi_2(G)$. Let $\pi_1 : \varphi(G) \twoheadrightarrow \varphi_1(G)$ and $\pi_2 : \varphi(G) \twoheadrightarrow \varphi_2(G)$ denote the projections of $\varphi(G)$ to $\varphi_1(G)$ and $\varphi_2(G)$, respectively. Let $N_1 = \operatorname{Ker} \pi_2$ and $N_2 = \operatorname{Ker} \pi_1$. Then $N_1 = \varphi(G) \cap (\varphi_1(G) \times \{1\})$ and $N_2 = \varphi(G) \cap (\{1\} \times \varphi_2(G))$. Thus we may identify N_1 (resp. N_2) with a normal subgroup of $\varphi_1(G)(= \varphi_1(G) \times \{1\})$ (resp. $\varphi_2(G)(= \{1\} \times \varphi_2(G))$). So we have a diagram

$$\begin{tikzcd}
\varphi_1(G) \arrow[d] & \varphi(G) \arrow[l, two heads, "\pi_1"'] \arrow[r, two heads, "\pi_2"] \arrow[d] & \varphi_2(G) \arrow[d] \\
\varphi_1(G)/N_1 & \varphi(G)/(N_1.N_2) \arrow[l] \arrow[r] & \varphi_2(G)/N_2
\end{tikzcd} \tag{6.1}$$

where $N_1.N_2$ denotes the subgroup generated by N_1 and N_2. The following result is well-known.

Lemma 6.1.1 (Goursat's Lemma)**.** *Consider the above situation. Then*
(1) $\varphi(G)/(N_1.N_2) \simeq \varphi_i(G)/N_i$ *for* $i = 1, 2$*;*
(2) We have an isomorphism $\varphi(G) \simeq \varphi_1(G) \times_C \varphi_2(G)$*, from diagram (6.1), where* $C = \varphi(G)/(N_1.N_2)$*.*

Proof. See, for example, Lemma 5.2.1 in [Ri76]. □

In the above situation, let $A_1' := \operatorname{Ker}\varphi_2$ and $A_2' := \operatorname{Ker}\varphi_1$. Then we have the following

Corollary 6.1.2. *The homomorphism $\varphi = (\varphi_1, \varphi_2)$ is surjective if and only if $G = A_1'.A_2'$.*

Proof. ($\Leftarrow$) Assume that $G = A_1'.A_2'$. Let $h = (h_1, h_2)$ be an element of $\varphi_1(G) \times \varphi_2(G)$. Then there exists $g_i \in G$ such that $\varphi_i(g_i) = h_i$ for $i = 1, 2$. For $i = 1, 2$, we write

$$g_i = \prod_j g_{i,j}' g_{i,j}'', \qquad \text{where } g_{i,j}' \in A_1' \text{ and } g_{i,j}'' \in A_2'.$$

Let $g_1' = \prod_j g_{1,j}' \in A_1'$ and $g_2' = \prod_j g_{2,j}'' \in A_2'$. Put $g := g_1'g_2'$. Then

$$\begin{aligned}\varphi(g) &= (\varphi_1(g), \varphi_2(g)) = (\varphi_1(g_1'g_2'), \varphi_2(g_1'g_2')) \\ &= (\varphi_1(g_1'), \varphi_2(g_2')) = (\varphi(g_1), \varphi(g_2)) \\ &= h.\end{aligned}$$

Therefore φ is surjective.
($\Rightarrow$) Clearly $A_1'.A_2' \subseteq G$. Suppose φ is surjective. Goursat's Lemma implies that $\varphi(G) = N_1.N_2$, $N_1 = \varphi_1(G) \times \{1\}$ and $N_2 = \{1\} \times \varphi_2(G)$. Then if $g \in G$, we may write its image under φ as

$$\varphi(g) = \prod_j h_j h_j'$$

where $h_j \in N_1$ and $h_j' \in N_2$. For each j we can find g_j (resp. g_j') in G such that $\varphi(g_j) = h_j$ (resp. $\varphi(g_j') = h_j'$). In fact, $g_j \in A_1'$ and $g_j' \in A_2'$. Hence, g can be written as as a product of the g_j's and g_j''s and some factors belonging to $\operatorname{Ker}\varphi = A_1' \cap A_2'$. Therefore $g \in A_1'.A_2'$, which shows that $G = A_1'.A_2'$. □

Corollary 6.1.3. *The group $\varphi(G)$ is open (that is, a closed subgroup of finite index) in $\varphi_1(G) \times \varphi_2(G)$ if and only if $A_1'.A_2'$ is open in G.*

Proof. Put $H = \varphi_1(G) \times \varphi_2(G)$. We identify N_i with a normal subgroup of $\varphi_i(G)$ for $i = 1, 2$. The diagram (6.1) and Goursat's Lemma give us an isomorphism $\psi : \varphi_1(G)/N_1 \simeq \varphi_2(G)/N_2$. Then the map $f : H/\varphi(G) \to \varphi_2(G)/N_2$ given by $f(h_1, h_2) := \bar{h}_2\psi(\bar{h}_1)^{-1}$ defines an isomorphism from $H/\varphi(G)$ to $\varphi_2(G)/N_2$. Here, the $\bar{(\cdot)}$ denotes the image of $(\cdot)$ in the quotient group. Thus $[H : \varphi(G)]$ is finite if and only if $[\varphi_2(G) : N_2]$ (equivalently $[\varphi_1(G) : N_1]$) is finite. If $\varphi(G)$ is open in H, then $N = N_1 \times N_2$ is open in

H. Thus, N is open in $\varphi(G)$. Since $G \to \varphi(G)$ is surjective and continuous, the inverse image U of N by φ is an open subgroup of G which maps to N. Then we see that

$$\varphi_1(U) \times \varphi_2(U) \subseteq N_1 \times N_2 = N = \varphi(U).$$

Therefore, $\varphi|_U = (\varphi_1|_U, \varphi_2|_U)$ maps U onto $\varphi_1(U) \times \varphi_2(U)$. Letting $A_1'' := \operatorname{Ker} \varphi_2|_U$ and $A_2'' := \operatorname{Ker} \varphi_1|_U$, Corollary 6.1.2 shows that $U = A_1''.A_2''$. We clearly have $U \subseteq A_1'.A_2' \subseteq G$ and since U is open in G, we see that $A_1'.A_2'$ is open in G. Conversely, if $A = A_1'.A_2'$ is open in G then $\varphi_1(A)$ (resp. $\varphi_2(A)$) is an open subgroup of $\varphi_1(G)$ (resp. $\varphi_2(G)$). Corollary 6.1.2 shows that $\varphi(A) = \varphi_1(A) \times \varphi_2(A)$, so $\varphi(A)$ is an open subgroup of H. We see that $\varphi(G)$ is open in H from the inclusion:

$$\varphi(A) \subseteq \varphi(G) \subseteq H.$$

□

6.2 Almost independent systems of representations

Let G be a profinite group and $(\varrho_i : G \to G_i)_{i \in I}$ be a system of continuous homomorphisms of G into a locally compact group G_i. This system defines a continuous homomorphism $\varrho = (\varrho_i)_{i\in I} : G \to \prod_{i \in I} G_i$ where the product is endowed with the product topology. Following Serre we make the following

Definition 6.2.1 ([Se13], §1)**.** The system $(\varrho_i)_{i\in I}$ is said to be *independent* if $\varrho(G) = \prod_{i\in I} \varrho_i(G)$. We say that it is *almost independent* if there exists an open subgroup Γ in G such that $\varrho(\Gamma) = \prod_{i\in I} \varrho_i(\Gamma)$.

Remark 6.2.2. (1) Let φ_1 and φ_2 be continuous representations of a profinite group G as above. Consider the continuous homomorphism $\varphi = (\varphi_1, \varphi_2) : G \to \varphi_1(G) \times \varphi_2(G)$. The following statements are equivalent:
(i) (φ_1, φ_2) is almost independent;
(ii) $\varphi(G)$ is an open subgroup of $\varphi_1(G) \times \varphi_2(G)$;
(iii) $C = \varphi(G)/(N_1.N_2)$ is finite (see §6.1 for the definition of N_1 and N_2).
We clearly have (ii) ⇔ (iii) as the cardinality of C equals the index of $\varphi(G)$ in $\varphi_1(G) \times \varphi_2(G)$. The equivalence (i) ⇔ (ii) follows from Corollary 6.1.3.

(2) Let $(\varrho_i)_{i\in I}$ be a system of continuous homomorphisms of a profinite group G into a locally compact group G_i and ϱ be the continuous homomorphism defined by their product as in the definition above. Let S be a subset

of I and put $S' = I \setminus S$. We consider the subsystem $(\varrho_i)_{i\in\bullet}$ and the homomorphism $\varrho_\bullet$ given by the product, where $\bullet = S, S'$. If $(\varrho_i)_{i\in I}$ is independent, then $(\varrho_S, \varrho_{S'})$ is independent. Indeed, since subsystems of an independent system are independent (cf. [Se13], §1), the systems $(\varrho_i)_{i\in\bullet}$ are independent (where $\bullet = S, S'$). Then the equalities $\varrho(G) = \prod_{i\in S}\varrho_i(G) \times \prod_{i\in S'}\varrho_i(G) = \varrho_S(G) \times \varrho_{S'}(G)$ imply the surjectivity of $\varrho = \varrho_S \times \varrho_{S'} : G \to \varrho_S(G) \times \varrho_{S'}(G)$.

(3) Applying (1) to the situation of (2), we have $\varrho(G) = \varrho_S(G) \times_C \varrho_{S'}(G)$ with finite C as in (1).

(3) Note that the converse of the observation in (3) does not hold: if the group C in the fiber product $\varrho_S \times_C \varrho_{S'}$ is finite, the system $(\varrho_i)_{i\in S\cup S'}$ may not be almost independent. For instance, we may consider $\varrho_S = \varrho_1 \times \varrho_1$ and $\varrho_{S'} = \varrho_2$ with finite C in $\varrho_S \times_C \varrho_{S'}$. But then it is clear that $(\varrho_1, \varrho_1, \varrho_2)$ is not almost independent.

Suppose the index set I is a set of prime numbers. For $\ell \in I$, assume that the $\varrho_\ell : G \to G_\ell$ is a continuous homomorphism of the profinite group G on a compact ℓ-adic Lie group G_ℓ. In this setting Serre gave a useful criterion for determining almost independence of systems of representations comprised of such homomorphisms.

Lemma 6.2.3 ([Se13], §7.2, Lemma 3)**.** *If there exists a finite subset J of I such that the system $(\varrho_\ell)_{\ell\in I\setminus J}$ is almost independent then the system $(\varrho_\ell)_{\ell\in I}$ is almost independent.*

The next result is a consequence of Theorem 1 of [Se13] which made use of Lemma 6.2.3. Serre proved it in the case of abelian varieties and conjectured that the result should also hold in the general case of separated schemes of finite type. Illusie [Il10] showed that it can indeed be generalized.

Theorem 6.2.4 ([Se13], §3.1; [Il10], Corollaire 4.4)**.** *Let X be a separated scheme of finite type over a number field F and i be a non-negative integer. Put $V_\ell = H^i_{\acute{e}t}(X_{\overline{F}}, \mathbb{Q}_\ell)$. Then the system $(\rho_\ell : G_F \to \mathrm{GL}(V_\ell))_{\ell\in\Lambda}$ is almost independent.*

Remark 6.2.5. In general, we need a finite extension F' of F so that the system $(\rho_\ell|_{G_{F'}})$ is independent. This is observed in the case where $S = \Lambda$ and $X = E$ is an elliptic curve which has complex multiplication over $\overline{F}$ with CM field $\mathbb{Q}(\sqrt{d})$ such that $\sqrt{d} \notin F$. Also note that there are examples of elliptic curves without complex multiplication such that ρ_ℓ is surjective for all prime ℓ but ρ_Λ is not (so the system $(\rho_\ell)_{\ell\in\Lambda}$ is not independent). This is illustrated by the following example.

Example 6.2.6. Consider the system $(\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell))_{\ell\in\Lambda}$ associated with the elliptic curve E over $\mathbb{Q}$ of conductor 1728 with minimal Weierstrass model $y^2 = x^3+6x-2$. It has no complex multiplication and its discriminant is $\Delta = -2^6 3^5$. This curve was considered in §5.9.2 of [Se72], where it was verified that the mod ℓ representation $\overline{\rho}_\ell$ associated with E is surjective for all ℓ. A group-theoretic result (cf. e.g. [Gr10], Corollary 2.13-(iii)) implies that ρ_ℓ is surjective for all $\ell \geq 5$. The proof for the surjectivity of ρ_ℓ for $\ell = 2, 3$ was carried out in §I-7 of [LT76]. Hence ρ_ℓ is surjective for all ℓ. But $\sqrt{\Delta} \in \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cyc}}$, where $\mathbb{Q}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathbb{Q}$. Therefore, ρ is not surjective by Theorem 1.2 of [Gr10]. This shows that the system $(\rho_\ell)_{\ell\in\Lambda}$ is not independent.

6.3 Restrictions and Quotients of independent systems

We show that the independence of a system is inherited by the system of representations obtained by restriction to a closed normal subgroup and by its corresponding system of quotients. Consider a system $(\varrho_i)_{i\in I}$ as above. Let H be a closed normal subgroup of G. For each $i \in I$, we define the continuous homomorphism $\pi_i : \varrho_i(G) \to \bar{G}_i := \varrho_i(G)/\varrho_i(H)$ of compact groups. Then we obtain new systems of representations:

$$(\varrho_i|_H : H \to G_i)_{i\in I}$$

obtained by restriction of the ϱ_i's ($i \in I$) to H and

$$(\bar{\varrho}_i : G \xrightarrow{\varrho_i} \varrho_i(G) \xrightarrow{\pi_i} \bar{G}_i)_{i\in I}.$$

Write $\bar{\varrho} = \prod_{i\in I} \bar{\varrho}_i$.

Lemma 6.3.1. *Let $(\varrho_i)_{i\in I}$ be a system of representations of a profinite group G. Let H be a closed normal subgroup of G. Then $(\varrho_i)_{i\in I}$ is independent if and only if the systems $(\varrho_i|_H)_{i\in I}$ and $(\bar{\varrho}_i)_{i\in I}$ are independent.*

Proof. By definition of $\bar{\varrho}$, we have the following commutative diagram of (compact) topological groups with exact rows

$$\begin{tikzcd}
1 \arrow[r] & \varrho(H) \arrow[r] \arrow[d, "\alpha"] & \varrho(G) \arrow[r] \arrow[d, "\beta"] & \bar{\varrho}(G) \arrow[r] \arrow[d, "\gamma"] & 1 \\
1 \arrow[r] & \prod_{i\in I} \varrho_i(H) \arrow[r] & \prod_{i\in I} \varrho_i(G) \arrow[r, "\prod_{i\in I} \pi_i"] & \prod_{i\in I} \bar{\varrho}_i(G) \arrow[r] & 1
\end{tikzcd} \tag{6.2}$$

where the maps α, β and γ are injective by definition. The five lemma shows that the independence of the systems $(\varrho_i|_H)_{i\in I}$ and $(\bar{\varrho}_i)_{i\in I}$ implies the independence of $(\varrho_i)_{i\in I}$. Conversely if $(\varrho_i)_{i\in I}$ is independent; that is, β is an isomorphism, then the five lemma applied to the commutative diagram obtained by taking the first four terms of diagram (6.2) and adding trivial groups on the left end implies that the system $(\varrho_i|_H)_{i\in I}$ is independent. Applying the same argument to the commutative diagram obtained by taking the last four terms of diagram (6.2) and adding trivial groups on the right end implies that the system $(\bar{\varrho}_i)_{i\in I}$ is independent.

□

Now let us consider the case where the profinite group G in the definition above is the absolute Galois group G_F of a number field F and the index set I is the set Λ of all primes. Consider a system of continuous representations $(\varrho_\ell)_{\ell\in\Lambda} := (\varrho_\ell : G_F \to G_\ell)_{\ell\in\Lambda}$ of G_F into a locally compact ℓ-adic Lie group G_ℓ (e.g., $G_\ell = \mathrm{GL}_n(\mathbb{Q}_\ell)$). For each $\ell \in \Lambda$, let $F_\ell = \overline{F}^{\mathrm{Ker}\,\varrho_\ell}$, the fixed subfield of $\overline{F}$ by the kernel of ϱ_ℓ. Since G_F is compact, the Galois group $\mathrm{Gal}(F_\ell/F) \simeq \varrho_\ell(G_F)$ is a compact ℓ-adic Lie group. We write $\varrho_\Lambda = \prod_{\ell\in\Lambda} \varrho_\ell$ and F_Λ for the compositum of all F_ℓ as ℓ runs over the elements of Λ. The field F_Λ is the fixed subfield of $\overline{F}$ by the kernel of ϱ_Λ. We let F^{cyc} be the field extension obtained by adjoining to F all roots of unity.

Lemma 6.3.2. *Let $(\varrho_\ell)_{\ell\in\Lambda}$ be a system as above. Assume the following condition:*

$$F_\ell \supset F(\mu_{\ell^\infty}) \qquad \text{for each} \qquad \ell \in \Lambda. \tag{$*$}$$

For $\ell \in \Lambda$, let $N_\ell = F_\ell \cap F^{\mathrm{cyc}}$. Then
(i) if the system $(\varrho_\ell)_{\ell\in\Lambda}$ is independent then $N_\ell = F(\mu_{\ell^\infty})$ for each $\ell \in \Lambda$;
(ii) if the system $(\varrho_\ell)_{\ell\in\Lambda}$ is almost independent then $N_\ell/F(\mu_{\ell^\infty})$ is a finite extension for each $\ell \in \Lambda$.

Remark 6.3.3. The condition $(*)$ implies that F_Λ contains the field F^{cyc}.

Proof. Statement (ii) follows from (i) after replacing F by a suitable finite extension. For the proof of (i), we apply Lemma 6.3.1 to the system $(\rho_\ell)_{\ell\in\Lambda}$ with $H = G_{F^{\mathrm{cyc}}}$. Then we may identify diagram (6.2) with the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(F_\Lambda/F^{\mathrm{cyc}}) \arrow[r] \arrow[d] & \mathrm{Gal}(F_\Lambda/F) \arrow[r] \arrow[d] & \mathrm{Gal}(F^{\mathrm{cyc}}/F) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \prod_{\ell\in\Lambda} \mathrm{Gal}(F_\ell/N_\ell) \arrow[r] & \prod_{\ell\in\Lambda} \mathrm{Gal}(F_\ell/F) \arrow[r] & \prod_{\ell\in\Lambda} \mathrm{Gal}(N_\ell/F) \arrow[r] & 1
\end{tikzcd} \tag{6.3}$$

By hypothesis and Lemma 6.3.1, diagram (6.3) gives an isomorphism $\mathrm{Gal}(F^{\mathrm{cyc}}/F) \simeq \prod_{\ell\in\Lambda} \mathrm{Gal}(N_\ell/F)$. Since $\mathrm{Gal}(F^{\mathrm{cyc}}/F) \simeq \prod_{\ell\in\Lambda} \mathrm{Gal}(F(\mu_{\ell^\infty})/F)$ we get an isomorphism

$$\prod_{\ell\in\Lambda} \mathrm{Gal}(F(\mu_{\ell^\infty})/F) \simeq \prod_{\ell\in\Lambda} \mathrm{Gal}(N_\ell/F). \tag{6.4}$$

Let $\ell' \in \Lambda$. Taking the composition of (6.4) with the projection $\prod_{\ell\in\Lambda} \mathrm{Gal}(N_\ell/F) \twoheadrightarrow \mathrm{Gal}(N_{\ell'}/F)$ to the ℓ'-th component, we obtain a surjective homomorphism

$$\prod_{\ell\in\Lambda} \mathrm{Gal}(F(\mu_{\ell^\infty})/F) \twoheadrightarrow \mathrm{Gal}(N_{\ell'}/F). \tag{6.5}$$

The independence of the system $(\varrho_\ell)_{\ell\in\Lambda}$ means that the fields $(F_\ell)_{\ell\in\Lambda}$ are linearly disjoint over F. That is, if $\ell \neq \ell'$ then $F = F_\ell \cap F_{\ell'} \supset F(\mu_{\ell^\infty}) \cap N_{\ell'}$. So $F(\mu_{\ell^\infty}) \cap N_{\ell'} = F$ whenever ℓ differs from ℓ'. This implies that the image of $\prod_{\ell\in\Lambda\setminus\{\ell'\}} \mathrm{Gal}(F(\mu_{\ell^\infty})/F)$ in $\mathrm{Gal}(N_{\ell'}/F)$ under the map (6.5) is trivial. Hence, (6.5) factors through $\mathrm{Gal}(F(\mu_{\ell'^\infty})/F) \twoheadrightarrow \mathrm{Gal}(N_{\ell'}/F)$. On the other hand we clearly have a surjection $\mathrm{Gal}(N_{\ell'}/F) \twoheadrightarrow \mathrm{Gal}(F(\mu_{\ell'^\infty})/F)$ because $F(\mu_{\ell'^\infty})$ is contained in $N_{\ell'}$. Therefore we have $\mathrm{Gal}(F(\mu_{\ell'^\infty})/F) \simeq \mathrm{Gal}(N_{\ell'}/F)$ for each $\ell' \in \Lambda$. This completes the proof of Lemma 6.3.2. $\square$

We saw from the previous lemma a precise description of each intersection N_ℓ under some suitable conditions. What can be said in general (without the independence hypothesis and condition $(*)$) about the N_ℓ's is given by the following result.

Lemma 6.3.4. *Let ℓ be a prime and F_ℓ be an ℓ-adic Lie extension of F (that is, $\mathrm{Gal}(F_\ell/F)$ is an ℓ-adic Lie group). Let $N_\ell = F_\ell \cap F^{\mathrm{cyc}}$. Then $N_\ell/F_\ell \cap F(\mu_{\ell^\infty})$ is a finite extension.*

Proof. Since $N_\ell(\mu_{\ell^\infty})$ is contained in F^{cyc} we have a surjection of Galois groups

$$\mathrm{Gal}(F^{\mathrm{cyc}}/F) \twoheadrightarrow \mathrm{Gal}(N_\ell(\mu_{\ell^\infty})/F). \tag{6.6}$$

As the Galois group $\mathrm{Gal}(N_\ell(\mu_{\ell^\infty})/F)$ is an abelian ℓ-adic Lie group, we may view it as a direct product of finitely many copies of $\mathbb{Z}_\ell$ and a finite abelian group. But note that any homomorphism $\mathrm{Gal}(F^{\mathrm{cyc}}/F) \to \mathbb{Z}_\ell$ factors through $\mathrm{Gal}(F(\mu_{\ell^\infty})/F)$. Hence the homomorphism (6.6) factors through $\mathrm{Gal}(F(\mu_{\ell^\infty})/F) \times C \twoheadrightarrow \mathrm{Gal}(N_\ell(\mu_{\ell^\infty})/F)$ where C is a finite abelian group. The finite abelian group C maps onto $\mathrm{Gal}(N_\ell(\mu_{\ell^\infty})/F(\mu_{\ell^\infty}))$, and since $N_\ell \cap F(\mu_{\ell^\infty}) = F_\ell \cap F(\mu_{\ell^\infty})$ we see that $\mathrm{Gal}(N_\ell/F_\ell \cap F(\mu_{\ell^\infty})) \simeq \mathrm{Gal}(N_\ell(\mu_{\ell^\infty})/F(\mu_{\ell^\infty}))$ is finite. $\square$

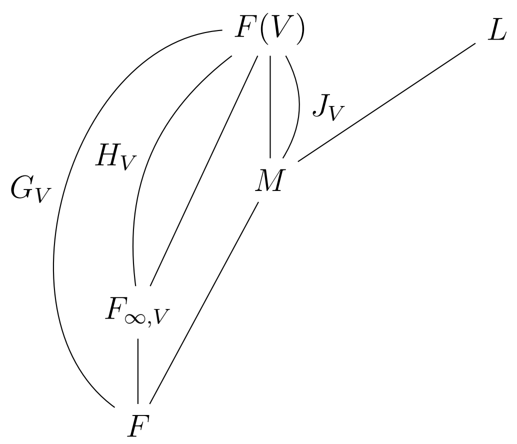
Chapter 7

Proofs

7.1 The Setup

We follow the notations as in Chapter 1. Suppose that F is a global or a local field and $\rho : G_F \to \mathrm{GL}(V)$ is a continuous linear representation of G_F. For an arbitrary Galois extension L/F, we may identify $J_V = \rho(G_L)$ with a closed normal subgroup of G_V, whose fixed field $M = F(V)^{J_V}$ is the intersection of $F(V)$ and L. Then the Galois group $\mathrm{Gal}(M/F)$ may be identified with a quotient of G_V. If the representation ρ is a p-adic representation, then the group G_V is a p-adic Lie group and thus, so is $\mathrm{Gal}(M/F)$ (cf. [DDSMS99], Theorem 9.6 (ii)). Hence, M/F is a p-adic Lie extension. If $L = F(\mu_{p^\infty})$, the field M will be written as $F_{\infty,V} := F(V) \cap F(\mu_{p^\infty})$.

We have the following diagram of fields:



In particular, if L contains $F(\mu_{p^\infty})$, then J_V is a closed normal subgroup of H_V and M contains $F_{\infty,V}$.

7.2 Proofs in the local setting

Throughout this section, we work with a p-adic local field K as our base field.

7.2.1 Some lemmas

Let L be a Galois extension of K which contains $K(\mu_{p^\infty})$. Put $\mathcal{G} = \mathrm{Gal}(L/K)$ and $\mathcal{H} = \mathrm{Gal}(L/K(\mu_{p^\infty}))$. Let $\varepsilon : \mathcal{G} \to \mathbb{Z}_p^\times$ be a continuous character of $\mathcal{G}$ whose image is open in $\mathbb{Z}_p^\times$. The group $\mathcal{G}$ acts on $\mathcal{H}$ by inner automorphisms, that is, for $\sigma \in \mathcal{G}$ and $\tau \in \mathcal{H}$, we have $\sigma \cdot \tau = \sigma\tau\sigma^{-1}$. Assume that the following relation holds:

$$\sigma \cdot \tau = \tau^{\varepsilon(\sigma)} \tag{7.1}$$

for all $\sigma \in \mathcal{G}$, $\tau \in \mathcal{H}$.

Lemma 7.2.1. *Let $\psi : \mathcal{G} \to \mathrm{GL}(W)$ be a p-adic representation of $\mathcal{G}$. Let ε be a character as above and suppose the action of $\mathcal{G}$ on $\mathcal{H}$ satisfies relation (7.1). Then after a finite extension K'/K, the subgroup $\mathcal{H}$ acts unipotently on W.*

Proof. Put $d = \dim_{\mathbb{Q}_p} W$. The result is trivial if $d = 0$. We assume henceforth that d is nonzero. We may argue in the same manner as the proof of Lemma 2.2 of [KT13]. Let $\tau \in \mathcal{H}$ and $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of $\psi(\tau)$. Then relation (7.1) shows that

$$\{\lambda_1, \ldots, \lambda_d\} = \{\lambda_1^{\varepsilon(\sigma)}, \ldots, \lambda_d^{\varepsilon(\sigma)}\}$$

for all $\sigma \in \mathcal{G}$. Let e be a positive integer such that $1 + p^e$ lies in $\varepsilon(\mathcal{G})$. Such an integer exists since $\varepsilon(\mathcal{G})$ is open in $\mathbb{Z}_p^\times$. For each $i = 1, \ldots, d$, there exists an integer r_i with $1 \leq r_i \leq d$ such that $\lambda_i^{(1+p^e)^{r_i}} = \lambda_i$. We then put

$$m = \mathrm{LCM}\{(1 + p^e)^r - 1 | r = 1, \cdots, d\}.$$

With this choice of m we see that $\psi(\tau)^m$ is unipotent since $\lambda_i^m = 1$ for all $i = 1, \ldots, d$. Hence $\mathcal{H}^m = \{\tau^m | \tau \in \mathcal{H}\}$ acts unipotently on W. Then the semisimplification of the restriction $\psi|_{\mathcal{H}}$ to $\mathcal{H}$ is a sum of characters $\mathcal{H}/\mathcal{H}^m \to \mu_m$, after a suitable extension of scalars. These characters become trivial upon replacing $K(\mu_{p^\infty})$ by a finite extension, say K_μ. In fact, $K_\mu = K'(\mu_{p^\infty})$ for some finite extension K' of K. $\square$

Lemma 7.2.2. *Let $\varphi : \mathcal{U} \to \mathrm{GL}_{\mathbb{Q}_p}(W)$ be a representation of a group $\mathcal{U}$ on a finite-dimensional $\mathbb{Q}_p$-vector space W. Suppose $\mathcal{U}$ acts unipotently on W. Then $W^{\mathcal{U}} = 0$ if and only if $W = 0$.*

Proof. Let $d = \dim_{\mathbb{Q}_p} W$. It is known that for a suitable choice of basis the image of $\mathcal{U}$ can be identified with a subgroup of the group U_d of upper-triangular matrices in $\mathrm{GL}_d(\mathbb{Q}_p)$ (cf. e.g. [Bor91], Chapter I, §4.8, Theorem). Hence, since $\mathcal{U}$ acts unipotently, W always has a nonzero vector fixed by $\mathcal{U}$ if $d > 0$. $\square$

7.2.2 Preliminary Results

We follow the notations as in Section 7.1. We consider the p-adic representation $\rho : G_K \to \mathrm{GL}(V)$ with $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$. Here X is a proper smooth variety over K with potential good reduction and i is a positive integer. We consider a Galois extension L of K and consider the image J_V of G_L under ρ.

Lemma 7.2.3. *(1) If J_V has finite index in G_V, then V has vanishing J_V-cohomology.*
(2) Assume i is odd. If L contains $K(\mu_{p^\infty})$ and J_V has finite index in H_V, then V has vanishing J_V-cohomology.

Remark 7.2.4. By Galois theory, we have $\mathrm{Gal}(M/K) \simeq G_V/J_V$ (resp. $\mathrm{Gal}(M/K_{\infty,V}) \simeq H_V/J_V$) in the discussion above. So the condition that J_V has finite index in G_V (resp. H_V) is equivalent to the finiteness of the degree of the extension M over K (resp. $K_{\infty,V}$).

Proof. Replacing K with a finite extension, we may assume $G_V = J_V$ (resp. $H_V = J_V$). It follows immediately from Theorem 2 that V has vanishing J_V-cohomology. $\square$

Remark 7.2.5. Let V be any p-adic representation of G_K as above with odd i and L/K a Galois extension containing $K(\mu_{p^\infty})$. Take a G_K-stable $\mathbb{Z}_p$-lattice T of V. We know from Lemma 5 that the vanishing of $H^0(J_V, V)$ is equivalent to the finiteness of $(V/T)^{G_L}$. Hence, since V has vanishing H_V-cohomology, we have the relation (1) $\Rightarrow$ (2) $\Rightarrow$ (3) between the following statements:
(1) M is a finite extension of $K(\mu_{p^\infty})$,
(2) V has vanishing J_V-cohomology, and
(3) $(V/T)^{G_L}$ is a finite group.
However, converses may not necessarily hold. In some cases though, we have (3) $\Rightarrow$ (1), as we shall see in Corollary 7.2.25.

Lemma 7.2.6. *Let X be a proper smooth variety over a p-adic field K with potential good reduction and i be a positive integer. Consider the representation $\rho : G_K \to \mathrm{GL}(V)$, where $V = H^i_{\text{ét}}(X_{\bar{K}}, \mathbb{Q}_p)$ and let* $\det \rho : G_K \to \mathbb{Z}_p^\times$

be the character obtained by composing ρ *with the determinant map. Then* $\det\rho = \chi^{-\frac{in}{2}}$ *on an open subgroup of* G_K*, where* $n = \dim_{\mathbb{Q}_p} V$.

Proof. This follows from Lemma 5.2.6. $\square$

The following is a simple criterion for determining the vanishing of J_V-cohomology from the Lie algebras of $\mathrm{Gal}(K(V)/K_{\infty,V})$ and $\mathrm{Gal}(L/L\cap K(\mu_{p^\infty}))$.

Theorem 7.2.7. *Let* X *be a proper smooth variety over* K *with potential good reduction and* i *a positive odd integer. Put* $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ *and* $K_{\infty,V} := K(V) \cap K(\mu_{p^\infty})$*. Let* L/K *be any* p*-adic Lie extension such that* $K(\mu_{p^\infty})$ *is of finite degree over* $K_{\infty,L} := L \cap K(\mu_{p^\infty})$*. Assume that the Lie algebras*

$$\mathrm{Lie}(\mathrm{Gal}(K(V)/K_{\infty,V})) \text{ and } \mathrm{Lie}(\mathrm{Gal}(L/K_{\infty,L}))$$

have no common simple factor. Then V *has vanishing* J_V*-cohomology, where* $J_V = \rho(G_L)$.

Proof. The theorem clearly holds if $n = \dim_{\mathbb{Q}_p} V$ is zero. We assume henceforth that V is of positive dimension. Since the kernel of ρ is contained in the kernel of $\det\rho$, we see that $K(V)$ contains the fixed subfield $K(\det V)$ of $\overline{K}$ by the kernel of $\det\rho$. Note that the character $\det\rho$ is the $-in/2$-th power of the p-adic cyclotomic character on an open subgroup of G_K, by Lemma 7.2.6. Hence the field $K(V)$ contains a subfield K' of $K(\mu_{p^\infty})$ such that $K(\mu_{p^\infty})$ is of finite degree over K' since $n > 0$. Replacing K by a finite extension, we may then assume that $K(V)$ and L contains $K(\mu_{p^\infty})$. Put $\mathfrak{h} = \mathrm{Lie}(\mathrm{Gal}(K(V)/K(\mu_{p^\infty})))$ and $\mathfrak{h}' = \mathrm{Lie}(\mathrm{Gal}(L/K(\mu_{p^\infty})))$. Recall that M is the intersection of the fields $K(V)$ and L, which is a Galois extension of $K(\mu_{p^\infty})$. Let $\mathfrak{j}$ and $\mathfrak{j}'$ be the Lie algebras of $\mathrm{Gal}(K(V)/M)$ and $\mathrm{Gal}(L/M)$ respectively. The Lie algebra $\mathfrak{j}$ (resp. $\mathfrak{j}'$) is an ideal of $\mathfrak{h}$ (resp. $\mathfrak{h}'$), since $\mathrm{Gal}(K(V)/M)$ (resp. $\mathrm{Gal}(L/M)$) is a closed normal subgroup of $\mathrm{Gal}(K(V)/K(\mu_{p^\infty}))$ (resp. $\mathrm{Gal}(L/K(\mu_{p^\infty}))$). We have

$$\begin{aligned}\frac{\mathfrak{h}}{\mathfrak{j}} &\simeq \mathrm{Lie}\left(\frac{\mathrm{Gal}(K(V)/K(\mu_{p^\infty}))}{\mathrm{Gal}(K(V)/M)}\right) \simeq \mathrm{Lie}(\mathrm{Gal}(M/K(\mu_{p^\infty})))\\ &\simeq \mathrm{Lie}\left(\frac{\mathrm{Gal}(L/K(\mu_{p^\infty}))}{\mathrm{Gal}(L/M)}\right) \simeq \frac{\mathfrak{h}'}{\mathfrak{j}'}.\end{aligned}$$

The above expressions are all equal to zero by hypothesis. Therefore $\mathrm{Gal}(K(V)/M)$ has finite index in $\mathrm{Gal}(K(V)/K(\mu_{p^\infty}))$. We then apply Lemma 7.2.3 to obtain the desired conclusion. $\square$

It seems worthwhile to state the following corollaries for cohomological coprimality. More precisely, consider another proper smooth variety Y over K with potential good reduction. Let j be a positive odd integer and put $V_1 = V$, as above and $V_2 = H^j_{\text{ét}}(Y_{\overline{K}}, \mathbb{Q}_p)$. Put $J_1 = \rho_1(\mathrm{Ker}(\rho_2))$ and $J_2 = \rho_2(\mathrm{Ker}(\rho_1))$. Note that J_r is a closed normal subgroup of $H_r = \rho_r(G_{K(\mu_{p^\infty})})$ (after a finite extension) for $r = 1, 2$. We have the following special case of Lemma 7.2.3.

Corollary 7.2.8. *Let V_1 and V_2 be as above and let $K(V_1)$ and $K(V_2)$ be the fixed fields of $\mathrm{Ker}(\rho_1)$ and $\mathrm{Ker}(\rho_2)$, respectively. If $M := K(V_1) \cap K(V_2)$ is a finite extension of $M \cap K(\mu_{p^\infty})$, then V_1 and V_2 are cohomologically coprime.*

The cohomological coprimality can also be derived by comparing the Lie algebras $\mathfrak{h}_1 = \mathrm{Lie}(H_1)$ and $\mathfrak{h}_2 = \mathrm{Lie}(H_2)$.

Corollary 7.2.9. *With the assumptions and notations in the discussion above, suppose $\mathfrak{h}_1$ and $\mathfrak{h}_2$ have no common simple factor. Then V_1 and V_2 are cohomologically coprime.*

Proof. Apply Theorem 7.2.7 with $V = V_1$ and $L = K(V_2)$; and with $V = V_2$ and $L = K(V_1)$. $\square$

Remark 7.2.10. In view of Theorem 3 and Lemma 5.4.3, we note that analogues of all the results in this section also hold in the case where the variety X is defined over a number field without any assumption on reduction.

7.2.3 Lie algebras associated with elliptic curves

Let E be an elliptic curve over a p-adic field K. Consider the p-adic representation $\rho_E : G_K \to \mathrm{GL}(V_p(E))$ of G_K on the p-adic Tate module of E. We recall the well-known description of the structure of the Lie algebras associated to E:

Proposition 7.2.11 ([Se89], Appendix of Chapter IV)**.** *Let E be an elliptic curve over K. Let $\mathfrak{g} := \mathrm{Lie}(\rho_E(G_K))$ and $\mathfrak{i} := \mathrm{Lie}(\rho_E(I_K))$ be the Lie algebras of the image of G_K and its inertia subgroup I_K under ρ_E, respectively (These are Lie subalgebras of $\mathrm{End}(V_p(E))$).*

(i) If E has good supersingular reduction with formal complex multiplication, then $\mathfrak{g}$ is a non-split Cartan subalgebra of $\mathrm{End}(V_p(E))$ and $\mathfrak{i} = \mathfrak{g}$. We have $\dim \mathfrak{g} = \dim \mathfrak{i} = 2$.

(ii) If E has good supersingular reduction without formal complex multiplication, then $\mathfrak{g} = \mathrm{End}(V_p(E))$ and $\mathfrak{i} = \mathfrak{g}$. We have $\dim \mathfrak{g} = \dim \mathfrak{i} = 4$.

(iii) *If E has good ordinary reduction with complex multiplication, then $\mathfrak{g}$ is a split Cartan subalgebra of* $\mathrm{End}(V_p(E))$. *We have* $\dim \mathfrak{g} = 2$ *and* $\mathfrak{i}$ *is a* 1*-dimensional subspace of* $\mathfrak{g}$.

(iv) *If E has good ordinary reduction without complex multiplication, then $\mathfrak{g}$ is the Borel subalgebra of* $\mathrm{End}(V_p(E))$ *which corresponds to the kernel of the reduction map* $V_p(E) \to V_p(\widetilde{E})$. *We have* $\dim \mathfrak{g} = 3$ *and* $\mathfrak{i}$ *is a* 2*-dimensional subspace of* $\mathfrak{g}$ *with* $\mathfrak{i}/[\mathfrak{i}, \mathfrak{i}]$ *of dimension* 1.

(v) *If E has j-invariant with negative p-adic valuation, then $\mathfrak{g}$ is the subalgebra of* $\mathrm{End}(V_p(E))$ *which consists of the endomorphisms u for which* $u(V_p(E)) \subset W$, *where W is the unique G_K-stable* 1*-dimensional subspace of $V_p(E)$. Moreover,* $\mathfrak{i} = \mathfrak{g}$. *We have* $\dim \mathfrak{g} = \dim \mathfrak{i} = 2$

7.2.4 Proof of Theorem 2.1

The proof of Theorem 2.1 follows from the following more general result.

Theorem 7.2.12. *Let $\rho : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(V)$ be a potentially crystalline representation. Let K' be a finite extension of K such that $\rho|_{G_{K'}}$ are crystalline. Let Φ denote the associated endomorphism of the filtered module associated to $\rho|_{G_{K'}}$. Suppose the following conditions are satisfied:*
(i) the eigenvalues of Φ are q-Weil numbers of odd weight;
(ii) the determinant of Φ is a rational number;
(iii) there exists a filtration

$$0 = V_{-1} \subsetneq V_0 \subsetneq V_1 = V$$

of $G_{K'}$-stable subspaces such that $I_{K'}$ acts on V_0 by χ^a and $I_{K'}$ acts on V_1/V_0 by χ^b, where a and b are distinct integers;
Let L be a Galois extension of K such that the residue field of $L(\mu_{p^\infty})$ is a potential prime-to-p extension of k and $V^{G_{L'}} = 0$ for every finite extension L' of L. Then V has vanishing J_V-cohomology, where $J_V = \rho(G_L)$.

For the proof we make some preparations. First of all replacing K with K', we may assume that V is crystalline so that assumptions (i) and (ii) hold. We may also suppose that assumption (iii) holds with $K = K'$. The assumption (iii) allows us to obtain an explicit description of the representation ρ.

Proposition 7.2.13. *Let V be a finite-dimensional p-adic Galois representation of G_K such that there exists a filtration*

$$0 = V_{-1} \subsetneq V_0 \subsetneq V_1 = V$$

of G_K-stable subspaces such that I_K acts on V_0 by χ^a and I_K acts on V_1/V_0 by χ^b, where a and b are distinct integers. Let $n = \dim_{\mathbb{Q}_p} V$ and $d = \dim_{\mathbb{Q}_p} V_0$. Then, for some suitable basis of V, the representation ρ has the form

$$\begin{pmatrix} S_1 & T \\ 0 & S_2 \end{pmatrix},$$

where

(i) $S_1 : G_K \to \mathrm{GL}_d(\mathbb{Z}_p)$ and $S_2 : G_K \to \mathrm{GL}_{n-d}(\mathbb{Z}_p)$ are continuous homomorphisms and

(ii) $T : G_K \to \mathrm{Mat}_{d\times(n-d)}(\mathbb{Z}_p)$ is a continuous map.

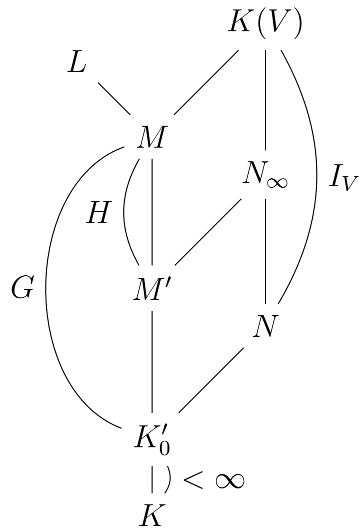
Moreover, S_1 (resp. S_2) is of the form $(\chi^a)^{\oplus d}\cdot U_1$ (resp. $(\chi^b)^{\oplus(n-d)}\cdot U_2$), where $U_1 : G_K \to \mathrm{GL}_d(\mathbb{Z}_p)$ and $U_2 : G_K \to \mathrm{GL}_{n-d}(\mathbb{Z}_p)$ are continuous unramified homomorphisms.

Proof. This follows immediately from the hypotheses upon choosing a basis $\{v_1, \ldots, v_n\}$ of V such that $\{v_1, \ldots, v_d\}$ is a basis of V_0. □

We now proceed to the proof of Theorem 7.2.12. First we note that we may reduce the proof to the case $L = L(\mu_{p^\infty})$. Indeed letting $L' = L(\mu_{p^\infty})$ and $J'_V = \rho(G_{L'})$, then J'_V is a closed normal subgroup of J_V. We see that if V has vanishing J'_V-cohomology then Corollary 3.1.5 implies

$$H^n(J_V, V) \simeq H^n(J_V/J'_V, H^0(J'_V, V)) \qquad n \geq 0,$$

and a priori, V has vanishing J_V-cohomology. We assume henceforth that $L = L(\mu_{p^\infty})$. After replacing K by a finite extension we may also assume that $K(V) \supset K(\mu_{p^\infty})$ by assumptions (i) and (ii) together with Lemma 5.2.6. Put $M := L \cap K(V)$. Recall that M is a p-adic Lie extension of K. Moreover, the residue field of M is a potential prime-to-p extension over k. Thus the maximal unramified subextension K'_0 of M/K is of finite degree over K. Put $N = K(V) \cap K^{\mathrm{nr}}$, the maximal subextension of $K(V)$ which is unramified over K. This is the fixed subfield of $\overline{K}$ by the kernel of the restriction $\rho|_{I_K}$ of ρ to the inertia subgroup. Recall that $I_V = \rho(I_K)$, and so we may identify I_V with $\mathrm{Gal}(K(V)/N)$. We also let $N_\infty := N(\mu_{p^\infty})$. Let $M' = M \cap N_\infty$ and we put $G := \mathrm{Gal}(M/K'_0)$ and $H := \mathrm{Gal}(M/M')$. Note that $M' = K'_0(\mu_{p^\infty})$. We have the following diagram of fields from which we observe that we may identify G with a quotient of I_V:



We have the following

Lemma 7.2.14. *Assume the hypothesis in Theorem 7.2.12. Let* $\psi : \mathrm{Gal}(M/K) \to \mathrm{GL}_{\mathbb{Q}_p}(W)$ *be a continuous linear representation of* $\mathrm{Gal}(M/K)$*. Then up to a finite extension, the quotient* $H_V/J_V \simeq \mathrm{Gal}(M/K(\mu_{p^\infty}))$ *acts unipotently on* W*.*

Proof. We use the diagram of fields shown above to give an explicit description of the action of G on H. Replacing K by K'_0, we may assume that $G = \mathrm{Gal}(M/K)$, so that $H = \mathrm{Gal}(M/K(\mu_{p^\infty}))$. The diagram of fields clearly induces the following commutative diagram, having exact rows and surjective left and middle vertical maps:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(K(V)/N_\infty) \arrow[r] \arrow[d, two heads] & I_V \arrow[r] \arrow[d, two heads] & \mathrm{Gal}(N_\infty/N) \arrow[r] \arrow[d, "\wr"'] & 1 \\
1 \arrow[r] & H \arrow[r] & G \arrow[r] & G/H \arrow[r] & 1
\end{tikzcd} \tag{7.2}$$

Moreover the above diagram is compatible with the actions by inner automorphism, in the sense that if $\sigma \in G$ and $\tau \in H$, and $\tilde{\sigma}$ (resp. $\tilde{\tau}$) is a lifting of σ (resp. τ) to I_V, then $\tilde{\sigma} \cdot \tilde{\tau} \cdot \tilde{\sigma}^{-1}$ lies in $\mathrm{Gal}(K(V)/N_\infty)$. The representation ρ factors through G_V and so we obtain from ρ a faithful representation $G_V \to \mathrm{GL}_{\mathbb{Q}_p}(V)$.

We now choose a suitable basis of V whose first d elements is a basis of V_0. By Proposition 7.2.13, the representation of G_V on V can be written as:

$$\begin{pmatrix} (\chi^a)^{\oplus d} \cdot U_1 & T \\ 0 & (\chi^b)^{\oplus (n-d)} \cdot U_2 \end{pmatrix},$$

where $U_1 : G_V \to \mathrm{GL}_d(\mathbb{Z}_p)$ and $U_2 : G_V \to \mathrm{GL}_{n-d}(\mathbb{Z}_p)$ are continuous unramified homomorphisms and $T : G_V \to \mathrm{Mat}_d(\mathbb{Z}_p)$ is a continuous map. Let $\sigma \in G$ and $\tau \in H$. We take a lifting $\tilde{\sigma}$ (resp. $\tilde{\tau}$) of σ (resp. τ) to I_V. Let I_r denote the $r \times r$ identity matrix. We have $U_1(\tilde{\sigma}) = U_1(\tilde{\tau}) = I_d$ and $U_2(\tilde{\sigma}) = U_2(\tilde{\tau}) = I_{n-d}$. Note that $\tilde{\tau}$ belongs to $\mathrm{Gal}(K(V)/N_\infty)$, so we have $(\chi^a)^{\oplus d} \cdot U_1(\tilde{\tau}) = I_d$ and $(\chi^b)^{\oplus(n-d)} \cdot U_2(\tilde{\tau}) = I_{n-d}$. We have

$$\begin{aligned}
\rho(\tilde{\sigma} \cdot \tilde{\tau} \cdot \tilde{\sigma}^{-1}) &= \rho(\tilde{\sigma})\rho(\tilde{\tau})\rho(\tilde{\sigma})^{-1} \\
&= \begin{pmatrix} (\chi^a)^{\oplus d}(\tilde{\sigma}) & T(\tilde{\tau}) \\ 0 & (\chi^b)^{\oplus n-d}(\tilde{\sigma}) \end{pmatrix} \begin{pmatrix} I_d & T(\tilde{\tau}) \\ 0 & I_{n-d} \end{pmatrix} \\
&\quad \begin{pmatrix} \left((\chi^a)^{\oplus d}(\tilde{\sigma})\right)^{-1} & -\left((\chi^a)^{\oplus d}(\tilde{\sigma})\right)^{-1} T(\tilde{\tau}) \left((\chi^b)^{\oplus n-d}(\tilde{\sigma})\right)^{-1} \\ 0 & \left((\chi^b)^{\oplus n-d}(\tilde{\sigma})\right)^{-1} \end{pmatrix} \\
&= \begin{pmatrix} I_d & \left((\chi^{a-b})^{\oplus d}(\tilde{\sigma})\right) T(\tilde{\tau}) \\ 0 & I_{n-d} \end{pmatrix}.
\end{aligned}$$

Here $(\chi^s)^{\oplus r}(\bullet) \in \mathrm{GL}_r(\mathbb{Z}_p)$ is the $r \times r$ diagonal matrix with entries $\chi^s(\bullet)$. Writing $(\chi^{a-b})^{\oplus r}(\tilde{\sigma})$ as a product of the scalar $\chi^{a-b}(\tilde{\sigma})$ with I_r, we see that the last term in the above series of equations is just

$$\begin{pmatrix} I_d & T(\tilde{\tau}) \\ 0 & I_{n-d} \end{pmatrix}^{\chi^{a-b}(\tilde{\sigma})} \left(= \rho(\tilde{\tau})^{\chi^{a-b}(\tilde{\sigma})} \right).$$

This gives the relation

$$\sigma \cdot \tau \cdot \sigma^{-1} = \tau^{\varepsilon(\sigma)}, \tag{7.3}$$

with $\varepsilon = \chi^{a-b}$, from the compatibility of (7.2) with the actions by inner automorphisms. The desired result follows from Lemma 7.2.1. This completes the proof of Lemma 7.2.14. $\square$

We may now complete the proof of Theorem 7.2.12.

Proof of Theorem 7.2.12. As $\mathrm{Gal}(M/K) \simeq G_V/J_V$ we may consider $H^r(J_V, V)$ as a representation of $\mathrm{Gal}(M/K)$. Replacing K by a finite extension, we may assume that H_V/J_V acts unipotently on $H^r(J_V, V)$ for all $r \geq 0$, by Lemma 7.2.14. We prove the vanishing by induction on r. The case $r = 0$ is done by hypothesis. By assumptions (i) and (ii) and Proposition 5.2.4, we know that V has vanishing H_V-cohomology. Now let $r \geq 1$ and assume that $H^m(J_V, V) = 0$ for all $1 \leq m < r$. Then Corollary 3.1.4 gives the following exact sequence:

$$H^r(H_V, V) \to H^0(H_V/J_V, H^r(J_V, V)) \to H^{r+1}(H_V/J_V, V^{J_V}).$$

As the first and last terms both vanish, we have $H^0(H_V/J_V, H^r(J_V, V)) = 0$. The vanishing of J_V-cohomology follows from Lemma 7.2.2 since H_V/J_V acts unipotently on $H^r(J_V, V)$. □

As a corollary, we obtain necessary and sufficient conditions for the vanishing of J_V-cohomology groups for p-adic representations given by an abelian variety with good ordinary reduction over K. Let $\tilde{A}$ denote the reduction of A modulo the maximal ideal of $\mathcal{O}_K$.

Corollary 7.2.15. *Let A be an abelian variety over K with good ordinary reduction and L be a Galois extension with residue field k_L. Assume that L contains $K(\mu_{p^\infty})$ and the coordinates of the p-torsion points of A. Put $V = V_p(A)$ and $J_V = \rho_A(G_L)$. Then the following statements are equivalent:*
(1) $A(L)[p^\infty]$ is finite,
(2) $A^\vee(L)[p^\infty]$ is finite,
(3) $\tilde{A}(k_L)[p^\infty]$ is finite,
(4) $\tilde{A}^\vee(k_L)[p^\infty]$ is finite,
(5) k_L is a potential prime-to-p extension of k
(6) V has vanishing J_V-cohomology.

Proof. The equivalence of the first five statements is given by Corollary 2.1 in [Oz09]. Theorem 7.2.12 shows that condition (5) implies condition (6). Note that condition (1) is equivalent to $H^0(J_V, V) = 0$ by Lemma 5, so condition (6) implies (1). □

We are ready to give the proof of Theorem 2.1.

Proof of Theorem 2.1. Our goal is to show that
(1) V has vanishing J_V-cohomology, where $J_V = \rho(\operatorname{Ker}\rho') = \rho(G_{K(V')})$; and
(2) V' has vanishing $J_{V'}$-cohomology, where $J_{V'} = \rho'(\operatorname{Ker}\rho) = \rho'(G_{K(V)})$.
Note that $K(V)(\mu_{p^\infty})$ is a finite extension of $K(V)$. The same is true for $K(V')$. Thus, statement (1) is a special case of Theorem 7.2.12 with $L = K(V')$. To prove statement (2), we consider $H^r(J_{V'}, V')$ $(r \geq 0)$ as a representation of $\operatorname{Gal}(M/K)$, where $M = K(V) \cap K(V')$. Then Lemma 7.2.14 implies that by replacing the base field with a suitable finite extension we may assume that $H_{V'}/J_{V'} (\simeq \operatorname{Gal}(M/K(\mu_{p^\infty})))$ acts unipotently on $H^r(J_{V'}, V')$. Arguing as in the proof of Theorem 7.2.12, we see that V' has vanishing $J_{V'}$-cohomology. □

Before proving Theorem 2.2, we first recall the following result on the étale cohomology groups of a proper smooth variety with good ordinary reduction due to Illusie.

Theorem 7.2.16 ([Il94], Cor. 2.7). *Let X be a proper smooth variety over K which has good ordinary reduction over K. Then the étale cohomology group $V = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ $(i \geq 0)$ has the following property: there exists a filtration by G_K-invariant subspaces $\{\operatorname{Fil}^r V\}_{r\in\mathbb{Z}}$ which satisfies*

$$\operatorname{Fil}^{r+1} V \subseteq \operatorname{Fil}^r V \text{ for all } r,$$
$$\operatorname{Fil}^r V = V \text{ for } r \ll 0 \text{ and } \operatorname{Fil}^r V = 0 \text{ for } r \gg 0,$$

such that the inertia subgroup I_K acts on the rth graded quotient $\operatorname{gr}^r V = \operatorname{Fil}^r V/\operatorname{Fil}^{r+1} V$ by the rth power of the p-adic cyclotomic character.

We now prove Theorem 2.2. For convenience let us recall the statement of the said theorem.

Theorem 7.2.17. *Let X be a proper smooth variety over K with potential good ordinary reduction and let E/K be an elliptic curve with potential good supersingular reduction. Let i be a positive odd integer and we put $V = H^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)$ and $V' = V_p(E)$. Then V and V' are cohomologically coprime.*

Proof. To prove the theorem we have to show that the following statements hold:
(a) If we put $L = K(E_{p^\infty})$ and $J_V = \rho(G_L)$, then V has vanishing J_V-cohomology; and
(b) If we put $L' = K(V)$ and $J_{V'} = \rho_E(G_{L'})$, then V' has vanishing $J_{V'}$-cohomology.
We only prove statement (a) since statement (b) can be proved in a similar manner. Replacing K with a finite extension, we may assume that X has good ordinary reduction and E has good supersingular reduction over K. We may also assume that $K(V)$ contains $K(\mu_{p^\infty})$ by extending K further (cf. Lemma 7.2.6). Put $N_\infty = K(V) \cap K^{\mathrm{nr}}(\mu_{p^\infty})$. The assumption on V implies that the inertia subgroup I_K of G_K acts on the associated graded quotients $\operatorname{gr}^r V = \operatorname{Fil}^r V/\operatorname{Fil}^{r+1} V$ by the rth power of the p-adic cyclotomic character. In particular the group

$$\operatorname{Gal}(K(V)/N_\infty) \simeq \operatorname{Gal}(K^{\mathrm{nr}}(V)/K^{\mathrm{nr}}(\mu_{p^\infty}))$$

acts unipotently on V. Hence, $\operatorname{Lie}(\operatorname{Gal}(K(V)/N_\infty))$ is a nilpotent Lie algebra contained in $\operatorname{Lie}(H_V) = \operatorname{Lie}(\operatorname{Gal}(K(V)/K_{\infty,V}))$. Recall that we may identify $\operatorname{Gal}(L/K)$ with the subgroup $\rho_E(G_K)$ of $\operatorname{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$. Put $\mathfrak{g} = \operatorname{Lie}(\operatorname{Gal}(L/K))$ and $\mathfrak{h} = \operatorname{Lie}(\operatorname{Gal}(L/K(\mu_{p^\infty})))$. If E has no formal complex multiplication, then $\mathfrak{g} \simeq \mathfrak{gl}_2(\mathbb{Q}_p)$ by Proposition 7.2.11 (*ii*) and so $\mathfrak{h} \simeq \mathfrak{sl}_2(\mathbb{Q}_p)$. In particular, $\mathfrak{h}$ is simple. It immediately follows from Theorem 7.2.7 that V has vanishing J_V-cohomology. This proves (a) when E has no formal complex multiplication. We now suppose that E has formal complex multiplication. We claim that $M = K(V) \cap L$ is a finite extension of $K(\mu_{p^\infty})$. The restriction map induces a surjection

$$\mathrm{Gal}(K(V)/N_\infty) \twoheadrightarrow \mathrm{Gal}(MN_\infty/N_\infty) \simeq \mathrm{Gal}(M/M \cap N_\infty),$$

from which we obtain a surjection of Lie algebras

$$\mathrm{Lie}(\mathrm{Gal}(K(V)/N_\infty)) \twoheadrightarrow \mathrm{Lie}(\mathrm{Gal}(M/M \cap N_\infty)).$$

As $\mathrm{Lie}(\mathrm{Gal}(K(V)/N_\infty))$ is nilpotent, we see that $\mathrm{Lie}(\mathrm{Gal}(M/M \cap N_\infty))$ is a nilpotent subalgebra of $\mathrm{Lie}(\mathrm{Gal}(M/K(\mu_{p^\infty})))$. Since E has formal complex multiplication, we know from Proposition 7.2.11 (i) that $\mathfrak{g}$ is a non-split Cartan subalgebra of $\mathrm{End}(V_p(E)) \simeq \mathfrak{gl}_2(\mathbb{Q}_p)$. Thus Proposition B.7 in Appendix B implies that $\mathfrak{g}$ contains the center $\mathfrak{c}$ of $\mathfrak{gl}_2(\mathbb{Q}_p)$ and $\mathfrak{h} \simeq \mathfrak{g}/\mathfrak{c}$ is a Cartan subalgebra of $\mathfrak{sl}_2(\mathbb{Q}_p)$. Its elements are semisimple in $\mathfrak{sl}_2(\mathbb{Q}_p)$ by Proposition B.9 in Appendix B. Thus, the elements of $\mathrm{Lie}(\mathrm{Gal}(M/K(\mu_{p^\infty})))$ are also semisimple since it is a quotient of $\mathfrak{h}$. Since the Lie algebra $\mathrm{Lie}(\mathrm{Gal}(M/M \cap N_\infty))$ is a nilpotent factor of $\mathrm{Lie}(\mathrm{Gal}(M/K(\mu_{p^\infty})))$, we then see that $\mathrm{Lie}(\mathrm{Gal}(M/M \cap N_\infty)) = 0$. This means $M/M \cap N_\infty$ is a finite extension. But note that $M \cap N_\infty$ is unramified over $K(\mu_{p^\infty})$. Since $\rho_E(I_K)$ is open in $\rho_E(G_K)$ again by Proposition 7.2.11 (i), $M \cap N_\infty$ is finite over $K(\mu_{p^\infty})$. Thus $M/K(\mu_{p^\infty})$ is a finite extension. By Remark 7.2.5, the finiteness of $[M : K(\mu_{p^\infty})]$ is equivalent to the finiteness of the index of $J_V = \rho(G_L)$ in H_V. By Lemma 7.2.3, we conclude that V has vanishing J_V-cohomology. □

Remark 7.2.18. In Theorem 2.2 when the elliptic curve E has potential good ordinary reduction, the vanishing statement (b) may not hold because $H^0(J_{V'}, V')$ may be nontrivial. This is easily observed by taking $X = E$ and considering $V = H^1_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$. This observation in fact holds in a more general case. Indeed, take any abelian variety A/K with potential good ordinary reduction and consider $V = V_p(A) \simeq H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_p)^\vee$. Since A has potential good ordinary reduction, the field $L' = K(A_{p^\infty})$ contains an unramified $\mathbb{Z}_p$-extension. Hence, the residue field $k_{L'}$ is not a potential prime-to-p extension over k. Replacing K and L' with appropriate finite extensions (so that the hypothesis of Corollary 7.2.15 is satisfied), we conclude that the representation V' does not have vanishing $J_{V'}$-cohomology. Thus V and V' are not cohomologically coprime.

7.2.5 Vanishing results for elliptic curves

In this section, we give the proof of Theorem 2.3. We determine the cohomological coprimality of two Galois representations $V_p(E)$ and $V_p(E')$ given by elliptic curves E and E', respectively.

7.2.6 The case of good reduction

We first treat the case where E and E' both have potential good reduction over K.

Theorem 7.2.19. *Let E and E' be elliptic curves with potential good reduction over K. Then the representations $V_p(E)$ and $V_p(E')$ are cohomologically coprime if one of the following conditions is satisfied:*

(i) E has potential good ordinary reduction and E' has potential good supersingular reduction, or vice versa;

(ii) E has potential good supersingular reduction with formal complex multiplication and E' has potential good supersingular reduction without formal complex multiplication, or vice versa;

(iii) E and E' both have potential good supersingular reduction with formal complex multiplication and the group $E(L')[p^\infty]$ of p-power division points of E over L' is finite for every finite extension L' of $K(E'_{p^\infty})$;

(iv) E and E' both have potential good supersingular reduction without formal complex multiplication and the group $E(L')[p^\infty]$ is finite for every finite extension L' of $K(E'_{p^\infty})$.

Thanks to [Oz09], we have at our disposal some results in connection to the finiteness of the group of p-power torsion points when E has potential good supersingular reduction over K. Let us first recall these results. In general we have the following

Proposition 7.2.20 ([Oz09], Lemma 3.1)**.** *Let E be an elliptic curve over K which has good supersingular reduction over K. Let L be a Galois extension of K. Then the group $E(L)[p^\infty]$ is finite if and only if $K(E_{p^\infty})$ is not contained in L.*

In the case where $L = K(E'_{p^\infty})$ as in *(iii)* and *(iv)* of Theorem 7.2.19, we have the following two results.

Proposition 7.2.21 ([Oz09], Proposition 3.7)**.** *Let E and E' be elliptic curves over K which have good supersingular reduction with formal complex multiplication. Let $\mathcal{F} \subset K$ (resp. $\mathcal{F}' \subset K$) be the field of formal complex multiplication for E (resp. E'). Put $L = K(E'_{p^\infty})$. Then $E(L)[p^\infty]$ is finite if $\mathcal{F} \neq \mathcal{F}'$.*

Proposition 7.2.22 ([Oz09], Proposition 3.8). *Let E and E' be elliptic curves over K which have good supersingular reduction without formal complex multiplication. Put $L = K(E'_{p^\infty})$.*
(i) If there is a non-trivial homomorphism of formal groups $\hat{E}' \to \hat{E}$ over $\mathcal{O}_K$, then $E(L)[p^\infty]$ is infinite.
(ii) If $E(L)[p^\infty]$ is infinite, then there is a non-trivial homomorphism of formal groups $\hat{E}' \to \hat{E}$ over $\mathcal{O}_{K'}$ for some finite extension K' of K.

We now give the proof of Theorem 7.2.19. By symmetry, it suffices to verify the following:

Theorem 7.2.23. *Let E and E' be elliptic curves with potential good reduction over K. Put $L = K(E'_\infty)$. If one of the conditions (i) - (iv) in Theorem 7.2.19 is satisfied then $V = V_p(E)$ has vanishing J_V-cohomology, where $J_V = \rho_E(G_L)$.*

The case *(i)* of the theorem is already covered by Theorem 2.2. For case *(ii)*, we may replace K with a finite extension so that E and E' both have good supersingular reduction over K. Put $\mathfrak{h} = \mathrm{Lie}(\mathrm{Gal}(K(E_{p^\infty})/K(\mu_{p^\infty})))$. The Lie algebra of $\mathrm{Gal}(L/K)$ is isomorphic to $\mathrm{End}(V_p(E')) \simeq \mathfrak{gl}_2(\mathbb{Q}_p)$ by Proposition 7.2.11 *(ii)*. The Lie algebra $\mathfrak{h}' = \mathrm{Lie}(\mathrm{Gal}(L/K(\mu_{p^\infty})))$ is isomorphic to $\mathfrak{sl}_2(\mathbb{Q}_p)$. In particular, $\mathfrak{h}'$ is simple. As $\mathfrak{h}$ is abelian, we see that $\mathfrak{h}$ and $\mathfrak{h}'$ have no common simple factor. By Theorem 7.2.7, the desired result follows.

In view of Corollary 7.2.8, to prove the case of (*iii*) and (*iv*), it suffices to show that the field $K(E_{p^\infty}) \cap L$ is a finite extension of $K(\mu_{p^\infty})$. We obtain this by the following lemma.

Lemma 7.2.24. *Let E and E' be elliptic curves over K which have potential good supersingular reduction. Consider the following conditions:*
(FCM) E and E' have formal complex multiplication;
(NFCM) E and E' do not have formal complex multiplication.
Suppose (FCM) or (NFCM) holds. Assume further that $E(L')[p^\infty]$ is a finite group for every finite extension L' of L. Then $M := K(E_{p^\infty}) \cap L$ is a finite extension of $K(\mu_{p^\infty})$.

Proof. We split the proof into two cases:
(Case 1) Assume that both E and E' have formal complex multiplication. The Lie algebra $\mathrm{Lie}(\rho_E(G_K))$ attached to E is 2-dimensional, by Proposition 7.2.11 *(i)*. Thus $\mathrm{Gal}(K(E_{p^\infty})/K)$ is a 2-dimensional p-adic Lie group and so $\mathrm{Gal}(K(E_{p^\infty})/K(\mu_{p^\infty}))$ is 1-dimensional. The same statements hold when E is replaced by E'. Replacing K with a finite extension, we may assume

that $\mathrm{Gal}(K(E_{p^\infty})/K(\mu_{p^\infty}))$ is isomorphic to $\mathbb{Z}_p$. If M is infinite over $K(\mu_{p^\infty})$, then $\mathrm{Gal}(K(E_{p^\infty})/M)$ is of infinite index in $\mathrm{Gal}(K(E_{p^\infty})/K(\mu_{p^\infty}))$. Since the only closed subgroup of $\mathbb{Z}_p$ of infinite index is the trivial subgroup, the group $\mathrm{Gal}(K(E_{p^\infty})/M)$ must be trivial, and thus $K(E_{p^\infty}) = M$. That is, $K(E_{p^\infty})$ is contained in L. Hence, $E(L)[p^\infty]$ is infinite by Proposition 7.2.20. This contradicts our hypothesis. Therefore, M is a finite extension of $K(\mu_{p^\infty})$.
(Case 2) Suppose both E and E' do not have formal complex multiplication. Put $\mathfrak{g} = \mathrm{Lie}(\mathrm{Gal}(K(E_{p^\infty})/K))$ and $\mathfrak{h} = \mathrm{Lie}(\mathrm{Gal}(K(E_{p^\infty})/K(\mu_{p^\infty})))$. Then $\mathfrak{g}$ (resp. $\mathfrak{h}$) is isomorphic to $\mathfrak{gl}_2(\mathbb{Q}_p)$ (resp. $\mathfrak{sl}_2(\mathbb{Q}_p)$). In particular, $\mathfrak{h}$ is simple. The Lie algebra $\mathfrak{j} = \mathrm{Lie}(\mathrm{Gal}(K(E_{p^\infty})/M))$ is an ideal of $\mathfrak{h}$ since $\mathrm{Gal}(K(E_{p^\infty})/M)$ is a normal subgroup of $\mathrm{Gal}(K(E_{p^\infty})/K(\mu_{p^\infty}))$. Thus $\mathfrak{j}$ is either (0) or $\mathfrak{sl}_2(\mathbb{Q}_p)$. In the former case, $\mathrm{Gal}(K(E_{p^\infty})/M)$ is a finite group and thus $K(E_{p^\infty})/M$ is a finite extension. Replacing K with a finite extension, we have $K(E_{p^\infty}) = M \subset L$. But then this implies $E(L)[p^\infty]$ is infinite, in contrast to our hypothesis. Thus $\mathfrak{j} = \mathfrak{sl}_2(\mathbb{Q}_p)$, which means that $\mathrm{Gal}(K(E_{p^\infty})/M)$ is an open subgroup of $\mathrm{Gal}(K(E_{p^\infty})/K(\mu_{p^\infty}))$. This completes the proof of the lemma and of Theorem 7.2.23. □

Theorem 7.2.19 gives another proof of some finiteness results in [Oz09]. For instance, in view of Remark 7.2.5, condition (i) of Theorem 7.2.19 implies a part of Proposition 3.2 in [Oz09]. We also obtain the following corollary.

Corollary 7.2.25. *Let E and E' be elliptic curves with potential good supersingular reduction over K, $L = K(E'_{p^\infty})$ and $L' = K(E_{p^\infty})$. Put $V = V_p(E)$, $V' = V_p(E')$, $J_V = \rho_E(G_L)$ and $J_{V'} = \rho_{E'}(G_{L'})$. Suppose (FCM) or (NFCM) in Lemma 7.2.24 holds. Then the following statements are equivalent:*
(1) V and V' are cohomologically coprime;
(2) $L \cap L'$ is a finite extension of $K(\mu_{p^\infty})$;
(3) V has vanishing J_V-cohomology;
(3') V' has vanishing $J_{V'}$-cohomology;
(4) $E(L'')[p^\infty]$ is a finite group for any finite extension L'' of L;
(4') $E'(L'')[p^\infty]$ is a finite group for any finite extension L'' of L';
(5) The p-divisible groups $\mathcal{E}(p)$ and $\mathcal{E}'(p)$ attached to E and E', respectively, are not isogenous over $\mathcal{O}_{K'}$ for any finite extension K' of K.

Proof. It remains to prove the equivalence of each of the first six conditions with the last one. Replacing K by a finite extension, we may assume that E and E' have good supersingular reduction over K. We prove the equivalence (4) $\Leftrightarrow$ (5). If E and E' both do not have formal complex multiplication then this equivalence is given by Proposition 7.2.22. Assume that E and E' both have formal complex multiplication. Let L'' be a finite extension of L such that $E(L'')[p^\infty]$ is infinite. Replacing K by a finite extension, we may assume that $L = L''$. Then Proposition 7.2.21 implies that E and E' have the same fields of formal complex multiplication, say $\mathcal{F}$. The representations $\rho_E : G_K \to \mathrm{GL}(V_p(E))$ and $\rho_{E'} : G_K \to \mathrm{GL}(V_p(E'))$ factor through $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, where K^{ab} denotes the maximal abelian extension of K. Moreover ρ_E and $\rho_{E'}$ both have values in $\mathcal{O}_{\mathcal{F}}^{\times}$ and their restrictions to the inertia subgroup are respectively given by

$$\rho_E|_{I_K}, \rho_{E'}|_{I_K} : I(K^{\mathrm{ab}}/K) \simeq \mathcal{O}_K^{\times} \to \mathcal{O}_{\mathcal{F}}^{\times}.$$

Here, $I(K^{\mathrm{ab}}/K)$ is the inertia subgroup of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, with the isomorphism $I(K^{\mathrm{ab}}/K) \simeq \mathcal{O}_{K^{\times}}$ coming from local class field theory. In fact, $\rho_E|_{I_K}$ and $\rho_{E'}|_{I_K}$ are equal since they are both given by the map $x \mapsto \mathrm{Nr}_{K/\mathcal{F}}(x^{-1})$, where $\mathrm{Nr}_{K/\mathcal{F}} : K^{\times} \to \mathcal{F}^{\times}$ is the norm map (cf. [Se89], Chap. IV, A.2.2). From Proposition 7.2.11 (i), we know that $\rho_E(I_K)$ (resp. $\rho_{E'}(I_K)$) is an open subgroup of $\rho_E(G_K)$ (resp. $\rho_{E'}(G_K)$). This, together with the assumption that $E(L)[p^{\infty}]$ is infinite implies that $\rho_E(I_{K'}) = \rho_E(G_{K'}) = \rho_{E'}(G_{K'}) = \rho_{E'}(I_{K'})$ after a finite extension K'/K. We see that the Tate modules $T_p(E)$ and $T_p(E')$ become isomorphic over K'. By a well-known result due to Tate (cf. [Ta67], Corollary 1), the p-divisible groups $\mathcal{E}(p)$ and $\mathcal{E}'(p)$ are isogenous over $\mathcal{O}_{K'}$. Conversely, if there exists a finite extension K' over K such that $\mathcal{E}(p)$ and $\mathcal{E}'(p)$ are isogenous over $\mathcal{O}_{K'}$ then $V_p(E)$ and $V_p(E')$ are isomorphic as representations of $G_{K'}$, showing that $K'(E_{p^{\infty}}) = K'(E'_{p^{\infty}})$ which is a finite extension of L. Therefore we obtain a finite extension L'' of L such that $E(L'')[p^{\infty}]$ is infinite. □

7.2.7 The case of multiplicative reduction

We now treat the case where E' has potential multiplicative reduction over K. For this case, the Lie algebra of $\mathrm{Gal}(K(E'_{p^{\infty}})/K)$ is given by Proposition 7.2.11 *(v)*. We have the following result.

Theorem 7.2.26. *Let E and E' be elliptic curves over K such that E has potential good reduction over K and E' has potential multiplicative reduction over K. Put $L = K(E'_{p^{\infty}})$. Then $V = V_p(E)$ has vanishing J_V-cohomology, where $J_V = \rho_E(G_L)$.*

Proof. Replace K with a finite extension so that E and E' have good and multiplicative reductions over K, respectively. We first note that the residue field k_L of L is a potential prime-to-p extension of k since $\mathrm{Lie}(\rho_{E'}(G_K)) = \mathrm{Lie}(\rho_{E'}(I_K))$. Thus, the case where E has good ordinary reduction is just a consequence of Theorem 7.2.12. It remains to settle the case where E has good supersingular reduction over K. If E has no formal complex multiplication, note that the Lie algebra $\mathfrak{h}_1 = \mathrm{Lie}(\mathrm{Gal}(K(E_{p^{\infty}})/K(\mu_{p^{\infty}}))) \simeq \mathfrak{sl}_2(\mathbb{Q}_p)$ is simple. On the other hand, the Lie algebra $\mathfrak{h}_2 = \mathrm{Lie}(\mathrm{Gal}(K(E'_{p^\infty})/K(\mu_{p^\infty})))$ is a abelian. The result follows from Theorem 7.2.7. If E has formal complex multiplication, then by virtue of Corollary 7.2.8, it suffices to prove that $M := L \cap K(E_{p^\infty})$ is a finite extension of $K(\mu_{p^\infty})$. The Lie algebra $\mathrm{Lie}(\rho_E(G_K))$ attached to E is 2-dimensional, by Proposition 7.2.11 *(i)*. Thus $\mathrm{Gal}(K(E_{p^\infty})/K)$ is a 2-dimensional p-adic Lie group and so $\mathrm{Gal}(K(E_{p^\infty})/K(\mu_{p^\infty}))$ is 1-dimensional. As in the proof for Case (1) of Lemma 7.2.24, if we assume that M is of infinite degree over $K(\mu_{p^\infty})$, then the group $\mathrm{Gal}(K(E_{p^\infty})/M)$ must be finite, and thus $K(E_{p^\infty}) = M$ after a finite extension of K. That is, $K(E_{p^\infty})$ is contained in L. Thus we have a natural surjection $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(K(E_{p^\infty})/K)$ which induces a surjection of Lie algebras $\mathrm{Lie}(\mathrm{Gal}(L/K)) \twoheadrightarrow \mathrm{Lie}(\mathrm{Gal}(K(E_{p^\infty})/K))$. Since both Lie algebras are two-dimensional, the above surjection of Lie algebras must be an isomorphism. In view of Proposition 7.2.11 *(i)* and *(v)*, we have a contradiction. Therefore, M is a finite extension of $K(\mu_{p^\infty})$. □

Remark 7.2.27. Despite the above result, we cannot expect much about the cohomological coprimality of $V = V_p(E)$ and $V' = V_p(E')$ if at least one of E and E' has multiplicative reduction over K. For instance if E' has split multiplicative reduction, the theory of Tate curves shows that $H^0(H_{V'}, V')$ is non-trivial. On the other hand if E' has non-split multiplicative reduction, we are not certain if all the $J_{V'}$-cohomology groups of V' vanish or not. (But see Proposition 3.10 in [Oz09] for conditions where $H^0(J_{V'}, V')$ vanishes).

7.2.8 ℓ-adic cohomologies

In this section we give the proof of Theorem 2.4. Let us recall the hypotheses in the said theorem. Let ℓ and ℓ' be primes. Let X and X' be proper smooth varieties with potential good reduction over K and i and i' be non-zero integers. We consider the ℓ-adic representation $\rho_\ell : G_K \to \mathrm{GL}(V_\ell)$ where $V_\ell = H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell)$. We also consider the ℓ'-adic representation $\rho'_{\ell'} : G_K \to \mathrm{GL}(V'_{\ell'})$, where $V'_{\ell'} = H^{i'}_{\text{ét}}(X'_{\overline{K}}, \mathbb{Q}_{\ell'})$.

Theorem 7.2.28. *Let ℓ and ℓ' be distinct primes. Assume the above conditions. Then V_ℓ and $V'_{\ell'}$ are cohomologically coprime.*

Proof. We let $J_\ell = \rho_\ell(G_{K(V'_{\ell'})})$ and $J'_{\ell'} = \rho'_{\ell'}(G_{K(V_\ell)})$ We must show that V_ℓ has vanishing J_ℓ-cohomology and $V'_{\ell'}$ has vanishing $J'_{\ell'}$-cohomology. We identify G_ℓ with the Galois group $\mathrm{Gal}(K(V_\ell)/K)$ and J_ℓ with $\mathrm{Gal}(K(V_\ell)/K(V_\ell) \cap K(V'_{\ell'}))$. As ℓ and ℓ' are distinct, $K(V_\ell) \cap K(V'_{\ell'})$ must be a finite extension of K. Hence, J_ℓ is an open subgroup of G_ℓ. It follows from Lemma 7.2.3 that V_ℓ has vanishing J_ℓ-cohomology. Similarly, it can be shown that $V'_{\ell'}$ has vanishing $J'_{\ell'}$-cohomology. Therefore V_ℓ and $V'_{\ell'}$ are cohomologically coprime as claimed. □

Remark 7.2.29. In the above situation if $\ell \neq p$ and X has potential good reduction over K, then the field extension $K(V_\ell)$ contains the unique unramified $\mathbb{Z}_\ell$-extension of K. Thus if $\ell, \ell' \neq p$ and $\ell = \ell'$, then after a suitable extension of the base field K we may obtain $K(V_\ell) = K(V'_\ell)$. Hence, V_ℓ and V'_ℓ are *not* cohomologically coprime (after a finite extension).

7.3 Proofs in the global setting

In the following discussion F denotes an algebraic number field.

7.3.1 A preliminary lemma

Let S be a set of primes. Given a proper smooth variety X over F, we consider the system of ℓ-adic representations $(\rho_\ell : G_F \to \mathrm{GL}(V_\ell))_{\ell \in S}$ of G_F, where $V_\ell = H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_\ell)$, and the continuous representation $\rho_S = \prod_{\ell \in S} \rho_\ell$ as defined in Chapter 1. Recall from Lemma 5.4.3 that $F(\mu_{\ell^\infty})$ is a finite extension of $F(V_\ell) \cap F(\mu_{\ell^\infty})$ for each prime ℓ.

Lemma 7.3.1. *Let S be a set of primes and L be a Galois extension of F. Assume that $F(V_\ell) \cap L$ is a finite extension of F or of $F(V_\ell) \cap F(\mu_{\ell^\infty})$ for each $\ell \in S$. Put $J_S = \rho_S(G_L)$. Then V_S has vanishing J_S-cohomology.*

Proof. By Theorem 6.2.4, there exists a finite extension F'/F such that $(\rho_\ell|_{G_{F'}})_{\ell \in S}$ is an independent system. Let L' be the compositum of L and F'. It is a Galois extension of F'. Thus, Lemma 6.3.1 implies that $(\rho_\ell|_{G_{L'}})_{\ell \in S}$ is an independent system. Let L'' be the Galois closure of L'/L. This is of finite degree over L. Put $J''_S = \rho_S(G_{L''})$. Then J''_S is an open normal subgroup of J_S and applying Lemma 6.3.1 to the system $(\varrho_\ell|_{G_{F'}})$ with $H = G_{L''}$, we have $J''_S = \prod_{\ell \in S} \rho_\ell(G_{L''})$. It suffices to show that V_S has vanishing J''_S-cohomology. Indeed if this is so, then the vanishing of J_S-cohomology follows by Corollary 3.1.5 from the isomorphism

$$H^r(J_S, V_S) \simeq H^r(J_S/J''_S, {V_S}^{J''_S}), \tag{7.4}$$

for $r \geq 1$. Thus V_S has vanishing J_S-cohomology if V_S has vanishing J''_S-cohomology. Now, as cohomology commutes with direct sums (Proposition 3.1.2) we have

$$H^r(J''_S, V_S) = \bigoplus_{\ell \in S} H^r(J''_S, V_\ell)$$

for $r \geq 0$. Thus, it is enough to show that the cohomology groups $H^r(J''_S, V_\ell)$ vanish for each $\ell \in S$. For $\ell \in S$, let us write $J''_\ell = \rho_\ell(G_{L''})$. We identify $G_\ell = \rho_\ell(G_F)$ (resp. $H_\ell = \rho_\ell(G_{F(\mu_{\ell^\infty})})$) with the Galois group $\mathrm{Gal}(F(V_\ell)/F)$ (resp. $\mathrm{Gal}(F(V_\ell)/F(V_\ell) \cap F(\mu_{\ell^\infty}))$). Then we may identify J''_ℓ with $\mathrm{Gal}(F(V_\ell)/F(V_\ell) \cap L'')$. As $[F(V_\ell) \cap L'' : F(V_\ell) \cap L] \leq [L'' : L] < \infty$, our hypothesis implies that J''_ℓ is an open subgroup of G_ℓ or of H_ℓ. Thus V_ℓ has vanishing J''_ℓ-cohomology by Theorem 3. Arguing using an isomorphism similar to (7.4) applied to the extension $0 \to J''_\ell \to J''_S \to J''_S/J''_\ell \to 0$, it follows that V_ℓ has vanishing J''_S-cohomology. □

The above lemma allows us to obtain the S-adic version of Theorem 3:

Theorem 7.3.2. *Let S be a set of primes. Write $G_S = \rho_S(G_F)$ and $H_S = \rho_S(G_{F^{\mathrm{cyc}}})$. Then V_S has vanishing G_S-cohomology and vanishing H_S-cohomology.*

Proof. The statements of the theorem follow from Lemma 7.3.1 applied to $L = F$ and $L = F^{\mathrm{cyc}}$ respectively. The hypothesis of the said lemma clearly holds if $L = F$. If $L = F^{\mathrm{cyc}}$, the required hypothesis is true because of Theorem 6.2.4, Lemma 5.4.3 and Lemma 6.3.4. □

Let S and S' be sets of primes. Let X and X' be proper smooth varieties over F and i, i' be integers ≥ 0. We put $V_\ell = H^i_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_\ell)$ (resp. $V'_\ell = H^{i'}_{\text{ét}}(X'_{\overline{F}}, \mathbb{Q}_\ell)$) for $\ell \in S$ (resp. $\ell \in S'$). We consider two systems of ℓ-adic representations associated to X and X' respectively:

$$(\rho_\ell : G_F \to \mathrm{GL}(V_\ell))_{\ell \in S}$$

and

$$(\rho'_\ell : G_F \to \mathrm{GL}(V'_\ell))_{\ell \in S'}.$$

We also put $\rho_S = \prod_{\ell \in S} \rho_\ell$ and $\rho'_{S'} = \prod_{\ell \in S'} \rho'_\ell$, whose representation spaces are respectively denoted by V_S and $V'_{S'}$.

Theorem 7.3.3. *If $S \cap S' = \emptyset$, then V_S and $V'_{S'}$ are cohomologically coprime.*

Proof. We show that V_S has vanishing J_S-cohomology, where $J_S = \rho_S(G_{F(V'_{S'})})$. In view of Lemma 7.3.1, it suffices to show that $M := F(V_\ell) \cap F(V'_{S'})$ is a finite extension of F for each $\ell \in S$. We know from Theorem 6.2.4 that the system $(\rho'_{\ell'})_{\ell' \in S'}$ is almost independent. If $\ell \in S$ then the hypothesis and Lemma 6.2.3 implies that the system $(\rho'_{\ell'}, \rho_\ell)_{\ell' \in S'}$ obtained by adjoining ρ_ℓ to the system $(\rho'_{\ell'})_{\ell' \in S'}$ is almost independent. Replacing F by a finite extension we may assume that this system is independent. Thus the fields $F(V_\ell)$ and $F(V'_{S'})$ are linearly disjoint over F after some finite extension showing that M is a finite extension of F in the first place. By Lemma 7.3.1, V_S has vanishing J_S-cohomology. In a similar manner, we can show that $V'_{S'}$ has vanishing $J'_{S'}$-cohomology, where $J'_{S'} = \rho'_{S'}(G_{F(V_S)})$. □

7.3.2 The proof of Theorem 2.5

We recall the statement of the Theorem under consideration.

Theorem 7.3.4. *Let S and S' be sets of primes. Let E and E' be elliptic curves over F.*
(i) Assume that E and E' are not isogenous over $\overline{F}$. Then V_S and $V'_{S'}$ are cohomologically coprime.
(ii) If $S \cap S' = \emptyset$, then V_S and $V'_{S'}$ are cohomologically coprime.

For sets S and S' of primes, we write $F(E_{S^\infty})$ (resp. $F(E'_{S'^\infty})$) for the compositum of all the $F(E_{\ell^\infty})$ (resp. $F(E'_{\ell^\infty})$) as ℓ runs over the elements of S (resp. S'). We put $J_S := \rho_S(G_{F(E'_{S'^\infty})})$ and $J'_{S'} := \rho_{S'}(G_{F(E_{S^\infty})})$.

Proof of (i). To prove this, we must show that V_S has vanishing J_S-cohomology and $V'_{S'}$ has vanishing $J'_{S'}$-cohomology. We prove the former. First, we observe that if S'' is a subset of S' then J_S is a closed normal subgroup of $\mathcal{J}_S = \rho_S(G_{F(E'_{S''^\infty})})$. We see that the vanishing of J_S-cohomology implies the vanishing of $\mathcal{J}_S$-cohomology by using an isomorphism in the shape of (7.4) given by the extension $0 \to J_S \to \mathcal{J}_S \to \mathcal{J}_S/J_S \to 0$. Thus, we may assume that $S' = \Lambda$. We verify the hypothesis of Lemma 7.3.1 with $L = F(E'_{\Lambda^\infty})$; that is, we show that $M_\ell := F(E_{\ell^\infty}) \cap L$ is a finite extension of $F(\mu_{\ell^\infty})$ for each $\ell \in S$. We let $M = F(E_{\Lambda^\infty}) \cap L$. It is known that M is a finite extension of F^{cyc} (cf. [Se72], Théorèmes 6″ and 7). We also let

$$\begin{aligned} M_S &= F(E_{S^\infty}) \cap L = F(E_{S^\infty}) \cap M, \\ N_S &= F(E_{S^\infty}) \cap F^{\mathrm{cyc}}, \qquad \text{and} \\ N_\ell &= F(E_{\ell^\infty}) \cap F^{\mathrm{cyc}} = F(E_{\ell^\infty}) \cap N_S. \end{aligned}$$

Note further that $M_\ell = F(E_{\ell^\infty}) \cap M = F(E_{\ell^\infty}) \cap M_S$ for each $\ell \in S$. We have the following diagram of fields.

$$\begin{tikzcd}[column sep=small]
& & F(E_{\Lambda^\infty}) \arrow[dl, dash] \arrow[ddrr, dash] & & & & L = F(E'_{\Lambda^\infty}) \arrow[ddll, dash] \\
& F(E_{S^\infty}) \arrow[dl, dash] \arrow[ddrr, dash] & & & & & \\
F(E_{\ell^\infty}) \arrow[ddrr, dash] & & & & M \arrow[dl, dash] \arrow[dr, dash, bend left, "<\infty"] & & \\
& & & M_S \arrow[dl, dash] \arrow[dr, dash] & & F^{\mathrm{cyc}} \arrow[dl, dash] & \\
& & M_\ell \arrow[dr, dash] & & N_S \arrow[dl, dash] & & \\
& & & N_\ell \arrow[d, dash] & & & \\
& & & F(\mu_{\ell^\infty}) & & &
\end{tikzcd}$$

The extension M_ℓ/N_ℓ is of finite degree since $\mathrm{Gal}(M_\ell/N_\ell)$ is isomorphic to a quotient of the finite group $\mathrm{Gal}(M/F^{\mathrm{cyc}})$. Moreover N_ℓ is a finite extension of $F(\mu_{\ell^\infty})$ by Lemma 6.3.4. Thus the hypothesis of Lemma 7.3.1 holds. Therefore V_S has vanishing J_S-cohomology. Similarly, $V'_{S'}$ has vanishing $J'_{S'}$-cohomology. This completes the proof of (i). $\square$

Proof of (ii). This is a special case of Theorem 7.3.3 but we give another proof. If E and E' are not isogenous over $\overline{F}$, then this follows from (i). Suppose that E and E' are isogenous over $\overline{F}$. Then they are isogenous over some finite extension of F. Let F' be the Galois closure of this finite extension. Then the Isogeny Theorem (see Chapter 2) implies that $V_\ell \simeq V'_\ell$ as $G_{F'}$-modules for each $\ell \in S'$. We identify $\rho_S(G_{F'})$ (resp. $\rho_{S'}(G_{F'})$) with the Galois group $\mathrm{Gal}(F'(E_{S^\infty})/F')$ (resp. $\mathrm{Gal}(F'(E_{S'^\infty})/F')$). As S and S' are disjoint, applying Remark 6.2.2-(3) to the system $(\rho_\ell|_{G_{F'}}, \rho'_{\ell'}|_{G_{F'}})_{\ell \in S, \ell' \in S'} = (\rho_\ell|_{G_{F'}})_{\ell \in S \cup S'}$ shows that $[F'(E_{\ell^\infty}) \cap F'(E_{S'^\infty}) : F'] \leq [F'(E_{S^\infty}) \cap F'(E_{S'^\infty}) : F'] < \infty$ for each $\ell \in S$. Therefore V_S has vanishing $\mathcal{J}_S$-cohomology by Lemma 7.3.1, where $\mathcal{J}_S = \rho_S(G_{F'(E_{S'^\infty})})$. Then V_S has vanishing J_S-cohomology by arguing using the isomorphism of the form (7.4) with the extension $0 \to \mathcal{J}_S \to J_S \to J_S/\mathcal{J}_S \to 0$. In the same manner, we see that $V'_{S'}$ has vanishing $J'_{S'}$-cohomology. This ends the proof of Theorem 2.5. $\square$

Appendix A

Tannakian formalism

Let F be a field and Vec_F be the category of finite-dimensional vector spaces over F.

Definition A.1. A *neutral Tannakian category* over a field F is a rigid abelian tensor category $(\mathcal{C}, \otimes)$ such that $F = \mathrm{End}(\mathbb{1})$ for which there exists an exact faithful F-linear tensor functor $\omega : \mathcal{C} \to \mathrm{Vec}_F$.

Example A.2. Trivially, the category Vec_F is a neutral Tannakian category. If G is an affine group scheme over F, then the category $\mathrm{Rep}_F(G)$ of finite-dimensional representations of G over F is a neutral Tannakian category.

The main theorem of Tannakian formalism implies that every neutral Tannakian category is equivalent to the category of finite-dimensional representations of an affine group scheme.

Let $F : \mathcal{C} \to \mathcal{C}'$ and $G : \mathcal{C} \to \mathcal{C}'$ be tensor functors between two neutral Tannakian categories $\mathcal{C}$ and $\mathcal{C}'$. A *morphism of tensor functors* $\mathcal{F} \to \mathcal{G}$ is a morphism $\lambda : \mathcal{F} \to \mathcal{G}$ such that, for all families $(X_i)_{i \in I}$ of objects in $\mathcal{C}$, the diagram

$$\begin{tikzcd}
\otimes_{i\in I}\mathcal{F}(X_i) \arrow[r] \arrow[d, "\otimes_{i\in I}\lambda_{X_i}"] & \mathcal{F}(\otimes_{i\in I}X_i) \arrow[d, "\lambda_{\otimes_{i\in I}X_i}"] \\
\otimes_{i\in I}\mathcal{G}(X_i) \arrow[r] & \mathcal{G}(\otimes_{i\in I}X_i)
\end{tikzcd}$$

is commutative. An *isomorphism* of tensor functors is a morphism as above with two-sided inverse that is again a morphism of tensor functors.

Proposition A.3. Let $\mathcal{F} : \mathcal{C} \to \mathcal{C}'$ and $\mathcal{G} : \mathcal{C} \to \mathcal{C}'$ be tensor functors between two neutral Tannakian categories. Then every morphism of tensor functors $\lambda : \mathcal{F} \to \mathcal{G}$ is an isomorphism.

Let G be an affine group scheme over F. For two tensor functors $\mathcal{F}$: $\mathrm{Rep}_F(G) \to \mathrm{Vec}_F$ and $\mathcal{G}$: $\mathrm{Rep}_F(G) \to \mathrm{Vec}_F$, we denote by $\mathrm{Isom}^{\otimes}(F, G)$ the set of morphisms of tensor functors $\mathcal{F} \to \mathcal{G}$. For an F-algebra R, there is a canonical tensor functor $\phi_R : \mathrm{Vec}_F \to \mathrm{Mod}_R$, namely the extension of scalar functor $\phi_R(V) = V \otimes_F R$. Here, Mod_R denotes the category of finitely-generated modules over R.

We define $\underline{\mathrm{Isom}}^{\otimes}(\mathcal{F}, \mathcal{G})$ to be the functor of F-algebras such that

$$\underline{\mathrm{Isom}}^{\otimes}(\mathcal{F}, \mathcal{G})(R) = \mathrm{Isom}^{\otimes}(\phi_R \circ \mathcal{F}, \phi_R \circ \mathcal{G}).$$

For an F-algebra R, $\underline{\mathrm{Isom}}^{\otimes}(\mathcal{F}, \mathcal{G})(R)$ consists of the families $(\lambda_X)_{X \in \mathrm{Obj}(\mathrm{Rep}_F(G))}$, where $\lambda_X : \mathcal{F}(X) \otimes R \xrightarrow{\cong} \mathcal{G}(X) \otimes R$ is R-linear such that
(1) $\lambda_{X_1 \otimes X_2} = \lambda_{X_1} \otimes \lambda_{X_2}$
(2) $\lambda_{\mathbb{1}} = \mathrm{id}_R$, and
(3) for all G-equivariant maps $\alpha : X \to Y$, the diagram

$$\begin{tikzcd}
\mathcal{F}(X) \otimes_F R \arrow[r, "\mathcal{F}(\alpha) \otimes 1"] \arrow[d, "\lambda_X"] & \mathcal{F}(Y) \otimes_F R \arrow[d, "\lambda_Y"] \\
\mathcal{G}(X) \otimes_F R \arrow[r, "\mathcal{G}(\alpha) \otimes 1"] & \mathcal{G}(Y) \otimes_F R
\end{tikzcd}$$

is commutative.

When $\mathcal{F} = \mathcal{G}$, we use the notation

$$\underline{\mathrm{Aut}}^{\otimes}(\mathcal{F}) := \underline{\mathrm{Isom}}^{\otimes}(\mathcal{F}, \mathcal{F}).$$

Let ω : $\mathrm{Rep}_F(G) \to \mathrm{Vec}_F$ be the forgetful functor. Every $g \in G(R)$ defines an element of $\underline{\mathrm{Aut}}^{\otimes}(\omega)(R)$. Indeed, for each object X of $\mathrm{Rep}_F(G)$, we obtain a representation $\rho_X : G \to \mathrm{GL}(X \otimes_F R)$ by extension of scalars. Then we see that the family $(\rho_X(g))_{X \in \mathrm{Obj}(\mathrm{Rep}_F(G))}$ belongs to $\underline{\mathrm{Aut}}^{\otimes}(\omega)(R)$.

Proposition A.4 ([DM82], Proposition 2.8)**.** Let G be an affine group scheme over F. There is an isomorphism of functors of F-algebras $G \to \underline{\mathrm{Aut}}^{\otimes}(\omega)$.

Proposition A.5 ([DM82], Proposition 2.20)**.** Let G be an affine group scheme over F. Then G is algebraic if and only if $\mathrm{Rep}_F(G)$ has a tensor generator X; that is, every object of $\mathrm{Rep}_F(G)$ is isomorphic to a subquotient of $P(X, X^{\vee})$, where $P(t, s)$ is polynomial with coefficients in $\mathbb{N}$.

Let K be a p-adic field and denote by $\mathrm{Rep}(G_K)$ the category of p-adic representations of G_K. For an object $\rho : G_K \to \mathrm{GL}(V)$ of $\mathrm{Rep}(G_K)$ with non-zero dimension, we write G_V^{alg} for the Zariski closure of $G_V = \rho(G_K)$. Let

$\mathrm{Rep}(G_V^{\mathrm{alg}})$ denote the category of finite-dimensional p-adic representation of G_V^{alg}. We also write $\mathrm{Rep}_V(G_K)$ for the smallest sub-category of $\mathrm{Rep}(G_K)$ containing V.

Proposition A.6 ([Fo94], Proposition 1.2.3)**.** The categories $\mathrm{Rep}(G_V^{\mathrm{alg}})$ and $\mathrm{Rep}_V(G_K)$ are $\otimes$-equivalent.

Appendix B

Lie Algebras

Let F be a field of characteristic 0.

Definition B.1. A *Lie algebra* over a field F is a vector space $\mathfrak{g}$ over F together with an F-bilinear map

$$[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

(called the *bracket*) such that
(a) $[x, x] = 0$ for all $x \in \mathfrak{g}$,
(b) (Jacobi identity) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in \mathfrak{g}$.

A *homomorphism of Lie algebras* is an F-linear map $\alpha : \mathfrak{g} \to \mathfrak{g}'$ such that

$$\alpha([x, y]) = [\alpha(x), \alpha(y)] \qquad \text{for all } x, y \in \mathfrak{g}$$

A *Lie subalgebra* of a Lie algebra $\mathfrak{g}$ is an F-subspace $\mathfrak{h}$ such that $[x, y] \in \mathfrak{h}$ whenever $x, y \in \mathfrak{h}$. It becomes a Lie algebra with the bracket.

A Lie algebra $\mathfrak{g}$ is said to be *abelian* if $[x, y] = 0$ for all $x, y \in \mathfrak{g}$.

A subspace $\mathfrak{a}$ of $\mathfrak{g}$ is called an *ideal* if $[x, a] \in \mathfrak{a}$ for all $x \in \mathfrak{g}$ and $a \in \mathfrak{a}$.

Example B.2. (1) The associative F-algebra $\mathrm{Mat}_n(F)$ consisting of $n \times n$ matrices with entries from F is a Lie algebra (denoted by $\mathfrak{gl}_n$) endowed with the bracket

$$[A, B] = AB - BA \qquad A, B \in \mathrm{Mat}_n(F).$$

Let E_{ij} denote the matrix with 1 in the ijth position and 0 elsewhere. These matrices form a basis for $\mathfrak{gl}_n$, and

$$[E_{ij}, E_{i',j'}] = \begin{cases} E_{ij'} & \text{if } j = i' \\ -E_{i'j} & \text{if } i = j' \\ 0 & \text{otherwise.} \end{cases}$$

The following subspaces are Lie subalgebras of $\mathfrak{gl}_n$:

$$\mathfrak{sl}_n = \{A \in \mathrm{Mat}_n(F) : \mathrm{trace}(A) = 0\}$$
$$\mathfrak{b}_n = \{A = (a_{ij}) \in \mathrm{Mat}_n(F) : a_{ij} = 0 \text{ if } i > j\} \text{(upper triangular matrices)}$$

(2) More generally, let V be a vector space over F. From the associative algebra $\mathrm{End}_F(V)$ of F-linear endomorphisms of V, we obtain the Lie algebra $\mathfrak{gl}_V$ of endomorphisms of V with bracket

$$[\alpha, \beta] = \alpha \circ \beta - \beta \circ \alpha \qquad \alpha, \beta \in \mathrm{End}_F(V).$$

Similar to above, the endomorphism with trace 0 of a finite-dimensional vector space V form a Lie subalgebra $\mathfrak{sl}_V$ of $\mathfrak{gl}_V$.

Representations of Lie algebras

Definition B.3. A *representation* of a Lie algebra $\mathfrak{g}$ on an F-vector space V is a homomorphism $\rho : \mathfrak{g} \to \mathfrak{gl}_V$.

The F-vector space V is often called a $\mathfrak{g}$-module and we write $x \cdot v$ for $\rho(x)(v)$. With this notation,

$$[x, y] \cdot v = x \cdot (y \cdot v) - y \cdot (x \cdot v).$$

We say that the representation ρ is *faithful* if it is injective.

Example B.4. Let $\mathfrak{g}$ be a Lie algebra. For a fixed $x \in \mathfrak{g}$, the linear map $\mathfrak{g} \to \mathfrak{g}$ defined by $y \mapsto [x, y]$ is called the *adjoint map* of x, denoted by $\mathrm{ad}_{\mathfrak{g}}(x)$ or simply ad x. The representation $\mathrm{ad}_{\mathfrak{g}} : \mathfrak{g} \to \mathrm{End}_{\mathfrak{g}}$ defined by $x \mapsto \mathrm{ad}\, x$ is called the *adjoint representation* of $\mathfrak{g}$.

Borel and Cartan subalgebras

Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over a field F of characteristic 0. The *derived series* $(D^m\mathfrak{g})_{m \in \mathbb{Z}_{\geq 1}}$ of ideals of $\mathfrak{g}$ is defined inductively by $D^1\mathfrak{g} = \mathfrak{g}$, and $D^m\mathfrak{g} = [D^{m-1}\mathfrak{g}, D^{m-1}\mathfrak{g}]$ for $m > 1$. A Lie algebra $\mathfrak{g}$ is said to be *solvable* if its derived series terminates in the zero subalgebra; that is, there exists an integer m such that $D^m\mathfrak{g} = \{0\}$.

Definition B.5. A *Borel subalgebra* $\mathfrak{b}$ of a Lie algebra $\mathfrak{g}$ is a maximal solvable Lie subalgebra of $\mathfrak{g}$.

The *descending central series* $(C^m\mathfrak{g})_{m \in \mathbb{Z}_{\geq 1}}$ of ideals of $\mathfrak{g}$ is defined inductively by $C^1\mathfrak{g} = \mathfrak{g}$, and $C^m\mathfrak{g} = [\mathfrak{g}, C^{m-1}\mathfrak{g}]$ for $m \geq 2$. A Lie algebra $\mathfrak{g}$ is said to be *nilpotent* if its descending central series terminates in the zero subalgebra; that is, there exists an integer m such that $C^m\mathfrak{g} = \{0\}$.

Definition B.6. A *Cartan subalgebra* $\mathfrak{h}$ of a Lie algebra $\mathfrak{g}$ is a nilpotent Lie subalgebra which is equal to its own normalizer.

Proposition B.7 ([Bo08-2], Ch.7, §2.1, Proposition 5)**.** Let $\mathfrak{g}$ be a Lie algebra with center $\mathfrak{c}$ and $\mathfrak{h}$ be a vector subspace of $\mathfrak{g}$. Then $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$ if and only if $\mathfrak{h}$ contains $\mathfrak{c}$ and $\mathfrak{h}/\mathfrak{c}$ is a Cartan subalgebra of $\mathfrak{g}/\mathfrak{c}$.

Definition B.8. A Lie algebra $\mathfrak{g}$ over F is called *semisimple* if its only abelian ideal is $\{0\}$. An element x of a semisimple Lie algebra $\mathfrak{g}$ is said to be *semisimple* if ad x is semisimple (that is, represented by a diagonal matrix after extending the base field).

Proposition B.9 ([Bo08-2], Ch.7, §2.4, Theorem 2)**.** Let $\mathfrak{g}$ be a semisimple Lie algebra over F and $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$. Then $\mathfrak{h}$ is commutative, and all its elements are semisimple in $\mathfrak{g}$.

Bibliography

[Ber02] L. Berger, *Représentations p-adiques et équations différentielles*, Invent. Math. **148**, 2002, 219–284.

[BK86] S. Bloch and K. Kato, *p-adic étale cohomology*, Inst. Hautes Études Sci. Publ. Math. No. 63 (1986), 107–152.

[Bo80] F. A. Bogomolov, *Sur l'algébricité des représentations ℓ-adiques*, C. R. Acad. Sc. Paris, **t. 290**, 1980, pp. 701–703.

[Bor91] A. Borel, *Linear Algebraic Groups*, 2nd edition, *Graduate Texts in Math.* **126** Springer, 1991.

[Bo08-1] N. Bourbaki, *Lie Groups and Lie Algebras, Chapters 1–3*, Translated from the French, *Elements of Mathematics* (Berlin), Springer-Verlag Berlin Heidelberg, 2008.

[Bo08-2] N. Bourbaki, *Lie Groups and Lie Algebras, Chapters 7–9*, Translated from the French, *Elements of Mathematics* (Berlin), Springer-Verlag Berlin Heidelberg, 2008.

[CE48] C. Chevalley and S. Eilenberg, *Cohomology Theory of Lie Groups and Lie Algebras* Trans. Amer. Math. Soc. **63**, 1, 1948, pp. 85–124.

[CLS98] B. Chiarellotto and B. Le Stum , *Sur la pureté de la cohomologie cristalline*, C.R. Acad. Sci. Paris **326**, Série I 1998, pp. 961–963.

[CH01] J. Coates and S. Howson, *Euler Characteristics and elliptic curves II*, Journal of Math. Society of Japan, **53**, 2001, 175–235.

[CSS03] J. Coates, P. Schneider, and R. Sujatha, *Links Between Cyclotomic and* GL_2 *Iwasawa Theory*, Documenta Mathematica, Extra Volume Kato, 2003, 187–215.

[CS99] J. Coates and R. Sujatha, *Euler-Poincaré characteristics of abelian varieties*, C.R. Acad. Sci. Paris, **329**, Série I, 1999, 309–313.

[CSW01] J. Coates, R. Sujatha, and J-P. Wintenberger, *On Euler-Poincaré characteristics of finite dimensional p-adic Galois representations*, Inst. Hautes Études Sci. Publ. Math., **93** 2001, 107–143.

[De74] P. Deligne, *La conjecture de Weil I*, Inst. Hautes Études Sci. Publ. Math., **43** 1974, 273–308.

[De80] P. Deligne, *La conjecture de Weil II*, Inst. Hautes Études Sci. Publ. Math., **52** 1980, 137–252.

[DM82] P. Deligne and J. S. Milne, *Tannakian Categories*, in: P. Deligne, J. S. Milne, A. Ogus, K. Y. Shih (ed.), *Hodge cycles, motives and Shimura varieties*, Lecture Notes in Math. **900**, Springer, 1982.

[Di14-1] J. Dimabayao, *On the vanishing of cohomologies of p-adic Galois representations associated with elliptic curves*, to appear in Kyushu Journal of Mathematics.

[Di14-2] J. Dimabayao, *On the cohomological coprimality of Galois representations associated with elliptic curves*, preprint 2014.

[DDSMS99] J.D. Dixon, M.P.F. Du Sautoy, A. Mann, and D. Segal, *Analytic Pro-p Groups*, Cambridge Studies in Advanced Mathematics **61**, Cambridge University Press, 2nd ed., 1999.

[Fa83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73**, 1983, no.3, 349–366.

[Fa88] G. Faltings, *p-adic Hodge theory*, J. Amer. Math. Soc. **1**, 1988, 255–288.

[Fa02] G. Faltings, *Almost étale extensions*, in *Cohomologies p-adiques et applications arithmetiques*, II. Astérisque **279**, 2002, 185–270.

[Fo94] J.-M. Fontaine, *Représentations p-adiques semistables*, in *Périodes p-adiques (Bures-sur-Yvette, France, 1988),* (J-M Fontaine ed.), Astérisque **223**, Soc.Math.France, Montrouge, 1994, 113–184.

[Gr10] A. Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19**, 2010, no.4, 495–507.

[HS53] G. Hochschild and J.-P. Serre, *Cohomology of group extensions*, Trans. Amer. Math. Soc. **74**, 1953, 110–134.

[Il94] L. Illusie, *Réduction semi-stable ordinaire, cohomologie étale p-adique et Cohomologie de de Rham, d'apres Bloch-Kato et Hyodo* in *Périodes p-adiques (Bures-sur-Yvette, France, 1988),* (J-M Fontaine ed.), Astérisque **223**, Soc.Math.France, Montrouge, 1994, 209–220.

[Il10] L. Illusie, *Constructibilité générique et uniformité en ℓ*, Orsay, 2010, unpublished.

[Im75] H. Imai, *A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions*, Proc. Japan Acad. **51**, 1975, 12–16.

[Ja10] U. Jannsen, *Weights in arithmetic geometry*, Japan J. Math. **5**, 2010, 73–102.

[KM74] N. Katz and W. Messing, *Some consequences of the Riemann hypothesis for varieties over finite fields*, Invent. Math. **23**, 1974, 73–77.

[Ko02] H. Koch, *Galois theory of p-extensions* With a foreword by I. R. Shafarevich. Translated from the 1970 German original by Franz Lemmermeyer. With a postscript by the author and Lemmermeyer. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.

[KT13] Y. Kubo and Y. Taguchi, *A generalization of a theorem of Imai and its applications to Iwasawa theory*, Mathematische Zeitschrift(2013), DOI 10.1007/s00209-103-1176-3.

[LT76] S. Lang and H. Trotter, *Frobenius Distributions in* GL_2*-Extensions*, Lecture Notes in Mathematics **504**, Berlin: Springer, 1976.

[La65] M. Lazard, *Groupes analytiques p-adiques*, Inst. Hautes Études Sci. Publ. Math. **26**, 1965, 389–603.

[NSW08] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Grundlehren der Mathematischen Wissenschaften, **323**, Springer-Verlag, 2nd ed., 2008.

[Oz09] Y. Ozeki, *Torsion Points of Abelian Varieties with Values in Infinite Extensions over a p-adic Field*, Publ. RIMS, Kyoto University, **45**, 2009, 1011–1031.

[OT14] Y. Ozeki and Y. Taguchi, *On congruences of Galois representations of number fields*, Publ. RIMS, Kyoto University, **50**, 2014, 287–306.

[PR94] B. Perrin-Riou, *Représentations p-adiques ordinaires* in *Périodes p-adiques (Bures-sur-Yvette, France, 1988),* (J-M Fontaine ed.), Astérisque **223**, Soc.Math.France, Montrouge, 1994, 185–208.

[Ri76] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98**, 1976, no. 3, 751–804.

[Sen73] S. Sen, *Lie algebras of Galois groups arising from Hodge-Tate modules*, Ann. of Math. **97**, 1973, 160–170.

[Se71] J.-P. Serre, *Sur les groupes de congruence des variétiés abéliennes II*, Izv. Akad. Nauk SSSR Ser. Mat., **35** : 4, 1971, 731–735.

[Se72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15**, 1972, no. 4, 259–331.

[Se76] J.-P. Serre, *Représentations ℓ-adiques*, Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci. Univ. Kyoto, Kyoto, 1976), 177-193. Japan Soc. Promotion Sci., Tokyo, 1977.

[Se89] J-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, With the collaboration of Willem Kuyk and John Labute. Second Edition. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[Se13] J.-P. Serre, *Un critére d'indépendance pour une famille de représentations ℓ-adiques*, Commentarii Mathematici Helvetici **88** (2013), 543–576.

[Su00] R. Sujatha, *Euler-Poincaré characteristics of p-adic Lie groups and arithmetic*, Proceedings of the International Conference on Algebra, Arithmetic and Geometry TIFR (2000), 585–619.

[Ta67] J. Tate, *p-divisible groups*, Proceedings of a Conference on Local Fields, Driebergen, 1966, Springer, 1967, pp. 158–183.

[Ts99] T. Tsuji, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Invent. Math. **137**, 1999, pp. 233–411.

[Ze09] S. L. Zerbes, *Generalised Euler characteristics of Selmer groups*, Proc. London Math. Soc. (2009), DOI: 10.1112/plms/pdn049.