ℓ-adic Representations of Curves over Local Fields

Lambert A'Campo
Supervised by Vladimir Dokchitser

April 22, 2020

Abstract

This text is the result of a 'mini-project' part of the first year of the London School of Geometry and Number Theory (LSGNT). It is written for a reader familiar with first properties of the Galois theory of local fields and the arithmetic of elliptic curves over local fields, in particular the reduction of elliptic curves. The aim is to describe the ℓ-adic representations associated to curves over non-archimedean local fields. For this we first discuss some generalities on the structure of such representations. Then we move on to Tate modules of elliptic curves which form an important simplified case in which the description we give is very explicit, so that the tools given should allow the reader to determine the ℓ-adic representation of any elliptic curve they are presented with. Our treatment of higher genus curves is less in-depth and refers to the literature for most proofs but should nonetheless show the methods in examples and discuss the differences to the case of elliptic curves. We conclude with a small application of the theory to the inverse Galois problem and prove a restriction on the dimension of absolutely irreducible ℓ-adic representations of local Galois groups.

Contents

1 Introduction

Amongst the many new developments inspired by the highly influential conjectures posed by André Weil [Wei49] about 70 years ago is the theory of ℓ-adic cohomology and with it the theory of ℓ-adic Galois representations. His conjectures concern the number of $\mathbb{F}_q$-points on projective varieties and his revolutionary idea was to study the number of such solutions with tools from algebraic topology such as the Lefschetz trace formula. For this, a cohomology theory for general algebraic varieties in characteristic p was necessary. To obtain results on the absolute number of solutions and not just their congruence class modulo p, the coefficient field of such a cohomology theory would need to have characteristic 0, it turns out that one can take $\mathbb{Q}_\ell$ as such a field [Mil13, I.19]. Then to count the number of solutions one has to calculate the eigenvalues of the Frobenius automorphism acting on these cohomology groups [Mil13, II]. This is already an example of an ℓ-adic representation of the absolute Galois group of the finite field $\mathbb{F}_q$, i.e. a continuous homomorphism $G_{\mathbb{F}_q} \to \mathrm{GL}_n(\mathbb{Q}_\ell)$, where $G_{\mathbb{F}_q} \cong \hat{\mathbb{Z}}$ carries the profinite topology.

The subject of this text are continuous representations $G_K \to \mathrm{GL}_n(\mathbb{Q}_\ell)$, where K is a discretely valued, complete field with finite residue field k and ℓ is a prime different from the characteristic of k. The case when ℓ equals the characteristic of k is completely different and falls under the name p-adic Hodge Theory which we do not discuss. Since there is a natural surjection $G_K \to G_k$ one can see the representations involved with the Weil conjectures as a special case and indeed they play an important role in understanding the more general representations. Nowadays ℓ-adic representations of Galois groups are a major area of research. Especially the representations of the absolute Galois group $G_\mathbb{Q}$ remain mysterious and are the protagonist of many conjectures, as outlined in [Tay04]. Although we only study the local case, i.e. representations of groups such as $G_{\mathbb{Q}_p}$, this still has consequences for the group $G_\mathbb{Q}$ since $G_{\mathbb{Q}_p}$ sits inside $G_\mathbb{Q}$ as a decomposition group and by the Chebotarev Density Theorem we even know that in theory studying all of these decomposition groups should answer all questions about $G_\mathbb{Q}$. Later we give an example application of this idea to the inverse Galois problem.

For whichever reasons one might be interested in ℓ-adic representations of G_K, section 2 should explain their shape. We can usually assume that a lift of the Frobenius from G_k to G_K acts by a diagonalisable operator. In that case ℓ-adic representations differ from continuous representations $G_K \to \mathrm{GL}_n(\mathbb{C})$ which always have a finite image by two classes of representations. Firstly, there are unramified characters $\chi : G_k \to \overline{\mathbb{Q}_\ell}^\times$ which are determined by their value on the Frobenius and can have infinite image such as the cyclotomic character. Secondly for any integer $n \geq 2$, there is a reducible but indecomposable n-dimensional representation $sp(n)$, called the special ℓ-adic representation on which the inertia group of K acts through an infinite image, see definition 8. Then theorems 6 and 13 describe how these representations combine with representations with finite image to produce all ϕ_K-semisimple representations of G_K. Moreover, we introduce the concept of a Weil-Deligne representation as in [Del72] and show how it is used to define 'independence of ℓ' (definition 17). This allows us to say what it means for an ℓ-adic and ℓ'-adic representation to be isomorphic.

In section 3, the heart of this document, we discuss the representation on the ℓ-adic Tate module of an elliptic curve E/K which we denote by $V_\ell E$. Theorem 37 describes $V_\ell E$ in terms of the reduction types of E and its content is summarised in figure 3. For instance the representation is unramified if and only if E has good reduction. Moreover, in theorem 38 we show that this representation is independent of ℓ. This also shows that in practice the finite group representations involved in the structure of the representation associated to E are not very big, see for instance corollary 39. The case of elliptic curves illustrates many proof methods while at the same time not requiring too much technical machinery. Further it is possible to compute explicit examples such as

Example 42. *Consider the elliptic curve $E : y^2 = x^3 - px$ over $\mathbb{Q}_p$ where $p > 3$. It has additive reduction which becomes good over $\mathbb{Q}_p(p^{1/4})$ and the automorphism g of $\mathbb{Q}_p(p^{1/4}, i)$ which sends*

$p^{1/4} \mapsto ip^{1/4}$ acts on $\tilde{E} : y^2 = x^3 - x$ by $(x, y) \mapsto (-x, iy)$ where $i \in \overline{\mathbb{Q}_p}$ is a root of $x^2 + 1 = 0$. Moreover, the characteristic polynomial of g acting on $V_\ell E$ is $T^2 + 1$.

If $p \equiv 3 \pmod 4$, then $V_\ell E \otimes \overline{\mathbb{Q}_\ell}$ has the form

$$\rho(g) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \rho(\mathrm{Frob}_p) = \begin{pmatrix} 0 & \sqrt{-p} \\ \sqrt{-p} & 0 \end{pmatrix}$$

If $p \equiv 1 \pmod 4$, then $V_\ell E \otimes \overline{\mathbb{Q}_\ell}$ has the form

$$\rho(g) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \rho(\mathrm{Frob}_p) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

for some explicitly computable α, β.

This is very helpful for the next section, where we outline the same theory for higher genus curves. The main focus in that section lies on showing examples to illustrate the general results rather than explaining why they are true. For instance we show

Example 67. *Consider the plane curve $C : xy(x + 2y - 1)(2x + y - 1) = p$ over $\mathbb{Q}_p$ for $p > 2$. Then $V_\ell \operatorname{Pic}^0(C) \cong \chi_{cyc} \otimes sp(2)^{\oplus 3}$.*

In section 5 we end by showing some applications of the theory by constructing explicit Galois representations with special properties. In particular we construct an elliptic curve $E/\mathbb{Q}$ and a large set of primes ℓ such that the map $G_\mathbb{Q} \to \mathrm{Aut}(E[\ell])$ is surjective:

Proposition 72. *Let $E : y^2 = x^3 + 5x^2 + 7^4 \cdot 5^2$, then the action $G_\mathbb{Q} \to \mathrm{Aut}(E[\ell])$ is surjective for all primes $\ell \notin \{5, 7\}$.*

Finally, our propositions 74 and 75 pose a restriction on the dimension of absolutely irreducible ℓ-adic representations of G_K as hinted at in [AD17, footnote 2]. These imply for instance

Corollary 76. *Let $p \neq 2, 3$ and $K/\mathbb{Q}_p$ a finite extension. Moreover, let d be a prime such that $2d + 1$ is not a prime, then there is no abelian variety A/K of dimension d whose associated Galois representation $V_\ell A$ is absolutely irreducible. In particular there are no abelian varieties $A/\mathbb{Q}_p$ of dimension $7, 13$ or 17 with absolutely irreducible $V_\ell A$.*

This restriction explains why constructing an abelian variety $A/\mathbb{Q}$ of arbitrary dimension with surjective Galois representation is more difficult than in the elliptic curve case.

1.1 Notation

For convenience we list some common notations that are used throughout the text. For any field F we write $\overline{F}$ for a separable closure of F and G_F for $\mathrm{Gal}(\overline{F}/F)$ and K is always a local field with finite residue field.

Symbol	Meaning
K	field, complete with respect to a discrete valuation and finite residue field
$\mathcal{O}_K$	ring of integers of K
$\mathfrak{m}_K$	maximal ideal of $\mathcal{O}_K$
k	residue field of K
p	characteristic of k
q	cardinality of k
ℓ	prime different from p
I_K	inertia group of K
P_K	wild inertia group of K
Frob_k	the Frobenius automorphism of k
Frob_K	the arithmetic Frobenius, i.e. a lift of Frob_k to G_K
ϕ_K	The geometric Frobenius, i.e. a lift of Frob_k^{-1} to G_K

Figure 1: Notation for objects related to the local field K.

Symbol	Meaning
χ_{cyc}	The ℓ-adic cyclotomic character, see definition 5.
$V(n)$	nth Tate twist of V, i.e. $V(n) = V \otimes \chi_{cyc}^n$
t_ℓ	The tame ℓ-adic character, see definition 7.
$sp(n)$	The special ℓ-adic representation, see definition 8.
$T_\ell E$	The ℓ-adic Tate module of an elliptic curve E or abelian group E, see subsection 3.1.
$V_\ell E$	$T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$

Figure 2: Notation for representations of G_K.

2 Representation Theory

The subject of the present section is the structure of continuous representations $\rho : G_K \to \mathrm{GL}_n(F)$, where F is a finite extension of $\mathbb{Q}_\ell$ and K is a field complete with respect to a discrete valuation and finite residue field k of characteristic $p \neq \ell$. These are called ℓ-adic representations. The aim is to explain and prove the structural theorems stated in [DA14]. These are also proven in [Del72, §4, §8] and its elaboration [Roh94] but we reprove all the statements we need to make the exposition more readable and self-contained.

One of the reasons for the interest in the coefficient field $\mathbb{Q}_\ell$ is the existence of continuous representations of G_K with infinite image, as opposed continuous representations $G_K \to \mathrm{GL}_n(\mathbb{C})$ which land in a compact and hence finite subgroup of $\mathrm{GL}_n(\mathbb{C})$. Recall [CF67, I.§7 Theorem 2] that there is a short exact sequence $1 \to I_K \to G_K \to G_k \to 1$, where I_K is the inertia group of K and the map $G_K \to G_k$ is given by the action of G_K on $k = \mathcal{O}_K/\mathfrak{m}_K$, where $\mathcal{O}_K$ is the ring of integers of K and $\mathfrak{m}_K$ is its maximal ideal. Fix a geometric Frobenius $\phi_K \in G_K$, i.e. an element which reduces to $\mathrm{Frob}_k^{-1} \in G_k$. It turns out that for the ℓ-adic representations of K which interest us, ϕ_K acts as a diagonalisable operator. In particular this is the case for the Tate module of an elliptic curve or more generally of an abelian variety. The essence of this section boils down to the classification of the possible infinite pieces of such so-called ϕ_K-semisimple representations.

Definition 1 (ϕ_K-semisimplicity)**.** Let V be a continuous G_K-representation, then V is ϕ_K-semisimple if ϕ_K acts semisimply on $V^{I'}$ for all open subgroups $I' < I_K$, where I_K is the inertia group of K.

There are only two kinds of such infinite pieces. Firstly there are unramified characters: For any $a \in \mathcal{O}_{\overline{\mathbb{Q}_\ell}}$, there is a unique continuous character $\chi : G_K \to \overline{\mathbb{Q}_\ell}^\times$ such that $\chi(\phi_K) = a$ and $\chi(I_K) = 1$. The prototypical example is the cyclotomic character $\chi_{cyc} : G_K \to \mathbb{Z}_\ell^\times$ which is determined by the equation $g(\zeta_{\ell^r}) = \zeta_{\ell^r}^{\chi_{cyc}(g)}$, where ζ_{ℓ^r} is a primitive ℓ^rth root of unity. Thus we have $\chi_{cyc}(\phi_K) = q^{-1}$, where q is the cardinality of k.

Secondly, for each integer $n \geq 2$, there is a reducible, indecomposable representation $sp(n)$ of dimension n, called the special ℓ-adic representation (definition 8). The special ℓ-adic representation arises from a surjection $t_\ell : I_K \to \mathbb{Z}_\ell$ called the tame ℓ-adic character (definition 7) which in the case of $K = \mathbb{Q}_p$ simply satisfies $g(p^{1/\ell^r}) = \zeta_{\ell^r}^{t_\ell(g)} p^{1/\ell^r}$. Now $g \in I_K$ acts on $sp(n)$ by $\exp(t_\ell(g)N)$ where N is an indecomposable nilpotent operator on $\mathbb{Q}_\ell^n$.

Then theorems 6 and 13 below describe how these infinite pieces combine with representations with finite image to produce all ϕ_K-semisimple representations of G_K:

Theorem 6. *Let F be a topological perfect field and $\rho : G_K \to \mathrm{GL}_n(F)$ a continuous ϕ_K-semisimple representation with underlying vector space V such that $\rho(I_K)$ is finite and the eigenvalues of $\rho(\phi_K)$ are contained in F. Then there exists an isomorphism of G_K-representations*

$$V \cong \bigoplus_i \chi_i \otimes V_i,$$

where χ_i are unramified characters such that the $\chi_i(\phi_K)$ are the eigenvalues of $\rho(\phi_K)$ and V_i are representations of G_K over F such that the kernel of $G_K \to \mathrm{GL}(V_i)$ is an open subgroup.

Theorem 13. *Let F be a finite extension of $\mathbb{Q}_\ell$, $\ell \neq p$. Let $\rho : G_K \to \mathrm{GL}_n(F)$ be a continuous ϕ_K-semisimple representation with underlying vector space V such that all the eigenvalues of ϕ_K are contained in F. Then*

$$V \cong \bigoplus_i V_i \otimes_{\mathbb{Q}_\ell} sp(n_i),$$

for some positive integers n_i and continuous ϕ_K-semisimple representations V_i such that I_K acts through a finite quotient on V_i.

Theorem 6 says that ϕ_K-semisimple representations on which inertia acts through a finite quotient consist of unramified characters and representations of finite Galois groups (representations which factor through a finite quotient of G_K are also called Artin representations). If inertia acts through an infinite image then theorem 13 says that the only new ingredients are the the special ℓ-adic representations, which are reducible, indecomposable representations of G_K such that I_K acts through an infinite image. In summary, indecomposable ϕ_K-semisimple ℓ-adic representations of G_K over a sufficiently large coefficient field look like

$$(\text{ unramified character }) \otimes (\text{ Artin representation }) \otimes sp(n).$$

Finally, we discuss how we can vary ℓ, i.e. we define what it means for an ℓ-adic and an ℓ'-adic representation to be compatible, see definition 17. This is done via the formalism of Weil-Deligne representations. Often one has many possible choices for the prime ℓ and this explains in what sense ρ_ℓ can be independent of ℓ. Below we show that Tate modules of elliptic curves have this independence of ℓ property and again any 'geometric' example is expected to have this property. Beyond providing a conceptual reassurance that we don't have to consider all primes ℓ this has explicit consequences for the arithmetic of elliptic curves (e.g. Corollary 39).

2.1 Structure Theory

We need generalities about semisimplicity and change of coefficient field.

Lemma 2. *Let F be a perfect field and F'/F a field extension. If V is a semisimple $F[x]$-module, then $V \otimes_F F'$ is a semisimple $F'[x]$-module.*

Proof. Since the tensor product distributes over direct sums we may assume without loss of generality that V is simple. Then $V \cong F[x]/(f)$ for some irreducible polynomial $f \in F[x]$. Since F is perfect, f has distinct factors in any field extension. Consequently the chinese remainder theorem shows that $F' \otimes_F V \cong F'[x]/(f)$ is semisimple. □

Lemma 3. *Let A, B be not necessarily commutative rings with a ring map $A \to B$ which makes B into a free A-module. Assume M is an A-module such that $B \otimes_A M$ is a semisimple B-module. Then M is a semisimple A-module.*

Proof. We show that every short exact sequence of A-modules of the form $0 \to M' \to M \to M'' \to 0$ splits. If we are given such a sequence, then

$$0 \to B \otimes M' \to B \otimes M \to B \otimes M'' \to 0$$

is exact since B is free over A. By semisimplicity of $B \otimes M$ the sequence splits with a B-linear section $\sigma : B \otimes M'' \to B \otimes M$.

The map $M \to B \otimes M : m \mapsto 1 \otimes m$ is injective and so we may define a section $\tilde{\sigma} : M'' \to M$ by $\tilde{\sigma}(x) = \pi(\sigma(1 \otimes x))$, where $\pi : B \otimes M \to B \otimes M$ is induced by a A-linear projection $B \to A$ with $1 \mapsto 1$. $\tilde{\sigma}$ is A-linear and furnishes the desired splitting of the original sequence. □

Corollary 4. *Let F be a perfect field and $\rho : G_K \to \mathrm{GL}_n(F)$ a representation, then the following are equivalent*

(a) ρ is ϕ_K-semisimple;

(b) $\rho \otimes_F F'$ is ϕ_K-semisimple for all field extensions F'/F;

(c) $\rho(\phi_K)$ is diagonalisable over a finite extension F'/F.

Proof. Lemma 2 shows $(a) \implies (b)$. The implication $(b) \implies (c)$ just follows from taking F' to be extension obtained by adjoining the eigenvalues of $\rho(\phi_K)$. For $(c) \implies (a)$ we not that if $\rho(\phi_K)$ is diagonalisable then clearly ρ is ϕ_K-semisimple and apply lemma 3 to the ring map $F[\phi_K] \to F'[\phi_K]$. □

The absolute Galois group G_K of K is a split extension

$$1 \to I_K \to G_K \to \overline{\langle \phi_K \rangle} \to 1,$$

where $I_K < G_K$ is the inertia group of K and $\overline{\langle \phi_K \rangle}$ is the closure of the group generated by ϕ_K. There is a natural isomorphism $\overline{\langle \phi_K \rangle} \cong \hat{\mathbb{Z}} \cong G_k$, where G_k is the absolute Galois group of k. A representation ρ is called unramified if $\rho(I_K) = 1$, i.e. it is just a representation of G_k. In particular an unramified character is determined by its value on ϕ_K. The first example of such a character and an ℓ-adic representation with infinite image is the cyclotomic character:

Definition 5. The ℓ-adic cyclotomic character $\chi_{cyc} : G_K \to \mathbb{Z}_\ell^\times$ is the character such that $g(\zeta_{\ell^r}) = \zeta_{\ell^r}^{\chi_{cyc}(g)}$ for any $g \in G_K$ and primitive ℓ^rth root of unity ζ_{ℓ^r}.

Note that $\chi_{cyc}(\phi_K) = q^{-1}$. This character appears very often in the sequel and we also write $\mathbb{Z}_\ell(1)$ for the free $\mathbb{Z}_\ell$-module of rank one equipped with a G_K-action by χ_{cyc}. More generally for a $\mathbb{Z}_\ell[G_K]$-module V we write $V(n) := V \otimes_{\mathbb{Z}_\ell} \chi_{cyc}^n$ for $n \in \mathbb{Z}$. The first part of the structure theory basically just comes from the split exact sequence $1 \to I_K \to G_K \to G_k \to 1$.

Theorem 6. *Let F be a topological perfect field and $\rho : G_K \to \mathrm{GL}_n(F)$ a continuous ϕ_K-semisimple representation with underlying vector space V such that $\rho(I_K)$ is finite and the eigenvalues of $\rho(\phi_K)$ are contained in F. Then there exists an isomorphism of G_K-representations*

$$V \cong \bigoplus_i \chi_i \otimes V_i,$$

where χ_i are unramified characters such that the $\chi_i(\phi_K)$ are the eigenvalues of $\rho(\phi_K)$ and V_i are representations of G_K over F such that the kernel of $G_K \to \mathrm{GL}(V_i)$ is an open subgroup.

Proof. Let ρ be a ϕ_K-semisimple representation such that $\rho(I_K)$ is finite and V its underlying vector space. Set $G = \rho(G_K)$ and $I = \rho(I_K)$, then there is a split short exact sequence

$$1 \to I \to G \to \langle \rho(\phi_K) \rangle \to 1. \tag{1}$$

Since I is finite, so is $\mathrm{Aut}(I)$ and thus $(g \mapsto \rho(\phi_K)^a g \rho(\phi_K)^{-a}) = \mathrm{id}_I$ for some $a \geq 1$. By assumption $\rho(\phi_K)$ is diagonalisable and

$$V \cong \bigoplus_i W_i,$$

where W_i are Eigenspaces of ϕ_K with eigenvalues λ_i. Let $v \in W_i$, and $g \in I_K$, then $\rho(g)$ and $\rho(\phi_K^a)$ commute, hence $\phi_K^a g v = g \phi_K^a v = \lambda_i^a g v$. Thus for any eigenvalue μ of ϕ_K^a, G_K acts on the eigenspace $V_\mu = \bigoplus_{j:\lambda_j^a = \mu} W_j$.

For each such μ choose an index i satisfying $\lambda_i^a = \mu$ and let χ_μ be the unramified character such that $\chi_\mu(\phi_K) = \lambda_i$. Then

$$V \cong \bigoplus_\mu \chi_\mu \otimes (\chi_\mu^{-1} \otimes V_\mu)$$

and it remains to show that an open subgroup of G_K acts trivially on $(\chi_\mu^{-1} \otimes V_\mu)$. One such group is $H = \overline{\langle \phi_K^a \rangle}(\ker \rho \cap I_K)$. H acts trivially on V_μ by construction and it is open since it is closed and has finite index in G_K since the sequence (1) shows that $I \times \mathbb{Z}/a\mathbb{Z}$ surjects onto G_K/H. □

To treat the case of I_K acting through an infinite image we need to do more work. Recall that I_K contains a unique pro-p-Sylow subgroup P_K, where p is the characteristic of k [CF67, I.§8 Theorem 1]. P_K is called the wild inertia group and I_K/P_K is the tame inertia group. The fact that P_K is a pro-p-group tells us that it must through a finite quotient when $\ell \neq p$ (see lemma 11). Moreover, there is an isomorphism $I_K/P_K \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$, where ϕ_K acts by conjugation as multiplication by q^{-1} [NSW08, Chapter VII.§5] which turns out to be very useful. It provides us with first examples of representations infinite image on inertia:

Definition 7 (Tame Character)**.** Let ℓ be a prime different from the characteristic of k. Then the projection from $I_K/P_K \cong \prod_{v \neq p} \mathbb{Z}_v$ to the ℓth factor is denoted by $t_\ell : I_K \to \mathbb{Z}_\ell$ and called the tame ℓ-adic character. This is only well-defined up to multiplication by a constant $c \in \mathbb{Z}_\ell^\times$.

Definition 8 (Special ℓ-adic Representation)**.** For integers $n \geq 1$ we define the ℓ-adic special representation $sp(n) : G_K \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ by

$$sp(n)(h) = \exp \begin{pmatrix} 0 & t_\ell(h) & 0 & \cdots \\ 0 & 0 & t_\ell(h) & \cdots \\ \vdots & & \ddots & \\ 0 & \cdots & & 0 \end{pmatrix} \qquad \text{for } h \in I_K$$

and

$$sp(n)(\phi_K) = \begin{pmatrix} 1 & & & \\ & q & & \\ & & \ddots & \\ & & & q^{n-1} \end{pmatrix}$$

and for $g \in G_K$ there is a unique factorisation $g = \phi_K^a h$ with $a \in \hat{\mathbb{Z}}$ and $h \in I_K$ so we can set $sp(n)(g) = sp(n)(\phi_K)^a sp(n)(h)$.

Lemma 9. *$sp(n)$ is well-defined and its isomorphism class is independent of the choices of ϕ_K and t_ℓ.*

Proof. Note that q^a is well defined for $a \in \hat{\mathbb{Z}}$ since $|q|_\ell = 1$ and $q^a \in \mathbb{Z}/\ell^N\mathbb{Z}$ only depends on $a \pmod{\ell^{N-1}(\ell-1)}$. Hence it is clear that $sp(n)$ defines a continuous function $G_K \to \mathrm{GL}_n(\mathbb{Q}_\ell)$. It remains to show that it is a group homomorphism. This requires two ingredients. Firstly, conjugation by ϕ_K acts on I_K/P_K as multiplication by q^{-1} [NSW08, Chapter VII.§5]. Secondly, an easy matrix computation shows $\rho(\phi_K)^{-1}\rho(h)\rho(\phi_K) = \rho(h)^q$, where $\rho = sp(n)$. Using this we find

$$\rho(\phi_K^a u \phi_K^b v) = \rho(\phi_K^{a+b}\phi_K^{-b} u \phi_K^b v) = \rho(\phi_K^{a+b} u^{bq} v) = \rho(\phi_K)^{a+b}\rho(u)^{bq}\rho(v) = \rho(\phi_K)^a\rho(u)\rho(\phi_K)^b\rho(v)$$

for integers $a, b \geq 0$. Now a density argument shows that ρ is indeed a group homomorphism.

If we make a different choice $t'_\ell = ct_\ell$ for the tame character, then it is easily seen that

$$sp'(n)(g) = \begin{pmatrix} 1 & & & \\ & c & & \\ & & \ddots & \\ & & & c^{n-1} \end{pmatrix}^{-1} sp(n)(g) \begin{pmatrix} 1 & & & \\ & c & & \\ & & \ddots & \\ & & & c^{n-1} \end{pmatrix} \qquad \forall g \in G_K.$$

Suppose we make a different choice of Frobenius $\phi'_K = \phi_K w$ with $w \in I_K$. Set $s = -t_\ell(w)/(q-1)$ and

$$N = \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \\ & & & 0 \end{pmatrix}.$$

Then we have the relation $N\rho(\phi_K) = q\rho(\phi_K)N$ and hence

$$\exp(sN)\rho(\phi_K)\exp(-sN) = \rho(\phi_K)\exp((q-1)sN) = \rho(\phi_K)\rho(w^{-1}).$$

On the other hand, using ϕ'_K instead of ϕ_K leads to the representation ρ' with

$$\rho'(\phi_K) = \rho'(\phi'_K w^{-1}) = \rho(\phi_K)\rho(w^{-1}).$$

Further, $\exp(sN)$ commutes with $\rho(h)$ for all $h \in I_K$ and so

$$\exp(sN)\rho(g)\exp(-sN) = \rho'(g)$$

for all $g \in G_K$. □

What follows is a series of lemmas to form the proof of theorem 13.

Lemma 10. *Let G be a profinite group and $\rho : G \to \mathrm{GL}_n(F)$ a continuous representation, where F is a field with discrete valuation. Then ρ is equivalent to a representation $\rho' : G \to \mathrm{GL}_n(\mathcal{O}_F)$, where $\mathcal{O}_F = \{x \in F : v(x) \geq 0\}$.*

Proof. Let $V \cong F^n$ be the F-vector space underlying ρ, then it suffices to find a free $\mathcal{O}_F$-submodule $\Lambda \subset V$ of rank n which is G-stable, i.e. such that $G\Lambda \subset \Lambda$. Let $\Lambda_0 = \mathcal{O}_F^n \subset F^n$, then $H\Lambda_0 \subset \Lambda_0$ where $H = \cap_{i=1}^n \mathrm{Stab}(e_i) < G$ is open. Choose a set of left coset representatives R of G/H. Since H is open and G is compact, R is finite and we define $\Lambda := R\Lambda_0$. Then Λ is G-stable by construction. Moreover, it is a finitely generated, torsion-free $\mathcal{O}_F$-module and hence free as $\mathcal{O}_F$ is a discrete valuation ring. Since $\Lambda_0 \subset \Lambda$ we have $\mathrm{rank}(\Lambda) \geq n$ and since $\Lambda \subset F^n$ also $\mathrm{rank}(\Lambda) \leq n$. □

Lemma 11. *Let $\rho : G_K \to \mathrm{GL}_n(F)$ be a continuous representation, where $F/\mathbb{Q}_\ell$ is a finite extension and $\ell \neq p$. Then $\rho(P_K)$ is finite and its cardinality divides $|\mathrm{GL}_n(\mathcal{O}_F/\mathfrak{m}_F)|$.*

Proof. This proof is the reason for the hypothesis $\ell \neq p$. First by lemma 10 we may assume that ρ has image in $GL_n(\mathcal{O}_F)$. P_K is a pro-p-group and all the kernels

$$\ker\Big(\mathrm{GL}_n(\mathcal{O}_F/\mathfrak{m}_F^k) \to \mathrm{GL}_n(\mathcal{O}_F/\mathfrak{m}_F)\Big) = 1 + \mathrm{Mat}_n(\mathfrak{m}_F/\mathfrak{m}_F^k)$$

are ℓ-groups. Thus if $H < G_K$ is an open subgroup such that $\rho(h) \equiv 1 \pmod{m_K}$ for all $h \in H$, then $\rho(H \cap P_K) = 1$ and so the image of P_K under ρ equals the image of the monomorphism $P_K/(P_K \cap H) \to \mathrm{GL}_n(\mathcal{O}_F/\mathfrak{m}_F)$. □

Lemma 12 (Grothendieck Monodromy Theorem [SeTa, Appendix])**.** *Let $\rho : G_K \to \mathrm{GL}_n(F)$ be a continuous representation with underlying vector space V, where $F/\mathbb{Q}_\ell$ is a finite extension. Then there is a unique nilpotent $N \in \mathrm{End}(V)$ and an open subgroup $\phi_K \in H < G_K$ such that $\rho(h) = \exp(t_\ell(h)N)$ for $h \in H \cap I_K$.*

Proof. As usual apply lemma 10 to assume that ρ has its image in $GL_n(\mathcal{O}_F)$. Similarly to the proof of lemma 11 we take $\phi_K \in H < G_K$ open such that $\rho(h) = 1 \pmod{\mathfrak{m}_F}$ for all $h \in H \cap I_K$. Then we saw that ρ maps I_K onto a pro-ℓ-group. $t_\ell : I_K \to \mathbb{Z}_\ell$ defines an isomorphism of the maximal ℓ-quotient of I_K onto $\mathbb{Z}_\ell$. Hence $\rho|_{I_K}$ factors through t_ℓ. Let $h \in I_K \cap H$ such that $t_\ell(h)$ generates $t_\ell(I_K \cap H)$, then it suffices to show that $\rho(h) = \exp(t_\ell(h)N)$ for some nilpotent N. Equip V with the maximum norm $\|(x_1, \ldots, x_n)\| = \max_i |x_i|$ so that the induced matrix norm is given by $\|A\| = \max_{ij} |A_{ij}|$ for $A \in \mathrm{Mat}_n(F)$. If necessary, shrink $H < G_K$ such that $\|1 - \rho(I_K \cap H)\| < 1$, then $N := t_\ell(h)^{-1} \log \rho(h) \in \mathrm{Mat}_n(F)$ converges. Moreover, $\phi_K^{-1} N \phi_K = qN$ [NSW08, Chapter VII.§5] and hence if λ is a non-zero eigenvalue of N, then so is $q\lambda$. As F has characteristic 0 this would imply that N has infinitely many distinct eigenvalues. Absurd. Consequently N is nilpotent and the uniqueness follows from the formula $N = t_\ell(h)^{-1} \log \rho(h)$. □

Theorem 13. *Let F be a finite extension of $\mathbb{Q}_\ell$, $\ell \neq p$. Let $\rho : G_K \to \mathrm{GL}_n(F)$ be a continuous ϕ_K-semisimple representation with underlying vector space V such that all the eigenvalues of ϕ_K are contained in F. Then*

$$V \cong \bigoplus_i V_i \otimes_{\mathbb{Q}_\ell} sp(n_i),$$

for some positive integers n_i and continuous ϕ_K-semisimple representations V_i such that I_K acts through a finite quotient on V_i.

Proof. By lemma 12 there is a nilpotent $N \in \mathrm{End}(V)$ and an open subgroup $\phi_K \in H < G_K$ such that

(a) $\rho(h) = \exp(t_\ell(h)N)$ for $h \in H \cap I_K$;

(b) $\rho(h) = 1$ for $h \in H \cap P_K$.

Let V be the vector space underlying ρ. By assumption $\rho(\phi_K)$ is diagonalisable on $V^{I_K \cap H} = \ker N$. Let $v_1, \ldots, v_m$ be an eigenbasis with $\rho(\phi_K)v_i = \lambda_i v_i$ of $\ker N$. Set

$$V_i = \{v \in V : N^s v = \mu v_i \text{ for some } \mu \in F, s \in \mathbb{Z}_{\geq 0}\},$$

then $V \cong \bigoplus_{i=1}^m V_i$ and each V_i is H-invariant since if $N^s v = \mu v_i$, then the relation

$$qN = \phi_K^{-1} N \phi_K$$

shows that $N^s \phi_K v = q^s \lambda_i \mu v_i$, hence $\phi_K v \in V_i$.

Suppose $N w_i = v_i$ for some $w_i \in V_i$, then $\phi_K w_i - q\lambda_i w_i \in \ker N \cap V_i$ and hence $\phi_K w_i = q\lambda_i w_i + \mu v_i$ for some $\mu \in F'$. Let $v_{i,1} = w_i - \mu/\lambda_i$, then $\phi_K v_{i,1} = q\lambda_i v_{i,1}$ and $N v_{i,1} = v_i$. Successively we find a basis $v_i, v_{i,1}, \ldots, v_{i,d_i}$ of V_i such that $\phi_K v_{i,j} = q^j \lambda_i v_{i,j}$ and $N v_{i,j} = v_{i,j-1}$. In other words, H acts on V_i like $\chi_i \otimes sp(d_i + 1)$ restricted to H, where $\chi_i : G_K \to (F')^\times$ is the unramified character of K such that $\chi_i(\phi_K) = \lambda_i$.

Let $\rho_1 = \bigoplus_{i=1}^m \chi_i \otimes_{\mathbb{Q}_\ell} sp(n_i)$, where $n_i = d_i + 1$. Then we have shown that $\rho|_H = \rho_1|_H$. By Frobenius reciprocity we conclude

$$\mathrm{Ind}_H^{G_K} V \cong \mathrm{Ind}_H^{G_K} \bigoplus_{i=1}^m \chi_i \otimes_{\mathbb{Q}_\ell} sp(n_i).$$

Shrinking H if necessary we may assume that it is an open normal subgroup and hence for any $F'[G_K]$-module M we have $\mathrm{Ind}_H^{G_K} M \cong F'[G_K/H] \otimes_{F'} M \cong \bigoplus_\eta \eta^{\oplus \dim \eta} \otimes_{F'} M$, where η runs through the irreducible representations of G_K/H. In particular V is a direct summand of a representation of the form

$$\bigoplus_j \rho_j \otimes_{\mathbb{Q}_\ell} sp(n_j),$$

where the ρ_j are continuous irreducible representations of $G_K/(I_K \cap H)$ and ϕ_K acts semisimply on ρ_j. It remains to show that each $M := \rho_j \otimes_{\mathbb{Q}_\ell} sp(n_j)$ is indecomposable. Let $h \in H \cap I_K$ such that $t_\ell(h) \neq 0$ and let $N : M \to M : x \mapsto hx - x$. Since h fixes $e_1 \in sp(n_j)$ and acts trivially on ρ_j, N is nilpotent. Moreover, N preserves subrepresentations of M and gives rise to a filtration $0 < \ker N < \ker N^2 < \cdots < \ker N^{n_j} = M$. From the definition of $sp(n_j)$ and choice of h it is clear that $\ker N \subset M$ is a subrepresentation isomorphic to ρ_j and more generally $\ker N^s / \ker N^{s-1}$ is isomorphic to $\chi_{cyc}^{1-s} \otimes_{\mathbb{Q}_\ell} \rho_j$ which is in particular an irreducible representation.

Now suppose $M = A \oplus B$ is a decomposition into smaller G_K-representations. Then by the irreducibility for each $1 \leq t \leq n_j$, either $A \cap \ker N^t + \ker N^{t-1} = \ker N^t$ and $B \cap \ker N^t \subset \ker N^{t-1}$ or vice versa. Without loss of generality we may assume that $A \cap \ker N = \ker N$ and $B \cap \ker N = 0$. We now show by induction that for $t \geq 2$ we also have $A \cap \ker N^t = \ker N^t$ and $B \cap \ker N^t = 0$ which yields the desired contradiction. So suppose that $A \cap \ker N^{t-1} = \ker N^{t-1}$ and $B \cap \ker N^{t-1} = 0$, then we need to exclude the possibility that $A \cap \ker N^t = \ker N^{t-1}$ and $B \cap \ker N^t + \ker N^{t-1} = \ker N^t$. If this were the case, then by inductive hypothesis $NB \cap \ker N^{t-1} \subset B \cap \ker N^{t-1} = 0$ and hence $B \subset \ker N \subset A$ which is absurd. □

2.2 Independence of ℓ and Weil-Deligne Representations

Suppose we have two prime ℓ, ℓ' different from p and continuous representations $\rho : G_K \to \mathrm{GL}_n(\mathbb{Q}_\ell), \rho' : G_K \to \mathrm{GL}_n(\mathbb{Q}_{\ell'})$. How can we compare ρ and ρ'? A first attempt might be to choose an isomorphism $\overline{\mathbb{Q}_\ell} \cong \overline{\mathbb{Q}_{\ell'}}$ and compare the representations there. The problem with this is that we lose information by going to the algebraic closure and much more seriously that no such isomorphism is continuous.

For example consider the cyclotomic character χ_{cyc}, it is determined by $\chi_{cyc}(\phi_K) = q^{-1}$ which does not depend on ℓ. However, for non-integral $a \in \hat{\mathbb{Z}}$, $\chi_{cyc}(\phi_K^a) = q^{-a}$ depends on

the topology of $\mathbb{Q}_\ell$. To address this issue we restrict our representations to the Weil group $W_K \subset G_K$.

Definition 14. The Weil group $W_K \subset G_K$ is the subgroup formed by elements of the form $\phi_K^a g$ with $a \in \mathbb{Z}$ and $g \in I_K$, this is depicted in the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_K & \longrightarrow & G_K & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \\ & & \| & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & I_K & \longrightarrow & W_K & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

Since $W_K \subset G_K$ is dense, $\rho|_{W_K}$ determines ρ and now there is a character $\chi_{cyc} : W_K \to \mathbb{Q}^\times$ such that $\chi_{cyc}(\phi_K) = q^{-1}$ and $\chi_{cyc}(I_K) = 1$. The second source of representations which depend on the topology of $\mathbb{Q}_\ell$ come from the tame character t_ℓ and this is not yet dealt with by the W_K construction. However, if we take N as in 12, then $\sigma : I_K \to \mathrm{GL}_n(\mathbb{Q}_\ell) : g \mapsto \rho(g)\exp(-t_\ell(g)N)$ is continuous with respect to the discrete topology on $\mathbb{Q}_\ell$ and has a chance of being independent of ℓ. This leads to the following definition.

Definition 15 (Weil-Deligne Representation [Del72, 8.4.1])**.** A Weil-Deligne Representation of W_K over a field F is a pair (V, N), where V is a finite dimensional F-vector space with W_K-action such that an open subgroup of I_K acts trivially and $N : V \to V$ is a nilpotent linear map such that $\phi_K^{-1} N \phi_K = qN$ and $hN = Nh$ for all $h \in I_K$. A morphism of Weil-Deligne representations is a W_K-equivariant linear map which commutes with the nilpotent operator.

Below we will show that for an elliptic curve E/K there exists a Weil-Deligne Representation (V, N) over $\mathbb{C}$ such that for all $\ell \neq p$ we have $\rho_\ell(\phi_K^a g) = \rho(\phi_K^a g)\exp(t_\ell(g)N)$ for all $\phi_K^a g \in W_K$, where $\rho : W_K \to \mathrm{GL}(V)$ is the action on V and ρ_ℓ is the ℓ-adic representation on the Tate module of E. In particular the isomorphism class of ρ_ℓ is determined by data which is completely independent of ℓ. The trick is that a Weil-Deligne representation does not use the topology of the coefficient field. Thus the significance of the next proposition is that ℓ-adic representations of G_K can be understood without referring to the topology of $\mathbb{Q}_\ell$.

Proposition 16. *Let $F/\mathbb{Q}_\ell$ be a finite extension, then there is an equivalence of categories between continuous representations of W_K over F, denoted $\mathbf{Rep}_F(W_K)$ and Weil-Deligne representations of W_K over F such that the eigenvalues of ϕ_K are in $\mathcal{O}_F^\times$, denoted $\mathbf{WD}_F(W_K)$. The equivalence is given by $\mathbf{Rep}_F(W_K) \to \mathbf{WD}_F(W_K) : \rho \mapsto (\phi_K^a g \mapsto \rho(\phi_K^a g)\exp(-t_\ell(g)N), N)$, where N is the operator from lemma 12 (which holds also for W_K instead of G_K with the same proof) and $\mathbf{WD}_F(W_K) \to \mathbf{Rep}_F(W_K) : (\rho, N) \mapsto (\phi_K^a g \mapsto \rho(\phi_K^a g)\exp(t_\ell(g)N))$,*

Proof. It is clear that those two functors are inverse to each other given that they are well-defined. This just follows from the relations $t_\ell(\phi_K^{-1} g \phi_K) = q t_\ell(g)$ and $\phi_K^{-1} N \phi_K = qN$. Moreover, the statement about the eigenvalues ensures that the F-representation associated to a Weil-Deligne representation is continuous. See also [Del72, 8.3.7]. □

Finally we reach our definition of compatibility.

Definition 17. Let ℓ, ℓ' be primes different from p, $F/\mathbb{Q}_\ell$, $F'/\mathbb{Q}_{\ell'}$ finite extensions and ρ, ρ' continuous representations of G_K over F and F' respectively. Then we say that ρ and ρ' are compatible if their associated Weil-Deligne representations of W_K are isomorphic when considered as representations over $\mathbb{C} \cong \overline{\mathbb{Q}_\ell} \cong \overline{\mathbb{Q}_{\ell'}}$.

Consider a family of G_K-representations (ρ_ℓ) where each ρ_ℓ is ℓ-adic. If the ρ_ℓ are pairwise compatible then the Weil-Deligne representation associated to any ρ_ℓ determines all the other $\rho_{\ell'} \otimes \overline{\mathbb{Q}_{\ell'}}$ completely. Or more formally one can chain together the equivalences from proposition 16 to get an equivalence of categories $\mathbf{Rep}_{\overline{\mathbb{Q}_\ell}}(W_K) \sim \mathbf{Rep}_{\overline{\mathbb{Q}_{\ell'}}}(W_K)$ for any $\ell, \ell' \neq p$.

Remark 18. In our definition of compatibility we only consider Weil-Deligne representations over $\mathbb{C}$. Since the characteristic polynomials of the Weil-Deligne of an elliptic curve have rational coefficients one might hope that one can take the whole representation to be defined over $\mathbb{Q}$ and avoid going to the algebraic closure. This is not possible as shown in example 44 below.

3 Elliptic Curves

In this section we discuss our first examples of Galois Representations, namely Tate modules of elliptic curves. To any elliptic curve E over a field F and a prime ℓ such that $\ell^{-1} \in F$ one can associate a free $\mathbb{Z}_\ell$-module $T_\ell E$ of rank 2 [AEC, III.7]. If $F = \mathbb{C}$, then there is a natural isomorphism $T_\ell E \cong H_1(E, \mathbb{Z}_\ell)$ and in general $T_\ell E$ is dual to the first ℓ-adic cohomology group of E/F [CS86, V.15.1]. The Tate module comes with a natural continuous G_F-action and defines a 2-dimensional representation $V_\ell E := T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. This is the ℓ-adic representation associated to an elliptic curve. It is an isogeny invariant and is used for instance to define the conductor or the L-function associated to an elliptic curve over $\mathbb{Q}$. Thus there are many reasons to be interested in $V_\ell E$. Later we also show how to realise the groups $GL_2(\mathbb{F}_\ell)$ as Galois groups of finite extensions $L/\mathbb{Q}$ using Tate modules.

When F is a local field K we describe $V_\ell E$ rather explicitly in terms of its reduction types using the structure theory from the previous section. Namely, we show the following theorem

Theorem 37. *Let E/K an elliptic curve, then $V_\ell E$ is a 2-dimensional ϕ_K-semisimple continuous representation of G_K such that* $\det(V_\ell E) \cong \mathbb{Q}_\ell(1)$ *and*

(a) If E has good reduction, then $V_\ell E$ is unramified and Frob_K *has characteristic polynomial $T^2 - aT + q$, where $a = q + 1 - |\tilde{E}(k)|$, i.e. over $\mathbb{Q}_\ell(\sqrt{a^2 - 4q})$ $V_\ell E$ splits as the sum of two characters.*

(b) If E has split multiplicative reduction, then $V_\ell E \cong \chi_{cyc} \otimes sp(2)$.

(c) If E has non split multiplicative reduction which splits over the unramified quadratic extension K'/K, then $V_\ell E \cong \chi' \otimes \chi_{cyc} \otimes sp(2)$, where χ' is the character of K'.

(d) If E has additive reduction, then $(V_\ell E)^{I_K} = 0$ and if the reduction is potentially multiplicative then $V_\ell E \cong \chi \otimes sp(2)$ for some finitely ramified character χ.

Moreover, we prove the independence of ℓ of $V_\ell E$, that is we prove

Theorem 38. *For any $g \in W_K$ and prime $\ell \neq p$, the characteristic polynomial of g acting on $V_\ell E$ has coefficients in $\mathbb{Q}$ which are independent of ℓ. Moreover, there exists a Weil-Deligne representation (V, N) of W_K over $\mathbb{C}$ such that for every $\ell \neq p$, the Weil-Deligne representation associated to $V_\ell E$ is isomorphic to (V, N), i.e. $V_\ell E$ and $V_{\ell'} E$ are compatible (definition 17).*

The methods involved allow us to show that in fact even in the case of potentially good or potentially multiplicative reduction one can still completely describe the representation $V_\ell E$. This is illustrated in example 42. The aim is to convince the reader that the local ℓ-adic Galois representation of an elliptic curve is a very explicit object. Finally we provide a computation of the integral Tate module $T_\ell E$ in the case when E has split multiplicative reduction using the Tate uniformisation.

Remark 19. Note that the independence of ℓ shows that in theorem 37 (d), the character χ must have image in $\mathbb{Q}^\times$. Further $\chi \cdot \chi_{cyc}^{-1}$ has finite image by parts (b) and (c). Since the only roots of unity in $\mathbb{Q}$ are ± 1, we must have $\chi = \chi' \cdot \chi_{cyc}$, where $\chi' : G_K \to \{\pm 1\}$ is a ramified character. A similar argument gives corollary 39. This illustrates that independence of ℓ is a strong restriction on the representations $V_\ell E$.

The description of $V_\ell E$ is summarised in figure 3, where we use the previous remark and the fact that E has potentially good reduction if and only if $j(E)$ is integral [AEC, VII.5.5].

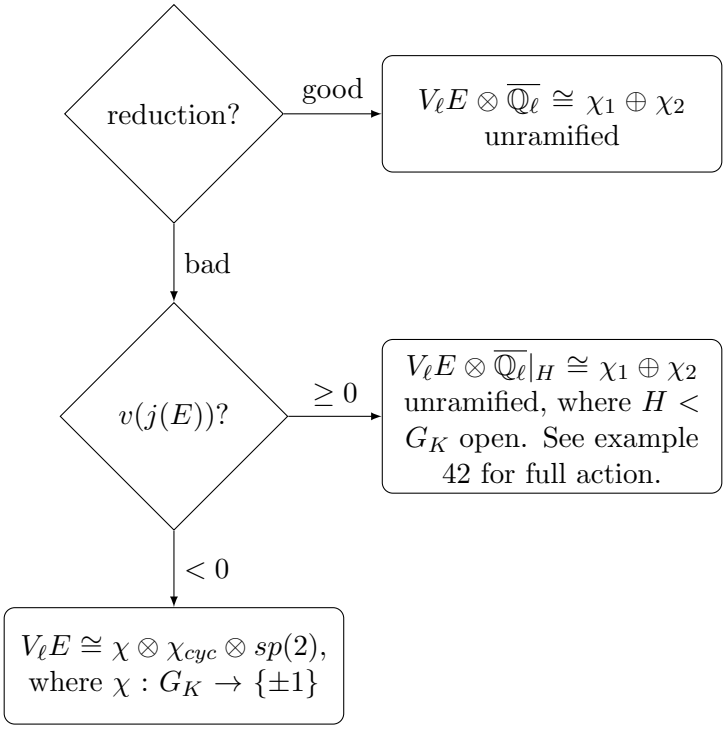


Figure 3: How to determine $V_\ell E$?

3.1 Tate Modules

Fix a prime $\ell \neq p$ and a field F of characteristic 0 or p. For any abelian group A we define the $\mathbb{Z}_\ell$-module $T_\ell A$ as the limit of the diagram

$$A[\ell] \xleftarrow{\cdot \ell} A[\ell^2] \xleftarrow{\cdot \ell} A[\ell^3] \leftarrow \dots$$

In other words, elements of $T_\ell A$ are sequences (a_n) such that $a_n \in A[\ell^n] = \{a \in A : \ell^n a = 0\}$ and $\ell a_n = a_{n-1}$ and for example $\mathbb{Z}_\ell = T_\ell \mathbb{Z}$. The action of $x \in \mathbb{Z}_\ell$ on (a_n) is given by the multiplication action of $\mathbb{Z}/\ell^n\mathbb{Z}$ on $A[\ell^n]$. This defines an additive functor T_ℓ from the category of abelian groups to the category of $\mathbb{Z}_\ell$-modules. Similarly we define the functor V_ℓ from the category of abelian groups to the category of $\mathbb{Q}_\ell$-vector spaces by $V_\ell A := T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

Example 20. If $A = \overline{F}^\times$, then $T_\ell A \cong \mathbb{Z}_\ell$ with a continuous G_F-action given by the ℓ-adic cyclotomic character.

Lemma 21. *$T_\ell A$ is torsion free for any abelian group A.*

Proof. Suppose $x = (x_n) \in T_\ell A$ is killed by $\ell^r u \in \mathbb{Z}_\ell$ where $u \in \mathbb{Z}_\ell^\times$, then for all $n \geq r$, $x_{n-r} = \ell^r x_n = 0$ and hence $x = 0$. □

Lemma 22. *The functor V_ℓ is left exact.*

Proof. Since $\mathrm{Hom}(\mathbb{Z}/\ell^r\mathbb{Z}, -)$ is left exact, so is T_ℓ. Let

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

be a short exact sequence of abelian groups. Since tensoring with $\mathbb{Q}_\ell$ is right exact, it remains to show that $f : V_\ell A \to V_\ell B$ is injective. Since $\mathbb{Q}_\ell \cong \mathbb{Z}_\ell[\ell^{-1}]$, every element $a \in V_\ell A$ can be written as a pure tensor $a = (a_n) \otimes \ell^{-r}$ for some r. Thus if $f(a) = 0$, then $f((a_n)) \otimes \ell^{-r} = 0$ implies that $f((a_n)) \in T_\ell B$ is a torsion element and hence 0 by lemma 21. Now the left exactness of T_ℓ shows that $a = 0$. □

Definition 23. Let F be a field and E/F be an elliptic curve. For a prime ℓ, we define $T_\ell E = T_\ell E(\overline{F})$ and $V_\ell E := V_\ell E(\overline{F})$.

Since G_F acts continuously on each $E[\ell^n]$, G_F acts continuously on $V_\ell E$, i.e. $V_\ell E$ is a continuous representation of G_F. One can show that $T_\ell E$ is a free $\mathbb{Z}_\ell$-module of rank 2 [AEC, III.7.1.]. For instance in the characteristic 0 case one can reduce to the complex case by the Lefschetz principle and use that elliptic curves over $\mathbb{C}$ are complex tori.

Proposition 24. *$V_\ell E$ is an isogeny invariant.*

Proof. Let $\phi : E \to E'$ be an isogeny of elliptic curves over F, then $\phi : E(\overline{F}) \to E'(\overline{F})$ is surjective with finite kernel. The finite kernel is killed by V_ℓ by lemma 21. The left exactness of V_ℓ furnishes an injective G_F-equivariant map $V_\ell E \to V_\ell E'$ between 2-dimensional vector spaces and thus an isomorphism $V_\ell E \cong V_\ell E'$. □

Remark 25. In some cases there is a converse to the above proposition, namely over finite fields (Tate) and over number fields (Faltings) the representation $V_\ell E$ is the only isogeny invariant of E. [AEC, III.7.7.] However, over local fields it is not the only isogeny invariant already for cardinality reasons. The set of possible representations is countable but the set of isomorphism classes of elliptic curves over $\mathbb{Q}_p$ is uncountable.

Corollary 26. *Two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if then they have the same number of $\mathbb{F}_q$-points.*

Proof. The number of $\mathbb{F}_q$ points determines the characteristic polynomial of the frobenius acting on $V_\ell E$ [AEC, V.2.3.1]. Moreover we show in lemma 33 below that $V_\ell E$ is semisimple and so the characteristic polynomial determines $V_\ell E$. This shows that isogenous curves have the same number of $\mathbb{F}_q$-points and Tate's isogeny theorem yields the converse. □

3.2 Reduction Types and $V_\ell E$

The core result of this subsection is the famous criterion of Neron-Ogg-Shafarevich and its refinement, theorem 37. It relates the reduction types of E/K to properties of $V_\ell E$. Recall that there are 3 basic types of reduction for an elliptic curve E/K:

- good reduction
- multiplicative reduction (split, non-split)
- additive reduction (potentially good, potentially multiplicative)

They are defined by taking a minimal Weierstrass model of E and looking at its reduction $\tilde{E}$. This is a cubic curve over k which has at most one singularity. If there are no singularities the reduction is good. If there is a nodal singularity the reduction is multiplicative and the reduction map defines a surjective group homomorphism onto $\tilde{E}_{ns}(\overline{k}) \cong \overline{k}^\times$. If there is a cuspidal singularity the reduction is additive and the reduction map defines a surjective group homomorphism onto $\tilde{E}_{ns}(\overline{k}) \cong \overline{k}$. In this case there is a finite field extension K'/K such that over K', E has either good or multiplicative reduction. See [AEC, VII.2] for details.

Example 27. Let $K = \mathbb{Q}_p$, where $p > 3$ and $E_1 : y^2 = x^3 - x, E_2 : y^2 = x^3 + x^2 + p, E_3 : y^2 = x^3 - p$. Then E_1 has good reduction, E_2 has split multiplicative reduction and E_3 has additive, potentially good reduction.

Further there are subgroups $E_1(K) \subset E_0(K) \subset E(K)$ such that $E_0(K)$ consists of the K-points of E which reduce to a non-singular point of $\tilde{E}$ and $E_1(K)$ consists of of the K-points of E reduce to the identity of the group $\tilde{E}_{ns}(k)$. The group $E_1(K)$ has the useful description

as $\mathfrak{m}_K$-points of the formal group of E which implies for instance that it has no ℓ-torsion or non-trivial ℓ-quotients.

All of the above reduction types have an interpretation in terms of $V_\ell E$ (in particular they are isogeny invariant) and in fact they determine a lot of the structure of $V_\ell E$, for instance any curve E with split multiplicative reduction satisfies $V_\ell E \cong \chi_{cyc} \otimes sp(2)$.

Proposition 28. *There is an isomorphism of G_K representations $(V_\ell E)^{I_K} \cong V_\ell \tilde{E}_{ns}(\overline{k})$.*

Proof. It is a fundamental fact that $E(K^{un})/E_0(K^{un})$ is finite. However, the proof relies on Tate's algorithm which uses the classification of possible special fibres of neron models of elliptic curves [AAEC, IV.9.2d]. In particular this finiteness means that $V_\ell(E(K^{un})/E_0(K^{un})) = 0$ and by left exactness of V_ℓ,

$$(V_\ell E)^{I_K} \cong V_\ell E(K^{un}) \cong V_\ell E_0(K^{un}).$$

Recall that there is an exact sequence

$$0 \to E_1(K^{un}) \to E_0(K^{un}) \to \tilde{E}_{ns}(\overline{k}) \to 0$$

of G_K-modules and $E_1(K^{un})$ is isomorphic to the $\mathfrak{m}_{K^{un}}$-points of the formal group of E. Thus $E_1(K^{un})$ contains no ℓ-torsion and $\mathrm{Ext}^1(\mathbb{Z}/\ell^n\mathbb{Z}, E_1(K^{un})) = \mathbb{Z}/\ell^n\mathbb{Z} \otimes E_1(K^{un}) = 0$ and $T_\ell E_0(K^{un}) \to T_\ell \tilde{E}_{ns}(\overline{k})$ is an isomorphism. □

Theorem 29 (Neron-Ogg-Shafarevich)**.** *Let $d = \dim(V_\ell E)^{I_K}$, then the reduction of E is*

(a) good if $d = 2$,

(b) multiplicative if $d = 1$,

(c) additive if $d = 0$.

Proof. The idea is that we can read off the reduction type from the group structure of $A := T_\ell \tilde{E}_{ns}(\overline{k})$ and to apply the proposition.

(a) If E has good reduction, then there is an isomorphism of $\mathbb{Z}_\ell$-modules $A \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$ and hence $d = 2$.

(b) If E has multiplicative reduction, then there is an isomorphism of $\mathbb{Z}_\ell$-modules $A \cong T_\ell(\overline{k}^\times) \cong \mathbb{Z}_\ell$ and $d = 1$.

(c) If E has additive reduction, then there is an isomorphism of $\mathbb{Z}_\ell$-modules $A \cong T_\ell(\overline{k})$ and since ℓ is invertible in k, $A = 0$. □

Corollary 30. *The reduction type (good, multiplicative or additive) of E is an isogeny invariant.*

Corollary 31. *The integrality of $j(E)$ is an isogeny invariant.*

Proof. The j-invariant is integral if and only if E has potentially good reduction [AEC, VII.5.5]. This is the case if and only $V_\ell E$ is finitely ramified. But $V_\ell E$ only depends on the isogeny class of E. □

Remark 32. The valuation $v(j(E))$ is not an isogeny invariant. For instance this can be seen in the 11-adic valuation of the j-invariants in [LMFDB, Isogeny class 32a].

Lemma 33. *Let E be an elliptic curve over L where L is a field of characteristic $p > 0$. Then the Frobenius automorphism ϕ of L acts semisimply on $V_\ell E$ for $\ell \neq p$.*

Proof. The degree of an isogeny is a positive definite quadratic form on $\mathrm{End}(E)$. [AEC, III. Corollary 6.3.]. We can extend this to a hermitian form on $\mathrm{End}(E)\otimes\mathbb{C}$. Consider $\phi : E \to E$ as a degree p isogeny, then $p^{-1/2}\phi$ acts unitarily on $\mathrm{End}(E)\otimes\mathbb{C}$. Hence the ring $\mathbb{C}[\phi] \subset \mathrm{End}(E)\otimes\mathbb{C}$ is semisimple and so is every module over it. Since $\mathbb{C}$ and $\overline{\mathbb{Q}_\ell}$ are both algebraically closed, of characteristic 0 and have the same cardinality we may choose a field isomorphism $\mathbb{C} \cong \overline{\mathbb{Q}_\ell}$ [Ste10]. Hence we can view $V_\ell E \otimes \overline{\mathbb{Q}_\ell}$ as a $\mathbb{C}[\phi]$-module. In particular ϕ acts semisimply on $V_\ell E \otimes \overline{\mathbb{Q}_\ell}$ and hence on $V_\ell E$ by lemma 3. □

Theorem 34. *Let E be an elliptic curve over K, and ℓ a prime different from the characteristic of k. Then ϕ_K acts semisimply on $V_\ell E$.*

Proof. If E has good reduction then the reduction map $E \to \tilde{E}$ induces an isomorphism of tate modules [AEC, VII.3.1] and the result follows from lemma 33.

Note that we may replace K by a totally ramified extension since this does not change the Frobenius. Hence the theorem also holds for curves with potentially good reduction.

If this is not the case then by theorem 29 any open subgroup $I' < I_K$ acts non-trivially and so $\dim(V_\ell E)^{I'} \leq 1$. In particular ϕ_K acts semisimply on $(V_\ell E)^{I'}$ and theorem 13 shows that it in fact acts semisimply on the whole space. □

Remark 35. In general it is an open problem to decide whether the Frobenius acts semisimply on the etale cohomology of a variety over a finite field.

Lemma 36. $\det(V_\ell E) \cong \mathbb{Q}_\ell(1)$.

Proof. The Weil pairing [AEC, III.8] induces a non-zero map $\det(V_\ell E) \to \mathbb{Q}_\ell(1)$ which is the desired isomorphism. □

Theorem 37. *Let E/K an elliptic curve, then $V_\ell E$ is a 2-dimensional ϕ_K-semisimple continuous representation of G_K such that* $\det(V_\ell E) \cong \mathbb{Q}_\ell(1)$ *and*

(a) If E has good reduction, then $V_\ell E$ is unramified and Frob_K *has characteristic polynomial $T^2 - aT + q$, where $a = q + 1 - |\tilde{E}(k)|$, i.e. over $\mathbb{Q}_\ell(\sqrt{a^2 - 4q})$ $V_\ell E$ splits as the sum of two characters.*

(b) If E has split multiplicative reduction, then $V_\ell E \cong \chi_{cyc} \otimes sp(2)$.

(c) If E has non split multiplicative reduction which splits over the unramified quadratic extension K'/K, then $V_\ell E \cong \chi' \otimes \chi_{cyc} \otimes sp(2)$, where χ' is the character of K'.

(d) If E has additive reduction, then $(V_\ell E)^{I_K} = 0$ and if the reduction is potentially multiplicative then $V_\ell E \cong \chi \otimes sp(2)$ for some finitely ramified character χ.

Proof. The first part is theorem 34 and lemma 36.

If E has good reduction then this follows from [AEC, V.2.3.1.], the isomorphism $V_\ell E \cong V_\ell \tilde{E}$ and theorem 34.

If E has multiplicative reduction, then by [AEC, VII.5.4.] E also has multiplicative reduction over all finite extensions of K. The Neron-Ogg-Shafarevich Criterion shows that I_K does not act through a finite quotient on $V_\ell E$. Consequently $(V_\ell E)^{I'}$ is one-dimensional for all $I' < I_K$ open, ϕ_K acts diagonally on it and theorem 13 implies that $V_\ell E \cong \chi \otimes_{\mathbb{Q}_\ell} sp(2)$ for some character $\chi : G_K \to \mathbb{Q}_\ell^\times$. Now by definition of $sp(2)$ we have $(V_\ell E)^{I_K} \cong \chi$ and χ must be unramified since otherwise $\dim(V_\ell E)^{I_K} = 0$. Thus is suffices to check how ϕ_K acts on $\tilde{E}_{ns}(\overline{k}) \cong \overline{k}^\times$. If E has split multiplicative reduction then clearly ϕ_K just acts as multiplication by q^{-1}. If E has non-split multiplicative reduction, then we still know that ϕ_K^2 acts as multiplication by q^{-2} because the reduction is split over a quadratic extension. If ϕ_K also acts as q^{-1} here then the

reduction would be split since then there is an isomorphism $\tilde{E}_{ns}(k) \cong k^\times$. Thus ϕ_K acts as $-q^{-1}$ as required.

If E has additive reduction, then $(V_\ell E)^{I_K} = 0$ by theorem 29. If the reduction is potentially multiplicative, then we see from the above and theorem 13 that $V_\ell E \cong \chi \otimes sp(2)$ for some finitely ramified character χ. □

3.3 Independence of ℓ

When given an elliptic curve E/K we have constructed representations $V_\ell E$ for all primes $\ell \neq p$. We now show that these are all compatible in the sense of definition 17. Our main ingredient for establishing this independence of ℓ is [AEC, III.8.6] which states that for an isogeny $\phi \in \mathrm{End}(E)$, the induced map ϕ_ℓ on $V_\ell E$ satisfies

$$\det(\phi_\ell) = \deg(\phi) \qquad \mathrm{Tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi).$$

In particular these values are in $\mathbb{Z}$ and independent of ℓ. If E is an elliptic curve over a finite field, then the Frobenius has the fantastic property of being both a field automorphism and and a morphism of algebraic varieties.

Theorem 38. *For any $g \in W_K$ and prime $\ell \neq p$, the characteristic polynomial of g acting on $V_\ell E$ has coefficients in $\mathbb{Q}$ which are independent of ℓ. Moreover, there exists a Weil-Deligne representation (V, N) of W_K over $\mathbb{C}$ such that for every $\ell \neq p$, the Weil-Deligne representation associated to $V_\ell E$ is isomorphic to (V, N), i.e. $V_\ell E$ and $V_{\ell'} E$ are compatible (definition 17).*

Proof. If E has good reduction then this follows directly from [AEC, III.8.6.] and the isomorphism $V_\ell E \cong V_\ell \tilde{E}(\overline{k})$.

If E has multiplicative reduction, then 37 shows that $V_\ell E \cong \chi \otimes sp(2)$ for some unramified character χ which takes rational values on integral powers of frobenius which are independent of ℓ (either $(-q)^{-a}$ or q^{-a}). Thus the characteristic polynomial of $g \in I_K$ acting on $V_\ell E$ is $(T-1)^2$ and the characteristic polynomial of ϕ_K^a is $(T - \chi(\phi_K^a))(T - q\chi(\phi_K^a))$ which both have rational values, independent of ℓ.

If E has additive reduction, then there is a finite Galois extension K'/K such that E has good or split multiplicative reduction over K' [AEC, VII.5.4.]. First suppose that E has good reduction over K' and let I be the inertia group of K'/K, then by the Neron-Ogg-Shafarevich criterion, the action of I_K on $V_\ell E$ factors through I. Since I is finite, so is $\mathrm{Aut}(I)$ and after possibly enlarging K' by an unramified extension, we may assume that conjugation by $\phi_{K'}$ acts trivially on I. Let $\tilde{E}$ be the reduction of E over K'. It is an elliptic curve over k' the residue field of K'. The action of I on E induces an action on $\tilde{E}$ and since conjugation by $\phi_{K'}$ acts trivially on I, this is even an action by k'-isogenies. Given $\tilde{P} \in \tilde{E}(k')$ lift it to $P \in E(K')$ and then take the reduction of $g(P)$. This is well-defined since g acts continuously on E. In particular

$$\det(g|_{V_\ell \tilde{E}}) = \deg(g) = 1, \qquad \mathrm{Tr}(g|_{V_\ell \tilde{E}}) = 1 + \deg(g) - \deg(1-g) \in \mathbb{Z}$$

by [AEC, III.8.6]. One can argue in the same fashion for elements of the form $g\phi_K^a$ with $a \geq 0$. Finally since $g\phi_K^{-a} = (g^{-1}\phi_K^a)^{-1}$ also elements of the form $g\phi_K^a$ with $a < 0$ have characteristic polynomials with rational coefficients independent of ℓ. The compatibility of $V_\ell E$ and $V_{\ell'} E$ follows because in this case the nilpotent operator of the associated Weil-Deligne representation is 0 and so we are just dealing with semisimple representations of W_K which are determined by their characters [Bou62, ch. 8, §12, n° I, prop. 3].

Now suppose that E has potentially multiplicative reduction then again we may assume that the finite group I acts by k'-morphisms on $\tilde{E}_{ns}$. Such morphisms are of the form $x \mapsto x^{\pm q^r}$ for some $r \in \mathbb{Z}$ and give rise to the eigenvalue $\pm q^r \in \mathbb{Q}$ on $V_\ell \tilde{E}_{ns}(\overline{k})$ which determines the character χ such that $V_\ell E \cong \chi \otimes sp(2)$. The characteristic polynomial of $g\phi_K^a \in W_K$ is then given by

$(T-\chi(g))(T-\chi(g)q^a)$ and independent of ℓ and the associated Weil-Deligne representation is $\left(\chi \oplus \chi \cdot \chi_{cyc}^{-1}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)$. □

Corollary 39. *Suppose $p \geq 5$, then if E has potentially good reduction it acquires good reduction over a totally ramified Galois extension of degree 4 or 6.*

Proof. By assumption on p, we can choose an ℓ such that $p \nmid (\ell^2 - 1)$ and thus $V_\ell E$ is tamely ramified by lemma 11. In such a representation I acts through a cyclic quotient. But the characteristic polynomial of this action has coefficients in $\mathbb{Q}$ and so it must act through a cyclic quotient of order $1, 2, 3, 4$ or 6. □

Corollary 40. *Assume that the residue characteristic of K is ≥ 5. Let E have potentially good reduction, then the residue class mod 12 of $v_K(\Delta_E)$ is not invertible* $\pmod{12}$.

Proof. Let K'/K be the quartic or sextic extension from above and $u \in K'$ such that $x \mapsto u^2 x, y \mapsto u^3 y$ transforms E to a curve with good reduction, then the discriminant gets multiplied by u^{12} and hence $v_K(\Delta_E)$ must be divisible by 2 or 3, i.e. not invertible $\pmod{12}$. □

Example 41. The elliptic curve $E : y^2 = x^3 + x + 1$ does not have potentially good reduction over $\mathbb{Q}_{31}$ since $v_{31}(\Delta_E) = 1$. Thus its ℓ-adic representation of $G_{\mathbb{Q}_{31}}$ must be of the form $\chi \otimes sp(2)$ for some character $\chi : G_K \to \{\pm 1\}$.

Example 42. Consider the elliptic curve $E : y^2 = x^3 - px$ over $\mathbb{Q}_p$ where $p > 3$. It has additive reduction which becomes good over $\mathbb{Q}_p(p^{1/4})$ and the automorphism g of $\mathbb{Q}_p(p^{1/4}, i)$ which sends $p^{1/4} \mapsto ip^{1/4}$ acts on $\tilde{E} : y^2 = x^3 - x$ by $(x, y) \mapsto (-x, iy)$ where $i \in \overline{\mathbb{Q}_p}$ is a root of $x^2 + 1 = 0$. Moreover, the characteristic polynomial of g acting on $V_\ell E$ is $T^2 + 1$.

If $p \equiv 3 \pmod 4$, then $V_\ell E \otimes \overline{\mathbb{Q}_\ell}$ has the form

$$\rho(g) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \rho(\mathrm{Frob}_p) = \begin{pmatrix} 0 & \sqrt{-p} \\ \sqrt{-p} & 0 \end{pmatrix}$$

If $p \equiv 1 \pmod 4$, then $V_\ell E \otimes \overline{\mathbb{Q}_\ell}$ has the form

$$\rho(g) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \rho(\mathrm{Frob}_p) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

for some explicitly computable α, β.

Proof. Over $\mathbb{Q}_p(p^{1/4})$ there is an isomorphism $E \to E' : (x, y) \mapsto (p^{1/2}x, p^{3/4}y)$ where $E' : y^2 = x^3 - x$. To compute the action of g, take $(\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p(i))$, a lift $(x, y) \in E'(\mathbb{Q}_p)$ which corresponds to $(p^{-1/2}x, p^{-3/4}y) \in E(\mathbb{Q}_p)$ and is mapped by g to $(-p^{-1/2}x, ip^{-3/4}y)$ which reduces to $(-\tilde{x}, i\tilde{y})$. This is an isogeny $\tilde{g}$ which satisfies $\tilde{g}^2(P) + P = 0$ and hence we also have the relation $g^2 + 1 = 0$ on $V_\ell E$. This implies that the characteristic polynomial of g acting on $V_\ell E$ is $T^2 + 1$.

If $p \equiv 3 \pmod 4$ choose a basis of $V_\ell E \otimes \overline{\mathbb{Q}_\ell}$ which diagonalises g. Then the relation $\mathrm{Frob}_p \, g \, \mathrm{Frob}_p^{-1} = g^{-1}$ implies that we can scale this basis so that $\rho(\mathrm{Frob}_p)$ is of the form

$$\begin{pmatrix} 0 & \alpha \\ \alpha & 0 \end{pmatrix}$$

for some α. But we know that $\alpha^2 = -p$ from lemma 36.

If $p \equiv 1 \pmod 4$, then g and Frob_p commute and hence can be diagonalised simultaneously. To decide which eigenvalue of Frob_p shares an eigenvector with i, respectively $-i$ it suffices to compute the eigenvalues of $g \, \mathrm{Frob}_p$. To do so observe that $g \, \mathrm{Frob}_p$ is another choice of Frobenius

which fixes elements of the form $(ap)^{1/4}$ where $a \in \mathbb{Z}_p^\times$ is not a square. But over $\mathbb{Q}_p((ap)^{1/4})$, E obtains good reduction and so we can compute the eigenvalues of $g\,\mathrm{Frob}_p$ by counting points. This is explored in more detail in [DD11]. Let's illustrate the method for $p = 17$. $a = 3$ is not a square mod 17. Over $\mathbb{Q}_p((3^{-1}p)^{1/4})$ E has the model $y^2 = x^3 - 3x$ where Frobenius has trace -8 and eigenvalues $-4 \pm i$. Over $\mathbb{Q}_p(p^{1/4})$ E has the model $y^2 = x^3 - x$ where Frobenius has trace 2 and hence its eigenvalues are $1 \pm 4i$. We know that the Frobenius over $\mathbb{Q}_p((3^{-1}p)^{1/4})$ equals $g\,\mathrm{Frob}_p$ where Frob_p is the Frobenius over $\mathbb{Q}_p(p^{1/4})$. Thus $\{i\alpha, -i\beta\} = \{-4 + i, -4 - i\}$ and $\{\alpha, \beta\} = \{1 + 4i, 1 - 4i\}$ and consequently $\alpha = 1 + 4i$ and $\beta = 1 - 4i$. □

Corollary 43. *The elliptic curve $E : y^2 = x^3 - x$ is supersingular at all primes $p \equiv 3 \pmod 4$.*

Proof. [1] Any choice of Frobenius for $\mathbb{Q}_p(p^{1/4})$ is also one for $\mathbb{Q}_p$ and E is supersingular if and only if the trace of the Frobenius is zero $\pmod p$. Over $\mathbb{Q}_p(p^{1/4})$, E is isomorphic to the curve $y^2 = x^3 - px$ from the example where we computed that the Frobenius has trace 0. One doesn't actually need Galois representations to prove this and can use [AEC, V.4.1] instead. □

Example 44. Consider the elliptic curve $E : y^2 = x^3 - x^2 - 384x - 2772$ [LMFDB, Elliptic Curve 24.a1]. It has discriminant $\Delta = 2^{11} \cdot 3^2$, conductor $N = 2^3 \cdot 3$ and j-invariant $j = 2 \cdot 3^{-2} \cdot 1153^3$. Then the representation $G_{\mathbb{Q}_2} \to \mathrm{GL}(V_3 E)$ is not defined over $\mathbb{Q}$. This is about as ugly as potential good reduction can get and it shows that the Weil-Deligne representation associated to $E/\mathbb{Q}_2$ can not taken to be defined over $\mathbb{Q}$ even though we have the rationality statement from theorem 38.

Proof. We show that $I_{\mathbb{Q}_2}$ acts faithfully through a quotient which is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. Then we note that the quaternion group Q_8 is a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ and has a unique irreducible faithful representation whose Schur index is 2 and hence not defined over $\mathbb{Q}$.

By a strengthening of the Neron-Ogg-Shafarevich criterion [AAEC, IV.10.3], $E/\mathbb{Q}_2$ has good reduction over $\mathbb{Q}_2(E[3])$. Moreover since $v_2(\Delta) = 11$, the ramification degree e of $\mathbb{Q}_2(E[3])/\mathbb{Q}_2$ satisfies $e \geq 12$ and there is a natural embedding $\mathrm{Gal}(\mathbb{Q}_2(E[3])/\mathbb{Q}_2) \hookrightarrow \mathrm{Aut}(E[3])$. By the Weil Pairing, the image of $I_{\mathbb{Q}_2}$ in $\mathrm{Aut}(E[3])$ lands in $\mathrm{SL}_2(\mathbb{F}_3)$ which has no proper subgroups of order ≥ 12. Consequently the inertia group of $\mathbb{Q}_2(E[3])/\mathbb{Q}_2$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$ and since E has good reduction over $\mathbb{Q}_2(E[3])$ this completes the proof. □

3.4 Tate Uniformisation and Split Multiplicative Reduction

Over the complex numbers every elliptic curve has the form $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ with $\Im(\tau) > 0$ [AEC, VI.5.1.1]. In this subsection we present the analogue result for arbitrary complete fields. The trick is to first note that the exponential map $\exp : \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \to \mathbb{C}^\times/e^{2\pi i\tau\mathbb{Z}}$ is an isomorphism and then write out the power series which define the isomorphism $\mathbb{C}^\times/e^{2\pi i\tau\mathbb{Z}} \to E$. Luckily they have rational coefficients so that one can plug in numbers from other complete fields [AAEC, V.3]. As a consequence we will be able to describe the integral Tate module $T_\ell E$ for elliptic curves with split multiplicative reduction rather than just $V_\ell E$. Later we use this to solve the inverse Galois problem for the groups $GL_2(\mathbb{F}_\ell)$. The theory of the Tate curve can be summarised in the following theorem.

Theorem 45. *Let K be a finite extension of $\mathbb{Q}_p$ and $t \in K^\times$ such that $|t| < 1$, then $E_t : y^2 + xy = x^3 + a_4(t)x + a_6(t)$ is an elliptic curve over K such that $E_t(L) \cong L^\times/t^{\mathbb{Z}}$ for all algebraic extensions L/K, where*

$$a_4(t) = -\sum_{n\geq 1} \frac{n^3 t^n}{1 - t^n} \qquad a_6(t) = -\sum_{n\geq 1} \frac{(5n^3 + 7n^5)t^n}{12(1 - t^n)}.$$

[1] This proof is interesting because we take a question about good reduction and solve it by considering a 'degeneration' to bad reduction, similarly to how one can prove the degree-genus formula for plane curves by degeneration to a union of lines.

Moreover, if E/K is an elliptic curve such that $|j(E)| > 1$, then there exists a unique $t \in K^\times$ such that E is isomorphic to E_t over $\overline{K}$ and E is K-isomorphic to E_t if and only if E has split multiplicative reduction.

Proof. Omitted. See [AAEC, V.3.1] and [AAEC, V.5.3]. □

Corollary 46. *If E/K is an elliptic curve with split multiplicative reduction, then there is a $\mathbb{Z}_\ell$-basis of $T_\ell E$ in which the action of $\phi_K^s g \in G_K$ with $g \in I_K$ is given by*

$$\begin{pmatrix} q^{-s} & q^{-s}t_\ell(g) \\ 0 & 1 \end{pmatrix}$$

Proof. By [AEC, VII.5.5] $|j(E)| > 1$ and the theorem implies that E is isomorphic to a Tate curve $K^\times/t^{\mathbb{Z}}$ for some $|t| < 1$. Consider the functor $A \mapsto A[n] = \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A)$ which maps discrete G_K-modules to discrete G_K-modules. Its first right derived functor is $A \mapsto A/nA$. Hence the short exact sequence

$$0 \to t^{\mathbb{Z}} \to \overline{K}^\times \to E(\overline{K}) \to 0$$

induces the exact sequence

$$0 \to \mu_n \to E(\overline{K})[n] \to t^{\mathbb{Z}}/t^{n\mathbb{Z}} \to 0$$

for any n. Thus for choices of an nth root of unity ζ and an nth root γ of t any element of $E(\overline{K})[n]$ can be written uniquely as $\zeta^a\gamma^b$ with $a, b \in \mathbb{Z}/n\mathbb{Z}$. Now specialise to $n = \ell^k$, then $\phi_K^s g(\zeta^a\gamma^b) = \phi_K^s(\zeta^{a+t_\ell(g)b}\gamma^b) = \zeta^{q^{-s}a+q^{-s}t_\ell(g)b}$. It is clear that in the limit these give the claimed matrix representation of $T_\ell E$. □

4 Higher Genus Curves

In this section we generalise the results of the previous section to curves of genus ≥ 2 over K. Studying the ℓ-adic representation of such curves requires a few more steps than the study of Tate modules of elliptic curves. As a result there are few proofs in this section. The aim is rather to describe the theory and to highlight the similarities and differences to the case of elliptic curves.

The first hurdle is already the definition of the ℓ-adic representation attached to a curve C of genus $g \geq 2$. One can define it as the Tate dual of the first ℓ-adic cohomology group but this description is too general to work with. When C was an elliptic curve we were able to use the group structure on E. However, there is no group structure on C. For instance because over the complex numbers such curves are not even topological groups since their fundamental groups are not abelian.

However, we can still form the group $\mathrm{Pic}^0(C)$ of degree 0 divisor classes on C. Moreover this group carries a natural continuous G_K-action induced by the G_K-action on $C(\overline{K})$. Note that in the case of an elliptic curve E we have $E(\overline{K}) \cong \mathrm{Pic}^0(E)$ by the Riemann-Roch theorem [AEC, III.3.4] and so $V_\ell \mathrm{Pic}^0(C)$ is a generalisation of the Tate module of an elliptic curve. This is the representation we describe in the present section.

It turns out that $\mathrm{Pic}^0(C)$ is rather hard to study directly. Indeed I do not know of an elementary proof of even first properties such as the dimension of $V_\ell \mathrm{Pic}^0(C)$. Over the complex numbers, $\mathrm{Pic}^0(C)$ is isomorphic to the complex torus $H^0(C, \Omega^1_C)^\vee/H_1(C, \mathbb{Z})$ by the Abel-Jacobi theorem [Lan, IV] which reveals the structure of this abelian group. This does not directly have an analogue for general base fields. However, the aforementioned torus is also an abelian variety, called the Jacobian variety of C and this does generalise to other fields [CS86, VII]. There exists an abelian variety $J(C)/K$ of dimension g such that $\mathrm{Pic}^0(C) \cong J(C)(\overline{K})$.

The second hurdle lies in the fact that the reduction of general curves is considerably more complicated than the reduction of elliptic curves where we have the convenience of the minimal Weierstrass model. It is not easy to even define what the reduction of a higher genus curve should be and there are multiple 'correct' answers. In our context we will mainly discuss the minimal regular model. See [Con] for a comparison of the neron model, minimal regular model and minimal weierstrass model of an elliptic curve.

To conclude, the aim of this section is to explain the following theorem.

Theorem 47. *Let C/K be a curve of genus $g \geq 1$ and $\mathcal{C}$ the minimal regular model of C over $\mathcal{O}_K$. The G_K-representation $V_\ell \operatorname{Pic}^0(C)$ is continuous and ϕ_K-semisimple such that $\det(V_\ell \operatorname{Pic}^0(C)) \cong \mathbb{Q}_\ell(g)$. If we assume additionally, that the special fibre of $\mathcal{C}$ has semi-stable reduction, then*

$$V_\ell \operatorname{Pic}^0(C) \cong H_1(\Gamma, \mathbb{Z}) \otimes \chi_{cyc} \otimes sp(2) \oplus V_\ell \operatorname{Pic}^0(\widetilde{\mathcal{C}}_{\mathfrak{m}_K}),$$

where Γ is the dual graph (see definition 64) of $\mathcal{C}_{\mathfrak{m}_K}$ and $\widetilde{\mathcal{C}}_{\mathfrak{m}_K}$ is the normalisation of $\mathcal{C}_{\mathfrak{m}_K}$. Moreover, these representations are independent of ℓ (definition 17).

4.1 Integral Models and Reduction

We now recall some parts of the theory of arithmetic surfaces as explained in [Liu10, Chapter 10]. This is necessary to describe the G_K representation $V_\ell \operatorname{Pic}^0(C)$ associated to a curve C/K of genus $g \geq 2$. By a curve we will always mean a regular, irreducible, projective curve C/K. For example consider the plane curves $C_e : xy(x+y-1)(x-y+1) = p^e$ over $\mathbb{Q}_p$ and $e \in \mathbb{Z}$. The naive way of reducing C_e mod p is to just take the same equation and reduce its coefficients mod p. However, it turns out that this only gives the right result when $e = 1$ and for C_e with $e < 0$ one would have to multiply both sides by p^{-e} to be able to reduce mod p but then we just end up with the equation $0 = 1$, i.e. empty reduction.

Formally we can describe this process of reducing the equations of C mod $\mathfrak{m}$ as finding some $\mathcal{O}_K$-scheme $\mathcal{C}$ such that $\mathcal{C}_K \cong C$ and then $\mathcal{C}_k = \mathcal{C} \times_{\mathcal{O}_K} k$ is the reduction mod $\mathfrak{m}_K$. For instance if we consider C_e as an affine plane curve, then for $e \geq 1$ we can take $\mathcal{C}_e = \operatorname{Spec} \mathbb{Z}_p[x,y]/(xy(x+y-1)(x-y+1)-p^e)$ and then $\mathcal{C}_e \times k = \operatorname{Spec} \mathbb{F}_p[x,y](xy(x+y-1)(x-y+1))$ is the union of 4 lines in general position (at least if $p > 2$).

The issue is that there are many possibilities for $\mathcal{C}$ and they are not all interesting as we saw above when $e < 0$. Thus we ask $\mathcal{C}$ to satisfy additional properties which eventually uniquely determine it.

Definition 48. Let C be a curve over K. Then a model of C over $\mathcal{O}_K$ is an integral, normal, projective, flat $\mathcal{O}_K$-scheme $\mathcal{C}$ of dimension 2 together with a K-isomorphism $f : \mathcal{C} \times_{\mathcal{O}_K} K \to C$. We say that $\mathcal{C}$ is a regular model if the scheme $\mathcal{C}$ is regular. A morphism of models is a $\mathcal{O}_K$-morphism $\mathcal{C} \to \mathcal{C}'$ which respects the isomorphisms $\mathcal{C}_K \cong C$ and $\mathcal{C}'_K \cong C$.

If $K = k((t))$, then a model is an infinitesimal family of curves over k, so we can think of it as a deformation of the special fibre $\mathcal{C}_{\mathfrak{m}_K}$. This is a useful intuition to keep in mind. In fact the whole theory of models of curves and their reductions is completely analogous to the birational geometry of surfaces as shown in the book [Liu10]. For $K = \mathbb{Q}_p$ one can imagine a model as a deformation in p-direction. For instance this explains why the model $\operatorname{Spec} \mathbb{Z}_p[x,y]/(xy-p)$ should be regular but $\operatorname{Spec} \mathbb{Z}_p[x,y]/(xy-p^2)$ is not. Note that even though $\operatorname{Spec} \mathbb{Z}_p[x,y]/(xy-p)$ is regular, its special fibre $\operatorname{Spec} \mathbb{F}_p[x,y]/(xy)$ is not. This is a typical situation, for example any complex projective plane curve sits in a continuous family which comes arbitrarily close to the union of lines in general position.

Definition 49 (Good Reduction)**.** We say that a curve C/K has good reduction if there exists a model $\mathcal{C} \to \operatorname{Spec} \mathcal{O}_K$ such that the fibre $\mathcal{C}_{\mathfrak{m}_K}$ is geometrically regular. If there is no such model then C has bad reduction.

Definition 50 (Semi-Stable Reduction)**.** We say that a curve C/K has semi-stable reduction if there exists a model $\mathcal{C}$ of C over $\mathcal{O}_K$ such that the only singularities in its special fibre over $\overline{k}$ are ordinary double points.

Example 51. The curve $x^4 + y^4 + z^4 = 0$ has good reduction over $\mathbb{Q}_p$ for $p > 2$.

Proposition 52. *This definition of good reduction agrees with the definition of good reduction for elliptic curves.*

Proof. Let E/K be an elliptic curve and $W \to \operatorname{Spec} \mathcal{O}_K$ its minimal Weierstrass model. E has good reduction as an elliptic curve if and only if $W_{\mathfrak{m}_K}$ is regular. If this is the case then clearly E is also regular as a curve. The converse is harder and proven in [Liu10, 10.1.23]. □

By the nature of the definition it is much harder to prove that a curve has bad reduction than to prove good reduction since one has to consider all models. However, there is a best model in some sense, called the minimal regular model and it turns out that it suffices to check for good reduction or semi-stability on that model.

Definition 53. A model $\mathcal{C}$ of a curve C/K is a minimal regular model if it is regular and every morphism $\mathcal{C} \to \mathcal{C}'$ where $\mathcal{C}'$ is another regular model of C is an isomorphism.

Theorem 54. *If C/K is a curve of genus $g \geq 1$, then C admits a unique minimal regular model.*

Proof. See [Liu10, 10.1.8]. □

Theorem 55. *A curve C/K of genus $g \geq 1$ has good (resp. semi-stable) reduction if and only if it obtains good (resp. semi-stable) reduction over the minimal regular model of C*

Proof. This is [Liu10, 10.1.21] and [Liu10, 10.3.34]. □

To find a minimal regular model of a curve C/K of genus $g \geq 1$ one does the following. First it is usually not too hard to find any model by just taking equations with integral coefficients and possibly normalising. Then we have a normal scheme of dimension 2, which has only point singularities [Liu10, 4.2.24] which necessarily lie on the special fibre. After a finite number of blowups we can obtain a regular model $\mathcal{C}_0$. If the special fibre of $\mathcal{C}_0$ contains no (-1) curves then $\mathcal{C}_0$ is minimal by Castelnuovo's criterion [Liu10, 9.3.8]. Otherwise contract all such curves to obtain the minimal regular model. See examples 67 and 68 for this method and [Liu10, 10.1.12] for another example.

4.2 The Description of $V_\ell \operatorname{Pic}^0(C)$

Once we have found the minimal regular model we can describe the representation $V_\ell \operatorname{Pic}^0(C)$ in terms of its reduction type much like we did for elliptic curves. So lets start with the first part of theorem 47.

Lemma 56. *Let C/K be a curve, then $V_\ell \operatorname{Pic}^0(C)$ is a $2g$-dimensional continuous representation of G_K over $\mathbb{Q}_\ell$ and $\det(V_\ell \operatorname{Pic}^0(C)) = \mathbb{Q}_\ell(g)$.*

Proof. If C is geometrically regular, then by choosing an isomorphism $\overline{K} \cong \mathbb{C}$, $X := C \times_K \overline{K}$ becomes a complex projective curve of genus g and the Abel-Jacobi theorem provides an isomorphism $\operatorname{Pic}^0(C) \cong H^0(X, \Omega^1_X)^\vee / H_1(X, \mathbb{Z}) \cong \mathbb{C}^g/\Lambda$ where Λ is a lattice. This gives the dimension of $V_\ell \operatorname{Pic}^0(C)$.[2]

[2] In fact for any abelian variety over a field of characteristic $\neq \ell$ and dimension g one has $\dim V_\ell A = 2g$ and so one could also use Weil's algebraic construction of the Jacobian.

For the determinant we use that $J(C)$ is self-dual [CS86, VII. §6] so that again there is a Weil pairing $J(C)[n] \times J(C)[n] \to \mu_n$ [CS86, V.§16] which glues together to a non-zero map $\bigwedge^2 V_\ell \operatorname{Pic}^0(C) \to \mathbb{Q}_\ell(1)$ and thus there is an non-zero map $\det V_\ell \operatorname{Pic}^0(C) = \bigwedge^{2g} V_\ell \operatorname{Pic}^0(C) \to \mathbb{Q}_\ell(g)$, as required. □

For elliptic curves with good reduction we were able to compute the Galois representation just by counting points. The same is true for any curve C/K with good reduction. This follows from a base change theorem in etale cohomology, part of the Weil conjectures (the Lefschetz trace formula) and the fact that $(V_\ell \operatorname{Pic}^0(C))^\vee \cong H^1_{et}(C, \mathbb{Q}_\ell)$ [CS86, VII.9.6,V.15.1].

Theorem 57. *Let $\mathcal{X}/\mathcal{O}_K$ be an integral, projective, smooth and flat scheme , then there is a Galois-equivariant isomorphism $H^i_{et}(\mathcal{X}_{\overline{K}}, \mathbb{Q}_\ell) \cong H^i_{et}(\mathcal{X}_{\overline{k}}, \mathbb{Q}_\ell)$. In particular $H^i_{et}(\mathcal{X}_{\overline{K}}, \mathbb{Q}_\ell)$ is unramified.*

Proof. See [SGA5, XVI. 2.2 and 2.3]. □

Remark 58. For elliptic curves we saw that there is also a converse: if $V_\ell E$ is unramified, then E has good reduction. This is false in general. See example 70 for a genus 2 curve which has bad reduction but unramified Galois representation. However, for abelian varietes A/K it is still true that $V_\ell A$ is unramified if and only if A has good reduction [SeTa]. This shows that the relationship between the reduction of C and of $J(C)$ is somewhat subtle.

Theorem 59. *Let $X/\mathbb{F}_q$ be a geometrically irreducible projective variety, then*

$$Z(X,t) = \prod_{i=0}^{2\dim X} \det\left(1 - t \operatorname{Frob}_q^{-1}|_{H^i_{et}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)}\right)^{(-1)^{i+1}},$$

where $Z(X,t) = \exp\left(\sum_{m\geq 1} |X(\mathbb{F}_{q^m})| \frac{t^m}{m}\right)$ is the zeta function of X.

Proof. See [Del74, 1.5.4] for how to obtain the result from the Lefschetz formula which is proven in [SGA5, III]. □

Corollary 60. *Let $C/\mathbb{F}_q$ be a geometrically regular, irreducible, projective curve, then the eigenvalues of $\operatorname{Frob}_q^{-1}$ acting on $V_\ell \operatorname{Pic}^0(C)$ are the roots of $(1-t)(1-qt)Z(C,t)$ (with multiplicity).*

Proof. $\operatorname{Frob}_q^{-1}$ acts as 1 on H^0 and as q on H^2 [Del74, 2.3], hence

$$(1-t)(1-qt)Z(C,t) = \det\left(1 - \operatorname{Frob}_q^{-1} t|_{H^1}\right) = \det\left(1 - \operatorname{Frob}_q t|_{V_\ell \operatorname{Pic}^0(C)}\right). \qquad \square$$

Corollary 61. *Let $C/\mathbb{F}_q$ be a geometrically regular, irreducible, projective curve, then $V_\ell \operatorname{Pic}^0(C)$ is a semisimple $G_{\mathbb{F}_q}$-representation and hence completely determined by the eigenvalues of Frob_q.*

Proof. Since $\operatorname{Pic}^0(C) \cong J(C)$ and Frob_q acts on $J(C)$ by endomorphisms it suffices that $\operatorname{End}(A)$ is semisimple for any abelian variety $A/\mathbb{F}_q$. This is proven in [CS86, V. §12]. □

Remark 62. Since $Z(C,t)$ is 'easily' computable (one just has to count $\mathbb{F}_{q^m}$-points for $m \leq g$) the Galois representations of curves over finite fields are rather explicit objects.

Example 63. Let p be an odd prime, then the hyperelliptic curve $C : y^2 = x^5 - 1$ over $\mathbb{Q}_p$ has good reduction. If $p \not\equiv \pm 1 \pmod 5$, then $Z(C,t) = \frac{1+p^2t^4}{(1-t)(1-pt)}$ and so Frob_p acts on $V_\ell \operatorname{Pic}^0(C)$ with eigenvalues $\zeta_8\sqrt{p}, \zeta_8^3\sqrt{p}, \zeta_8^5\sqrt{p}, \zeta_8^7\sqrt{p}$, where ζ_8 is a primitive 8th root of unity.

Proof. Since $p, p^2 \not\equiv 1 \pmod 5$, $x \mapsto x^5$ is a bijection on $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$. Thus $C(\mathbb{F}_p) = p+1$ and $C(\mathbb{F}_{p^2}) = p^2+1$. This shows that $Z(C,t) = \exp((p+1)t + (p^2+1)t^2/2) + O(t^3)$ and so $(1-t)(1-pt)Z(C,t) = 1 + O(t^3)$. Since C has genus 2, Poincaré Duality [Del74, 2.3] implies the functional equation $Z(C,t) = pt^2 Z(C, p^{-1}t^{-1})$ or $P(t) = p^2t^4 P(p^{-1}t^{-1})$, where $P(t) = \det\left(1 - \operatorname{Frob}_p t|_{V_\ell \operatorname{Pic}^0(C)}\right)$. We already know $P(t) = 1 + O(t^3)$ and so $P(t) = 1 + p^2t^4$. □

This concludes the discussion for the case when C/K has good reduction. For the case of bad reduction we need the following combinatorial data which we will associate to the special fibre of the minimal regular model of C.

Definition 64. The dual graph of a one-dimensional algebraic variety X is a multigraph consisting of vertices for each irreducible component of X and an edge for every point of intersection between said components.

Theorem 65. *Let C/K be a curve of genus $g \geq 1$ and $\mathcal{C}$ the minimal regular model of C over $\mathcal{O}_K$. Assume that the special fibre of $\mathcal{C}$ has semi-stable reduction and Γ be the dual graph of $\mathcal{C}_{\mathfrak{m}_K}$, then Γ carries a natural unramified G_K-action induced by the action on $\mathcal{C}_{\mathfrak{m}_K}$ and*

$$V_\ell \operatorname{Pic}^0(C) \cong H_1(\Gamma, \mathbb{Z}) \otimes \chi_{cyc} \otimes sp(2) \oplus V_\ell \operatorname{Pic}^0(\widetilde{\mathcal{C}}_{\mathfrak{m}_K}),$$

where $\widetilde{\mathcal{C}}_{\mathfrak{m}_K}$ is the normalisation of $\mathcal{C}_{\mathfrak{m}_K}$.

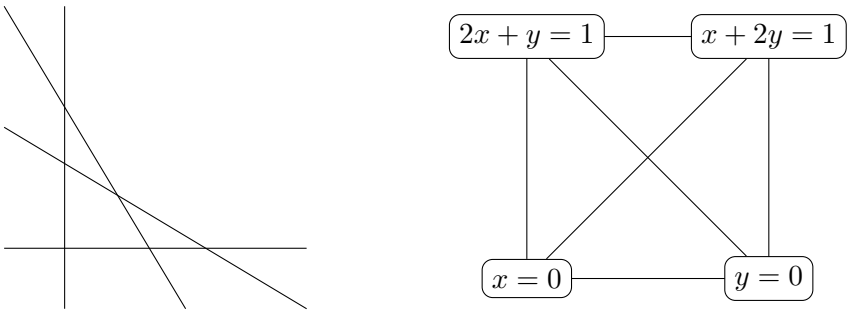
Proof. See [Dok+18, 2.18]. □

Corollary 66. *Let C/K be a curve of genus $g \geq 1$, then the representations $V_\ell \operatorname{Pic}^0(C)$ for $\ell \neq p$ are ϕ_K-semisimple and independent of ℓ (definition 17).*

Proof. The ϕ_K-semisimplicity follows from the fact that G_K acts through a finite quotient on Γ and Corollary 61. For the independence of ℓ we just observe that neither Γ, nor $\widetilde{\mathcal{C}}_{\mathfrak{m}_K}$ depend on ℓ and Corollary 60 establishes the independence of ℓ for the second summand. □

Example 67. Consider the plane curve $C : xy(x + 2y - 1)(2x + y - 1) = p$ over $\mathbb{Q}_p$ for $p > 2$. Then $V_\ell \operatorname{Pic}^0(C) \cong \chi_{cyc} \otimes sp(2)^{\oplus 3}$.

Proof. The obvious model given by the same equation over $\mathbb{Z}_p$ is a regular model. It is minimal since the special fibre contains no (-1)-curves (they are all (-3)-curves by [Liu10, 9.1.21]). Hence the special fibre $\mathcal{C}_{\mathfrak{m}_K}$ is given by 4 $\mathbb{F}_p$-lines in general position as shown in figure 4. The dual graph is a tetrahedron and the normalisation is the disjoint union of 4 lines and hence $\operatorname{Pic}^0(\widetilde{\mathcal{C}}_{\mathfrak{m}_K}) = 0$ and $H_1(\Gamma, \mathbb{Z}) = \mathbb{Z}^3$ with trivial G_K-action. □



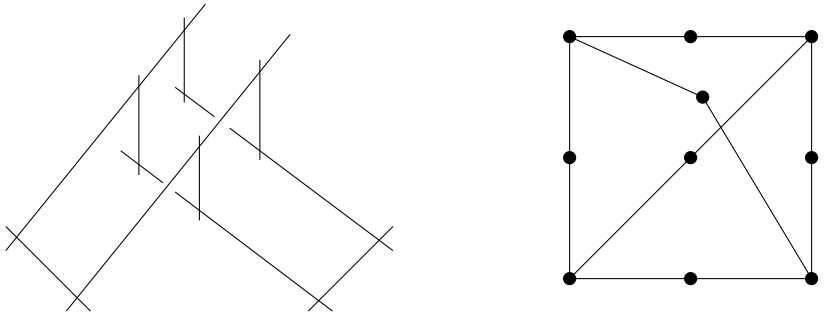
(a) Special Fibre (b) Dual Graph of Special Fibre

Figure 4: Reduction of $xy(x + 2y - 1)(2x + y - 1) = p$

Example 68. Consider the plane curve $C : xy(x + 2y - 1)(2x + y + 1) = p^2$ over $\mathbb{Q}_p$ for $p > 2$. Then again $V_\ell \operatorname{Pic}^0(C) \cong \chi_{cyc} \otimes sp(2)^{\oplus 3}$.

Proof. Now the obvious model given by the same equation over $\mathbb{Z}_p$ is not a regular model. However [Liu10, 8.3.53] shows that the blowup of $\mathbb{Z}_p[x, y]/(xy - p^2)$ at (x, y, p) is regular and its special fibre consists of 2 affine $\mathbb{F}_p$-lines joined by the exceptional divisor which is a projective $\mathbb{F}_p$-line. Since at every intersection of the 4 $\mathbb{F}_p$-lines, Zariski locally our model looks like

$\mathbb{Z}_p[x,y]/(xy-p^2)$ we can use this to find that the special fibre of the model obtained from blowing up the 6 intersection points of the $\mathbb{F}_p$-lines $x=0, y=0, x+2y=1$ and $2x+y=1$ consists of 10 lines as shown in figure 5 and is regular. Now the special fibre contains 6 (-2) and 4 (-3) curves and so we have found the minimal regular model by Castelnuovo's criterion [Liu10, 9.3.8]. Again this shows that $\mathrm{Pic}^0(\widetilde{\mathcal{C}}_{\mathfrak{m}_K}) = 0$ and $H_1(\Gamma,\mathbb{Z}) = \mathbb{Z}^3$ with trivial G_K-action. □



(a) Special Fibre (b) Dual Graph of Special Fibre

Figure 5: Reduction of $xy(x+2y-1)(2x+y-1) = p^2$

Remark 69. Every curve admits semi-stable reduction over a finite separable extension by the Deligne-Mumford theorem [Liu10, 10.4.3]. Thus theorem 65 already determines the representation of any curve up to 'finite index'. The complete representation is described in [Dok+18, 2.18].

If C/K is a hyperelliptic curve, then [Dok+18] basically answers all questions about the $V_\ell \operatorname{Pic}^0(C)$. The gist is that if C is given by $y^2 = f(x)$, then the arithmetic of the roots of f determines everything.

Example 70. Let $p > 2$ and $C/\mathbb{Q}_p$ the hyperelliptic curve $y^2 = x(x+p^2)(x+2p^2)(x-1)(x-1+p^2)(x-1+2p^2)$, then $V_\ell \operatorname{Pic}^0 C$ is unramified and C has bad reduction.

Proof. This follows from [Dok+18, Theorem 1.8 (2),(5)]. □

5 Application to the Inverse Galois Problem

The inverse Galois Problem is a notoriously hard question: Which finite groups appear as Galois groups of Galois extensions $L/\mathbb{Q}$? See the book [SD08] for a survey of classical methods in the field and [NSW08, IX.§6] for a proof of Shafarevic's famous result that any solvable group appears as the Galois group of a finite Galois extension of $\mathbb{Q}$. In this section we prove that $GL_2(\mathbb{F}_\ell)$ is the Galois group of a finite extension of $\mathbb{Q}$ for all primes ℓ. To do so we construct an elliptic curve such that the action $G_\mathbb{Q} \to \mathrm{Aut}(E[\ell])$ is surjective for all but an explicit finite set of primes ℓ. However, we also show that there are complications if one tries to use the same method in higher dimensions because there is a restriction on the dimensions of irreducible ℓ-adic representations of G_K whose characteristic polynomials have rational coefficients, see propositions 74 and 75.

We need the following group theoretic lemma.

Lemma 71. *Let $H < \mathrm{GL}_2(\mathbb{F}_\ell)$ be a subgroup such that the inclusion $H \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ is an irreducible representation and H contains an element of order ℓ, then H contains $SL_2(\mathbb{F}_\ell)$.*

Proof. See [Ser89, IV.3.2 Lemma 2]. □

Proposition 72. *Let $E : y^2 = x^3 + 5x^2 + 7^4 \cdot 5^2$, then the action $G_\mathbb{Q} \to \mathrm{Aut}(E[\ell])$ is surjective for all primes $\ell \notin \{5,7\}$.*

Proof. Fix a prime $\ell \notin \{5,7\}$ and let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ be the ℓ-adic representation of E. Since $\ell \neq 5,7$, the restrictions to $G_{\mathbb{Q}_5}$ and $G_{\mathbb{Q}_7}$ are the ℓ-adic representations of $E/\mathbb{Q}_5$ and $E/\mathbb{Q}_7$, respectively.

E has additive reduction at 5 which becomes good over $K = \mathbb{Q}_5(5^{1/3})$, where it has the model $E' : y^2 = x^3 + 5^{1/3}x^2 + 7^4$. So the Galois representation factors through $\mathrm{Gal}(K^{un}/\mathbb{Q}_5) \cong \mathbb{Z}/3\mathbb{Z} \rtimes \hat{\mathbb{Z}}$, where $(1,0) \in \mathbb{Z}/3\mathbb{Z} \rtimes \hat{\mathbb{Z}}$ corresponds to an automorphism σ such that $\sigma(5^{1/3}) = \zeta_3 5^{1/3}$ and $(0,1)$ corresponds to Frob_5. If σ acted trivially, then E would be unramified and have good reduction but this is not the case as can be seen by the minimal model. Hence $\rho(\sigma)$ has eigenvalues ζ_3, ζ_3^{-1}. As $|E'(\mathbb{F}_5)| = 6$, the characteristic polynomial of $\rho(\mathrm{Frob}_5)$ is $T^2 + 5$. The relation $\mathrm{Frob}_5 \, \sigma \, \mathrm{Frob}_p^{-1} = \sigma^{-1}$ shows that there is a $\overline{\mathbb{F}}_\ell$-basis of $E[\ell]$ in which

$$\rho(g) = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix}, \qquad \rho(\mathrm{Frob}_5) = \begin{pmatrix} 0 & \sqrt{-5} \\ \sqrt{-5} & 0 \end{pmatrix}.$$

In particular $G_{\mathbb{Q}_5} \to \mathrm{Aut}(E[\ell])$ is irreducible.

E has split multiplicative reduction at 7 and by corollary 46 the image of $G_{\mathbb{Q}_7}$ in $\mathrm{Aut}(E[\ell])$ contains an element of order ℓ. Now lemma 71 combined with the fact that $\det(V_\ell E) = \mathbb{Q}_\ell(1)$ shows that $G_{\mathbb{Q}}$ surjects onto $\mathrm{Aut}(E[\ell])$ as desired. □

Remark 73. To deal with the primes 5 and 7 one can easily construct a similar curve and replace 5 and 7 by different primes. Moreover, it is in fact a theorem of Serre that for any non-CM elliptic curve E over a number field L, the image of G_L in $\mathrm{Aut}(T_\ell E)$ is open for all ℓ and surjective for most ℓ [Ser71]. Moreover, for any such elliptic curve, the representation $G_L \to \mathrm{Aut}(V_\ell E)$ is irreducible [Ser89, IV.2.1].

In the previous proof we exploited that $V_\ell E$ is irreducible. One might be inclined to try a similar strategy to establish the inverse Galois problem for the groups $GSp_{2n}(\mathbb{F}_\ell)$. That is, construct an abelian variety of dimension n with suitable bad reductions at certain primes. Expanding on [AD17, footnote 2] we show why this strategy does not work in general.

Proposition 74. *Let p be the characteristic of k and $\ell \neq p$ a prime. Let V be a continuous ϕ_K-semisimple absolutely irreducible tamely ramified $\mathbb{Q}_\ell$-representation of G_K such that the characteristic polynomial of any $h \in I_K$ has rational coefficients, then there exists an integer m such that* $\dim V = \varphi(m)$.

Proof. Since $sp(n)$ is not semisimple for $n > 1$, theorem 13 implies that I_K acts through a finite quotient on V. The tame inertia group is pro-cyclic and so I_K acts on V through $\mathbb{Z}/m\mathbb{Z}$ for some integer m which we choose to be minimal. Let $\tau \in I_K$ be a generator of this action, then the eigenvalues of $\rho(\tau)$ are mth roots of unity. Suppose one of the eigenvalues is not a primitive root of unity. Then there is $n < m$ such that $\rho(\tau)^n$ has a non-zero fixed subspace. The relation $\phi_K^{-1}\tau\phi_K = \tau^q$ implies that this is an invariant subspace of the whole representation. However, it is not the whole representation since $\rho(\tau)$ has order m by the minimality of m. This contradicts the irreducibility of V.

Thus all eigenvalues of $\rho(\tau)$ are primitive mth roots of unity and so $\det(X\,\mathrm{id} - \rho(\tau)) = \Phi_m(X)^t$ for some t, where Φ_m is the mth cyclotomic polynomial. Moreover, finite group representation theory applied to $\mathbb{Z}/m\mathbb{Z}$ shows that $\rho(\tau)$ is diagonalisable over $\overline{\mathbb{Q}_\ell}$. The relation $\phi_K^{-1}\tau\phi_K = \tau^q$ shows that ϕ_K maps the λ-eigenspace to the λ^q-eigenspace. So by choosing an appropriate basis we can decompose $V \otimes \overline{\mathbb{Q}_\ell} = \oplus_{i=1}^t V_i$ where V_i contains each eigenvalue with multiplicity one. By absolute irreducibility we conclude that $t = 1$ and so $\dim V = \varphi(m) = |\{\zeta \in \overline{\mathbb{Q}_\ell} : \zeta \text{ is a primitive } m\text{th root of unity}\}|$. □

Proposition 75. *Assume that p is an odd prime and let $\ell \neq p$ be prime. Let V be a continuous ϕ_K-semisimple absolutely irreducible wildly ramified $\mathbb{Q}_\ell$-representation of G_K such that the characteristic polynomial of any $h \in I_K$, then $(p-1) \mid \dim V$.*

Proof. By lemma 11, P_K acts faithfully through a finite quotient G on V. Since P_K is a normal subgroup of G_K we can apply Clifford's theorem [Cli37, §1] to decompose the restriction of $V \otimes \overline{\mathbb{Q}_\ell}$ to G into irreducibles. Thus there is an isomorphism of G-representations $V \otimes \overline{\mathbb{Q}_\ell} \cong \bigoplus_i V_i$, where the V_i are irreducible G-representations which are all conjugate, i.e. if $\rho_i : G \to \mathrm{GL}(V_i)$ is the corresponding homomorphism, then for all j, $\rho_j(x) = \rho_i(gxg^{-1})$ for some $g \in G$.

Note that $V^G < V$ is a subrepresentation since $P_K < G_K$ is a normal subgroup. Thus $V^G = 0$ since otherwise V is tamely ramified. Consequently all the V_i are non-trivial. Let $G_i = G/\ker \rho_i$ be the quotient of G which acts faithfully on V_i. Since G_i is a p-group, there is a non-trivial element g_i in the center of G_i which acts as a scalar λ_i on V_i. As G_i acts faithfully we have $\lambda_i \neq 1$ and hence the Galois orbit of the character of V_i contains at least $(p-1)$ elements. Since the character of V is defined over $\mathbb{Q}$, this implies that the decomposition of V contains all these Galois conjugates and in particular that $(p-1) \mid \dim V$. □

Corollary 76. *Let $p \neq 2, 3$ and $K/\mathbb{Q}_p$ a finite extension. Moreover, let d be a prime such that $2d+1$ is not a prime, then there is no abelian variety A/K of dimension d whose associated Galois representation $V_\ell A$ is absolutely irreducible. In particular there are no abelian varieties $A/\mathbb{Q}_p$ of dimension $7, 13$ or 17 with absolutely irreducible $V_\ell A$.*

Proof. Suppose A was such an abelian variety A/K of dimension d. By theorem 13, I_K must act through a finite quotient on $V_\ell A$, i.e. A has potentially good reduction and the characteristic polynomials of elements $h \in I_K$ have integral coefficients independent of ℓ by [SeTa, Theorem 2]. If $V_\ell A$ is tamely ramified then proposition 74 shows that $2d = \dim V_\ell A = \varphi(m)$ for some m. Absurd. See [OEIS, A005277] for more examples of even integers which are not a value of φ. If $V_\ell A$ is wildly ramified, then proposition 75 shows that $(p-1) \mid 2d$, so $p \in \{2, 3, d+1, 2d+1\}$ contradicting the hypothesis that $p \neq 2, 3$ and $2d+1$ is not prime. □

References

[OEIS] OEIS Foundation Inc. (2020). *The On-Line Encyclopedia of Integer Sequences*. URL: https://oeis.org/.

[AD17] Samuele Anni and Vladimir Dokchitser. "Constructing hyperelliptic curves with surjective Galois representations". In: *arXiv e-prints*, arXiv:1701.05915 (Jan. 2017), arXiv:1701.05915. arXiv: 1701.05915 [math.NT].

[Bou62] Nicolas Bourbaki. *Algèbre*. Hermann, 1962.

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

[Cli37] A. H. Clifford. "Representations Induced in an Invariant Subgroup". In: *The Annals of Mathematics* 38.3 (1937), p. 533. DOI: 10.2307/1968599.

[Con] Brian Conrad. *Minimal Models for Elliptic Curves*. Accessed 10/04/2020 at http://math.stanford.edu/~conrad/papers/minimalmodel.pdf.

[CS86] Gary Cornell and Joseph H. Silverman. *Arithmetic geometry*. Springer, 1986.

[Del72] P. Deligne. "Les Constantes des Equations Fonctionnelles des Fonctions L". In: *Lecture Notes in Mathematics Modular Functions of One Variable II* (1972), pp. 501–597. DOI: 10.1007/978-3-540-37855-6_7.

[Del74] Pierre Deligne. "La conjecture de Weil. I". In: *Publications mathématiques de lIHÉS* 43.1 (1974), pp. 273–307. DOI: 10.1007/bf02684373.

[DD11] Tim Dokchitser and Vladimir Dokchitser. "Euler factors determine local Weil representations". In: *arXiv e-prints*, arXiv:1112.4889 (Dec. 2011), arXiv:1112.4889. arXiv: 1112.4889 [math.NT].

[Dok+18] Tim Dokchitser et al. “Arithmetic of hyperelliptic curves over local fields”. In: *arXiv e-prints*, arXiv:1808.02936 (Aug. 2018), arXiv:1808.02936. arXiv: 1808.02936 [math.NT].

[DA14] Vladimir Dokchitser and Samuele Anni. “l-Adic Representations and their Associated Invariants”. In: *arXiv e-prints*, arXiv:1410.1039 (Oct. 2014), arXiv:1410.1039. arXiv: 1410.1039 [math.NT].

[SGA5] Alexandre Grothendieck. *Séminaire de géométrie algébrique du Bois-Marie 1965-66, Cohomologie l-adique et fonctions L, SGA5*. Vol. 589. Springer Lecture Notes. Springer-Verlag, 1977, pp. xii+484.

[Lan] Serge Lang. *Introduction to algebraic and abelian functions*. Springer-Verlag.

[Liu10] Qing Liu. *Algebraic geometry and arithmetic curves*. Oxford Univ. Press, 2010.

[LMFDB] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. http://www.lmfdb.org. [Online; accessed 10 April 2020]. 2020.

[Mil13] James S. Milne. *Lectures on Etale Cohomology (v2.21)*. Accessed 10/04/2020 at www.jmilne.org/math/. 2013.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. eng. Second Edition. Vol. 323. Grundlehren der mathematischen Wissenschaften. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. ISBN: 9783540378884.

[Roh94] David Rohrlich. “Elliptic curves and the Weil-Deligne group”. In: *CRM Proceedings and Lecture Notes Elliptic Curves and Related Topics* (1994), pp. 125–157. DOI: 10.1090/crmp/004/10.

[Ser71] Jean-Pierre Serre. “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”. fre. In: *Inventiones mathematicae* 15.4 (1971), pp. 259–331. ISSN: 0020-9910.

[Ser89] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves / Jean-Pierre Serre*. eng. Advanced book classics. Redwood City, Calif.: Addison-Wesley, Advanced Book Program, 1989. ISBN: 0201093847.

[SD08] Jean-Pierre Serre and Henri Darmon. *Topics in Galois theory*. A K Peters, 2008.

[SeTa] Jean-Pierre Serre and John Tate. “Good Reduction of Abelian Varieties”. In: *The Annals of Mathematics* 88.3 (1968), p. 492. DOI: 10.2307/1970722.

[AAEC] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.

[AEC] Joseph H. Silverman. *The arithmetic of elliptic curves*. eng. 2nd ed. Graduate texts in mathematics ; 106. New York: Springer, 2009. ISBN: 1-282-12638-5.

[Ste10] Ernst Steinitz. “Algebraische Theorie der Körper.” In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1910.137 (Jan. 1910), pp. 167–309. DOI: 10.1515/crll.1910.137.167.

[Tay04] Richard Taylor. “Galois representations”. In: *Annales de la faculté des sciences de Toulouse Mathématiques* 13.1 (2004), pp. 73–119. DOI: 10.5802/afst.1065.

[Wei49] André Weil. “Numbers of solutions of equations in finite fields”. In: *Bulletin of the American Mathematical Society* 55.5 (Jan. 1949), pp. 497–509. DOI: 10.1090/s0002-9904-1949-09219-4.