UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

THE REPRESENTATIONS OF P-ADIC FIELDS ASSOCIATED TO ELLIPTIC CURVES

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

SALAM TURKI
Norman, Oklahoma
2015

THE REPRESENTATIONS OF P-ADIC FIELDS
ASSOCIATED TO ELLIPTIC CURVES

A DISSERTATION APPROVED FOR THE
DEPARTMENT OF MATHEMATICS

BY

Dr. Ralf Schmidt, Chair

Dr. Jonathan Kujawa

Dr. Kimball Martin

Dr. Alan Roche

Dr. Anne Dunn

Acknowledgments

It would be impossible for me to put into words my deepest appreciation for all the people who have helped and encouraged me during my time in graduate school.

My heartfelt appreciation goes out to Dr. Ralf Schmidt, my committee chairperson, for his assistance, guidance and patience during the many calls for advice and for the encouragement that was always present. Working with him is a huge learning experience and I thank him for giving me this golden opportunity. I would like to thank Dr. Jonathan Kujawa for being a great teacher. In fact, almost half of my courses I took while at the University of Oklahoma were taught by him. Additionally, I would like to thank both Dr. Kimball Martin and Dr. Alan Roche for their constructive feedback on my dissertation. My appreciation goes as well to the students, faculty and staff in the Department of Mathematics for providing a friendly and supportive environment for my academic endeavors.

I am forever grateful to my family who has always encouraged me, supported me financially but most important emotionally through all my life. Their love, sacrifice and hard work gave me the opportunity to pursue my education. No words can describe my gratitude and appreciation to everything you have done for me and I am forever indebted to you. The most monument thank you goes to my brother Houssein El Turkey who without him I would not even dream to get my doctorate degree. I dedicate my dissertation to my illiterate father, mother and sisters Ibtisam and Feryal who always appreciated and believed in

knowledge and education.

In addition, I would like to express my sincere appreciation to all my friends; in particular my friends in the Lebanese Student Association: Rami Akkari, Hiba Baroud, Pierre Karam, Karim Saadeddine, and Dania Sheaib. You brought joy to my life in Norman. My deepest and warm thank you goes to my friend Wassim Tabet for all the long conversations we had that helped me to keep moving forward when frustration creeped in. You were always there and listened to me when things were not going well. I wish you all the best. Finally, I would like to thank my teammates in the USTA tennis league. It was wonderful to meet all of you. My special thanks go to Noe Cruz for being my biggest fan on the tennis courts and for all his support and encouragement to finish this dissertation.

Contents

Abstract

The goal of this dissertation is to find the irreducible, admissible representation π of $\mathrm{GL}(2, F)$ attached to an elliptic curve E over a p-adic field F. Associated to E is a 2-dimensional complex representation σ' of the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$ via the action of the absolute Galois group on the Tate module. On the other hand, the local Langlands correspondence states that the 2-dimensional representations of $\mathcal{W}'(\bar{F}/F)$ are in bijection with equivalence classes of irreducible, admissible representations of $\mathrm{GL}(2, F)$. We consider a Weierstrass equation for E of the form

$$y^2 + a_1xy + a_2y = x^3 + a_2x^2 + a_4x + a_6. \tag{W}$$

We will determine the representation π in terms of the coefficients a_1, a_2, a_3, a_4, a_6. We also investigate a particular class of π called "triply imprimitive" representations.

Chapter 1

Introduction

Let F be a non-archimedean local field of characteristic zero. Let $\mathfrak{o}$, $\mathfrak{p}$, ϖ denotes the ring of integers of F, the maximal ideal in this ring, and a uniformizer for F, respectively. Let E/F be an elliptic curve defined over F, written in a general Weierstrass equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

with $a_i \in F$ for all i. We let Δ be the discriminant of this equation and $j(E)$ the j-invariant of E. A Weierstrass equation is called minimal if the valuation of the discriminant is minimized provided that $a_i \in \mathfrak{o}$ for all i. We then reduce a minimal equation modulo the maximal ideal $\mathfrak{p}$ to get a possibly singular curve $\tilde{E}$. We say E has good, multiplicative, or additive reduction if $\tilde{E}$ is nonsingular, has a node, or a cusp, respectively. A further classification can be made as follows. We say that E/F has potential good (multiplicative) reduction if there exists a finite extension K/F so that E/K has good (multiplicative) reduction. It is a well known fact that E/F has potential good reduction if and only if $j(E) \in \mathfrak{o}$. Assuming that E/F has potential multiplicative reduction, the γ-invariant, $\gamma(E/F) \in F^\times/F^{\times 2}$, is defined as in Tate's uniformization theorem.

Letting $G = \mathrm{GL}(2, F)$ be a general linear group over F, there are three types of irreducible, admissible representations π of G. These are the principal series, the twists of the Steinberg, and the supercuspidal representations. This

classification is outlined in Section 2.5.

The local Langlands correspondence (LLC) says that irreducible, admissible representations π of $\mathrm{GL}(2,F)$ are in bijection with admissible 2-dimensional representations of the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$. Thus, we can associate a representation π to every elliptic curve E defined over F as follows. We first choose a prime ℓ different from the residual characteristic of F. The Galois group $\mathrm{Gal}(\bar{F}/F)$ acts on the Tate module $T_\ell(E)$, yielding a two-dimensional ℓ-adic representation $\rho_\ell : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}(2,\mathbb{Q}_\ell)$. Then via the procedure outlined in Section 4 of [9], ρ_ℓ can be converted to a complex representation $\sigma' : \mathcal{W}'(\bar{F}/F) \to \mathrm{GL}(2,\mathbb{C})$ which corresponds to an irreducible, admissible representation π' of $\mathrm{GL}(2,F)$ by the LLC. After a twist by $\omega^{1/2}$, we have a representation π with trivial central character. Here ω is the one-dimensional representation of the Weil group $\mathcal{W}(\bar{F}/F)$ with the property $\omega(\Phi) = q^{-1}$ for any inverse Frobenius element and trivial on the inertia subgroup of $\mathcal{W}(\bar{F}/F)$.

An important feature of this construction is that the conductors of both E and π coincide,

$$a(E) = a(\pi).$$

The association $E \mapsto \pi$ can be considered a local version of the famous modularity theorem, which associates with every elliptic curve E over $\mathbb{Q}$ of conductor N a modular form $f \in \mathcal{S}_2(\Gamma_0(N))$.

A natural question then is this: Given an elliptic curve E/F by a Weierstrass equation as above, determine π. More precisely,

- When is π a principal series representation? When so, which one is it?
- When is π a twist of a Steinberg representation? When so, which twist?
- When is π supercuspidal? When so, which supercuspidal representation is

it?

We want to find π in terms of the coefficients of the Weierstrass equation (1.1) and without going through the Tate module $T_\ell(E)$ and its ℓ-adic representations. Also, we want to bypass the procedure of converting those representations into complex representations of the Weil-Deligne group.

As explained in Section 2.4, a complex representation σ' of the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$ is a pair (σ, N). Here σ is a representation of the Weil group $\mathcal{W}(\bar{F}/F)$ and N is the nilpotent part.

Our goal in this dissertation is to answer the above questions. To do so we consider two fundamentally disjoint cases:

1. E/F has *potential good reduction.*

2. E/F has *potential multiplicative reduction.*

If E has potential multiplicative reduction, then Theorem 3.4.3 answers the question above. It says that for such a curve E, the representation π is a Steinberg representation twisted by the quadratic character $(\gamma(E/F), .)$ where $(.,.)$ is the Hilbert symbol. Note that we must have a non-zero nilpotent part for the Weil-Deligne representation associated to E/F, since E/F has potential multiplicative reduction. Thus, π is a twist of the Steinberg representation, as explained in Table 2.5.2.

Now, assume that E/F has potential good reduction, then E has either good or additive reduction. If E has good reduction, then the Weil-Deligne representation σ' associated to E is of the form $(\sigma, 0)$. Moreover, it was proved in Section 14 of [Rohrlich, [9]] that σ is unramified and semisimple, i.e., $\sigma = \omega^{1/2}(\chi \oplus \chi^{-1})$. Then by Table 2.5.2, we have an unramified principal series representation π of $\mathrm{GL}(2, F)$. Namely, $\pi = \chi \times \chi^{-1}$ where χ is an unramified

character of $F^\times$ with $\chi(\varpi) = \alpha$ such that $|\alpha| = 1$ where $|.|$ is the normalized absolute value on $F^\times$.

Next we assume that E/F has additive reduction, but good reduction over some field extension F'/F. Let $\sigma' = (\sigma, N)$ be the associated Weil-Deligne representation. By the Proposition in Section 14 of [9], we have $N = 0$ and σ is ramified and semisimple. There are two cases: either σ is a sum of two characters or it is irreducible. Let $p \geq 5$ and $F = \mathbb{Q}_p$, then Rohrlich in Proposition 2 of [10] gives an easy criterion to differentiate the two cases. Explicitly, we have

$$\sigma \text{ is reducible} \iff (p-1)\upsilon_p(\Delta) \equiv 0 \mod 12.$$

In Theorem 4.2.2 we generalize this criterion to an arbitrary p-adic field F. Thus we have

$$\sigma \text{ is reducible} \iff (q-1)\upsilon_F(\Delta) \equiv 0 \mod 12.$$

Here, υ_F is the normalized valuation on F. Thus, by Table 2.5.2 the representation π is a principal series representation if $(q-1)\upsilon_F(\Delta) \equiv 0 \mod 12$ and supercuspidal otherwise.

In Theorem 4.3.1, we prove that $\pi = \chi \times \chi^{-1}$ such that χ is trivial on the group of principal units $1 + \mathfrak{p}$ and on the subgroup of index $e = \frac{12}{\gcd(12, \upsilon_F(\Delta))}$. Moreover, we show that the induced character on $\mathbb{Z}/e\mathbb{Z}$ has order e.

If π is supercuspidal, then in Theorem 4.4.1 we prove that π is a dihedral representation induced from a tamely ramified character ξ of $H^\times$, where H is the unique unramified quadratic extension of F. Also, we prove that the restriction of ξ to the units has order e and $\xi(\varpi) = -1$. Thus, the character ξ is completely determined.

In chapter 5 we consider π to be an irreducible, admissible, supercuspidal

representation of $\mathrm{GL}(2, F)$ with trivial central character and conductor 2. We then investigate when the base change $\mathrm{BC}_{L/F}(\pi)$ is a principal series representation for all quadratic extensions L of F. Assume that F has odd residual characteristic and π is triply imprimitive, which means that the base change $\mathrm{BC}_{L/F}(\pi)$ is a principal series representation for every quadratic field extension L of F. Assume further that π has conductor 2 and trivial central character; these are the supercuspidal representations relevant to elliptic curves. We then prove in Theorem 5.3.2 that there is no such π if $q \equiv 1 \mod 4$ and a unique one if $q \equiv 3 \mod 4$.

This result is applicable to elliptic curves with additive reduction. We thus get the following results. Assume that

- $q \equiv 3 \bmod 4$.
- $\upsilon_F(\Delta)$ is odd.
- $(q-1)\upsilon_F(\Delta) \equiv 0 \bmod 3$.

Then π is a triply imprimitive supercuspidal representation.

Many of the results of this thesis are well-known to experts or in one way or another contained in the literature. For example, Rohrlich in [9] provides a criterion to distinguish between reducible and irreducible representations of the Weil-Deligne group. However, the local Langlands correspondence is not usually invoked, and explicit results are difficult to come by. We stress again that the main point is to have an explicit procedure to determine the representation π directly from the Weierstrass coefficients. The material in Chapter 5 about triply imprimitive representations is completely new.

We dedicate Chapter 2 to give an overview on elliptic curves, the Weil-Deligne group and the representation theory of $\mathrm{GL}(2, F)$. We start in Section 2.1 with

some general background on elliptic curves. Then we move on to define their Tate modules. We devote Section 2.3 to talk about elliptic curves over a local field F. We define the minimality concept of a Weierstrass equation and introduce the reduction types modulo the maximal ideal $\mathfrak{p}$. In Section 2.4 we define the Weil and the Weil-Deligne groups. Also, we outline a procedure to convert the ℓ-adic representation of the Galois group $\mathrm{Gal}(\bar{F}/F)$ into a complex representation of the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$. Finally, Section 2.5 summarizes the basic representation theory of $\mathrm{GL}(2,F)$ and classifies the irreducible admissible ones.

In Chapter 3 we consider elliptic curves with potential multiplicative reduction, beginning by defining the γ-invariant, $\gamma(E/F)$. We introduce the quadratic twist of an elliptic curve in Section 3.2 and find the behavior of $\gamma(E/F)$ in Section 3.3. Also, we provide a criterion to distinguish the split and non-split multiplicative reduction involving $\gamma(E/F)$. We address the representation theory of $\mathrm{GL}(2,F)$ in Section 3.4. In particular, we prove that the irreducible, admissible representation of $\mathrm{GL}(2,F)$ attached to E/F is $\pi = (\gamma(E/F),.)\mathrm{St}_{\mathrm{GL}(2)}$.

We turn our attention to study elliptic curves with potential good reduction in Chapter 4. We dedicate the first section to find the complex representation $\sigma' = (\sigma, N)$ of the Weil-Deligne group associated to an elliptic curve E/F. In Section 4.2 we prove a reducibility criterion of σ that only requires one to calculate the valuation of the discriminant Δ of the Weierstrass equation of E. This criterion gives two possibilities for the irreducible, admissible representations of $\mathrm{GL}(2,F)$; namely, principal series and supercuspidals. We devote Section 4.3 to explicitly find the principal series representation π of $\mathrm{GL}(2,F)$ associated to an elliptic curve E/F. In Section 4.4 we consider the supercuspidal case and determine the dihedral representation π completely.

In Chapter 5 we address a special case of supercuspidal representations,

namely, the triply imprimitive representations. We start in Section 5.1 by setting up the problem to be solved. We develop representation theoretic knowledge for index-2 subgroups in Section 5.2 and apply it to the Weil group, our group of interest in this dissertation. Section 5.3 is dedicated to the case of conductor 2, since elliptic curves with additive but potential good reduction have conductor 2. In Section 5.4 we impose certain conditions to completely determine the triply imprimitive supercuspidal representation π of $\mathrm{GL}(2, F)$ attached to E.

Chapter 2

Background Material

In this chapter we give a quick introduction to elliptic curves, their Tate modules, elliptic curves defined over local fields, the Weil group, the Weil-Deligne group and its representations, and the local Langlands correspondence for $\mathrm{GL}(2, F)$.

Through out the next section, we will let F be any field and $\bar{F}$ be its algebraic closure.

2.1 Elliptic curves

In this this section we will define elliptic curves and their discriminants. Also, we will introduce the group law on elliptic curves and define their non-singular parts. More details on the subject can be found in [13].

Elliptic curves are non-singular curves of genus one having a specified base point. It is known that each elliptic curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point, the base point, on the line at ∞. This equation is called the Weierstrass equation for the elliptic curve and is generally written by using non-homogeneous coordinates x and y,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1.1}$$

with an extra point O at infinity and $a_1, a_2, a_3, a_4, a_6 \in \bar{F}$.

Note that if $a_i \in F$ for all i, then E is said to be *defined over* F.

Assuming that $\mathrm{char}(F) \neq 2$, we can simplify equation (2.1.1) by completing

the square, more precisely, the substitution

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$

and

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

We also define the quantities

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

and

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \qquad j = \frac{c_4^3}{\Delta},$$

By substituting the b_i's in Δ, we can show that

$$1728\Delta = c_4^3 - c_6^2. \tag{2.1.2}$$

The quantities Δ and j are very important in the theory of elliptic curves. Thus we give them names where Δ is called the discriminant of the Weierstrass equation and j is called the j-invariant of the elliptic curve.

Note that a Weierstrass equation can be either an equation of a singular

curve or of an elliptic curve depending on whether the discriminant Δ is zero or not. The following proposition describes these cases and the condition when two elliptic curves are isomorphic.

Proposition 2.1.1. *(a) For any curve given by a Weierstrass equation, we have the following possibilities:*

- *It is nonsingular, i.e., an elliptic curve if and only if* $\Delta \neq 0$.
- *It is singular and has a node if and only if* $\Delta = 0$ *and* $c_4 \neq 0$.
- *It is singular and has a cusp if and only if* $\Delta = c_4 = 0$.

(b) Two elliptic curves E_1 *and* E_2 *are isomorphic over* $\bar{F}$ *if and only if the* j*-invariants* $j(E_1)$ *and* $j(E_2)$ *are equal.*

One of the most important aspects of elliptic curves is that each elliptic curve E defines an abelian group. The group structure on E is defined geometrically as follows. Given two points $P, Q \in E$ and a line L that passes through them, then it is known, due to Bézout, that L intersects E in a third point R. Consider now the line L' through the points R and O. Then by the same result L' intersects E in a third point which we call $P + Q$. For an explicit arithmetic formulas for the group operations on E one can check Section 3.2 of [13].

Let E be a (possibly singular) curve which is given by a Weierstrass equation. The set of *nonsingular points* of E is denoted by E_{ns}. If E is defined over F, then we write $E_{ns}(F)$ for its nonsingular part.

We recall from Proposition 2.1.1 that if E is singular, then there are two possibilities for the singularity, namely a node or a cusp, and which one it is determined by the quantity c_4. We quote Proposition 3.2.5 from [13] to describe E_{ns}.

Proposition 2.1.2. *Let E be a curve given by a Weierstrass equation that has singular points. Then E_{ns} is an abelian group.*

(a) Suppose that E has a node, so $c_4 \neq 0$, and let

$$y = \alpha_1 x + \beta_1 \quad \textit{and} \quad y = \alpha_2 x + \beta_2$$

be the distinct tangent lines to E at a singular point S. Then the map

$$E_{ns} \longrightarrow \bar{F}^{\times}, \qquad (x, y) \mapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$$

is an isomorphism of abelian groups.

(b) Suppose that E has a cusp, so $c_4 = 0$, and let

$$y = \alpha x + \beta$$

be the tangent line to E at S. Then the map

$$E_{ns} \longrightarrow \bar{F}^{+}, \qquad (x, y) \mapsto \frac{x - x(S)}{y - \alpha x - \beta}$$

is an isomorphism of abelian groups.

Thus E_{ns} is a multiplicative group if E has a node and it is an additive group when E has a cusp.

The fact that elliptic curves are smooth algebraic ones implies that there exist rational morphisms between them. For two elliptic curves E_1 and E_2, an *isogeny* is a morphism

$$\phi : E_1 \longrightarrow E_2 \quad \text{satisfying} \quad \phi(O) = O.$$

Further, if ϕ is defined such that $\phi(E_1) \neq \{O\}$, then the two elliptic curves E_1 and E_2 are called *isogenous*. Let $m \in \mathbb{Z}$, an example of an isogeny is the morphism $[m] : E \longrightarrow E$ such that

$$[m](P) = \underbrace{P + P + \cdots + P}_{\text{m terms}},$$

for all positive integers m. Moreover, we define $[m](P) = [-m](-P)$, for all $m < 0$ and $[0](P) = O$. This isogeny is called the *multiplication-by-m* map. If $m \neq 0$, then it is easy to prove that $[m]$ is a nonconstant morphism. Using this fact one can show

- For two elliptic curves E_1 and E_2, the group of isogenies $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.
- The endomorphism ring $\mathrm{End}(E)$ is a ring of characteristic 0 with no zero divisors.

Moreover, assuming that $m \geq 1$, the set of points of E of order m is called the *m-torsion subgroup* of E and denoted by $E[m]$, i.e., it is the set

$$E[m] = \{P \in E : [m]P = O\}.$$

Then the union of all the m-torsion subgroups, namely $\bigcup_{m=1}^{\infty} E[m]$, is called the *torsion subgroup* of E and denoted by E_{tors}. More precisely, $E_{tors} = \bigcup_{m=1}^{\infty} E[m]$ is the set of points of finite order. Note that we write $E_{tors}(F)$ for the points of finite order in $E(F)$, if E is defined over F.

From the definition of an isogeny and the theory of algebraic curves, we notice that every isogeny $\phi : E_1 \longrightarrow E_2$, except the zero (trivial) isogeny which is defined by $[0](P) = O$ for all $P \in E_1$, is surjective, i.e., a finite map. Then for any

function $f \in F(E_2)$ where $F(E_2)$ is a field of functions, we know that ϕ induces an injective map $\phi^* : F(E_2) \longrightarrow F(E_1)$ such that $\phi^* f = f \circ \phi$. Hence we define the *degree* of ϕ to be $\deg(\phi) = [F(E_1) : \phi^* F(E_2)]$ which is the degree of the field extension $F(E_1)/\phi^* F(E_2)$. It is a well known fact that the multiplication-by-m map, $[m]$, has degree m^2 provided that $m \neq 0$. Moreover, if either $\mathrm{char}(F) = 0$ or $p = \mathrm{char}(F) > 0$ and $p \nmid m$, then $E[m] = (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ as groups. For the case $\mathrm{char}(F) = p > 0$, one of the following is true

- $E[p^e] = \{O\}$ for all $e = 1, 2, 3, \ldots$.
- $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ for all $e = 1, 2, 3, \ldots$.

Let $\phi : E_1 \longrightarrow E_2$ be a non-zero isogeny. Let $m = \deg\phi$, we define the *dual isogeny* to ϕ to be the isogeny $\hat{\phi} : E_1 \longrightarrow E_2$ satisfying $\hat{\phi} \circ \phi = [m]$. One can show that for every isogeny ϕ there exists a unique such $\hat{\phi}$. This fact implies that each isogeny defines an equivalence relation. The most important fact to keep in mind is that *every isogeny* is a *group homomorphism*.

2.2 The Tate module

In this section we give an overview of the Tate module and we refer the reader to Section 3.7 of [13] for more details and proofs. We let E/F be an elliptic curve and $\ell \in \mathbb{Z}$ be a prime. Let $m \geq 2$ be an integer which is prime to $\mathrm{char}(F)$ if $\mathrm{char}(F) > 0$. From Section 2.1 we then have $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

The Galois group of F, $\mathrm{Gal}(\bar{F}/F)$, acts on the group of points of order m, $E[m]$. To see that let $\sigma \in \mathrm{Gal}(\bar{F}/F)$ and $P \in E[m]$, i.e., $[m]P = O$. Then

$$[m](P^\sigma) = ([m]P)^\sigma = O^\sigma = O.$$

This action defines a representation

$$\mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{GL}(2, \mathbb{Z}/m\,\mathbb{Z}).$$

Note that the last isomorphism requires a choice for a basis for $E[m]$.

The natural maps

$$\ell : E[\ell^{n+1}] \longrightarrow E[\ell^n]$$

give rise to a $\mathbb{Z}_\ell$-module, namely, the Tate module. The *Tate module* of E is the group

$$T_\ell(E) = \varprojlim_n E[\ell^n].$$

The fact that the group $T_\ell(E)$ defines a $\mathbb{Z}_\ell$-module is because each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\,\mathbb{Z}$-module. The following is then immediate from the fact that $E[m] = \mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}/m\,\mathbb{Z}$.

Proposition 2.2.1. *As a $\mathbb{Z}_\ell$-module, the Tate module has the following structure:*

(a) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *if* $\ell \neq \mathrm{char}(F)$.

(b) $T_p(E) \cong \{0\}$ *or* $\mathbb{Z}_p$ *if* $p = \mathrm{char}(F) > 0$.

It is easy to see that the action of $\mathrm{Gal}(\bar{F}/F)$ on each $E[\ell^n]$ commutes with the multiplication-by-ℓ map. Thus we obtain an action of $\mathrm{Gal}(\bar{F}/F)$ on the Tate module $T_\ell(E)$. Then the *ℓ-adic representation* of $\mathrm{Gal}(\bar{F}/F)$ associated to E is the homomorphism

$$\rho_\ell : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{Aut}(T_\ell(E)) \tag{2.2.1}$$

induced by the action of $\mathrm{Gal}(\bar{F}/F)$ on the ℓ^n-torsion points of E.

Remark 2.2.2. *From now on, we fix the number ℓ to be a prime which is different from the characteristic of F.*

2.3 Elliptic curves over local fields

In this section, we give an overview of elliptic curves defined over local fields. We start by introducing the minimality concept of a Weierstrass equation which is necessary to define the notion of "reduction modulo $\mathfrak{p}$".

First, we fix the following notation. Let F be a local field with $\mathrm{char}(F) = 0$ that is complete with respect to a discrete valuation υ. Let $\mathfrak{o} = \{x \in F : \upsilon(x) \geq 0\}$ be the ring of integers of F and $\mathfrak{o}^\times = \{x \in F : \upsilon(x) = 0\}$ be its unit group. We denote the maximal ideal of $\mathfrak{o}$ by $\mathfrak{p} = \{x \in F : \upsilon(x) > 0\}$. Let ϖ be a uniformizer for $\mathfrak{o}$, i.e., $\mathfrak{p} = \varpi\,\mathfrak{o}$. Let $\kappa = \mathfrak{o}\,/\,\mathfrak{p}$ be the residue class field of $\mathfrak{o}$.

Let E/F be an elliptic curve defined over F. A *minimal equation* for E at υ is a Weierstrass equation for E if $a_1, a_2, a_3, a_4, a_6 \in \mathfrak{o}$ and $\upsilon(\Delta)$ is minimized. The *minimal value* of $\upsilon(\Delta)$ is called the valuation of the minimal discriminant of E. By definition the discriminant Δ is in $\mathfrak{o}$ since the coefficients $a_i \in \mathfrak{o}$ for all i. A minimal equation can be achieved since any coordinate change gives a new discriminant Δ' such that $\Delta' = u^{-12}\Delta \in \mathfrak{o}$. Therefore, the valuation of the discriminant, $\upsilon(\Delta)$, is changed by multiples of 12. We then have

$$a_i \in \mathfrak{o} \text{ and } \upsilon(\Delta) < 12 \Longrightarrow \text{the equation is minimal.} \tag{2.3.1}$$

Conversely, if the equation is minimal, then $\upsilon(\Delta) < 12$ if the characteristic of F is not equal to 2 or 3. The following proposition states these facts.

Proposition 2.3.1. *(a) Every elliptic curve E/F has a minimal Weierstrass equation.*

(b) A minimal Weierstrass equation is unique up to a change of coordinates

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t,$$

where $u \in \mathfrak{o}^\times$ *and* $r, s, t \in \mathfrak{o}$.

(c) *Conversely, starting by any Weierstrass equation with integral coefficients, a minimal Weierstrass equation is produced by any coordinates change of the form* $x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t$ *satisfying* $u, r, s, t \in \mathfrak{o}$.

Proposition 2.3.1 implies that we can choose the model of a minimal equation that we need. Thus when fixing a minimal Weierstrass equation for E/F, the *reduced curve* of E is

$$\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6, \tag{2.3.2}$$

where $a_i \equiv \tilde{a}_i \mod \mathfrak{p}$ for all i. Hence the curve $\tilde{E}$ is defined over the residue class field κ and it is a possibly singular curve. Thus we obtain the following reduction types of E.

(a) E has *good* reduction if $\tilde{E}$ is nonsingular, i.e., an elliptic curve over κ.

(b) E has *multiplicative* reduction if $\tilde{E}$ is singular and has a node.

(c) E has *additive* reduction if $\tilde{E}$ is singular and has a cusp.

The reduction type in (b) is called *split* if the slopes of the tangent lines at the node are in κ and *nonsplit* otherwise. We say that E has *bad* reduction if E has either multiplicative or additive reduction.

The reduction type of an elliptic curve can be determined from the coefficients of a minimal Weierstrass equation. Let E/F be an elliptic curve given by a minimal Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let Δ be the discriminant of this equation and c_4 be the usual expression involving $a_1, a_2, \ldots, a_6$. We quote Proposition 7.5.1 from [13]. Then we have

Proposition 2.3.2. *(a) E has good reduction if and only if $v(\Delta) = 0$, i.e., $\Delta \in \mathfrak{o}^\times$.*

(b) E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$. In this case $\tilde{E}_{ns}$ is the multiplicative group,

$$\tilde{E}_{ns}(\bar{\kappa}) \cong \bar{\kappa}^\times.$$

(c) E has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$. In this case $\tilde{E}_{ns}$ is the additive group,

$$\tilde{E}_{ns}(\bar{\kappa}) \cong \bar{\kappa}^+.$$

Proposition 2.3.2 explains the choice for the names of the reduction types.

Next consider a field extension F' of F. If E/F is an elliptic curve that has bad reduction, then one can ask is it possible for E to attain good reduction over F' or not. For an elliptic curve E/F we then have the following definitions. If there exists a finite extension F'/F such that E/F' has good reduction, then we say that E/F has *potential good* reduction. Similarly, if there exists a finite extension F'/F such that E/F' has multiplicative reduction, then we say that E/F has *potential multiplicative* reduction. The following facts about the reduction type behavior under field extensions are known.

- If F'/F is an unramified extension, then E/F and E/F' have the same reduction type.

- If E has either good or multiplicative reduction over F and F'/F is a finite extension, then E/F' has the same reduction type as E/F.

- There exists a finite extension F'/F such that E has either good or (split) multiplicative reduction over F'.

The next theorem provides an easy characterization of when an elliptic curve has potential good reduction. This characterization only involves the coefficients of the Weierstrass equation of E. We quote Proposition $VII.5.5$ of [13].

Theorem 2.3.3. *Let E/F be an elliptic curve. Then E has potential good reduction if and only if $j(E)$ is integral, where $j(E)$ is the j-invariant of E.*

We now let F^{unr} be the maximal unramified extension of F and I be the inertia subgroup of $\mathrm{Gal}(\bar{F}/F)$, i.e, $I = \mathrm{Gal}(\bar{F}/F^{unr})$. We say that a set Σ is *unramified* if the inertia subgroup I acts trivially on Σ. Consider an integer $m \geq 1$ such that $v(m) = 0$ and let Σ be the torsion subgroup $E[m]$. Then one can show that $E[m]$ is unramified if E/F has good reduction. Further, the Tate module $T_\ell(E)$ is unramified, since it is the inverse limit of $E[\ell^n]$. The converse is also true, namely, if $E[m]$ is unramified, then E/F has good reduction. This fact is known as the criterion of Néron-Ogg-Shafarevich. More precisely,

Theorem 2.3.4. *(Criterion of Néron-Ogg-Shafarevich). Let E/F be an elliptic curve. Then the following are equivalent:*

(a) E has good reduction at F.

(b) The Tate module $T_\ell(E)$ is unramified for some (all) prime(s) ℓ satisfying $\ell \neq \mathrm{char}(\kappa)$.

(c) $E[m]$ is unramified for infinitely many $m \geq 1$ that are relatively prime to $\mathrm{char}(\kappa)$.

An immediate consequence of the Néron-Ogg-Shafarevich criterion is that E has potential good reduction if and only if for some (all) prime(s) ℓ satisfying $\ell \neq \mathrm{char}(\kappa)$ the inertia subgroup acts through a finite quotient on the Tate module $T_\ell(E)$.

Recall that the condition $v(m) = 0$ implies that m is relatively prime to $\mathrm{char}(\kappa)$. For more details on this subject, we refer the reader to Section 7.7 of [13].

Finally, we make an important definition that measures the bad reduction. Namely, the *(exponent of the) conductor* of E/F is

$$a(E) = \begin{cases} 0 & \text{if } E \text{ has good reduction} \\ 1 & \text{if } E \text{ has multiplicative reduction} \\ 2+\delta & \text{if } E \text{ has additive reduction,} \end{cases} \tag{2.3.3}$$

where δ is a quantity that describes the "wild ramification" in the inertia subgroup's action on the Tate module $T_\ell(E)$.

Remark 2.3.5. *It is a well known fact $\delta = 0$ if the residual characteristic $p = \mathrm{char}(\kappa)$ is not 2 or 3. Thus, for $p \geq 5$, the conductor $a(E) = 2$ if E has additive reduction.*

For further details about the conductor, we refer the reader to Appendices C.15 and C.16 of [13].

2.4 The Weil-Deligne group

In this section we consider F to be a non-archimedean local field. Let $\kappa = \mathfrak{o} \,/\, \mathfrak{p}$ be its residue class field with characteristic $\mathrm{char}(\kappa) = p$ and cardinality q. Let $\bar{\kappa}$ denote an algebraic closure of κ. As above, let $I = \mathrm{Gal}(\bar{F}/F^{unr}) \leqslant \mathrm{Gal}(\bar{F}/F)$

be the inertia subgroup of $\mathrm{Gal}(\bar{F}/F)$ where $\bar{F}$ is a separable algebraic closure of F and F^{unr} is the maximal unramified extension of F contained in $\bar{F}$.

Let Frob : $\bar{\kappa} \longrightarrow \bar{\kappa}$ be the Frobenius automorphism. Consider a positive integer n and let k_n be the unique subfield of $\bar{\kappa}$ of degree n over κ. The inverse of the Frobenius automorphism ϕ is defined such that $\phi(x) = x^{q^n}$ for all $x \in k_n$.

The following material can be found in [9].

Definition 2.4.1. *(The Weil Group). The Weil group $\mathcal{W}(\bar{\kappa}/\kappa)$ of κ is the infinite cyclic group generated by ϕ. The group $\mathcal{W}(\bar{\kappa}/\kappa)$ is a topological group via the discrete topology.*

It is known that for a local field F the absolute Galois group decomposes as

$$1 \longrightarrow I \longrightarrow \mathrm{Gal}(\bar{F}/F) \xrightarrow{\pi} \mathrm{Gal}(\bar{\kappa}/\kappa) \longrightarrow 1,$$

where π is the decomposition map. Using this exact sequence, one can define the Weil group of F as follows

Definition 2.4.2. *The Weil group $\mathcal{W}(\bar{F}/F)$ of F is the inverse image of $\mathcal{W}(\bar{\kappa}/\kappa)$ under π, i.e., $\mathcal{W}(\bar{F}/F) = \pi^{-1}(\mathcal{W}(\bar{\kappa}/\kappa)$.*

By this definition, the following exact sequence is produced

$$1 \longrightarrow I \longrightarrow \mathcal{W}(\bar{F}/F) \longrightarrow \mathcal{W}(\bar{\kappa}/\kappa) \longrightarrow 1.$$

Moreover, for any element $\Phi \in \mathrm{Gal}(\bar{F}/F)$ such that $\pi(\Phi) = \phi$ we have

$$\mathcal{W}(\bar{F}/F) = \bigsqcup_{n\in\mathbb{Z}} \Phi^n I.$$

Note that Φ is called an *inverse* Frobenius element of $\mathrm{Gal}(\bar{F}/F)$ and it is only

unique up to multiplication by an element of I.

Representations of the Weil and Weil-Deligne group play an important rule in the theory of elliptic curves. More precisely, for an ℓ-adic representation of an elliptic curve E/F we can associate a complex representation of the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$ defined below.

Let V be a finite-dimensional complex vector space. Then

Definition 2.4.3. *(Representations of the Weil group). Every continuous homomorphism $\sigma : \mathcal{W}(\bar{F}/F) \longrightarrow \mathrm{GL}(V)$ defines a representation of the Weil group.*

The representation σ is called *unramified* if $\sigma|_I$ is trivial and it is called *ramified* otherwise. If V is one-dimensional then we call σ a character.

It is known that characters of both $\mathcal{W}(\bar{F}/F)$ and $F^\times$ are identified by composing with the Artin isomorphism $F^\times \cong \mathcal{W}(\bar{F}/F)^{ab}$ with $\mathcal{W}(\bar{F}/F)^{ab}$ being $\mathcal{W}(\bar{F}/F)$ modulo the closure of its commutator subgroup. This identification sends a uniformizer of F to an *inverse* Frobenius element Φ of $\mathcal{W}(\bar{F}/F)$ and the units $\mathfrak{o}^\times$ in F to the inertia subgroup I.

Note that a homomorphism $\sigma : \mathcal{W}(\bar{F}/F) \longrightarrow \mathrm{GL}(V)$ is a representation if and only if it is trivial on an open subgroup of I. This important fact is true because of real or complex Lie groups' property involving an open neighborhood of the identity element in $\mathrm{GL}(V)$.

Next we give an easy example of a Weil group representation.

Example 2.4.4. *The homomorphism*

$$\omega : \mathcal{W}(\bar{F}/F) \longrightarrow \mathbb{C}^\times$$

defined by $\omega(I) = 1$ and $\omega(\Phi) = q^{-1}$ is an unramified representation of $\mathcal{W}(\bar{F}/F)$.

The Weil group $\mathcal{W}(\bar{F}/F)$ is not large enough to correspond to all the ℓ-representations of elliptic curves. Namely, in the potential multiplicative reduction case, the Tate module of an elliptic curve E/F has an ℓ-adic representation of $\mathrm{Gal}(\bar{F}/F)$ which is *not* trivial on an open subgroup of I; as a result it cannot correspond to a complex representation of $\mathcal{W}(\bar{F}/F)$ since being trivial on open subgroup of I is a necessary and sufficient condition to have a Weil group representation. Thus we need to define the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$.

Definition 2.4.5. *(The Weil-Deligne group). The Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$ is the semi-direct product*

$$\mathcal{W}'(\bar{F}/F) = \mathcal{W}(\bar{F}/F) \ltimes \mathbb{C},$$

defined via the action

$$gzg^{-1} = \omega(g)z \quad \text{for all } g \in \mathcal{W}(\bar{F}/F),\ z \in \mathbb{C}. \tag{2.4.1}$$

In other words, $(g_1,\, z_1) \cdot (g_2,\, z_2) \mapsto (g_1 g_2,\, z_1 + \omega(g_1) z_2)$ for all $g_1,\, g_2 \in \mathcal{W}(\bar{F}/F)$ and $z_1,\, z_2 \in \mathbb{C}$. Here ω is being as in Example 2.4.4. As a set, the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$ is a cartesian product so we make it into a topological group via the product topology.

Definition 2.4.6. *(Representations of the Weil-Deligne group). Let V be a finite-dimensional complex vector space. A representation of $\mathcal{W}'(\bar{F}/F)$ is a continuous homomorphism*

$$\sigma' : \mathcal{W}'(\bar{F}/F) \longrightarrow \mathrm{GL}(V)$$

such that the restriction $\sigma'|_{\mathbb{C}}$ is complex analytic, i.e., $z \mapsto [f_{ij}(z)]_{n\times n}$ with $f_{ij}(z)$

being holomorphic in the usual sense.

Let σ be a representation of $\mathcal{W}(\bar{F}/F)$ on V and $N : V \longrightarrow V$ be a nilpotent endomorphism, that is $N^r = 0$ for some $r \in \mathbb{Z}$. Then the representation σ' can be realized as the pair (σ, N) provided that

$$\sigma(g)N\sigma(g)^{-1} = \omega(g)N \qquad \text{for all } g \in \mathcal{W}(\bar{F}/F). \tag{2.4.2}$$

This important fact is achieved using the following procedure. First, given the pair (σ, N) we define the representation σ' on the Weil-Deligne group by

$$\sigma'(g, \omega(g)z) = \sigma'(gz) = \sigma(g)\exp(zN), \tag{2.4.3}$$

for all $g \in \mathcal{W}(\bar{F}/F)$ and $z \in \mathbb{C}$ where

$$\exp(N) = \sum_{r \geq 0} \frac{N^r}{r!}.$$

On the other hand, assume that a representation σ' of $\mathcal{W}'(\bar{F}/F)$ is given. Then the restriction $\sigma'|_{\mathcal{W}(\bar{F}/F)}$ defines a representation σ of the Weil group and the formula

$$N = \frac{\log(\sigma'(z))}{z}, \qquad \text{for an arbitrary } z \in \mathbb{C} \tag{2.4.4}$$

gives a nilpotent map. Thus we have a pair (σ, N).

Any representation σ of the Weil group can be thought of as a representation of $\mathcal{W}'(\bar{F}/F)$ by considering a zero nilpotent map; in other words we write $\sigma' = (\sigma, 0)$.

Moreover, if σ is an unramified representation of $\mathcal{W}(\bar{F}/F)$ and N is zero,

then we call the representation σ' *unramified*. Otherwise, we call it *ramified*.

Let L be a finite extension of F. Let V and W be two complex vector spaces. Let $\sigma' = (\sigma, N)$ be a representation of $\mathcal{W}'(\bar{F}/F)$ on V and $\tau' = (\tau, P)$ a representation on W. Let $\mathcal{W}'(\bar{F}/L)$ be a finite index subgroup of $\mathcal{W}'(\bar{F}/F)$. Let $\rho' = (\rho, M)$ be a representation of $\mathcal{W}'(\bar{F}/L)$ on a vector space U. Then the following facts hold.

- The direct sum of the representations σ' and τ' carries over their pairs. More precisely, $\sigma' \oplus \tau' = (\sigma \oplus \tau, N \oplus P)$.

- Similarly, the tensor product carries over. In other words, $\sigma' \otimes \tau' = (\sigma \otimes \tau, N \otimes 1 + 1 \otimes P)$ with 1 being the identity automorphism of V or W as needed.

- Let V^* be the dual space of V and σ'^* denote the contragredient representation on V^*. Then σ'^* corresponds to the pair (σ^*, N^*) and satisfies

$$(\sigma^*(g)f)(v) = f(\sigma(g^{-1})v) \qquad \text{and} (N^* f)(v) = -f(Nv)$$

  for all $g \in \mathcal{W}(\bar{F}/F)$, $f \in V^*$, and $v \in V$.

- Let $\mathrm{res}_{L/F}$ and $\mathrm{ind}_{L/F}$ be the restriction and induction representations from either $\mathcal{W}'(\bar{F}/L)$ into $\mathcal{W}'(\bar{F}/F)$ or from $\mathcal{W}(\bar{F}/L)$ into $\mathcal{W}(\bar{F}/F)$ as appropriate. Then

$$\mathrm{res}_{L/F}\sigma' = (\mathrm{res}_{L/F}\sigma, N)$$

  and

$$\mathrm{ind}_{L/F}\rho' = (\mathrm{ind}_{L/F}\rho, M_{L/F}),$$

where $M_{L/F}$ is defined via

$$M_{L/F}(g \otimes u) = \omega(g)^{-1}(g \otimes Mu)$$

for all $g \in \mathcal{W}(\bar{F}/F)$ and $u \in U$.

Let ℓ denote a prime different from p and V_ℓ be a finite-dimensional vector space over $\mathbb{Q}_\ell$. We repeat the following definition.

Definition 2.4.7. *(ℓ-adic representation of Galois group). A continuous homomorphism $\sigma'_\ell : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{GL}(V_\ell)$ is called an ℓ-adic representation of* $\mathrm{Gal}(\bar{F}/F)$.

An example of this representation is the one defined in Equation (2.2.1).

The proposition below describes a procedure that associates a complex representation $\sigma'_{\ell,\iota}$ of $\mathcal{W}'(\bar{F}/F)$ to an ℓ-adic representation σ'_ℓ of $\mathrm{Gal}(\bar{F}/F)$.

Let $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ be a field embedding and $t_\ell : I \to \mathbb{Q}_\ell$ be a homomorphism.

Proposition 2.4.8. *(ℓ-adic representation of $\mathcal{W}'(\bar{F}/F)$). Let $\sigma'_\ell : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{GL}(V_\ell)$ be an ℓ-adic representation of* $\mathrm{Gal}(\bar{F}/F)$.

(a) There is a unique nilpotent endomorphism N_ℓ of V_ℓ such that

$$\sigma'_\ell(i) = \exp(t_\ell(i)N_\ell)$$

where i is an element in some open subgroup of I. Furthermore, the homomorphism t_ℓ and the representation σ'_ℓ satisfy the formulas

$$t_\ell(gig^{-1}) = \omega(g)t_\ell(i)$$

and

$$\sigma'_\ell(g)N_\ell\sigma'_\ell(g)^{-1} = \omega(g)N_\ell$$

for all $g \in \mathcal{W}(\bar{F}/F)$ *and* $i \in I$. *Furthermore,* N_ℓ *is a zero nilpotent map if and only if* σ'_ℓ *is trivial on an open subgroup of* I.

(b) The function $\sigma_\ell : \mathcal{W}(\bar{F}/F) \longrightarrow \mathrm{GL}(V_\ell)$ *defined by*

$$\sigma_\ell(g) = \sigma'_\ell(g)\exp(-t_\ell(i)N_\ell)$$

for all $g \in \mathcal{W}(\bar{F}/F)$ *is a continuous group homomorphism. Moreover, it satisfies the equation* $\sigma_\ell(g)N_\ell\sigma_\ell(g)^{-1} = \omega(g)N_\ell$ *for all* $g \in \mathcal{W}(\bar{F}/F)$.

(c) The isomorphism class of the representation

$$\sigma'_{\ell,\iota} = (\sigma_{\ell,\iota}, N_{\ell,\iota})$$

is independent of the choice of t_ℓ *and the inverse Frobenius element* Φ.

Proof. We refer the reader to Section 4 of [9]. □

Let n be a positive integer. We give an example of a Weil-Deligne representation.

Example 2.4.9. *Let* $e_0, e_1, \ldots, e_{n-1}$ *be the standard basis of* $\mathbb{C}^n$. *Let* σ *be a continuous homomorphism of* $\mathcal{W}(\bar{F}/F)$ *and* N *a nilpotent map of* V. *Then the formulas*

$$\sigma(g)e_j = \omega(g)^j e_j \qquad \text{for all } g \in \mathcal{W}(\bar{F}/F);\ 0 \le j \le n-1,$$

$$Ne_j = e_{j+1} \qquad \text{for } 0 \le j \le n-2$$

and

$$Ne_{n-1} = 0$$

define a representation σ' *of* $\mathcal{W}'(\bar{F}/F)$.

This representation is called the *special* representation of dimension n and denoted by $\mathrm{sp}(n)$. It is not irreducible, but indecomposable.

An *admissible* representation of $\mathcal{W}'(\bar{F}/F)$ is a representation $\sigma' = (\sigma, N)$ with semisimple σ-part.

Let ψ be an irreducible representation of $\mathcal{W}(\bar{F}/F)$ and n a positive integer. In Section 3 of [2], it is shown that every admissible indecomposable representation σ' of $\mathcal{W}'(\bar{F}/F)$ is isomorphic to $\psi \otimes \mathrm{sp}(n)$. Here, *indecomposable* means that σ' cannot be written as a direct sum of invariant proper subspaces.

2.5 The non-archimedean local Langlands correspondence for $\mathrm{GL}(2, F)$

The content of this section is adapted from [1]. We are going to develop the tools to discuss representations of the Weil-Deligne group in the context of the local Langlands correspondence (LLC).

2.5.1 Basic representation theory

Let F be a finite field extension of the p-adic number field or a field of formal power series in one variable over a finite field. Let $\mathfrak{o}$ be the ring of integers of F, $\mathfrak{p}$ the unique maximal ideal of $\mathfrak{o}$, and ϖ a generator of $\mathfrak{p}$. Let q be the cardinality of the residue field $\mathfrak{o}/\mathfrak{p}$ and υ be the valuation on F.

Let G be a totally disconnected locally compact group with a (possibly infinite-dimensional) complex representation (π, V). Let v be any element of V. If the stabilizer $\{g \in \mathrm{G} : \pi(\mathrm{g})\mathrm{v} = \mathrm{v}\}$ of v is open, then the representation π is called *smooth*.

Let $U \subset \mathrm{G}$ be an open subgroup of G. Let $V^U = \{\mathrm{v} \in V : \pi(u)\mathrm{v} = \mathrm{v}\text{for all } u \in U\}$ be the space of vectors stabilized by U, then

Definition 2.5.1. *A smooth representation π is called admissible if V^U is finite-dimensional.*

Let (π, V) be a smooth representation of G. Let $\check{\mathrm{v}} : V \longrightarrow \mathbb{C}$ be a smooth linear functional. We denote $\check{\mathrm{v}}(\mathrm{v})$ by $\langle \mathrm{v}, \check{\mathrm{v}} \rangle$. Here smooth means that for all $\mathrm{v} \in V$ we have $\langle \pi(g)\mathrm{v}, \check{\mathrm{v}} \rangle = \langle \mathrm{v}, \check{\mathrm{v}} \rangle$ where g is an element of an open neighborhood U of the identity in G. Let $\check{V}$ be the space of all smooth linear functionals on V. We define the dual representation of V as follows

Definition 2.5.2. *Let (π, V) be a smooth representation of* G*. For any $g \in \mathrm{G}$ the action*

$$\langle \mathrm{v}, \check{\pi}(g)\check{\mathrm{v}} \rangle = \langle \pi(g^{-1})\mathrm{v}, \check{\mathrm{v}} \rangle$$

on $\check{V}$ defines the contragredient representation $(\check{\pi}, \check{V})$ of G*.*

Then the following facts are true.

- The representation $(\check{\pi}, \check{V})$ is a smooth representation of G.
- The representation π of $\mathrm{GL}(2, F)$ is irreducible if and only if its dual $\check{\pi}$ is irreducible.
- If π is an admissible representation, then $\check{\pi}$ is also admissible and $\check{\check{\pi}} \cong \pi$.

Let (π_1, V_1) and (π_2, V_2) be two representations of a group G. The linear map $T : V_1 \longrightarrow V_2$ satisfying $T \circ \pi_1(g) = \pi_2(g) \circ T$ for all $g \in \mathrm{G}$ is called the *intertwining map*. Thus

Proposition 2.5.3. *(Schur's Lemma) Let (π, V) be an irreducible admissible representation of a totally disconnected locally compact group* G*. Let $T : V \longrightarrow V$*

be an intertwining operator for π. *Then there exists a complex number* c *such that* $T(\mathrm{v}) = c\mathrm{v}$ *for all* $\mathrm{v} \in V$.

An immediate consequence of Schur's Lemma is that the center Z of G acts by scalars on the irreducible admissible representation (π, V). Thus if $\mathrm{G} = \mathrm{GL}(2, \mathrm{F})$, where F is a non-archimedean local field, there exists a character ω of $F^\times$ which is called the *central character*, such that the center $Z(F)$ of $\mathrm{GL}(2, F)$ acts by:

$$\pi(\begin{bmatrix} z & \\ & z \end{bmatrix} \mathrm{v}) = \omega(z)\mathrm{v}.$$

Thus new representations of $\mathrm{GL}(2, F)$ can be defined using the central character ω. Namely, we have

Theorem 2.5.4 ([1], Thm. 4.2.2)**.** *Let* (π, V) *be an irreducible admissible representation of* $\mathrm{GL}(2, F)$.

a) Define a representation (π_1, V) *on the same space by* $\pi_1(g) = \pi({}^t g^{-1})$. *Then* $\check{\pi} \cong \pi_1$.

b) Let ω *be the central character of* π. *Define another representation* (π_2, V) *on the same space by* $\pi_2(g) = \omega(\det(g))^{-1}\pi(g)$. *Then* $\check{\pi} \cong \pi_2$.

2.5.2 Classification of admissible representations

Our purpose in this section is to describe the classification of all irreducible admissible representations of $\mathrm{GL}(2, F)$ where F is a non-archimedean local field. The main classification result is that every irreducible admissible representation π of $\mathrm{GL}(2, F)$ is a subrepresentation of some principal series representation unless π is a supercuspidal representation.

Another consequence of Schur's Lemma is that every finite-dimensional irreducible admissible representation of $\mathrm{GL}(2, F)$ is 1-dimensional and of the

form $\chi(\det(g))$ where χ is a character of $F^\times$. For more details we refer the reader to [[4], Remark 4.15].

Now, let G be a totally disconnected locally compact group. Let H be a closed subgroup of G and (π, V) be a smooth representation of H. Let V^{G} be the space of all functions $f : \mathrm{G} \longrightarrow \mathrm{V}$ satisfying the following properties:

a)
$$f(hg) = \delta_{\mathrm{G}}(h)^{-1/2}\delta_H(h)^{1/2}\pi(h)f(g)$$
for $h \in H$, $g \in \mathrm{G}$, where δ_{G} and δ_H are the modular characters of G and H, and

b) There exists an open subgroup K_0 of G such that $f(gk) = f(g)$ for all $g \in \mathrm{G}$ when $k \in K_0$.

Then the right translation $(\pi^{\mathrm{G}}(g)f)(x) = f(xg)$ by an element $g \in \mathrm{G}$ defines a smooth representation $\pi^{\mathrm{G}} : \mathrm{G} \longrightarrow \mathrm{End}(\mathrm{V}^{\mathrm{G}})$ on V^{G}. We call the representation $(\pi^{\mathrm{G}}, V^{\mathrm{G}})$ the *induced representation* of G and denote it by $\mathrm{Ind}_H^{\mathrm{G}}(\pi)$. Note that multiplying by the factor $\delta_H^{1/2}$ simplifies many formulas.

To describe the principal series representations of $\mathrm{GL}(2, F)$, let $B(F)$ be the Borel subgroup consisting of upper triangular matrices. If χ_1, χ_2 are two characters of $F^\times$, then we define a character χ of $B(F)$ by

$$\chi(\begin{bmatrix} y_1 & * \\ & y_2 \end{bmatrix}) = \chi_1(y_1)\chi_2(y_2).$$

Inducing this character to $\mathrm{GL}(2, F)$, we get a smooth representation

$$\chi_1 \times \chi_2 = \mathrm{Ind}_{B(F)}^{\mathrm{GL}(2,F)}(\chi).$$

The following facts are well known; see [1] for more details.

- The contragredient of $\chi_1 \times \chi_2$ is $\chi_1^{-1} \times \chi_2^{-1}$ for any two characters χ_1, χ_2 of $F^\times$.

- $\chi_1 \times \chi_2$ is irreducible except when

  (i) $\chi_1\chi_2^{-1}(y) = |y|^{-1}$. In this case $\chi_1 \times \chi_2$ contains a one-dimensional invariant subspace so that the quotient representation is irreducible.

  (ii) $\chi_1\chi_2^{-1}(y) = |y|$. In this case $\chi_1 \times \chi_2$ contains an irreducibly invariant subspace of codimension one.

- If $\chi_1 \times \chi_2 \to \mu_1 \times \mu_2$ is a non-zero intertwining map, then either $\chi_1 = \mu_1$ and $\chi_2 = \mu_2$ or $\chi_1 = \mu_2$ and $\chi_2 = \mu_1$.

- If $\chi_1 \times \chi_2$ is irreducible, then $\chi_1 \times \chi_2 \cong \chi_2 \times \chi_1$.

Let χ_1, χ_2 be two characters of $F^\times$. Then

Definition 2.5.5. *The irreducible representation $\chi_1 \times \chi_2$ is called the principal series representation.*

Definition 2.5.6. *If $\chi_1 \times \chi_2$ is reducible, then it has an infinite dimensional composition factor which is a subrepresentation or a quotient depending whether $\chi_1\chi_2^{-1}(y) = |y|$ or $|y|^{-1}$. This infinite dimensional factor is called a Steinberg representation and is denoted by $\mathrm{St}_{\mathrm{GL}(2)}$.*

By definition the Steinberg representation fits into one of the following exact sequences:

$$0 \longrightarrow \mathrm{St}_{\mathrm{GL}(2)} \longrightarrow |.|^{1/2} \times |.|^{-1/2} \longrightarrow 1_{\mathrm{GL}(2)} \longrightarrow 0,$$

or

$$0 \longrightarrow 1_{\mathrm{GL}(2)} \longrightarrow |.|^{-1/2} \times |.|^{1/2} \longrightarrow \mathrm{St}_{\mathrm{GL}(2)} \longrightarrow 0.$$

Now we give the definition of the supercuspidal representation of $\mathrm{GL}(2, F)$.

Definition 2.5.7. *Let* $N = \{\begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} : u \in F\}$ *and* (π, V) *be an irreducible admissible representation of* $\mathrm{GL}(2, F)$*. Let* $V(N)$ *denote the subspace of* V *spanned by the vectors* $\mathrm{v} - \pi(x)\mathrm{v}$ *for* $\mathrm{v} \in V$ *and* $x \in N$*. Then* (π, V) *is called supercuspidal if* $V_N = V/V(N) = \{0\}$*.*

The next theorem is a well known fact and characterizes the irreducible, admissible representations of $\mathrm{GL}(2, F)$.

Theorem 2.5.8 ([4], Thm. 4.21)**.** *Suppose* (π, V) *is an irreducible admissible representation of* $\mathrm{GL}(2, F)$*. Then if* π *is not supercuspidal it is a subrepresentation of some* $\chi_1 \times \chi_2$*, i.e., it is equivalent to some principal series or Steinberg representation. On the other hand, if* π *is supercuspidal, it is not equivalent to a subquotient of any* $\chi_1 \times \chi_2$*.*

As a summary we have three types of the irreducible, admissible representations of $\mathrm{GL}(2, F)$. These are

- The principal series representation.
- The Steinberg representation.
- The supercuspidal representation.

There is some data associated to each type of the representations above. Here we only introduce the definition of a conductor in Theorem 2.5.9 and Remark 2.5.10. The conductor plays an important role in finding the representation π of $\mathrm{GL}(2, F)$ associated to an elliptic curve E/F.

Theorem 2.5.9 ([4], Thm. 4.24)**.** *Let* (π, V) *denote any irreducible admissible representation of* $\mathrm{GL}(2, F)$*. Then there is a largest ideal* $a(\pi)$ *of* $\mathfrak{o}$ *such that the*

space of vectors v *with*

$$\pi(\begin{bmatrix} a & b \\ c & d \end{bmatrix})\mathrm{v} = \mathrm{v},$$

for all

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in K^{a(\pi)} := \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in K : c \equiv 0,\, d \equiv 1\,(mod\, c(\pi))\}$$

is not empty. Furthermore, this space has dimension one.

Remark 2.5.10 ([4], Rk. 4.25)**.** *We call* $a(\pi)$ *the conductor of* π *and the following holds:*

Representation π	Conductor $a(\pi)$
$\chi_1 \times \chi_2$	$a(\chi_1)a(\chi_2)$
$\chi\mathrm{St}$	$a(\chi)^2$, if χ is unramified $(\mathfrak{p})$, if χ is unramified
$\chi 1_{\mathrm{GL}(2,F)}$	$a(\chi)^2$
π is supercuspidal	$(\mathfrak{p}^n),\ n \geq 2$

Recall that the conductor of any character χ of $F^\times$ is the largest ideal $\mathfrak{p}^n$ such that χ is trivial on the subgroup $1 + \mathfrak{p}^n$.

A central result of the class field theory is the identification of the characters of the multiplicative group of a local non-archimedean field F with the characters of the Weil group $\mathcal{W}(\bar{F}, F)$. Langlands conjectured a generalization of this one-dimensional theory: a correspondence between irreducible admissible representations of $\mathrm{GL}(n, F)$ and admissible n-dimensional representations of the Weil-Deligne group $\mathcal{W}'(\bar{F}, F)$. The Langlands correspondence is the unique bijection that preserves certain natural invariants on both sides; in particular, it preserves the conductors. For $n = 2$, the case of our interest, the proof of the

conjecture was completed by Kutzko in [6]. Thus

$$\left\{\begin{matrix}\text{irreducible admissible rep-}\\ \text{resentations of } \mathrm{GL}(2,F)\end{matrix}\right\} \Longleftrightarrow \left\{\begin{matrix}\text{admissible 2-dimensional}\\ \text{representations of } \mathcal{W}'(\bar{F},F)\end{matrix}\right\} \quad (2.5.1)$$

Given in the table below is an explicit recipe for the above correspondence:

π	σ	N
$\chi_1 \times \chi_2$	$\chi_1 \oplus \chi_2$	0
$\chi\mathrm{St}_{\mathrm{GL}(2)}$	$\chi\lvert.\rvert^{1/2} \oplus \chi\lvert.\rvert^{-1/2}$	$\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$
$\chi 1_{\mathrm{GL}(2)}$	$\chi\lvert.\rvert^{1/2} \oplus \chi\lvert.\rvert^{-1/2}$	0
supercuspidal	irreducible	0

(2.5.2)

In this table, π is an irreducible admissible representation of $\mathrm{GL}(2,F)$, χ, χ_1, χ_2 and $|.|^{1/2}$ are characters of $F^\times$, and the pair (σ, N) is a complex representation of the Weil-Deligne group with N being the nilpotent part.

Most supercuspidal representations can be constructed as follows. Let K/F be a quadratic extension. Let $\xi : K^\times \to \mathbb{C}^\times$ be a non-Galois invariant character, then there is an irreducible, admissible representation $\omega_{K,\xi}$ of $\mathrm{GL}(2,F)$ constructed via the Weil representation; see §1 of [5]. We refer to $\omega_{K,\xi}$ as the *dihedral representation*. If the residual characteristic of F is odd, then all supercuspidal representations are of the form $\omega_{K,\xi}$ for certain K and ξ.

The local parameter corresponding to $\omega_{K,\xi}$ via (LLC) is the two-dimensional representation of $\mathcal{W}(\bar{F}/F)$ given by $\mathrm{ind}_{K/F}(\xi)$. By §10 of [9], we have the conductor formula

$$a(\mathrm{ind}_{K/F}(\xi)) = d(K/F) + f(K/F)a(\xi). \quad (2.5.3)$$

Here, $d(K/F)$ is the valuation of the discriminant of K/F and $f(K/F)$ is the residue class degree. Note that $a(\mathrm{ind}_{K/F}(\xi))$ is also the conductor of $\omega_{K,\xi}$; this is a feature of the LLC.

The number $f(K/F)$ is 1 or 2, depending on whether K/F is ramified or unramified. In odd residual characteristic, the number $d(K/F)$ is 0 or 1, again depending on whether K/F is ramified or unramified. Hence,

$$a(\mathrm{ind}_{K/F}(\xi)) = \begin{cases} 2a(\xi) & \text{if } K/F \text{ is unramified,} \\ 1 + a(\xi) & \text{if } K/F \text{ is ramified} \end{cases} \tag{2.5.4}$$

in the odd residual characteristic case. Moreover, the central character ψ of $\pi = \omega_{K,\xi}$ is given by

$$\psi = \xi|_{F^\times}\chi_{K/F}. \tag{2.5.5}$$

Here $\chi_{K/F}$ is the quadratic character of $K^\times$ corresponding to K/F.

Chapter 3

The Potential Multiplicative Case

In this chapter we study elliptic curves over local fields with potential multiplicative reduction. Recall from Theorem 2.3.3 that an elliptic curve E defined over a field F has potential multiplicative reduction if and only if its j-invariant is not integral. In the first section, we will discuss the Tate curve and define the γ-invariant of an elliptic curve.

Let F be a local field with characteristic zero. Let υ be the normalized valuation.

3.1 The Tate curve and the γ-invariant

The material of this section and further details can be found in Chapter V of [14]. Let k be a positive integer and $q \in F^{\times}$ be such that $\upsilon(q) > 0$. Define the quantities

$$s_k(q) = \sum_{n \geq 1} \frac{n^k q^n}{1 - q^n}, \quad a_4(q) = -5s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7s_3(q)}{12}.$$

Tate proved that these quantities converge and used them to define an elliptic curve E_q. Explicitly, for a local field F with characteristic zero Tate showed the following important facts

- The series $a_4(q)$ and $a_6(q)$ converge in F.

- The Tate curve

$$E_q : y^2 + a_1xy + a_3y = x^3a_2x^2 + a_4(q)x + a_6(q)$$

is an elliptic curve defined over F with discriminant

$$\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$$

and j-invariant

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n,$$

with $c(n) \in \mathbb{Z}$.

Let E/F be an elliptic curve defined over F, and choose a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for E/F. Let c_4 and c_6 be the usual quantities associated to this equation. In the next lemma, we define the γ-invariant. This invariant will play an important role in finding the irreducible, admissible representation of $\mathrm{GL}(2, F)$ attached to an elliptic curve E/F with potential multiplicative reduction.

Lemma 3.1.1. *Assuming that the j-invariant $j(E) \neq 0, 1728$, we define*

$$\gamma(E/F) = \frac{-c_4}{c_6} \in F^\times/F^{\times 2}.$$

Then,

(a) $\gamma(E/F)$ is well defined and independent of the choice of a Weierstrass

equation for E/F.

(b) Let E'/F be another elliptic curve with $j(E') \neq 0, 1728$. Then E and E' are isomorphic over F if and only if

$$j(E) = j(E') \qquad \text{and} \qquad \gamma(E/F) = \gamma(E'/F).$$

(c) Let E/F and E'/F be two elliptic curves having the same j-invariant which is not 0 or 1728. Further, suppose that $\gamma(E/F) \neq \gamma(E'/F)$, then

$$L = F(\sqrt{\frac{\gamma(E/F)}{\gamma(E'/F)}})$$

is a quadratic extension of F. Moreover, there is an isomorphism

$$\psi : E \to E'$$

such that

$$\psi(P^\sigma) = \chi(\sigma)\psi(P)^\sigma \quad \text{for all} \quad \sigma \in \mathrm{Gal}(\bar{F}/F) \quad \text{and all} \quad P \in E(\bar{F}),$$

where

$$\chi : \mathrm{Gal}(\bar{F}/F) \to \mathrm{Gal}(L/F) \to \{\pm 1\}$$

is the quadratic character associated to L/F.

After defining the γ-invariant of an elliptic curve, we present Tate's uniformization theorem. Among other things, it states that split multiplicative reduction occurs when $\gamma(E/F)$ is a square in $F^\times$.

Theorem 3.1.2. *(Tate) Let F be a non-archimedean local field and E/F be*

an elliptic curve defined over F with potential multiplicative reduction. Let $\gamma(E/F) \in F^\times/F^{\times 2}$ be the invariant defined in Lemma 3.1.1. Then

(a) There is a unique $q \in F^\times$ with $\upsilon_F(q) > 0$ such that E is isomorphic over $\bar{F}$ to the Tate curve E_q.

(b) Let q be such that $\upsilon_F(q) > 0$. Then the following are equivalent:

1. E is isomorphic to E_q over F.

2. $\gamma(E/F) = 1$.

3. E has split multiplicative reduction.

Proof. See [[14], Theorem (V.5.3)]. □

3.2 Quadratic twisting

In this section we study the notion of an elliptic curve twisted by an element of $F^\times$. We will continue to let F be a local field with characteristic zero. Let E/F be an elliptic curve with Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.2.1}$$

It is well known that under a standard change of variables of the form $x = u^2x' + r$ and $y = u^3y' + u^2sx' + t$ with $u \in \mathfrak{o}^\times$ and r, s, $t \in \mathfrak{o}$, the quantities c_4 and c_6 attached to the Weierstrass equation behave as follows,

$$u^4c_4' = c_4, \qquad u^6c_6' = c_6. \tag{3.2.2}$$

Now, since F has characteristic zero, from the discussion in Section 2.1 the Weierstrass equation (3.2.1) can be rewritten in the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{3.2.3}$$

Let $d \in F^\times$. Then

Definition 3.2.1. *The curve E^d defined by the equation*

$$dy^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{3.2.4}$$

is called the quadratic twist of E by d.

Note that E and E^d are isomorphic over $F(\sqrt{d})$ via the map

$$\varphi : E \longrightarrow E^d, \qquad (x, y) \longmapsto (x, d^{-1/2}y), \tag{3.2.5}$$

and the isomorphism class of E^d depends only on the class of d in $F^\times/F^{\times 2}$.

If $j(E)$ is not equal to 0 or 1728, and E'/F is another elliptic curve with $j(E) = j(E')$, then E' is F-isomorphic to E^d for some $d \in F^\times/F^{\times 2}$. If $j(E) = 1728$, then the parameterizing set for curves with that j-invariant is $F^\times/F^{\times 4}$ and if $j(E) = 0$, then the parameterizing set is $F^\times/F^{\times 6}$. For more details on this, we refer the reader to [13], Proposition X.5.4 and its corollary.

To obtain a standard Weierstrass equation for E^d, we replace (x, y) by (xd^{-1}, yd^{-2}) in equation (3.2.4). Then the result is

$$y^2 = x^3 + a_2dx^2 + a_4d^2x + a_6d^3. \tag{3.2.6}$$

Comparing with (3.2.3), we notice that twisting has the effect of replacing a_i by

$a_i d^{i/2}$. A similar statement holds for the quantities b_i and c_i. In particular,

$$c_4(E^d) = d^2 c_4(E), \qquad c_6(E^d) = d^3 c_6(E). \tag{3.2.7}$$

Note that, since twisting does not change the j-invariant, the class of elliptic curves over F consisting of curves with potential multiplicative reduction (respectively potential good reduction) is invariant under twisting.

3.3 Potential multiplicative reduction and the γ-invariant

In this section we will investigate the behavior of the γ-invariant under the quadratic twist and will use it to find the reduction type of E/F.

Let E/F be an elliptic curve with Weierstrass equation (3.2.1). Then

$$c_4 = 0 \iff j(E) = 0 \quad \text{and} \quad c_6 = 0 \iff j(E) = 1728.$$

This follows from the relations

$$1728\Delta = c_4^3 - c_6^2, \quad j = \frac{c_4^3}{\Delta}.$$

Now assume that E/F has potential multiplicative reduction. Then $j(E) \notin \mathfrak{o}$ and hence the quantities c_4 and c_6 cannot be zero. Thus, we can define the γ-invariant as in Tate's uniformization theorem,

$$\gamma(E/F) = -\frac{c_4}{c_6} \in F^\times / F^{\times 2}. \tag{3.3.1}$$

From (3.2.7), we find its behavior under quadratic twisting:

$$\gamma(E^d/F) = d\gamma(E/F). \tag{3.3.2}$$

Next, we use $\gamma(E/F)$ to distinguish between the split and non-split cases when E has potential multiplicative reduction.

Proposition 3.3.1. *Let E/F be an elliptic curve with potential multiplicative reduction.*

a) E has split multiplicative reduction if and only if $\gamma(E/F) = 1$.

b) E has non-split multiplicative reduction if and only if $F(\sqrt{\gamma(E/F)})$ is the unramified quadratic extension of F.

c) If E has multiplicative reduction, then $\gamma(E/F) \in \mathfrak{o}^\times / \mathfrak{o}^{\times 2}$.

Proof. *a*) is part (b) of Theorem 3.1.2.
For *b*), we refer the reader to [[14], Problem V.5.11].
c) Follows from *a*) and *b*). Alternatively, assume that E has multiplicative reduction, and is given in a minimal Weierstrass equation. Then $\upsilon(\Delta) > 0$ and $\upsilon(c_4) = 0$ by Proposition 2.3.2. Since $1728\Delta = c_4^3 - c_6^2$, this implies $\upsilon(c_6) = 0$. Hence c_4 and c_6 are both units, so that $\gamma(E/F)$ is represented by units. □

Proposition 3.3.1 and equation (3.3.2) imply that split and non-split are interchangeable under twisting. Hence E acquires split multiplicative reduction over some finite extension of F if E has potential multiplicative reduction. This fact has been used in [[9], Section 15] to prove Theorem 3.4.2 below.

3.4 The representations of $\mathrm{GL}(2, F)$ attached to an elliptic curve E/F

Keeping the assumption that E/F has potential multiplicative reduction, we will explicitly find the representation of $\mathrm{GL}(2, F)$ attached to E via the coefficients of a given Weierstrass equation of E.

Let $d \in F^\times$ be a non-square. Then we start by stating a lemma that relates the ℓ-adic representation of $\mathrm{Gal}(\bar{F}/F)$ on the twist E^d in terms of the ℓ-adic representation of $\mathrm{Gal}(\bar{F}/F)$ on E.

Lemma 3.4.1. *Let χ be the isomorphism $\mathrm{Gal}(F(\sqrt{d})/F) \to \{\pm 1\}$. We also consider χ a homomorphism $\mathrm{Gal}(\bar{F}/F) \to \{\pm 1\}$ via the projection $\mathrm{Gal}(\bar{F}/F) \to \mathrm{Gal}(F(\sqrt{d})/F)$. Then*

a) The isomorphism φ in Equation (3.2.5) satisfies

$$\varphi(P^g) = \chi(g)\varphi(P)^g,$$

for all points P on E and all $g \in \mathrm{Gal}(\bar{F}/F)$.

b) Let ℓ be a prime, and let $T_\ell(E)$ and $T_\ell(E^d)$ be the Tate modules of E/F and E^d/F. Then φ induces a map $T_\ell(E) \to T_\ell(E^d)$, which we also denote by φ. This map satisfies

$$\varphi(\mathrm{v}^g) = \chi(g)\varphi(\mathrm{v})^g,$$

for all $\mathrm{v} \in T_\ell(E)$ and all $g \in \mathrm{Gal}(\bar{F}/F)$.

c) If $\sigma_{E,\ell} : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}(2, \mathbb{Z}_\ell)$ is the ℓ-adic representation of $\mathrm{Gal}(\bar{F}/F)$ on E with respect to a basis $\mathrm{v}_1, \mathrm{v}_2$ of $T_\ell(E)$, then the ℓ-adic representation of $\mathrm{Gal}(\bar{F}/F)$ on E^d is $\sigma_{E^d,\ell}$, where $\sigma_{E^d,\ell}(g) = \chi(g)\sigma_{E,\ell}(g)$ for all $g \in \mathrm{Gal}(\bar{F}/F)$.

Proof. *a*) This is part *c*) of Lemma 3.1.1 with E^d and d replacing E' and $\frac{\gamma(E/F)}{\gamma(E'/F)}$ respectively. Alternatively, we need to prove this only for $g \in \mathrm{Gal}(\bar{F}/F)$ whose

restriction to $F(\sqrt{d})$ is non-trivial. For such g and $P = (x, y)$, we have

$$\begin{aligned}\varphi(P)^g &= (x, d^{-1/2}y)^g \\ &= (x^g, \chi(g)d^{-1/2}y^g) \\ &= (x^g, -d^{-1/2}y^g) \\ &= -(x^g, d^{-1/2}y^g) \\ &= \chi(g)\varphi(P^g).\end{aligned}$$

b) Follows from *a*).

c) By observing that the actions of $\mathbb{Z}_\ell$ and of $\mathrm{Gal}(\bar{F}/F)$ on $T_\ell(E)$ commute, we can derive *c*) from *b*). □

Now suppose that E/F is an elliptic curve with potential multiplicative reduction. Using the previous lemma and Proposition 3.3.1 and following the discussion in Section 15 of [9], one can show

Proposition 3.4.2. *Let E/F be an elliptic curve with potential multiplicative reduction. Then the associated Weil-Deligne representation $\sigma' = (\sigma, N)$ is given by $\sigma' = \chi\omega^{-1} \otimes \mathrm{sp}(2)$, where $\chi : \mathcal{W}(\bar{F}/F) \longrightarrow \{\pm 1\}$ is the character corresponding to the extension $F(\sqrt{\gamma(E/F)})/F$. Hence, $\chi = (\gamma(E/F), .)$, where $(.,.)$ is the Hilbert symbol. Moreover,*

a) $(\gamma(E/F), .)$ is trivial if and only if E/F has split multiplicative reduction.

b) $(\gamma(E/F), .)$ is non-trivial and unramified if and only if E/F has non-split multiplicative reduction.

c) $(\gamma(E/F), .)$ is ramified if and only if E/F has additive reduction.

Proof. See [[9], Section 15]. □

Next we invoke the local Langlands correspondence for GL(2). Recall that it is a bijection between (isomorphism classes of) 2-dimensional Weil-Deligne representations σ', and (isomorphism classes of) irreducible, admissible representations π of $\mathrm{GL}(2, F)$; See Equation (2.5.1) and Table 2.5.2. Thus the main theorem of this chapter is

Theorem 3.4.3. *Let E/F be an elliptic curve with potential multiplicative reduction. Then the corresponding representation π of $\mathrm{GL}(2, F)$ associated to the Weil-Deligne representation σ' is*

$$\pi = (\gamma(E/F), .)\mathrm{St}_{\mathrm{GL}(2)},$$

with $(.,.)$ being the Hilbert symbol.

Proof. By Proposition 3.4.2, the complex representation of the Weil-Deligne group is $\sigma' = (\gamma(E/F), .)\omega^{-1} \otimes \mathrm{sp}(2)$. Twisting by $\omega^{1/2}$ we obtain

$$(\gamma(E/F), .)\omega^{-1/2} \otimes \mathrm{sp}(2) = (\sigma,\, N),$$

with

$$\sigma(w) = \begin{bmatrix} (\gamma(E/F), .)\omega^{-1/2}(w) & \\ & (\gamma(E/F), .)\omega^{1/2}(w) \end{bmatrix}, \qquad N = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Hence by Table 2.5.2, $\pi = (\gamma(E/F), .)\mathrm{St}_{\mathrm{GL}(2)}$. □

Note that this result holds without any restrictions on the residual characteristic of F.

Chapter 4

The Potential Good Reduction Case

Through out this chapter we will assume that the elliptic curve E has potential good reduction. By Proposition 2.3.3, an elliptic curve has potential good reduction if and only if it has an integral j-invariant. This means that E acquires good reduction over some finite extension over the field of definition.

4.1 The complex representation of $\mathcal{W}(\bar{F}/F)$ attached to E

Let E be an elliptic curve defined over a non-archimedean local field F and let $\bar{F}$ be its algebraic closure. Let $K \subset \bar{F}$ be a finite extension of F over which E acquires good reduction and let I_K be the inertia subgroup of $\mathrm{Gal}(\bar{F}/K)$. Let ℓ be a prime different than $\mathrm{char}(F)$. The criterion of Néron-Ogg-Shafarevich implies that the ℓ-adic representation σ'_ℓ is trivial on I_K. Following the discussion in Section 14 of [9] we have the following basic facts about the complex representation $\sigma' = (\sigma, N)$ of the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$ associated to σ'_ℓ.

Proposition 4.1.1. *Suppose that E has potential good reduction. Then $\sigma' = (\sigma, 0)$ and σ is semisimple. Furthermore, E has good reduction over F if and only if σ is unramified.*

Proof. We refer the reader to [[9], Section 14]. □

We continue to let F be a non-archimedean local field and let $\mathfrak{o} \,/\, \mathfrak{p}$ be its residue class field with characteristic $\mathrm{char}(\mathfrak{o} \,/\, \mathfrak{p}) = p$. Let $m \geq 3$ be an integer

which is relatively prime to p and $E[m]$ be the subgroup of E consisting of all the points of order dividing m. By hypothesis and Section 5.6 of [11], we have $L = F^{unr}(E[m])$ is the minimal extension of F^{unr} over which E has good reduction. Recall that F^{unr} is the maximal unramified extension of F. Let Λ be the Galois group $\Lambda = \mathrm{Gal}(L/F^{unr})$ then there are the following possibilities for Λ.

a) If $p \neq 2, 3$, then Λ is a cyclic group of order $1, 2, 3, 4$, or 6. Moreover,

$$|\Lambda| = 2 \iff \upsilon_F(\Delta) \equiv 6 \pmod{12}$$

$$|\Lambda| = 3 \iff \upsilon_F(\Delta) \equiv 4 \text{ or } 8 \pmod{12}$$

$$|\Lambda| = 4 \iff \upsilon_F(\Delta) \equiv 3 \text{ or } 9 \pmod{12}$$

$$|\Lambda| = 6 \iff \upsilon_F(\Delta) \equiv 2 \text{ or } 10 \pmod{12}$$

Then it is obvious to see that

$$|\Lambda|.\upsilon_F(\Delta) \equiv 0 \mod 12. \tag{4.1.1}$$

b) If $p = 3$, then Λ is the semidirect product of a cyclic group of order 4 taken with respect to the unique nontrivial action on a group of order 3.

c) For $p = 2$, then Λ is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$.

Here $|\Lambda|$ means the cardinality of the group Λ.

The following proposition will be needed to complete the proof of Theorem 4.2.2. It provides a necessary and sufficient condition for the existence of a totally ramified cyclic finite extension of a local field.

Proposition 4.1.2. *Let F be a local field with residual characteristic p. Let q be the cardinality of the residue class field of F. Let t be a positive integer such that $p \nmid t$. Then the following are equivalent:*

1. $q \equiv 1 \ (mod\ t)$.

2. *There exists a totally ramified cyclic extension K/F of degree t.*

Proof. First, we start by proving (1) implies (2). Assume that $q \equiv 1 \,(\text{mod t})$, i.e., $t \mid q-1$. We have $F^\times = \langle \varpi \rangle \times W_{q-1} \times (1+\mathfrak{p})$, where $W_{q-1} \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Now, consider the subgroup $H = \langle \varpi \rangle \times W_{q-1}^t \times (1+\mathfrak{p})$. Then $(F^\times : H) = t$. By local class field theory there exists an abelian extension K/F such that $N_{K/F}K^\times = H$ and $\mathrm{Gal}(K/F) \cong F^\times/H = W_{q-1}/W_{q-1}^t \cong \mathbb{Z}/t\mathbb{Z}$. Hence K/F is a totally ramified cyclic extension.

Conversely, since $p \nmid t$ and K/F is a totally ramified extension then $t \mid q-1$ by [[8], p. 81, F5]. □

4.2 Criterion for reducible complex representation

Proposition 4.1.1 states that, in case of potential good reduction, the complex representation σ' of the Weil-Deligne group $\mathcal{W}'(\bar{F}/F)$ may be identified with the representation σ of $\mathcal{W}(\bar{F}/F)$. the latter is either irreducible or completely reducible. In the following theorem we find a criterion to distinguish among those two cases by looking at the Weierstrass equation of the elliptic curve E/F. Also, we find the degree of the finite extension over which E has good reduction. We only prove these results for residual characteristic $p \geq 5$.

For an integer $m > 3$, let $L = F^{unr}(E[m])$ be as in Section 4.1. Recall that the Weil group $\mathcal{W}(\bar{F}/F)$ is given by $\mathcal{W}(\bar{F}/F) = \bigsqcup_{n\in\mathbb{Z}} \Phi^n I$ where I is the inertia subgroup and Φ is an inverse Frobenius element. By definition we have

$\mathcal{W}(L/F) = \mathcal{W}(\bar{F}/F)/\mathrm{Gal}(\bar{F}/L) = \bigsqcup_{n\in\mathbb{Z}} \Phi^n I/\mathrm{Gal}(\bar{F}/L)$ and $\Lambda = I/\mathrm{Gal}(\bar{F}/L)$. Thus, it is easy to see that as a coset $\mathcal{W}(L/F)/\Lambda = \langle\Phi\rangle$. One can show that Λ is a normal subgroup of $\mathcal{W}(L/F)$. Thus $\mathcal{W}(L/F) \cong \Lambda \rtimes \langle\Phi\rangle$.

By the Proposition in Section 16 of [9] the complex representation σ' of the Weil-Deligne $\mathcal{W}'(\bar{F}/F)$ has the property $\det(\sigma') = \omega^{-1}$ where ω is the character of $\mathcal{W}(\bar{F}/F)$ defined in Example (2.4.4). By the above identification then we have $\det(\sigma) = \omega^{-1}$. Thus the kernel of σ is contained in I, since by definition $\omega(I) = 1$. In particular, by choosing the integer m large enough one can show that the representation σ factors through $\mathrm{Gal}(\bar{F}/L)$ and is in fact a faithful representation of $\mathcal{W}(L/F) = \Lambda \rtimes \langle\Phi\rangle$.

Remark 4.2.1. *The fact that σ is an injective homomorphism of $\mathcal{W}(L/F) = \Lambda \rtimes \langle\Phi\rangle$ into $\mathrm{GL}(2,\mathbb{C})$ implies that the image of Λ under σ has order $|\Lambda|$.*

We are ready now to present the reducibility criterion for σ in terms of the coefficients of some Weierstrass equation of E.

Theorem 4.2.2. *Let F be a non-archimedean local field with residual characteristic $p \geq 5$. Then the following are equivalent*

a) E acquires good reduction over some finite abelian extension of F.

b) The Weil group $\mathcal{W}(L/F)$ is abelian.

c) The representation σ of $\mathcal{W}(\bar{F}/F)$ is reducible.

d) E acquires good reduction over some totally ramified cyclic extension of F of degree $|\Lambda|$.

e) $(q-1)v_F(\Delta) \equiv 0 \mod 12$, where Δ is the discriminant of any generalized Weierstrass equation for E over F.

Proof. We omit the proof of the equivalence of $a, b, c,$ and d. It can be done in a similar way as the proof of Proposition 2 in Section 2 of [10].

To complete the proof, we prove that the statements of d) and e) are equivalent.

We start by proving d) implies e). Recall that $|\Lambda|.\upsilon_F(\Delta) \equiv 0 \mod 12$. Hence, replacing t with $|\Lambda|$ in Proposition 4.1.2 yields $q \equiv 1 \mod |\Lambda|$. Thus $(q-1)\upsilon_F(\Delta) = 12n$ for some integer n, which implies $(q-1)\upsilon_F(\Delta) \equiv 0 \mod 12$.

Conversely, assume that $12|(q-1)\upsilon_F(\Delta)$. We want to show that E has good reduction over some totally ramified cyclic extension of degree $|\Lambda|$. Let d be a positive divisor of $|\Lambda|$ and K/F^{unr} be a field extension of F^{unr} contained in L. When considering E as an elliptic curve over K the discriminant Δ of its Weierstrass equation might not have a minimal valuation. By Proposition 2.3.1 and Equation (2.3.1) we get a minimal Weierstrass equation for E/K with a new discriminant Δ' so that $\Delta' = u^{-12n}\Delta$ for some integer n and u being a unit in $K^\times$. Thus $\upsilon_K(\Delta) = \upsilon_K(\Delta') + 12n$ which is a necessary and sufficient condition for $p \neq 2, 3$. Then E/K has good reduction if and only if $\upsilon_K(\Delta) = 12n$. This implies that $\upsilon_K(\Delta) \equiv 0 \mod 12$. We have $\upsilon_K(\Delta) = d.\upsilon_{F^{unr}}(\Delta)$ because the extension K/F^{unr} has degree d and is totally ramified. Thus $\upsilon_K(\Delta) = d.\upsilon_F(\Delta)$, since $\upsilon_{F^{unr}}(\Delta) = \upsilon_F(\Delta)$. Therefore, E/K has good reduction if and only if $d.\upsilon_F(\Delta) \equiv 0 \mod 12$. By definition L is the minimal extension of F^{unr} over which E has good reduction, then $d.\upsilon_F(\Delta) \equiv 0 \mod 12$ if and only if $d = |\Lambda|$.

We claim that $|\Lambda| \mid q-1$. To prove this let K be a field extension of F of degree $d = \gcd(|\Lambda|, q-1)$ such that $d < |\Lambda|$. Then there are integers x and y such that $d = |\Lambda|x + (q-1)y$. Thus, $d.\upsilon_F(\Delta) = (|\Lambda|x + (q-1)y)\upsilon_F(\Delta) \equiv 0 \mod 12$ which implies that $\upsilon_K(\Delta) \equiv 0 \mod 12$. Then E/K has good reduction and $d < |\Lambda|$ which contradicts the above congruence. Therefore, $|\Lambda| = \gcd(|\Lambda|, q-1)$,

i.e., $|\Lambda| \mid q-1$. Hence, Proposition 4.1.2 implies that there is a totally ramified cyclic extension K of F of degree $|\Lambda|$. $\square$

Recall that $\Lambda = 1, 2, 3, 4,$ or 6. Then, we claim that

$$|\Lambda| = \frac{12}{\gcd(\upsilon_F(\Delta), 12)}. \tag{4.2.1}$$

To see this let $|\Lambda| = 4$. From the proof of Theorem 4.2.2 we have $4\upsilon_F(\Delta) = 12n$ for some $n \in \mathbb{Z}$ and $d.\upsilon_F(\Delta) \neq 12r$ for $d = 4$. Therefore, $\upsilon_F(\Delta)$ is a multiple of 3 but is not a multiple of 6. Thus $\gcd(\upsilon_F(\Delta), 12) = 3$ and $|\Lambda| = \frac{12}{\gcd(\upsilon_F(\Delta),12)}$. The other case can be proven in a similar fashion. We denote this fraction by e.

The importance of the reducibility criterion is that it allows us to determine the associated irreducible, admissible representation π of $\mathrm{GL}(2, F)$. Thus, we will examine this representation in the following two sections.

4.3 The principal series representation

Assume that E/F is an elliptic curve that has bad but potential good reduction. If the Weierstrass equation of E satisfies the condition $(q-1)\upsilon_F(\Delta) \equiv 0 \pmod{12}$ then the complex representation is $\sigma = \chi_1 \oplus \chi_2$ by Theorem 4.2.2 where χ_1, χ_2 are characters of $\mathcal{W}(\bar{F}/F)$. We tensor σ by $\omega^{1/2}$ to obtain the analytically normalized representation σ_{an}. We then have

$$\sigma_{an}(w) = \begin{bmatrix} \chi(w) & \\ & \chi(w)^{-1} \end{bmatrix},$$

for all $w \in \mathcal{W}(\bar{F}/F)$. Hence by Table 2.5.2, the corresponding irreducible, admissible representation π of $\mathrm{GL}(2, F)$ is a principal series representation.

Writing $\pi = \chi \times \chi^{-1}$ where χ is the character of $F^\times$ corresponding to the

character χ of $\mathcal{W}(\bar{F}/F)$, our goal in this section is to determine χ explicitly.

We continue to let $p \geq 5$. Assume that $(q-1)\upsilon_F(\Delta) \equiv 0 \mod 12$. Then we have

Theorem 4.3.1. *Let E/F be an elliptic curve with additive but potential good reduction. Then the corresponding irreducible, admissible representation of $\mathrm{GL}(2,F)$ is $\pi = \chi \times \chi^{-1}$ where χ satisfies the following*

a) χ is trivial on $1+\mathfrak{p}$. (The conductor is 1.)

b) $\chi|_{W_{q-1}}$ is trivial on the index e-subgroup W_{q-1}^e.

c) The induced character on $W_{q-1}/W_{q-1}^e \cong \mathbb{Z}/e\mathbb{Z}$ has order e. For $e = 2$, there is a unique such character, which is quadratic. Furthermore, for $e \in \{3,4,6\}$, there are two such characters, which are inverses of each other.

Here W_{q-1} is the group of $(q-1)$-th roots of unity.

Proof. We already know from the considerations above that $\pi = \chi \times \chi^{-1}$. Moreover, Theorem 4.2.2 shows the existence of a totally ramified extension K of F of degree e where $e = \frac{12}{\gcd(12,\upsilon_F(\Delta))}$ as defined in Section 4.1. Also, it states that E/K has good reduction. Therefore, the irreducible, admissible representation of $\mathrm{GL}(2,K)$ is a principal series representation $\pi_K = \mu \times \mu^{\times}$ where μ is an unramified character of $K^{\times}$ by Proposition 4.1.1. Let $N_{K/F}$ be the norm map. Since π_K is the base change of π, then $\mu = \chi \circ N_{K/F}$.

We start by proving a). Recall that since E has additive reduction the the conductor is $a(E) = 2$ by Remark 2.3.5. Thus $a(\pi) = a(E) = 2$ and hence $a(\chi) = 1$, i.e., χ is tamely ramified.

To prove b), let $x \in W_{q-1}^e \subset \mathfrak{o}^\times$, then $x = y^e$ for some $y \in W_{q-1} \subset \mathfrak{o}^\times$. Thus $x = N_{K/F}(z)$ for some $z \in \mathfrak{o}_K^\times$. Hence $\chi(x) = \chi(N_{K/F}(z)) = \mu(z) = 1$. Therefore, $\chi|_{W_{q-1}}$ is trivial on W_{q-1}^e.

The fact that $\mathfrak{o}^\times$ get mapped to the inertia subgroup under the Artin isomorphism and Remark 4.2.1 imply that the image of $\chi|_{\mathfrak{o}^\times}$ has e elements. Thus χ has order e on W_{q-1}/W_{q-1}^e. □

4.4 The supercuspidal representation

In this section we will discuss when the associated irreducible, admissible representation π is supercuspidal and we will explicitly determine which one it is.

Recall that by Theorem 4.2.2 the representation σ of the Weil group $\mathcal{W}(L/F)$ is irreducible if and only if $(q-1)v_F(\Delta) \not\equiv 0 \mod 12$.

Theorem 4.4.1. *Let E/F be an elliptic curve with additive but potential good reduction. Assume that $p \geq 5$ and assume that $(q-1)v_F(\Delta) \not\equiv 0 \mod 12$. Then the corresponding irreducible, admissible representation of $\mathrm{GL}(2,F)$ is $\pi = \omega_{H,\xi}$ where H is the unique unramified quadratic extension of F and ξ satisfies the following:*

a) $\xi : H^\times \longrightarrow \mathbb{C}^\times$ is a tamely ramified character.

b) $\xi|_{\mathfrak{o}^\times}$ has order e with e being as before.

c) $\xi(\varpi) = -1$.

Proof. In this proof we repeat the arguments in Section 2 of [10].

As mentioned above the hypothesis $12 \nmid (q-1)v_F(\Delta)$ means that the complex representation σ of $\mathcal{W}(L/F)$ is irreducible. Hence via the local Langlands

correspondence; see Table 2.5.2, σ corresponds to a supercuspidal representation π of $\mathrm{GL}(2,F)$. Also, it implies that the Weil group $\mathcal{W}(L/F)$ is non-abelian. Hence it is an honest semidirect product, namely $\mathcal{W}(L/F) = \Lambda \rtimes \langle \Phi \rangle$.

Let H be the field in L fixed by the abelian index-2 subgroup $\mathbb{Z}/e\mathbb{Z} \times \langle \Phi^2 \rangle$ of $\mathcal{W}(L/F)$. Then H/F is the unramified quadratic extension. Now since $\mathbb{Z}/e\mathbb{Z} \times \langle \Phi^2 \rangle$ has index 2 in $\mathcal{W}(L/F)$, then the representation σ of $\mathcal{W}(L/F)$ is induced from a character ξ of $\mathbb{Z}/e\mathbb{Z} \times \langle \Phi^2 \rangle$. Thus via the local Langlands correspondence we have $\pi = \omega_{H,\xi}$, where ξ is now considered as a character of $H^\times$. Here $\omega_{H,\xi}$ is the dihedral supercuspidal representation defined in Section 2.5.

By Equation (2.5.4) the conductor of π is $a(\pi) = a(\omega_{H,\xi}) = 2a(\xi)$. Moreover, $a(\pi) = a(E) = 2$ by Remark 2.3.5. Thus $a(\xi) = 1$ which proves a).

To prove b), we see that from Remark 4.2.1 $\xi|_{\mathfrak{o}_H^\times}$ has order e. Thus $\xi|_{\mathfrak{o}^\times}$ has order e, since H/F is unramified.

For c), we note that the representation π has trivial central character. Then by Equation (2.5.5)we have $1 = \xi|_{F^\times}(\varpi).\chi_{H/F}(\varpi) = \xi(\varpi)(-1)$ which implies $\xi(\varpi) = -1$. Here $\chi_{H/F}$ is the quadratic character of $F^\times$ corresponding to H/F. $\square$

Chapter 5

Triply Imprimitive Representations

5.1 The problem

In this chapter we will continue to let F be a non-archimedean local field of characteristic zero, $\mathfrak{o}$ its ring of integers, $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$, and ϖ a generator of $\mathfrak{p}$. Let q be the cardinality of the residue class field $\mathfrak{o}/\mathfrak{p}$.

Let π be an irreducible, admissible, supercuspidal representation of $\mathrm{GL}(2,F)$. For a quadratic field extension L/F there is a base change $\mathrm{BC}_{L/F}(\pi)$, which is an irreducible, admissible representation of $\mathrm{GL}(2,L)$. The base change may remain supercuspidal, or may be a principal series representation. In this chapter we investigate the following question:

Is it possible that $\mathrm{BC}_{L/F}(\pi)$ is a principal series representation for *all* quadratic extensions L? (5.1.1)

We reformulate this question in terms of the local parameters corresponding to the representations involved via the local Langlands correspondence (LLC). Since π is supercuspidal, its parameter is an irreducible, 2-dimensional representation (φ, V) of the Weil group $\mathcal{W}(\bar{F}/F)$,

$$\varphi:\ \mathcal{W}(\bar{F}/F) \longrightarrow \mathrm{GL}(2,V) \cong \mathrm{GL}(2,\mathbb{C}).$$

Quadratic base change corresponds to restricting φ to subgroups of index 2;

such subgroups are precisely the Weil groups $\mathcal{W}(\bar{L}/L)$ where L/F is a quadratic field extension. The restriction of φ to $\mathcal{W}(\bar{L}/L)$ remains irreducible precisely if $\mathrm{BC}_{L/F}(\pi)$ is supercuspidal. The above question is therefore equivalent to the following:

Is it possible that $\mathrm{res}_H^{\mathcal{W}(\bar{F}/F)}(\varphi)$ is reducible for *all* index-2 subgroups H of $\mathcal{W}(\bar{F}/F)$? (5.1.2)

It follows from the representation theory of $\mathcal{W}(\bar{F}/F)$ that if $\mathrm{res}_H^{\mathcal{W}(\bar{F}/F)}(\varphi)$ is reducible, then it is a direct sum of two one-dimensional representations. Via Table 2.5.2, this direct sum corresponds to a principal series representation of $\mathrm{GL}(2, F)$.

We will solve problem (5.1.1) for those π with trivial central character and conductor 2. Under the assumption that the residual characteristic is not 2 or 3, these are precisely the representations relevant for the theory of elliptic curves. Our main result is Theorem 5.3.2 below. It states that if $q \equiv 1 \bmod 4$, then there is no π satisfying (5.1.1), and if $q \equiv 3 \bmod 4$, then there is a unique such π. For reasons to be explained, we call such π *triply imprimitive*.

5.2 The problem for arbitrary groups

Let G be a group, and H an index-2 subgroup. We fix an element $\sigma \in G$ which is not in H, so that $G = H \sqcup \sigma H$. If ξ is a representation of H, then the *conjugate representation* ξ^σ is defined by $\xi^\sigma(h) = \xi(\sigma h \sigma^{-1})$. Then

Lemma 5.2.1. *Let G be a group, and H an index-2 subgroup. Let χ be the unique non-trivial character of G/H. Let φ be an irreducible representation of G.*

a) If $\varphi \ncong \varphi \otimes \chi$, *then* $\mathrm{res}_H^G(\varphi)$ *is irreducible. Moreover,*

$$\mathrm{ind}_H^G(\mathrm{res}_H^G(\varphi)) = \varphi \oplus (\varphi \otimes \chi).$$

b) If $\varphi \cong \varphi \otimes \chi$, *then* $\mathrm{res}_H^G(\varphi) = \xi \oplus \xi^\sigma$, *where* ξ *is an irreducible representation of* H. *Moreover,*

- $\xi \ncong \xi^\sigma$ *and*
- $\varphi = \mathrm{ind}_H^G(\xi) = \mathrm{ind}_H^G(\xi^\sigma)$.

Proof. This is a well known fact. □

We will also use the following simple result.

Lemma 5.2.2. *Let* G *be a group, and* H *an index-2 subgroup.*

a) Let ξ *be a representation of* H *and* μ *a character of* G. *Then*

$$\mathrm{ind}_H^G(\xi) \otimes \mu \cong \mathrm{ind}_H^G(\xi \otimes \mathrm{res}_H^G(\mu)). \tag{5.2.1}$$

b) Let ξ_1 *and* ξ_2 *be representations of* H. *Then*

$$\mathrm{ind}_H^G(\xi_1) \cong \mathrm{ind}_H^G(\xi_2) \quad \Longleftrightarrow \quad \big(\xi_1 \cong \xi_2 \text{ or } \xi_1 \cong \xi_2^\sigma\big). \tag{5.2.2}$$

Proof. It is easy to show this result. □

Let $H_1, \ldots, H_r$ be the index-2 subgroups of G. Let φ be an irreducible representation of G such that $\mathrm{res}_H^G(\varphi)$ is reducible for *some* H, say H_1.

Then we have the following result.

Proposition 5.2.3. *Let* G *be a group. Let* $H_1, \ldots, H_r$ *be the index-2 subgroups of* G. *Assume that* $r > 1$.

a) Assume that there exists an irreducible 2-dimensional representation φ of G such that $\mathrm{res}^G_{H_i}(\varphi)$ is reducible for $i = 1, \ldots, r$. Then $r = 3$.

b) Assume that $r = 3$. Let ξ be a character of H_1 with $\xi \neq \xi^\sigma$; here, σ is an element of G that is not in H_1. Let $\varphi = \mathrm{ind}^G_{H_1}(\xi)$. Then

$$\mathrm{res}^G_{H_i}(\varphi) \text{ is reducible for } i = 1, 2, 3 \iff (\xi^2)^\sigma = \xi^2. \tag{5.2.3}$$

Proof. To prove *a*), let φ be an irreducible 2-dimensional representation of G and $\mathrm{res}^G_{H_i}(\varphi)$ be a reducible representation of H_i for $i = 1, \ldots, r$. By *b*) of Lemma 5.2.1, there exists an irreducible representation, namely a character, ξ of H_1 such that $\mathrm{res}^G_{H_1}(\varphi) = \xi \oplus \xi^\sigma$. Moreover, we have $\xi \ncong \xi^\sigma$ and $\varphi = \mathrm{ind}^G_{H_1}(\xi)$.

For $i = 1, \ldots, r$ let χ_i be the non-trivial character of G/H_i. Let σ be an element of G that is not in H_1. By Lemmas 5.2.1 and 5.2.2, we have

$$\begin{aligned}
\mathrm{res}^G_{H_i}(\varphi) \text{ is reducible} &\iff \varphi \cong \varphi \otimes \chi_i \\
&\iff \mathrm{ind}^G_{H_1}(\xi) \cong \mathrm{ind}^G_{H_1}(\xi) \otimes \chi_i \\
&\iff \mathrm{ind}^G_{H_1}(\xi) \cong \mathrm{ind}^G_{H_1}\big(\xi \otimes \mathrm{res}^G_{H_1}(\chi_i)\big) \\
&\iff \Big(\xi \cong \xi \otimes \mathrm{res}^G_{H_1}(\chi_i) \ \text{ or } \ \xi^\sigma \cong \xi \otimes \mathrm{res}^G_{H_1}(\chi_i)\Big).
\end{aligned}$$

Now $\xi \cong \xi \otimes \mathrm{res}^G_{H_1}(\chi_i)$ if and only if $\mathrm{res}^G_{H_1}(\chi_i) = 1$, since ξ is a character. But if $i \geq 2$, then χ_i cannot be trivial on H_1, since its kernel is H_i. Hence, for $i \geq 2$,

$$\begin{aligned}
\mathrm{res}^G_{H_i}(\varphi) \text{ is reducible} &\iff \xi^\sigma \cong \xi \otimes \mathrm{res}^G_{H_1}(\chi_i) \\
&\iff \xi^\sigma = \xi \cdot \mathrm{res}^G_{H_1}(\chi_i).
\end{aligned}$$

Assume this condition is satisfied for $i \geq 2$ and $j \geq 2$ with $i \neq j$. Then

$\mathrm{res}^G_{H_1}(\chi_i) = \mathrm{res}^G_{H_1}(\chi_j)$. Hence $\chi_i\chi_j$ is a non-trivial quadratic character which is trivial on H_1. We conclude that $\chi_i\chi_j = \chi_1$. In particular, if $\mathrm{res}^G_{H_i}(\varphi)$ is reducible for *all* i, then necessarily $r \leq 3$.

However, we cannot have $r = 2$, since if χ_1 and χ_2 are two distinct quadratic characters of G, then $\chi_1\chi_2$ is a third such character. Thus $r = 3$.

To prove *b*), assume that $r = 3$. Let ξ be a character of H_1 and $\varphi = \mathrm{ind}^G_{H_1}(\xi)$. We also let $\mathrm{res}^G_{H_i}(\varphi)$ be reducible for $i = 1, 2, 3$. Then as we saw in part *a*), $\chi_2\chi_3 = \chi_1$, and hence $\mathrm{res}^G_{H_1}(\chi_2) = \mathrm{res}^G_{H_1}(\chi_3)$. Let this common restriction be denoted by α. The kernel of α is $H_1 \cap H_2 = H_1 \cap H_3$, which is an index-2 subgroup of H_1. From above, we see that

$$\mathrm{res}^G_{H_i}(\varphi) \text{ is reducible for } i = 1, 2, 3 \iff \xi^\sigma = \xi \cdot \alpha. \tag{5.2.4}$$

Hence,

$$\mathrm{res}^G_{H_i}(\varphi) \text{ is reducible for } i = 1, 2, 3 \implies (\xi^2)^\sigma = \xi^2. \tag{5.2.5}$$

It remains to prove that if ξ is a character of H_1 with $\xi \neq \xi^\sigma$ and $(\xi^2)^\sigma = \xi^2$, then $\mathrm{res}^G_{H_i}(\varphi)$ is reducible for $i = 1, 2, 3$. Let $M \subset H_1$ be the kernel of ξ/ξ^σ. Since $(\xi/\xi^\sigma)^2 = 1$ by hypothesis, M is an index-2 subgroup of H_1. We claim that σ normalizes M. Indeed, for $m \in M$,

$$\begin{aligned}\Big(\frac{\xi}{\xi^\sigma}\Big)(\sigma m\sigma^{-1}) &= \frac{\xi(\sigma m\sigma^{-1})}{\xi^\sigma(\sigma m\sigma^{-1})} = \frac{\xi(\sigma m\sigma^{-1})}{\xi^{\sigma^{-1}}(\sigma m\sigma^{-1})} \\ &= \frac{\xi(\sigma m\sigma^{-1})}{\xi(m)} = \Big(\Big(\frac{\xi}{\xi^\sigma}\Big)(m)\Big)^{-1} \\ &= 1.\end{aligned}$$

Hence $M \sqcup \sigma M$ is an index-2 subgroup of G, say $M \sqcup \sigma M = H_2$. Evidently, $M = H_1 \cap H_2$. It follows that ξ/ξ^σ equals the character α appearing in (5.2.4).

This concludes the proof. □

Recall that a representation φ of a group G is called *primitive* if it is not induced (from any subgroup), otherwise *imprimitive*. If the representation φ in b) of Proposition 5.2.3 satisfies (5.2.3), then, by b) of Lemma 5.2.1, φ is induced from any of the H_i. We will call such φ *triply imprimitive*. The same terminology is used in [3]. Now we consider G to be the Weil group $\mathcal{W}(\bar{F}/F)$ of our local field F.

By Definition (2.4.3), representations φ of $\mathcal{W}(\bar{F}/F)$ are always assumed to be finite-dimensional and continuous.

We apply Proposition 5.2.3 to $\mathcal{W}(\bar{F}/F)$ instead of any group G. Note that the quadratic field extensions L of F correspond to the index-2 subgroups $\mathcal{W}(\bar{L}/L)$ of $\mathcal{W}(\bar{F}/F)$. If φ is a representation of $\mathcal{W}(\bar{F}/F)$, we will abbreviate

$$\mathrm{res}_{L/F}(\varphi) := \mathrm{res}^{\mathcal{W}(\bar{F}/F)}_{\mathcal{W}(\bar{L}/L)}(\varphi),$$

and if ξ is a representation of $\mathcal{W}(\bar{L}/L)$, we will abbreviate

$$\mathrm{ind}_{L/F}(\xi) := \mathrm{ind}^{\mathcal{W}(\bar{F}/F)}_{\mathcal{W}(\bar{L}/L)}(\xi).$$

There are three quadratic extensions L/F if the residual characteristic of F is odd, and more than three otherwise. From Proposition 5.2.3 we therefore obtain the following result.

Proposition 5.2.4. *Let $L_1, \ldots, L_r$ be the quadratic field extensions of F.*

a) Assume that there exists an irreducible 2-dimensional representation φ of $\mathcal{W}(\bar{F}/F)$ such that $\mathrm{res}_{L_i/F}(\varphi)$ is reducible for $i = 1, \ldots, r$. Then the residual characteristic of F is odd.

b) Assume that the residual characteristic of F is odd, so that $r = 3$. Let ξ be a character of $\mathcal{W}(\bar{L}_1/L_1)$ with $\xi \neq \xi^\sigma$; here, σ is an element of $\mathcal{W}(\bar{F}/F)$ that is not in $\mathcal{W}(\bar{L}_1/L_1)$. Let $\varphi = \mathrm{ind}_{L_1/F}(\xi)$. Then

$$\mathrm{res}_{L_i/F}(\varphi) \text{ is reducible for } i = 1, 2, 3 \iff (\xi^2)^\sigma = \xi^2. \tag{5.2.6}$$

5.3 The case of conductor 2

Let K/F be a quadratic extension. Recall that characters of $\mathcal{W}(\bar{K}/K)$ correspond to characters of $K^\times$ via the local Langlands correspondence for GL(1). We will denote both kinds of characters by the symbol ξ. Thus we get the *dihedral representations* $\omega_{K,\xi}$ of $\mathrm{GL}(2, F)$ defined in Section 2.5.

Let σ be the non-trivial Galois automorphism of K/F, and define the character ξ^σ of $K^\times$ by $\xi^\sigma(x) = \xi(\sigma(x))$. By Theorem 4.6 of [5], the representation $\omega_{K,\xi}$ is given as follows. If $\xi \neq \xi^\sigma$, then $\omega_{K,\xi}$ is supercuspidal. If $\xi = \xi^\sigma$, then $\xi = \mu \circ N_{K/F}$ for a character μ of $F^\times$, and

$$\omega_{K,\xi} = \mu \times (\mu\, \chi_{K/F}),$$

a principal series representation. Here, $N_{K/F}$ is the norm map from K to F, and $\chi_{K/F}$ is the quadratic character of $F^\times$ corresponding to K/F.

In the odd residual characteristic case, we are especially interested in the case of conductor 2, since this case is relevant for elliptic curves. Thus from Equation (2.5.4), we see that

$$a(\mathrm{ind}_{K/F}(\xi)) = 2 \quad \iff \quad a(\xi) = 1.$$

Such ξ are *tamely ramified*, meaning their restriction to the unit group $\mathfrak{o}_K^\times$ is non-trivial, but further restriction to $1+\mathfrak{p}_K$ is trivial. Hence, such ξ descend to a character of the multiplicative group of the residue class field $\mathfrak{o}_K/\mathfrak{p}_K$. Conversely, given $\xi:\ (\mathfrak{o}_K/\mathfrak{p}_K)^\times \to \mathbb{C}^\times$, we can inflate ξ to a character of $\mathfrak{o}_K^\times$, give it some value on a uniformizer ϖ_K, and thus obtain a tamely ramified character of $K^\times$.

In the following we will assume that the residual characteristic of F is odd and look for characters ξ of $K^\times$ satisfying the following conditions:

$$\begin{aligned}
&\text{(A)}\ \ \xi^\sigma \neq \xi.\\
&\text{(B)}\ \ \xi\big|_{F^\times} = \chi_{K/F}.\\
&\text{(C)}\ \ a(\xi) = 1.\\
&\text{(D)}\ \ (\xi^2)^\sigma = \xi^2.
\end{aligned} \tag{5.3.1}$$

Condition (A) assures that $\pi := \omega_{K,\xi}$ is supercuspidal. Condition (B) is equivalent to π having trivial central character; see Equation (2.5.5). Condition (C) is equivalent to π having conductor 2. Finally, by Proposition 5.2.4 *b*), condition (D) means that $\mathrm{BC}_{L/F}(\pi)$ is a principal series representation for *all* quadratic field extensions L of F; observe here that base change corresponds to restricting the local parameter to index-2 subgroups of $\mathcal{W}(\bar{F}/F)$.

5.3.1 The unramified case

Assume first that K/F is the *unramified* quadratic extension of F. Then the residue class field $\mathfrak{o}_K/\mathfrak{p}_K$ is a quadratic extension of $\mathfrak{o}/\mathfrak{p}$. Assume ξ has the properties (A) – (D) in (5.3.1). By (C), ξ determines a character $\bar{\xi}$ of $(\mathfrak{o}_K/\mathfrak{p}_K)^\times$

with the following properties.

$$\begin{aligned}
&(\bar{\mathrm{A}})\ \ \bar{\xi}^{\bar{\sigma}} \neq \bar{\xi}.\\
&(\bar{\mathrm{B}})\ \ \text{The restriction of } \bar{\xi} \text{ to } (\mathfrak{o}\,/\,\mathfrak{p})^{\times} \text{ is trivial.}\\
&(\bar{\mathrm{D}})\ \ (\bar{\xi}^2)^{\bar{\sigma}} = \bar{\xi}^2.
\end{aligned} \tag{5.3.2}$$

Here, $\bar{\sigma}$ is the non-trivial Galois automorphism of the residue class field extension. Explicitly, $\bar{\sigma}$ is the Frobenius, given by $\bar{\sigma}(x) = x^q$.

Let g be a generator of the cyclic group $(\mathfrak{o}_K\,/\,\mathfrak{p}_K)^{\times}$. The order of g is q^2-1. Any character $\bar{\xi}$ of $(\mathfrak{o}_K\,/\,\mathfrak{p}_K)^{\times}$ is determined by its value on g, and this value can be any (q^2-1)-th root of unity:

$$\bar{\xi}(g) = e^{2\pi i \frac{k}{q^2-1}}, \qquad k = 1, 2, \ldots, q^2-1.$$

The conditions (5.3.2) are then equivalent to the following.

$$\begin{aligned}
&(\bar{\mathrm{A}})\ \ k \notin (q+1)\,\mathbb{Z}.\\
&(\bar{\mathrm{B}})\ \ k \in (q-1)\,\mathbb{Z}.\\
&(\bar{\mathrm{D}})\ \ 2k \in (q+1)\,\mathbb{Z}.
\end{aligned} \tag{5.3.3}$$

Conditions $\bar{\mathrm{A}}$ and $\bar{\mathrm{D}}$ imply that

$$k = \frac{q+1}{2}(1+2m), \qquad m \in \{0, 1, \ldots, q-2\}.$$

Assume that $\bar{\mathrm{B}}$ is also satisfied, i.e.,

$$\frac{q+1}{2}(1+2m) = (q-1)n$$

for some integer n. If $q \equiv 1 \bmod 4$, then the left side is odd and the right side is even, so this is impossible. Assume that $q \equiv 3 \bmod 4$. In the equation

$$\frac{q+1}{4}(1+2m) = \frac{q-1}{2}n$$

the integers $\frac{q+1}{4}$ and $\frac{q-1}{2}$ are relatively prime. Hence

$$1+2m = j\frac{q-1}{2}$$

for some $j \in \mathbb{Z}$. For reasons of size we must have $j \in \{1,2,3,4\}$. Also, j must be odd, so the only possibilities are $j=1$ and $j=3$. Hence the only possibilities for k are

$$k = \frac{q^2-1}{4} \qquad \text{and} \qquad k = 3\,\frac{q^2-1}{4}.$$

Note that

$$q\,\frac{q^2-1}{4} \equiv 3\,\frac{q^2-1}{4} \mod q^2-1$$

due to our hypothesis $q \equiv 3 \bmod 4$, so that the two possible values of k lead to Galois-conjugate characters $\bar{\xi}$. We might as well fix $k = \frac{q^2-1}{4}$. Our character $\bar{\xi}$ is then given by

$$\bar{\xi}(g) = e^{2\pi i/4} = i \tag{5.3.4}$$

(its Galois conjugate would have $g \mapsto -i$).

Conversely, assuming that $q \equiv 3 \bmod 4$, we can *define* $\bar{\xi}$ by (5.3.4). Let ξ be the inflation of $\bar{\xi}$ to $\mathfrak{o}_K^\times$. To obtain a character of $K^\times$, we also need to define the value $\xi(\varpi_K)$, where ϖ_K is a uniformizer in K. Since K/F is unramified, we can take $\varpi_K = \varpi$, where ϖ is a uniformizer in F. Condition (B) in (5.3.1) then forces us to define $\xi(\varpi) = -1$. Having defined ξ in this way, we see that all the conditions in (5.3.1) are satisfied.

5.3.2 The ramified case

Now assume that K/F is a *ramified* quadratic extension of F (there are two such extensions). In this case $\mathfrak{o}_K / \mathfrak{p}_K = \mathfrak{o} / \mathfrak{p}$. Assume that ξ satisfies the conditions in (5.3.1). Since $\mathfrak{o}_K^\times = \mathfrak{o}^\times(1 + \mathfrak{p}_K)$, the restriction of ξ to $\mathfrak{o}_K^\times$ is determined by $\xi|_{\mathfrak{o}^\times}$. In view of (B), ξ is completely determined on $\mathfrak{o}_K^\times$. We also see that $\xi = \xi^\sigma$ on $\mathfrak{o}_K^\times$.

Choose the uniformizer ϖ of F such that $K = F(\sqrt{\varpi})$. Then $\sigma(\sqrt{\varpi}) = -\sqrt{\varpi}$, and hence

$$\xi^\sigma(\sqrt{\varpi}) = \xi(-\sqrt{\varpi}) = \chi_{K/F}(-1)\xi(\sqrt{\varpi}).$$

In order to satisfy (A), we must have $\chi_{K/F}(-1) = -1$; this holds exactly if $q \equiv 3 \mod 4$. Assume this is the case, so that $\xi^\sigma(\sqrt{\varpi}) = -\xi(\sqrt{\varpi})$. We have

$$\xi(\sqrt{\varpi})^2 = \xi(\varpi) = \chi_{K/F}(\varpi) = \chi_{K/F}(-1)\chi_{K/F}(-\varpi) = \chi_{K/F}(-1) = -1,$$

since $-\varpi$ is a norm. It follows that $\xi(\sqrt{\varpi}) = \pm i$, and up to Galois conjugation we may assume $\xi(\sqrt{\varpi}) = i$. We proved that ξ is unique up to Galois conjugation. Conversely, we see how to construct a character ξ with the properties (A) – (D) provided that $q \equiv 3 \mod 4$.

Summary

Definition 5.3.1. *Assume that the residual characteristic of F is odd. Let an irreducible, admissible, supercuspidal representation π of* $\mathrm{GL}(2, F)$ *be called* triply imprimitive *if* $\mathrm{BC}_{L/F}(\pi)$ *is a principal series representation for every quadratic field extension L of F.*

For a quadratic extension K/F, assume that $\mathfrak{o}_K$, $\mathfrak{p}_K$ and ϖ_K denote the ring of integers of K, the maximal ideal in this ring, and a uniformizer for K,

respectively. Then the following theorem summarizes our results.

Theorem 5.3.2. *Assume that the residual characteristic of F is odd. Consider irreducible, admissible, supercuspidal representations π of $\mathrm{GL}(2,F)$ with the following properties.*

- *π has trivial central character.*
- *$a(\pi) = 2$.*
- *π is triply imprimitive.*

If $q \equiv 1 \bmod 4$, then there exists no such representation. If $q \equiv 3 \bmod 4$, then there exists a unique such representation π, given in either of the following two ways.

1. *Let K/F be the unramified quadratic extension. Let g be a generator of $(\mathfrak{o}_K / \mathfrak{p}_K)^\times$, and define a character $\bar{\xi}$ of this group by $\bar{\xi}(g) = i$. Inflate $\bar{\xi}$ to a character ξ of $\mathfrak{o}_K^\times$, and extend ξ to a character of $K^\times$ by setting $\xi(\varpi) = -1$. Then $\pi = \omega_{K,\xi}$.*
2. *Let K/F be a ramified quadratic extension. Let ξ be the character of $\mathfrak{o}_K^\times = \mathfrak{o}^\times(1+\mathfrak{p}_K)$ that is trivial on $1+\mathfrak{p}_K$ and coincides with $\chi_{K/F}$ on $\mathfrak{o}^\times$. Extend ξ to a character of $K^\times$ by setting $\xi(\sqrt{\varpi}) = i$; here ϖ is a uniformizer of F such that $K = F(\sqrt{\varpi})$. Then $\pi = \omega_{K,\xi}$.*

5.4 The relevance for elliptic curves

We continue to let F be a non-archimedean local field of characteristic zero. Let E/F be an elliptic curve. Then there is an irreducible, admissible representation π of $\mathrm{GL}(2,F)$ attached to E/F.

The correspondence between E and π is such that the conductors coincide

$$a(E) = a(\pi).$$

Assume that the residual characteristic of F is not 2 or 3. Then $a(E)$ can only take the values 0, 1 or 2. We have $a(E) = 0$ if E/F has good reduction, $a(E) = 1$ if E/F has multiplicative reduction, and $a(E) = 2$ if E/F has additive reduction; see [C15, Appendix,[13]].

To find π there are two fundamentally disjoint cases to consider:

1. E/F has *potential good reduction.*

2. E/F has *potential multiplicative reduction.* In this case π is a twist of a Steinberg representation by Theorem 3.4.3.

The case of potential multiplicative reduction is thus completely solved. Let us assume that E/F has potential good reduction. In this case π is either a principal series representation or a supercuspidal representation. And from Theorem 4.2.2

$$\pi \text{ is principal series} \quad \Longleftrightarrow \quad (q-1)\upsilon(\Delta) \equiv 0 \mod 12. \tag{5.4.1}$$

Here, υ is the normalized valuation on F and Δ is the discriminant of E/F.

Let L/F be a field extension. Then we may consider E over the field L. While the Weierstrass equation for E is exactly the same as before, the two curves E/F and E/L are not the same; the field of definition is part of the elliptic curve. To E/F we have attached a representation π of $\mathrm{GL}(2, F)$, and to E/L we have attached a representation Π of $\mathrm{GL}(2, L)$. It is easy to see from the

definitions that

$$\Pi = \mathrm{BC}_{L/F}(\pi). \tag{5.4.2}$$

In other words, base change for elliptic curves corresponds to base change for the associated irreducible, admissible representations.

These facts, combined with Theorem 5.3.2, can sometimes be used to completely determine the representation π:

Theorem 5.4.1. *Assume that the residual characteristic of F is ≥ 5. Let E/F be an elliptic curve with discriminant Δ. Assume that E has bad, but potential good reduction. Assume further that the following conditions are satisfied (where υ is the normalized valuation on F):*

- $q \equiv 3 \ mod\ 4$.
- $\upsilon(\Delta)$ *is odd.*
- $(q-1)\upsilon(\Delta) \equiv 0 \ mod\ 3$.

Then the irreducible, admissible representation π of $\mathrm{GL}(2,F)$ attached to E/F is the triply imprimitive supercuspidal representation from Theorem 5.3.2.

Proof. The three conditions imply that $(q-1)\upsilon(\Delta)$ is divisible by 6, but not by 12. By (5.4.1), π is supercuspidal. Also,

$$(q^2-1)\upsilon(\Delta) \equiv 0 \mod 12 \tag{5.4.3}$$

and

$$(q-1)2\upsilon(\Delta) \equiv 0 \mod 12. \tag{5.4.4}$$

Using (5.4.1) and (5.4.2), condition (5.4.3) implies that $\mathrm{BC}_{L/F}(\pi)$ is a principal series representation if L/F is the unramified quadratic extension. Similarly,

condition (5.4.4) implies that $\mathrm{BC}_{L/F}(\pi)$ is a principal series representation if L/F is a ramified quadratic extension. Hence π is triply imprimitive. $\square$

Example 5.4.2. *Let E be the elliptic curve*

$$y^2 + y = x^3 - 7x + 12.$$

This is the elliptic curve with Cremona's label 245a1. *We have*

$$N = 5 \cdot 7^2, \qquad \Delta = -5^3 \cdot 7^3, \qquad j = -2^{12} \cdot 3^3 \cdot 5^{-3}.$$

Here N is the conductor of E/F. We consider E over $F = \mathbb{Q}_7$, so that $q = 7$. Since j is in $\mathbb{Z}_7$, E/F has potential good reduction. The (exponent of the) conductor is $\upsilon(N) = 2$, so that E/F has additive reduction. All the conditions of Proposition 5.4.1 are satisfied, and it follows that the associated representation π of $\mathrm{GL}(2, \mathbb{Q}_7)$ is triply imprimitive.

Bibliography

[1] D. Bump, *Automorphic Forms and Representations*, Cambridge, 1997.

[2] P. Deligne, *Formes modulaires el représentation de* GL(2) , Modular Functions of One Variable, II, SLN 349, Springer-Verlag, New York, 1973, p. 55-105

[3] G. Henniart, *Représentations de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$, Volume 284 of C. R. Acad. Sci. Paris Sér. A-B, p. A1329–A1332, 1977.

[4] S. Gelbart, *Automorphic Forms on Adele Groups*, Annals of Mathematics Studies, no. 83, Princton University Press, 1975.

[5] H. Jacquet and R. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Mathematics, Vol. 114, Springer-Verlag, Berlin, 1970.

[6] P.C. Kutzko, *The Langlands conjecture for* GL_2 *of a local field*, Annals of Math., 112:381-412, 1980.

[7] S. Lang, *Algebraic Number Theory, Second edition*, Springer, 1994.

[8] F. Lorenz, *Algebra, Volume II: Fields with Structure, Algebras and Advanced Topics*, Springer, 2007.

[9] D. Rohrlich, *Elliptic Curves and the Weil-Deligne Group*, In Elliptic Curves and Related Topics, Volume 4 of CRM Proc. Lecture Notes, Amer. Math. Soc., Providence, RI, (1994), p. 125-157.

[10] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Mathematica, tome 87, no. 2,(1993), p. 119-151

[11] J-P. Serre, *Propriétés des galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259-331.

[12] J-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. Math. 68 (1968), 492-517.

[13] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1985.

[14] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.