Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint Nr. 127

On the Tate Modules of Elliptic Curves over a Local Field of Characteristic two

Jochen Frieden

Saarbrücken 2004

Fachrichtung 6.1 – Mathematik
Universität des Saarlandes

Preprint No. 127
submitted: February 22, 2005

On the Tate Modules of Elliptic Curves over a Local Field of Characteristic two

Jochen Frieden

Saarland University
Department of Mathematics
Postfach 15 11 50
D–66041 Saarbrücken
Germany
frieden@math.uni-sb.de

Edited by
FR 6.1 – Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-Mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

Abstract

Let $K := \mathbb{F}_{2^f}((T))$ be the field of Laurent series over the finite field with 2^f elements. Every non-supersingular elliptic curve $\mathcal{E}$ over K has a short Weierstraß form

$$Y^2 + XY = X^3 + \alpha X^2 + \beta$$

with appropriate $\alpha, \beta \in K$. The Tate module of $\mathcal{E}$ yields a two dimensional representation $\pi'_{\alpha,\beta}$ of the Weil-Deligne group $W'(K^{\mathrm{sep}}/K)$. Contrary to characteristics different from two, arbitrarily high ramification may occur. If β is integral, the rational points of $\mathcal{E}$ can be completely described in terms of periodic functions. As a consequence, $\pi'_{\alpha,\beta}$ is completely known.

We will deal with the case in which β is not integral. In this case we can consider $\pi'_{\alpha,\beta}$ as a representation $\pi_{\alpha,\beta}$ of the Weil group $W(K^{\mathrm{sep}}/K)$ of K. The aim of this article is to give an explicit description of $\pi_{\alpha,\beta}$ and to determine the ramification properties. As a consequence, we will be able to calculate the conductor.

1 Introduction

In the following we will recall the most important facts and definitions. For further information as well as a general introduction to this topic, we refer to [3]. Our notation concerning local fields is the notation from [4].

Let K be a local field with finite residue field of characteristic p with $q = p^f$ elements. By $G(K^{\mathrm{sep}}/K)$ we denote the absolute Galois group of K, thought of as the group of automorphisms of a fixed separable closure K^{sep} of K. The group $G(K^{\mathrm{sep}}/K)$ can be regarded as a topological group by taking $G(K^{\mathrm{sep}}/M)$, where M runs over all finite Galois extensions of K, as a fundamental system of open neighbourhoods of the identity element. Let K_0 be the maximal unramified extension. We consider the non-open subgroup $G_0(K^{\mathrm{sep}}/K) := G(K^{\mathrm{sep}}/K_0)$, which is called inertia group. The quotient

$$G(K^{\mathrm{sep}}/K)/G_0(K^{\mathrm{sep}}/K)$$

is canonically isomorphic to the absolute Galois group $G(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q)$ of the residue field. An element of $G(K^{\mathrm{sep}}/K)$ is called Frobenius if it is mapped to the Frobenius automorphism $x \longmapsto x^q$ of $G(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q)$.

The Weil group $W(K^{\mathrm{sep}}/K)$ is the subgroup of $G(K^{\mathrm{sep}}/K)$ generated by the inertia group $G_0(K^{\mathrm{sep}}/K)$ and a Frobenius element. We define $W(K^{\mathrm{sep}}/K)$ as a topological group by requiring that the topology on $G_0(K^{\mathrm{sep}}/K)$ is the topology induced from $G(K^{\mathrm{sep}}/K)$ and that $G_0(K^{\mathrm{sep}}/K)$ itself is open. A representation of $W(K^{\mathrm{sep}}/K)$ is a continuous group homomorphism

$$\rho : W(K^{\mathrm{sep}}/K) \longrightarrow \mathrm{GL}(W)\,,$$

where W is a finite dimensional vector space over $\mathbb{C}$ and $\mathrm{GL}(W)$ denotes the general linear group of W, endowed with its complex topology. We recall that there always exists a finite Galois extension L of K so that the restriction of ρ to $G_0(K^{\mathrm{sep}}/L)$ is trivial. As in [4] we can choose an uniformizer T_L of L and define for every $i \in \mathbb{N}_0$ the higher ramification group

$$G_i(L/K) := \{\sigma \in G(L/K) \mid \nu_L(\sigma(T_L) - T_L) \geq i + 1\}\,.$$

This definition does not depend on the choice of T_L. We now consider for every $i \in \mathbb{N}_0$ the action of $G_i(L/K)$ on W and denote by $W^{G_i(L/K)}$ the fixed space of W. Then the conductor of ρ is defined by

$$\mathrm{cond}(\rho) := \sum_{i=0}^{\infty} \frac{\#G_i(L/K)}{\#G_0(L/K)} \dim(W/W^{G_i(L/K)})\,.$$

We have to add that $\mathrm{cond}(\rho)$ is always an integer greater or equal zero, which does not depend on the choice of L. We think of $\mathrm{cond}(\rho)$ as a measure which describes the ramification properties of ρ, i.e., the complexity of the operation of the higher ramification groups on W.
We now consider an elliptic curve $\mathcal{E}$ over K and assume that $\mathcal{E}$ has potential good reduction, i.e., that the j-invariant of $\mathcal{E}$ is integral. We further fix an embedding $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ and consider the tensor product

$$V := \mathbb{C} \otimes_\iota T_\ell(\mathcal{E}),$$

where $T_\ell(\mathcal{E})$ is the ℓ-adic Tate module and ℓ a prime different from p. The action of $G(K^{\mathrm{sep}}/K)$ on the points of $\mathcal{E}$ induces an action of $G(K^{\mathrm{sep}}/K)$ on V. Restricting this action to the Weil group defines a continuous representation $\pi : W(K^{\mathrm{sep}}/K) \longrightarrow \mathrm{GL}(V)$. The isomorphism class of π is independent of the choices of ℓ and ι.
We can apply the same construction if the j-invariant fails to be integral, but then π will turn out to be not continuous. In this case, there is a construction due to Deligne and Grothendieck which gives us a representation π' of the so-called Weil-Deligne group $W'(K^{\mathrm{sep}}/K)$. This group can be realised as a semi-direct product of the form $W(K^{\mathrm{sep}}/K) \ltimes \mathbb{C}$. Since there is a satisfactory characterisation for π', if the j-invariant is non-integral, there is no need to treat this case in detail here. We restrict to presenting the result. The representation π' is then isomorphic to the two dimensional special representation

sp(2) iff $\mathcal{E}$ has multiplicative reduction. If the reduction of $\mathcal{E}$ is additive then there exists always a separable quadratic extension M/K so that $\mathcal{E}$ has multiplicative reduction over M. If χ is the unique non-trivial character of $W(K^{\text{sep}}/K)$ vanishing on $W(K^{\text{sep}}/M)$, then we have $\pi' \cong \chi \otimes \text{sp}(2)$. For the definitions and proofs we refer to [3].
The famous Neron-Ogg-Shafarevich criterion says that $\mathcal{E}$ has good reduction iff π is unramified, i.e., if π is trivial on $G_0(K^{\text{sep}}/K)$. Now an extension M of the ground field K causes a restriction of π to the corresponding subgroup $W(K^{\text{sep}}/M)$ of $W(K^{\text{sep}}/K)$. So if L is an extension of K such that $\mathcal{E}$ has good reduction over L, then $\pi(G_0(K^{\text{sep}}/M))$ has to be trivial. Further it is well known that such an L can be obtained by adjoining the coordinates of the set of all ℓ-torsion points.
We now restrict ourselves to the case that K is of equal characteristic 2. That is, K can be considered as a field of Laurent series $\mathbb{F}_{2^f}((T))$ over a finite field $\mathbb{F}_{2^f}$. In this case, every elliptic curve over K with non-vanishing j-invariant has a short Weierstraß form

$$\mathcal{E} : Y^2 + XY = X^3 + \alpha X^2 + \beta$$

for appropriate $\alpha, \beta \in K$. Using this short Weierstraß form the j-invariant is β^{-1}. So the condition of $\mathcal{E}$ having potential good reduction means that β^{-1} is integral. The aim of this article is to analyse the corresponding representation $\pi_{\alpha,\beta}$ of the Weil group $W(K^{\text{sep}}/K)$.
Since $\pi_{\alpha,\beta}$ is semi-simple, it has to be irreducible or the direct sum of two one dimensional representations. So there are two questions natural to ask about $\pi_{\alpha,\beta}$.

- First, when is $\pi_{\alpha,\beta}$ irreducible ?
- Secondly, how can we describe $\pi_{\alpha,\beta}$ explicitly in terms of α and β ?

Further, we want to describe the ramification properties of $\pi_{\alpha,\beta}$ and to calculate $\text{cond}(\pi_{\alpha,\beta})$.
The impact of the parameter α on $\pi_{\alpha,\beta}$ is already known and can easily be described. Viz., let γ be an element of K, and consider the splitting field M of the polynomial $X^2 + X + \gamma$. Define χ_γ as the unique one dimensional representation of $W(K^{\text{sep}}/K)$ whose kernel is $W(K^{\text{sep}}/M)$. Then for all $\alpha' \in K$ we have an isomorphism

$$\pi_{\alpha',\beta} \cong \chi_{\alpha+\alpha'} \otimes \pi_{\alpha,\beta} \, .$$

2 Adjoining coordinates of 3-torsion points

In this section we will give an explicit construction of a Galois extension L over K such that the restriction of $\pi_{\alpha,\beta}$ to $G_0(K^{\mathrm{sep}}/L)$ is trivial. This extension may be obtained by adjoining coordinates of the ℓ-torsion points. In order to minimise the calculation effort we choose $\ell = 3$. Applying the duplication formula [5, III.2.3 (d)] gives us the following system

$$0 = x^4 + x^3 + \beta$$

$$0 = y^2 + xy + x^3 + \alpha x^2 + \beta,$$

whose solutions (x, y) are precisely the coordinates of the non-trivial 3-torsion-points. For the construction of L we choose

- a primitive third root φ of the unit element 1,
- a third root γ of β,
- an element D of K^{sep} satisfying $D + D^2 = \gamma$,
- an element E of K^{sep} satisfying $E + E^2 = D$, and
- an element F_α of K^{sep} satisfying $F_\alpha + F_\alpha^2 = (D + 1)E + \alpha$.

We set $L := K(\varphi, E, F_\alpha)$. An explicit calculation shows that the 3-torsion points unequal to zero of $\mathcal{E}$ are exactly the points $P_{ij} = (x_i, y_{ij})$ with

$$\begin{array}{ll} x_1 := (D+1)E\,, & x_2 := (D+1)(E+1)\,, \\ x_3 := (E+\varphi)D\,, & x_4 := (E+\varphi+1)D \end{array}$$

and

$$\begin{array}{ll} y_{11} := x_1(x_1 + F_\alpha)\,, & y_{12} := x_1(x_1 + F_\alpha + 1)\,, \\ y_{21} := x_2(x_2 + F_\alpha + E + \varphi)\,, & y_{22} := x_2(x_2 + F_\alpha + E + \varphi + 1)\,, \\ y_{31} := x_3(x_3 + F_\alpha + (\varphi+1)E)\,, & y_{32} := x_3(x_3 + F_\alpha + (\varphi+1)E + 1)\,, \\ y_{41} := x_4(x_4 + F_\alpha + \varphi E)\,, & y_{42} := x_4(x_4 + F_\alpha + \varphi E + 1)\,. \end{array}$$

On the other hand, we can recover the generators φ, E, F_α by the formulas

$$\varphi = \tfrac{x_3}{E+E^2} + E\,, \qquad E = \tfrac{x_1}{x_1+x_2}\,, \qquad F_\alpha = \tfrac{y_{11}}{x_1} + x_1\,.$$

We conclude that L is the smallest extension of K containing the coordinates of all 3-torsion points.
We now consider $\mathcal{E}$ as an elliptic curve over L.

Proposition 2.1 *Over L the elliptic curve $\mathcal{E}$ is isomorphic to the elliptic curve*

$$\mathcal{E}_E : Y^2 + E^{-1}XY + Y = X^3 + E^{-3} + 1\,.$$

PROOF. First, we make the transformation $(X, Y) \longmapsto (X, Y + X(E + F_\alpha))$. This yields the equation

$$Y^2 + XY = X^3 + (F_\alpha + F_\alpha^2 + E + E^2 + \alpha)X^2 + \beta\,.$$

Using the identities

$$F_\alpha + F_\alpha^2 = (D + 1)E + \alpha = E^3 + E^2 + E + \alpha$$

and

$$\beta = \gamma^3 = (E + E^4)^3 = E^3 + E^6 + E^9 + E^{12}\,,$$

we obtain

$$Y^2 + XY = X^3 + E^3X^2 + E^3 + E^6 + E^9 + E^{12}\,.$$

Now we make the transformation $(X, Y) \longmapsto (X + E^3, Y + E^6)$, which gives us

$$Y^2 + XY + E^3Y = X^3 + E^3 + E^6\,.$$

Finally, the transformation $(X, Y) \longmapsto (E^2X, E^3Y)$ leads us to the result

$$Y^2 + E^{-1}XY + Y = X^3 + E^{-3} + 1\,.$$

□

Note that the curve $\mathcal{E}_E$ has integral coefficients. In order to simplify our exposition, we will further assume that the valuation $\nu_K(\beta)$ is strictly less than zero. Then we can consider the reduced curve, which is given by the equation

$$Y^2 + Y = X^3 + 1\,.$$

The coefficients are independent of α and β, and the curve $\mathcal{E}_E$ has good reduction. Now we can apply the criterion of Neron-Ogg-Shafarevich, which states that the action of $G_0(K^{\mathrm{sep}}/L)$ on V is trivial and the action of a Frobenius automorphism of $G(K^{\mathrm{sep}}/L)$ is given by the action of the Frobenius automorphism of $G(\mathbb{F}_2^{\mathrm{alg}}/\mathbb{F}_{2^g})$, where $\mathbb{F}_{2^g}$ is the residue field of L. On the other hand, the eigenvalues of the Frobenius automorphism can be obtained just by counting rational points.

In the following we will write $\pi^M_{\alpha,\beta}$ for the restriction of $\pi_{\alpha,\beta}$ to $W(K^{\mathrm{sep}}/M)$ for an arbitrary finite separable extension M of K. We recall that, if we

consider $\mathcal{E}$ as an elliptic curve over M, the construction of $\pi^M_{\alpha,\beta}$ is completely analogous to that of $\pi_{\alpha,\beta}$. To avoid confusion, we will sometimes write $\pi^K_{\alpha,\beta}$ instead of $\pi_{\alpha,\beta}$ if we like to emphasise that $\pi_{\alpha,\beta}$ is defined over the ground field K.
In order to characterise the representation $\pi^L_{\alpha,\beta}$, we define the one dimensional representation

$$\Omega_K : W(K^{\mathrm{sep}}/K) \longrightarrow \mathbb{C}^*$$

by requiring that it should be trivial on $G_0(K^{\mathrm{sep}}/K)$ and

$$\Omega_K(\Phi_K) = (\frac{\mathrm{i}}{\sqrt{2}})^f$$

for every Frobenius element Φ_K of $G(K^{\mathrm{sep}}/K)$. This definition ensures that, for every finite separable extension M of K, the representation Ω_M is equal to the restriction of Ω_K to $W(K^{\mathrm{sep}}/M)$.

Proposition 2.2 *The representation*

$$\Omega_K \otimes \pi^K_{\alpha,\beta} : W(K^{\mathrm{sep}}/K) \longrightarrow \mathrm{GL}(V)$$

is trivial on $W(K^{\mathrm{sep}}/L)$.

PROOF.
Let Φ_L be a Frobenius element of $G(K^{\mathrm{sep}}/L)$ and $\mathbb{F}_{2^g}$ the residue field of L. We only have to show that $\pi^K_{\alpha,\beta}(\Phi_L) = (\frac{\sqrt{2}}{\mathrm{i}})^g$. According to the Neron-Ogg-Shafarevich criterion, $\pi^K_{\alpha,\beta}(\Phi_L)$ is determined by the action of the Frobenius element $\Phi_{\mathbb{F}_{2^g}}$ of $G(\mathbb{F}_2^{\mathrm{alg}}/\mathbb{F}_{2^g})$ on the Tate module of the reduced curve

$$Y^2 + Y = X^3 + 1\,.$$

Since this curve is even defined over $\mathbb{F}_2$, we have only to regard the action of the Frobenius $\Phi_{\mathbb{F}_2}$ of $G(\mathbb{F}_2^{\mathrm{alg}}/\mathbb{F}_2)$. Over $\mathbb{F}_2$ the curve has precisely 3 points. As described in [5, p. 136], we get for the eigenvalues λ_1 and λ_2 of $\Phi_{\mathbb{F}_2}$ the relations

$$3 = 1 - \lambda_1 - \lambda_2 + 2\,,$$
$$\lambda_1 = \overline{\lambda_2}\,,$$

and

$$|\lambda_1| = |\lambda_2| = \sqrt{2}\,.$$

This is possible only if these eigenvalues are $\sqrt{2}\mathrm{i}$ and $-\sqrt{2}\mathrm{i}$. Since $\varphi \in L$, the subfield $\mathbb{F}_4 = \{0, 1, \varphi, \varphi + 1\}$ is contained in L. It follows that g is even.

Therefore $\pi^K_{\alpha,\beta}(\Phi_L)$ has two equal eigenvalues $(\frac{\sqrt{2}}{\mathrm{i}})^g$ and must be a scalar. $\square$

As a consequence of this proposition, we can divide out $W(K^{\mathrm{sep}}/L)$ and obtain a representation $\rho^K_{\alpha,\beta}$ of the finite Galois group

$$W(K^{\mathrm{sep}}/K)/W(K^{\mathrm{sep}}/L) \cong G(L/K)\,,$$

which contains all the information about $\pi_{\alpha,\beta}$.

Proposition 2.3 *The representation*

$$\rho^K_{\alpha,\beta} : G(L/K) \longrightarrow \mathrm{GL}(V)$$

is injective.

PROOF.
Suppose $\sigma \in G(L/K)$ with $\rho^K_{\alpha,\beta}(\sigma) = 1$. Then σ has to act as a scalar on the 3-torsion points. So we have $\sigma(P) = -P$ or P for all 3-torsion points $P = (x, y)$. It follows that $\sigma(x_i) = x_i$ for $i = 1, \ldots, 4$. So we conclude that $\sigma(\varphi) = \varphi$ and $\sigma(E) = E$, which means that σ is trivial on $K(\varphi, E)$. In the case $K(\varphi, E) = L$ we are done.
In the case $K(\varphi, E) \neq L$ it remains to show that the restriction

$$\Omega_{K(\varphi,E)} \otimes \pi^{K(\varphi,E)}_{\alpha,\beta}$$

of $\Omega_K \otimes \pi^K_{\alpha,\beta}$ is not trivial. We apply our remark in the end of the introduction. Since we have

$$(F_\alpha + E)^2 + F_\alpha + E + \alpha + E^3 = F_\alpha^2 + F_\alpha + D + \alpha + E^3 = 0\,,$$

we get

$$\pi^{K(\varphi,E)}_{\alpha,\beta} \cong \chi \otimes \pi^{K(\varphi,E)}_{E^3,\beta}\,,$$

where χ is the one dimensional representation of $W(K^{\mathrm{sep}}/K(\varphi, E))$ defined by the condition $\mathrm{Ker}(\chi) = W(K^{\mathrm{sep}}/L)$. From the identity

$$(F_{E^3})^2 + F_{E^3} = (D + 1)E + E^3 = D\,,$$

we conclude that $K(\varphi, E, F_{E^3}) = K(\varphi, E)$. Therefore $\Omega_{K(\varphi,E)} \otimes \pi^{K(\varphi,E)}_{E^3,\beta}$ has to be trivial, which means that $\Omega_{K(\varphi,E)} \otimes \pi^{K(\varphi,E)}_{\alpha,\beta}$ is not. $\square$

As a simple conclusion of this proposition, we can answer the first question asked in the introduction.

Conclusion 2.4 *The representation $\pi_{\alpha,\beta}$ is reducible iff $G(L/K)$ is abelian.*

3 Functorial properties of $\pi_{\alpha,\beta}$

In order to describe how $\pi_{\alpha,\beta}$ depends on β, we assume $\alpha = 0$. We now consider the smallest local subfield of K over which the curve $\mathcal{E}$ is defined. Obviously, this is the field $\tilde{K} := \mathbb{F}_2((\beta^{-1}))$. Note that this construction is only possible because we made the assumption $\nu_K(\beta) < 0$.
Considering $\mathcal{E}$ as an elliptic curve over $\tilde{K}$, we can apply the construction mentioned above and obtain a representation $\pi_{0,\beta}^{\tilde{K}}$ of the Weil group $W(\tilde{K}^{\mathrm{sep}}/\tilde{K})$. Similarly we get a representation $\rho_{0,\beta}^{\tilde{K}}$ of $G(\tilde{L}/\tilde{K})$, where $\tilde{L} = \tilde{K}(\varphi, E, F_0)$. Further, we may identify the underlying spaces of $\pi_{0,\beta}^{\tilde{K}}$ and $\pi_{0,\beta}^{K}$ as well as the underlying spaces of $\rho_{0,\beta}^{\tilde{K}}$ and $\rho_{0,\beta}^{K}$. If we do so, we get the following proposition.

Proposition 3.1 *The following diagram is commutative:*

Figure 1:

$$\begin{tikzcd}
G(L/K) \arrow[rr, "\sigma \longmapsto \sigma|_{\tilde{L}}"'] \arrow[dr, "\rho_{0,\beta}^{K}"'] & & G(\tilde{L}/\tilde{K}) \arrow[dl, "\rho_{0,\beta}^{\tilde{K}}"] \\
& \mathrm{GL}_2(V)\,. &
\end{tikzcd}$$

PROOF.
Comparing the action of $G(K^{\mathrm{sep}}/K)$ with that of $G(\tilde{K}^{\mathrm{sep}}/\tilde{K})$ on V, we get the commutative diagram

Figure 2:

$$\begin{tikzcd}
W(K^{\mathrm{sep}}/K) \arrow[rr, "\sigma \longmapsto \sigma|_{\tilde{K}^{\mathrm{sep}}}"'] \arrow[dr, "\pi_{0,\beta}^{K}"'] & & W(\tilde{K}^{\mathrm{sep}}/\tilde{K}) \arrow[dl, "\pi_{0,\beta}^{\tilde{K}}"] \\
& \mathrm{GL}_2(V)\,. &
\end{tikzcd}$$

We now compare Ω_K with $\Omega_{\tilde{K}}$. They are both trivial on the inertia groups $G_0(K^{\mathrm{sep}}/K)$ and $G_0(\tilde{K}^{\mathrm{sep}}/\tilde{K})$. We remark further that the rule $\sigma \longmapsto \sigma|_{\tilde{K}^{\mathrm{sep}}}$

maps the inertia group $G_0(K^{\mathrm{sep}}/K)$ to $G_0(\tilde{K}^{\mathrm{sep}}/\tilde{K})$. If Φ_K is a Frobenius element of $W(K^{\mathrm{sep}}/K)$, then $\Phi_K|_{\tilde{K}^{\mathrm{sep}}}$ is the f-th power of a Frobenius element $\Phi_{\tilde{K}}$ of $W(\tilde{K}^{\mathrm{sep}}/\tilde{K})$. This yields the equation

$$\Omega_{\tilde{K}}(\Phi_K|_{\tilde{K}^{\mathrm{sep}}}) = \Omega_{\tilde{K}}(\Phi_{\tilde{K}}^f) = (\frac{\mathrm{i}}{\sqrt{2}})^f = \Omega_K(\Phi_K).$$

So we have the commutative diagram

Figure 3:

$$\begin{tikzcd}
W(K^{\mathrm{sep}}/K) \arrow[rr, "\sigma \longmapsto \sigma|_{\tilde{K}^{\mathrm{sep}}}"'] \arrow[dr, "\Omega_K"'] & & W(\tilde{K}^{\mathrm{sep}}/\tilde{K}) \arrow[dl, "\Omega_{\tilde{K}}"] \\
& \mathrm{GL}_2(V)\,. &
\end{tikzcd}$$

Now we get the required result by tensoring both diagrams and dividing out the subgroup $W(K^{\mathrm{sep}}/L)$ on the left and $W(\tilde{K}^{\mathrm{sep}}/\tilde{L})$ on the right hand side. □

The significance of the last proposition is that we only have to consider the case $K = \mathbb{F}_2((T))$ and $\beta = T^{-1}$, what we will do now.

4 The special case $K = \mathbb{F}_2((T))$ and $\beta = T^{-1}$

Throughout this section we assume $K = \mathbb{F}_2((T))$ and $\beta = T^{-1}$. We note that $K(\varphi)/K$ is an unramified extension. Further we have the equations

$$\beta = E^3 + E^6 + E^9 + E^{12}$$

and

$$F_0 + F_0^2 = E^3 + E^2 + E\,.$$

Since $\nu_K(\beta) = -1$, we conclude that $\nu_K(E) = -\frac{1}{12}$ and $\nu_K(F_0) = -\frac{1}{24}$. In particular $L/K(\varphi)$ must be totally ramified of degree 24. So L/K has maximal degree 48. Since we obtained L by adjoining coordinates of 3-torsion points, we have the inclusion $G(L/K) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ and therefore an isomorphism

$$G(L/K) \cong \mathrm{GL}_2(\mathbb{F}_3)\,.$$

So we can consider $\rho_{0,\beta}^K$ as a representation of $\mathrm{GL}_2(\mathbb{F}_3)$. We now apply the representation theory of $\mathrm{GL}_2(\mathbb{F}_3)$, which can be found for example in [2]. We briefly recall some basic facts.

Referring to the table on page 70, loc. cit., all two dimensional irreducible representations of $\mathrm{GL}_2(\mathbb{F}_3)$ are cuspidal. The cuspidal representations of the group $\mathrm{GL}_2(\mathbb{F}_3)$ are parametrised by the regular characters of $\mathbb{F}_9^*$. A character $\mu : \mathbb{F}_9^* \longrightarrow \mathbb{C}^*$ is called regular if it does not agree with the conjugate character $\bar{\mu}$. The conjugate character $\bar{\mu}$ is defined by $\bar{\mu}(x) := \mu(\bar{x})$, where $\bar{x}$ is the conjugate of x over $\mathbb{F}_3$. This conjugation of characters yields an equivalence relation on the set of all regular characters of $\mathbb{F}_9$. Each equivalence class corresponds to an isomorphism class of cuspidal representations of $\mathrm{GL}_2(\mathbb{F}_3)$. As a generator of $\mathbb{F}_9^*$ we choose the element $\zeta = 1 + \sqrt{-1}$. We further choose the characters μ_1, μ_2, and μ_5 defined by $\mu_k(\zeta) = (\mathrm{e}^{\mathrm{i}\frac{\pi}{4}})^k$ for $k = 1, 2, 5$ as a system of representatives of the equivalence classes of regular characters. By ρ_k for $k = 1, 2, 5$ we denote the corresponding isomorphism classes of cuspidal representations of $\mathrm{GL}_2(\mathbb{F}_3)$. Since μ_2 is not injective, the representation ρ_2 is not injective either. So we only have to decide whether $\rho_{0,\beta}^K$ is isomorphic to ρ_1 or ρ_5.

To do so we must identify $G(L/K)$ and $\mathrm{GL}_2(\mathbb{F}_3)$ by choosing a basis for the $\mathbb{F}_3$-vector space of 3-torsion points. Our choice is the basis (P_{11}, P_{21}). Then we have the following result.

Proposition 4.1 *The representation $\rho_{0,\beta}^K$ is isomorphic to ρ_5.*

PROOF.
Let $\sigma \in G(L/K)$ be the automorphism whose operation on the 3-torsion points is expressed by the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -\zeta\bar{\zeta} \\ 1 & \zeta + \bar{\zeta} \end{pmatrix}.$$

According to [2, p. 70] we have

$$\begin{aligned} \mathrm{Tr}\left(\mu_1 \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\right) &= -\mu_1(\zeta) - \mu_1(\bar{\zeta}) \\ &= -\mu_1(\zeta) - \mu_1(\zeta^3) \\ &= -\mathrm{e}^{\mathrm{i}\frac{\pi}{4}} - \mathrm{e}^{\mathrm{i}\frac{3\pi}{4}} \\ &= -\mathrm{i}\sqrt{2}\,. \end{aligned}$$

We now determine the action of $\sigma(\varphi)$. Recall that $\mathrm{SL}_2(\mathbb{F}_3)$ is the only subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ of index two. As a consequence, $K(\varphi)/K$ is the only

subfield of L quadratic over K. Since the matrix corresponding to σ is not contained in $\mathrm{SL}_2(\mathbb{F}_3)$, we must have $\sigma(\varphi) \neq \varphi$.
Next we construct an appropriate extension of σ, which will enable us to calculate $\rho_{0,\beta}^K(\sigma)$ approximately. Therefore let $\tilde{\sigma} \in W(K^{\mathrm{sep}}/K)$ be an arbitrary extension of σ. For a fixed Frobenius element Φ_K we have $\tilde{\sigma} = \Phi_K^j \sigma_0$, where $j \in \mathbb{Z}$ and $\sigma_0 \in G_0(K^{\mathrm{sep}}/K)$. Since $f(L/K) = 2$ and $\sigma(\varphi) \neq \varphi$, we conclude that j is odd and Φ_K^{j-1} is trivial on L. So $\sigma^* := \Phi_K \sigma_0$ is also an extension of σ. Further we have

$$\Omega_K(\sigma^*) = \frac{\mathrm{i}}{\sqrt{2}}\,.$$

Now assume that $\rho_{0,\beta}^K$ is isomorphic to ρ_1. Then we have

$$\begin{aligned}
\mathrm{Tr}(\pi_{0,\beta}^K(\sigma^*)) &= \Omega_K^{-1}(\sigma^*)\,\mathrm{Tr}\left(\rho_{0,\beta}^K(\sigma)\right) \\
&= \frac{\sqrt{2}}{\mathrm{i}}\left(-\mathrm{i}\sqrt{2}\right) \\
&= -2\,.
\end{aligned}$$

On the other hand, the operation of σ^* on the 3-torsion points yields the congruence

$$\begin{aligned}
\mathrm{Tr}\left(\pi_{0,\beta}^K(\sigma^*)\right) &\equiv \mathrm{Tr}\left(\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\right) \mod 3\mathbb{Z}_3 \\
&\equiv 2 \mod 3\mathbb{Z}_3.
\end{aligned}$$

This is clearly a contradiction. So our assumption needs to be false and we conclude that $\rho_{0,\beta}^K$ is isomorphic to ρ_5. □

Now the second question asked in the introduction is completely answered. But this answer is less satisfactory than it appears on a first view, since it fails to reveal the ramification properties of $\pi_{\alpha,\beta}$.This question will be addressed in the next section.

5 The ramification properties of $\pi_{\alpha,\beta}$

In this section we will calculate the conductor of $\pi_{\alpha,\beta}$ in the general case, where α is arbitrary and $\nu_K(\beta) < 0$. Therefore we need to consider the extension L/K more closely. We define the elements

$$D_\varphi := \varphi E + (\varphi E)^2 \qquad \text{and} \qquad D_{\varphi^2} := \varphi^2 E + (\varphi^2 E)^2\ .$$

This yields $D_\varphi + (D_\varphi)^2 = \varphi\gamma$ and $D_{\varphi^2} + (D_{\varphi^2})^2 = \varphi^2\gamma$, which should be compared with the relation $D + D^2 = \gamma$. So the elements D_φ and D_{φ^2} describe how D changes if we choose $\varphi\gamma$ or $\varphi^2\gamma$ instead of γ as a third root of β. Later we will see that this change of D in dependence of the choice of γ becomes important for the calculation of the conductor.
In order to calculate $\mathrm{cond}(\pi_{\alpha,\beta})$ (see section 1), we have to calculate the higher ramification groups $G_i(L/K)$ for $i > 0$. We begin with a closer look at $G_1(L/K)$. Since $K(\varphi,\gamma)/K$ is tamely ramified, we have

$$G_1(L/K) \subset G(L/K(\varphi,\gamma))\,.$$

Lemma 5.1 *Let $\sigma \in G_1(L/K)$. Then all possible values for the pair*

$$(\sigma(E), \sigma(F_\alpha))$$

are listed in the following table:

Table 1: Possible elements of $G_1(L/K)$

$\sigma(\mathbf{E})$	$\sigma(\mathbf{F}_\alpha)$
E	F_α
E	$F_\alpha + 1$
$E+1$	$F_\alpha + E + \varphi$
$E+1$	$F_\alpha + E + \varphi + 1$
$E+\varphi$	$F_\alpha + (\varphi+1)E$
$E+\varphi$	$F_\alpha + (\varphi+1)E + 1$
$E+\varphi+1$	$F_\alpha + \varphi E$
$E+\varphi+1$	$F_\alpha + \varphi E + 1$

For the order of σ we have

$$\mathrm{ord}(\sigma) = \begin{cases} 1 & \textit{if } \sigma(E) = E \textit{ and } \sigma(F_\alpha) = F_\alpha \\ 2 & \textit{if } \sigma(E) = E \textit{ and } \sigma(F_\alpha) = F_\alpha + 1 \\ 4 & \textit{else.} \end{cases}$$

PROOF.
Since σ leaves $\gamma = E + E^4$ invariant, we have the identity

$$\sigma(E) + \sigma(E^4) = E + E^4\,.$$

On the other hand, we have $E + a + (E+a)^4 = E + E^4 + a + a^4$ for all $a \in \mathbb{F}_4 = \{0, 1, \varphi, \varphi+1\}$. So $E, E+1, E+\varphi, E+\varphi+1$ are exactly the possible values for $\sigma(E)$.

In the case $\sigma(E) = E$ we obtain from $F_\alpha + F_\alpha^2 = (D+1)E + \alpha$ the equation

$$\sigma(F_\alpha) + \sigma(F_\alpha)^2 = (D+1)E + \alpha\,,$$

which has the solutions $\sigma(F_\alpha) = F_\alpha$ and $\sigma(F_\alpha) = F_\alpha + 1$. We leave it to the reader as an exercise to check that we obtain the equation

$$\sigma(F_\alpha) + \sigma(F_\alpha)^2 = (D+1)(E+1) + \alpha$$

in the case $\sigma(E) = E + 1$, the equation

$$\sigma(F_\alpha) + \sigma(F_\alpha)^2 = D(E+\varphi) + \alpha$$

in the case $\sigma(E) = E + \varphi$, and

$$\sigma(F_\alpha) + \sigma(F_\alpha)^2 = D(E+\varphi+1) + \alpha$$

in the case $\sigma(E) = E+\varphi+1$. Further the reader should check that the values for $\sigma(F_\alpha)$ given in the table are all possible solutions of these equations.
There remains the calculation of $\mathrm{ord}(\sigma)$. In the case $\sigma(E) = E$ it is clear that $\mathrm{ord}(\sigma) = 1$ if $\sigma(F_\alpha) = F_\alpha$ and $\mathrm{ord}(\sigma) = 2$ if $\sigma(F_\alpha) = F_\alpha+1$. In all other cases we have only to show that $\sigma^2(E) = E$ and $\sigma^2(F_\alpha) = F_\alpha + 1$, which we leave again as an exercise. □

We now calculate for every possible $\sigma \in G_1(L/K)$ the numbers

$$i_{L/K}(\sigma) := \nu_L(\sigma(T_L) + T_L)\,,$$

where T_L is an arbitrary uniformizer of L. Let us recall some basic facts about these numbers, which can be found in [4, Chap. 4]. We assume that we have a tower $M \supset N \supset K$, where M/K is Galois. First we have the identity

$$i_{M/K}(\sigma) = i_{M/N}(\sigma) \tag{1}$$

for every $\sigma \in G(M/N)$. Secondly, if N/K is Galois then

$$i_{N/K}(\sigma) = \frac{1}{e(M/N)} \sum_{\substack{s\in G(M/K)\\ s|_N=\sigma}} i_{M/K}(s) \tag{2}$$

for each $\sigma \in G(N/K)$. Finally we have the relation

$$d(M/K) = \sum_{\sigma\in G(M/K)\setminus\{\mathrm{id}_M\}} i_{M/K}(\sigma)\,, \tag{3}$$

where $d(M/K)$ denotes the different exponent of M/K.

Lemma 5.2 1. *Let $\sigma \in G_1(L/K)$ with $\sigma(E) = E$ and $\sigma(F_\alpha) = F_\alpha + 1$. Then we have*

$$i_{L/K}(\sigma) = d(L/K(\varphi, E)) .$$

2. *If $d(L/K(\varphi, E)) > 0$ then there is a $\sigma \in G_1(L/K)$ with $\sigma(E) = E$ and $\sigma(F_\alpha) = F_\alpha + 1$.*

PROOF.
Assertion *(1)* is just a simple application of (1) and (3). To show *(2)*, just note that $L/K(\varphi, E)$ has to be wildly ramified of degree two. Therefore an automorphism σ with the required properties exists. □

Lemma 5.3 1. *Let $\sigma \in G_1(L/K)$ with $\sigma(E) = E + 1$. Then we have*

$$i_{L/K}(\sigma) = d(K(E)/K(D)) .$$

2. *If $d(K(E)/K(D)) > 0$ then there are two different automorphisms $\sigma \in G_1(L/K)$ with the property $\sigma(E) = E + 1$.*

PROOF.
Ad *(1)*. An easy calculation shows that σ has order 4 and that $\sigma^3(E) = E+1$. Every subgroup of $G(L/K)$ which contains σ also contains σ^3 and vice versa. Therefore we have $i_{L/K}(\sigma) = i_{L/K}(\sigma^3)$. Applying (1), (2), and (3) we get

$$\begin{aligned}
\frac{2}{e(L/K(\varphi, E))} i_{L/K}(\sigma) &= i_{K(\varphi,E)/K}(\sigma \mid_{K(\varphi,E)}) \\
&= i_{K(\varphi,E)/K(\varphi,D)}(\sigma \mid_{K(\varphi,E)}) \\
&= d(K(\varphi, E)/K(\varphi, D)) .
\end{aligned}$$

Since $K(\varphi, D)$ is the fixed field of $< \sigma >$ and $\sigma \in G_1(L/K) \subset G_1(L/K(\varphi, D))$, the extension $L/K(\varphi, D)$ needs to be totally ramified. It follows that

$$i_{L/K}(\sigma) = d(K(\varphi, E)/K(\varphi, D)) .$$

Finally note that the transitivity property of the different gives us

$$d(K(\varphi, E)/K(\varphi, D)) = d(K(E)/K(D)) .$$

Ad *(2)*. Let $\tilde{\sigma}$ be the unique non-trivial element of $G(K(\varphi, E)/K(\varphi, D))$ and $\sigma \in G(L/K(\varphi, D))$ an extension of $\tilde{\sigma}$. Then we have $\sigma(E) = E + 1$. In order to show that σ is in $G_1(L/K)$, it suffices to show that $L/K(\varphi, D)$ is totally ramified. Since σ has order 4, the extension $L/K(\varphi, D)$ is cyclic of degree 4. Let K' be the maximal unramified subextension of $L/K(\varphi, D)$. From $d(K(E)/K(D)) > 0$ we conclude that the degree of $K'/K(\varphi, D)$ is at most two. If it were two we had $K' = K(\varphi, E)$, which is impossible. Thus we have shown that σ has the required properties. Finally it is easily seen that σ^3 is also an element of $G_1(L/K)$ for which $\sigma^3(E) = E + 1$ holds. $\square$

In the same way we get the following two lemmata.

Lemma 5.4 *1. Let $\sigma \in G_1(L/K)$ with $\sigma(E) = E + \varphi + 1$. Then we have*

$$i_{L/K}(\sigma) = d(K(\varphi E)/K(D_\varphi)) .$$

2. If $d(K(\varphi E)/K(D_\varphi)) > 0$ then there are two different automorphisms $\sigma \in G_1(L/K)$ with the property $\sigma(E) = E + \varphi + 1$.

Lemma 5.5 *1. Let $\sigma \in G_1(L/K)$ with $\sigma(E) = E + \varphi$. Then we have*

$$i_{L/K}(\sigma) = d(K(\varphi^2 E)/K(D_{\varphi^2})) .$$

2. If $d(K(\varphi^2 E)/K(D_{\varphi^2})) > 0$ then there are two different automorphisms $\sigma \in G_1(L/K)$ with the property $\sigma(E) = E + \varphi$.

Now we are able to calculate the numbers $\#G_i(L/K)$.

Proposition 5.6 *Let*

$$r := \min\{d(K(E)/K(D)), d(K(\varphi E)/K(D_\varphi)), d(K(\varphi^2 E)/K(D_{\varphi^2}))\},$$

$$s := \max\{d(K(E)/K(D)), d(K(\varphi E)/K(D_\varphi)), d(K(\varphi^2 E)/K(D_{\varphi^2}))\},$$

and

$$t := d(L/K(\varphi, E)) .$$

Then we have

$$\#G_i(L/K) = \begin{cases} 8 & \textit{if } i < r \\ 4 & \textit{if } r \leq i < s \\ 2 & \textit{if } s \leq i < t \\ 1 & \textit{if } t \leq i \end{cases}$$

for all $i \in \mathbb{N}_0$.

PROOF.
Since $G_i(L/K)$ is a 2-group for $i > 0$, the only possible values for $\#G_i(L/K)$ are $1, 2, 4$, and 8. We now only have to apply the last four lemmata.
If $i < r$ then $G_1(L/K)$ must contain two automorphisms which send E to $E+1$, two which send E to $E+\varphi$ and another two which send E to $E+\varphi+1$. So we have $\#G_i(L/K) = 8$.
If $r \leq i < s$ then there is either no element of $G_1(L/K)$ which takes E to $E+1$ or no element which takes E to $E+\varphi$ or no element which takes E to $E+\varphi+1$. So we have $\#G_i(L/K) \leq 4$. On the other hand there must be two elements of $G_i(L/K)$ which take E to $E+1$, $E+\varphi$ or $E+\varphi+1$. Since $G_i(L/K)$ contains the identity element, we get $\#G_i(L/K) = 4$.
In the case $s \leq i < t$ the group $G_i(L/K)$ contains no automorphism which takes E to $E+1$, $E+\varphi$ or $E+\varphi+1$, but an automorphism σ with $\sigma(E) = E$ and $\sigma(F_\alpha) = F_\alpha + 1$. This gives us $\#G_i(L/K) = 2$.
In the case $t \leq i$ the group $G_i(L/K)$ contains only the identity element. $\square$

Lemma 5.7 *For all $i \in \mathbb{N}$ the fixed space $V^{G_i(L/K)}$ is either V or 0.*

(Recall that V is the representation space of $\pi_{\alpha,\beta}$.)
PROOF.
If $G_i(L/K)$ is trivial then we have $V^{G_i(L/K)} = V$. If $G_i(L/K)$ is not trivial then it contains an element σ which has order two. According to 5.1 we have $\sigma(E) = E$ and $\sigma(F_\alpha) = F_\alpha + 1$. Since σ leaves the values x_1, x_2, x_3, and x_4 invariant it has to act as the scalar -1 on the 3-torsion points. Applying [2, p. 70] gives us $\mathrm{Tr}(\rho^K_{\alpha,\beta}(\sigma)) = -2$. So $\rho^K_{\alpha,\beta}(\sigma)$ needs to be the scalar -1. Therefore $\pi_{\alpha,\beta}(\sigma)$ is a non-trivial scalar, so $V^{G_i(L/K)} = 0$. $\square$

Now we can state our main result.

Theorem 5.8 *Let*

$$r' := \min\{d(K(E)/K(D)t), d(K(\varphi E)/K(D_\varphi)), d(K(\varphi^2 E)/K(D_{\varphi^2}))\}\ ,$$

$$s' := \max\{d(K(E)/K(D)), d(K(\varphi E)/K(D_\varphi)), d(K(\varphi^2 E)/K(D_{\varphi^2}))\}\ ,$$

and

$$t' := d(L/K(\varphi, E))\ .$$

Further we define the numbers $r := \max\{r'-1, 0\}$, $s := \max\{s'-1, 0\}$, and $t := \max\{t'-1, 0\}$. Then we have

$$\mathrm{cond}(\pi_{\alpha,\beta}) = \begin{cases} 0 & \textit{if } L/K \textit{ is unramified} \\ 2 + \frac{8r+4(s+t)}{e(L/K)} & \textit{if } L/K \textit{ is ramified.} \end{cases}$$

PROOF.
If L/K is unramified then clearly $G_i(L/K) = \{1\}$ for all $i \geq 1$. Therefore $\mathrm{cond}(\pi_{\alpha,\beta}) = 0$. We now consider the case where L/K is ramified. Using the abbreviation $g_i := \# G_i(L/K)$ we have

$$\begin{aligned} \mathrm{cond}(\pi_{\alpha,\beta}) &= \frac{2}{e(L/K)} \sum_{i=0}^{t} g_i \\ &= 2 + \frac{2}{e(L/K)} \left(\sum_{i=1}^{r} g_i + \sum_{i=r+1}^{s} g_i + \sum_{i=s+1}^{t} g_i \right) \\ &= 2 + \frac{2}{e(L/K)} \left(8r + 4\,(s-r) + 2\,(t-s)\right) \\ &= 2 + \frac{8r + 4(s+t)}{e(L/K)}\,. \end{aligned}$$

$\square$

6 Concluding Remark

The descriptions of the higher ramification groups $G_i(L/K)$ in 5.6 and of the conductor of $\pi_{\alpha,\beta}$ in 5.8 are not quite explicit, since they depend on the calculation of the different exponents of the extensions

$$K(E)/K(D), \quad K(\varphi E)/K(D_\varphi), \quad K(\varphi^2 E)/K(D_{\varphi^2}), \quad \text{and} \quad L/K(\varphi, E)\,.$$

Therefore, we would like to add that there is a way to determine these differents by explicit calculations in K in dependence of β and α. These calculations, too involved to present here, are carried out in [1].

References

[1] J. Frieden, *Zur darstellungstheoretischen Beschreibung von elliptischen Kurven über lokalen Körpern der Charakteristik* 2, doctoral thesis, Universität des Saarlandes, Saarbrücken, 2004.

[2] I. Piatetski-Shapiro, *Complex Representations of* GL$(2, K)$ *for Finite Fields* K, Contemporary Mathematics **16**, Amer. Math. Soc. 1983.

[3] D. E. Rohrlich, *Elliptic Curves and the Weil-Deligne Group*, in: Elliptic Curves and Related Topics, CRM Proceedings & Lecture Notes **4**, ed. by H. Kisilevsky and R. Murty, Amer. Math. Soc. Providence, RI, 1994, S. 125-157.

[4] J-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[5] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.