Some write-ups on computing quaternion quotient graphs

Ralf Butenuth

February 22, 2010

Introduction

Contents

List of Figures

1 Quaternion quotient graphs

Let $k = \mathbb{F}_q$ be a finite field, $A = k[T]$ and $K = \mathrm{Quot}(A)$. Let v_∞ be the valuation on K defined as $v_\infty(\frac{f}{g}) = \deg(g) - \deg(f)$ for $f, g \in A \smallsetminus \{0\}$ and $v_\infty(0) = \infty$, and let K_∞ be the completion with respect to this valuation. We fix the uniformizer $\pi = \frac{1}{T}$ and view K_∞ as the field of formal Laurent series $k((\pi))$. Let O_∞ be the ring of integers in K_∞. For any finite place $\mathfrak{p}$ of K we let $K_\mathfrak{p}$ denote the completion of K at $\mathfrak{p}$, $O_{K_\mathfrak{p}}$ the ring of integers and $q_\mathfrak{p}$ the residue degree $[A/\mathfrak{p} : k]$.

1.1 Notation from graph theory

Definition 1.1 *(a) A (directed multi-)graph $\mathcal{G}$ is a pair $(\mathrm{Ver}(\mathcal{G}), \mathrm{Edg}(\mathcal{G}))$ where $\mathrm{Ver}(\mathcal{G})$ is a (possibly infinite) set and $\mathrm{Edg}(\mathcal{G})$ is a list of triples (v, v', i) with $v, v' \in \mathrm{Ver}(\mathcal{G})$ and $i \in \{0, \ldots, n_{(v,v')}\}$ with $n_{(v,v')} \in \mathbb{N}_0$, where we assume that to each $e = (v, v', i) \in \mathrm{Edg}(\mathcal{G})$ we have $e^\star := (v', v, i) \in \mathrm{Edg}(\mathcal{G})$ and that for each $v \in \mathrm{Ver}(\mathcal{G})$ the set*

$$\mathrm{Nbs}(v) := \{v' \in \mathrm{Ver}(\mathcal{G}) \mid (v, v', 0) \in \mathrm{Edg}(\mathcal{G})\}$$

is finite.

(b) A subgraph $\mathcal{G}' \subset \mathcal{G}$ is a pair of subsets $(\mathrm{Ver}(\mathcal{G}'), \mathrm{Edg}(\mathcal{G}'))$ with $\mathrm{Ver}(\mathcal{G}') \subseteq \mathrm{Ver}(\mathcal{G})$ and $\mathrm{Edg}(\mathcal{G}') \subseteq \mathrm{Edg}(\mathcal{G})$ such that $\mathcal{G}'$ is a graph.

An element $v \in \mathrm{Ver}(\mathcal{G})$ is called vertex, an element $e \in \mathrm{Edg}(\mathcal{G})$ is called (oriented) edge. The oriented edges (v, v', i) and (v', v, i) denote the same edge of $\mathcal{G}$ however with opposite orientation. For each edge $e = (v, v', i) \in \mathrm{Edg}(\mathcal{G})$ we call $o(e) := v$ the origin of e and $t(e) := v'$ the target of e. An edge with $o(e) = t(e)$ is called a loop. Two vertices v, v' are called adjacent, if there is an edge e such that $\{v, v'\} = \{o(e), t(e)\}$.

Definition 1.2 *(a) A graph $\mathcal{G}$ is finite, if $\# \mathrm{Ver}(\mathcal{G}) < \infty$.*

(b) For $v \in \mathrm{Ver}(\mathcal{G})$ the degree of v is defined as

$$\mathrm{degree}(v) := \sum_{v' \in \mathrm{Nbs}(v)} n_{(v,v')}.$$

(c) A graph $\mathcal{G}$ is called k-regular if for all vertices $v \in \mathrm{Ver}(\mathcal{G})$ we have $\mathrm{degree}(v) = k$.

(d) Let $v, v' \in \mathrm{Ver}(\mathcal{G})$. A finite path (or simply path) from v to v' is a finite subset $\{e_1, \ldots, e_k\}$ of $\mathrm{Edg}(\mathcal{G})$ such that $t(e_i) = o(e_{i+1})$ for all $i = 1, \ldots, k-1$ and $o(e_1) = v, t(e_k) = v'$. The integer k is called the length of the path $\{e_1, \ldots, e_k\}$.

(e) A graph $\mathcal{G}$ is connected if for any two vertices $v, v' \in \mathrm{Ver}(\mathcal{G})$ there is a finite path from v to v'.

(f) A path $\{e_1, \ldots, e_k\}$ is a path without backtracking if for all $i = 1, \ldots, k-1$ we have $e_{i+1} \neq e_i^\star$.

(g) A geodesic from v to v' of $\mathcal{G}$ is a finite path from v to v' without backtracking.

(h) A cycle of $\mathcal{G}$ is a geodesic from v to v for some vertex v.

(i) A graph $\mathcal{G}$ is cycle-free if it contains no cycles.

(j) A tree is a connected, cycle-free graph.

Note that if $\mathcal{G}$ is a tree, then for each two vertices $v, v' \in \mathrm{Ver}(\mathcal{G})$ there is exactly one geodesic between v and v'. In this case we call the length of the unique geodesic the distance from v to v', denoted by $d(v, v')$.

Definition 1.3 *(a) We define the first Betti number $h_1(\mathcal{G})$ of a finite connected graph to be*

$$h_1(\mathcal{G}) := \frac{\#\,\mathrm{Edg}(\mathcal{G})}{2} - \#\,\mathrm{Ver}(\mathcal{G}) + 1.$$

Any finite graph $\mathcal{G}$ can be viewed as an abstract simplicial complex, and one obtains in this way a topological space $|\mathcal{G}|$, the geometrical realization of $\mathcal{G}$. The first Betti number $h_1(\mathcal{G})$ is the dimension of $H^1(|\mathcal{G}|, \mathbb{Q})$. The Betti number of the graph $\mathcal{G}$ counts the number of independent cycles of $\mathcal{G}$.

1.2 The Bruhat-Tits tree

We will define a combinatorial object, the Bruhat-Tits tree of $\mathrm{PGL}_2(K_\infty)$, which plays an important role in the arithmetic of K:

Definition 1.4 *The graph $\mathcal{T}$, the Bruhat-Tits tree of $\mathrm{PGL}_2(K_\infty)$, is defined as follows: $\mathrm{Ver}(\mathcal{T})$ is the set of equivalence classes $\Lambda = [L]$ of O_∞-lattices in K_∞^2. For two such lattice classes $\Lambda, \Lambda' \in \mathrm{Ver}(\mathcal{T})$ we define $(\Lambda, \Lambda', 0) \in \mathrm{Edg}(\mathcal{T})$ if and only if there are $L \in \Lambda, L' \in \Lambda'$ such that $L' \subseteq L$ and $L/L' \cong k$.*

We have the following theorem:

Theorem 1.5 *The graph $\mathcal{T}$ is a $(q+1)$-regular tree.*

Proof: See [Se1, Chapter II.1]. ∎

Let $e_1 = (1, 0), e_2 = (0, 1)$ be the standard basis of K_∞^2. An O_∞-lattice $v_1 O_\infty \oplus v_2 O_\infty$ in K_∞^2 corresponds to a matrix $(v_1, v_2) \in \mathrm{GL}_2(K_\infty)$. Since $\mathrm{GL}_2(K_\infty)$ acts transitively on these matrices and $\mathrm{Stab}_{\mathrm{GL}_2(K_\infty)}(e_1 O_\infty \oplus e_2 O_\infty) = \mathrm{GL}_2(O_\infty)$, the set of O_∞-lattices in K_∞^2 is in bijection with $\mathrm{GL}_2(K_\infty)/\mathrm{GL}_2(O_\infty)$, and hence we obtain:

Proposition 1.6 *The map*

$$\begin{array}{rcl} \varphi : \mathrm{GL}_2(K_\infty)/\mathrm{GL}_2(O_\infty)K_\infty^\star & \to & \mathrm{Ver}(\mathcal{T}) \\ A & \mapsto & \left[(e_1, e_2) A O_\infty^2\right] \end{array}$$

is a bijection.

Our next goal is to identify the vertices in the tree with explicitly given matrices and to see, which matrices correspond to adjacent vertices in the tree. The next Lemmas will help us with that.

Lemma 1.7 *Every class of* $\mathrm{GL}_2(K_\infty)/\mathrm{GL}_2(O_\infty)K_\infty^\star$ *has a unique representative of the form*

$$\begin{pmatrix} \pi^n & g(\pi) \\ 0 & 1 \end{pmatrix}$$

with $n \in \mathbb{Z}$ *and* $g \in K_\infty/\pi^n O_\infty$.

We call this representative the vertex normal form of a matrix $\gamma \in \mathrm{GL}_2(K_\infty)$ or of the corresponding vertex $\varphi(\gamma)$.

Proof: Let $\gamma = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \in \mathrm{GL}_2(K_\infty)$. If $v_\infty(x_3) < v_\infty(x_4)$ we multiply from the right with $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ to swap the columns of γ. Hence we can assume $v_\infty(x_3) \geq v_\infty(x_4)$. Multiplying from the right with $\begin{pmatrix} 1 & 0 \\ -\frac{x_3}{x_4} & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_\infty)$ gives

$$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\frac{x_3}{x_4} & 1 \end{pmatrix} = \begin{pmatrix} x_1 - \frac{x_2 x_3}{x_4} & x_2 \\ 0 & x_4 \end{pmatrix}.$$

Multiplying with $x_4^{-1} \in K_\infty^\star$ we obtain an equivalent matrix of the form

$$\begin{pmatrix} z_1 & z_2 \\ 0 & 1 \end{pmatrix}.$$

Write $z_1 = \pi^n \varepsilon$ with $\varepsilon \in \mathcal{O}_\infty^\star$ and multiply from the right with $\begin{pmatrix} \varepsilon^{-1} & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_\infty)$ to obtain a matrix of the form $\begin{pmatrix} \pi^n & y \\ 0 & 1 \end{pmatrix}$.
If we have

$$\begin{pmatrix} \pi^n & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \pi^m & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} \pi^m r + bt & \pi^m s + bu \\ t & u \end{pmatrix}$$

with $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathcal{O}_\infty)K_\infty^\star$, we conclude from the last row $u = 1, t = 0$ and hence $r = 1$ and $m = n$. The entry in the upper right corner is therefore only determined up to $\pi^n \mathcal{O}_\infty$. ∎

Remark 1.8 The proof of the previous Lemma was constructive and gives us an algorithm to compute the vertex normal form of a matrix γ.

Lemma 1.9 *Let* A *and* B *be the two matrices*

$$A := \begin{pmatrix} \pi^n & g(\pi) \\ 0 & 1 \end{pmatrix}, B := \begin{pmatrix} \pi^{n+1} & g(\pi) + \alpha\pi^n \\ 0 & 1 \end{pmatrix}$$

with $n \in \mathbb{Z}, \alpha \in k, g \in K_\infty/\pi^n O_\infty$ *and let* L_1 *and* L_2 *be the two lattices*

$$L_1 := (e_1, e_2)A, L_2 := (e_1, e_2)B.$$

Then $L_1 \supset L_2$ *and* $L_1/L_2 \cong k$.

Proof: Set

$$v_1 = \begin{pmatrix} \pi^n \\ 0 \end{pmatrix} \text{ and } v_2 = \begin{pmatrix} g(\pi) \\ 1 \end{pmatrix}.$$

Then $L_1 = \langle v_1, v_2 \rangle_{O_\infty}$ and $L_2 = \langle \pi v_1, v_2 + \alpha v_1 \rangle_{O_\infty}$. Hence

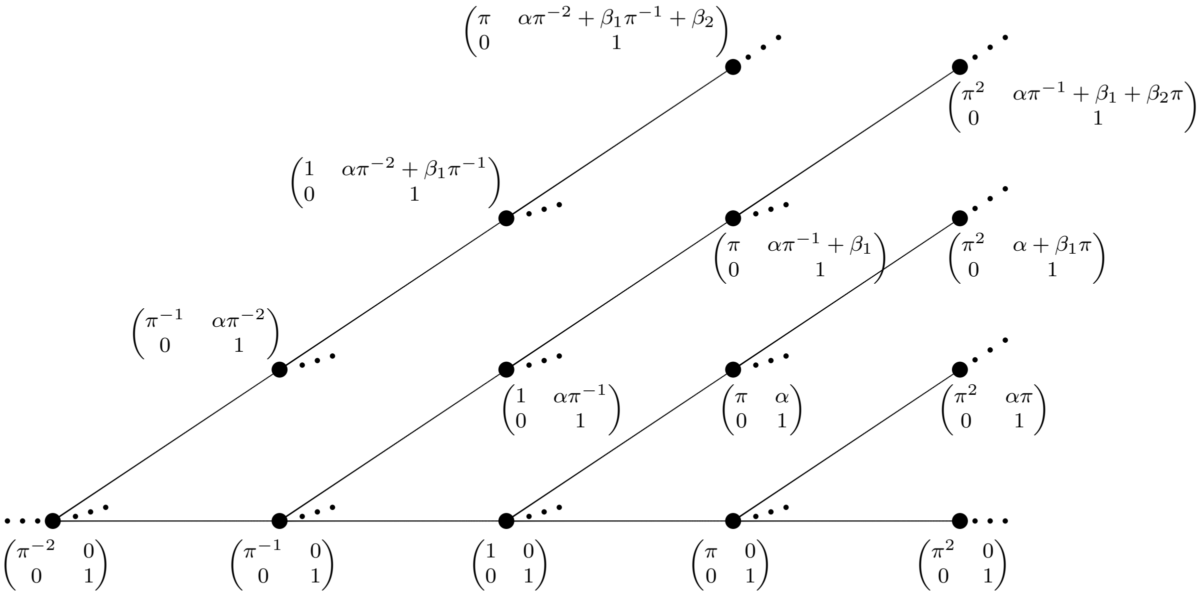
$$L_1 \supseteq L_2 \supseteq \pi L_1.$$

But $v_1 \notin L_2$ and $v_2 + \alpha v_1 \notin \pi L_1$, so

$$L_1 \supsetneq L_2 \supsetneq \pi L_1$$

and therefore $L_1/L_2 \cong k$. ∎

Using the Lemma we find $q+1$ adjacent vertices to a vertex corresponding to a given matrix γ of the form $\begin{pmatrix} \pi^n & g(\pi) \\ 0 & 1 \end{pmatrix}$. Since we know that every vertex has exactly $q+1$ adjacent vertices, these have to be all adjacent vertices of γ. In Figure 1 we have illustrated the tree together with the matrices corresponding to vertices. Note that each line in the picture symbolizes actually a whole fan expanding to the right. The elements $\alpha \in k^\star$, $\beta \in k$ agree on each fan.


$\begin{pmatrix} \pi & \alpha\pi^{-2}+\beta_1\pi^{-1}+\beta_2 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi^2 & \alpha\pi^{-1}+\beta_1+\beta_2\pi \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & \alpha\pi^{-2}+\beta_1\pi^{-1} \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi & \alpha\pi^{-1}+\beta_1 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi^2 & \alpha+\beta_1\pi \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi^{-1} & \alpha\pi^{-2} \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & \alpha\pi^{-1} \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi & \alpha \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi^2 & \alpha\pi \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi^{-2} & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi^{-1} & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} \pi^2 & 0 \\ 0 & 1 \end{pmatrix}$

with $\alpha \in k^\star$, $\beta_i \in k$ compatibly chosen

Figure 1: The tree $\mathcal{T}$ with the corresponding matrices

Notation 1.10 *In text-mode we write $L(n, g(\pi))$ for the O_∞-lattice $\langle v_1, v_2 \rangle_{O_\infty}$ where $v_1 = \begin{pmatrix} \pi^n \\ 0 \end{pmatrix}$ and $v_2 = \begin{pmatrix} g(\pi) \\ 1 \end{pmatrix}$.*

1.3 Quaternion algebras

Let K denote for a moment an arbitrary field.

Definition 1.11 *A quaternion algebra D over K is a central simple algebra of dimension 4 over K.*

There is a unique anti-involution $^- : D \to D$ such that $\gamma + \bar{\gamma}$ and $\gamma\bar{\gamma}$ are in K for all $\gamma \in D$. This map is called conjugation on D and we can use it to define the reduced trace and norm of an element $\gamma \in D$ as $\mathrm{trd}(\gamma) := \gamma + \bar{\gamma}$ and $\mathrm{nrd}(\gamma) := \gamma\bar{\gamma}$.

Definition 1.12 *Let $a, b \in K^\star$. We define $\left(\frac{a,b}{K}\right)$ to be the K-algebra with basis $1, i, j, ij$ and relations*

- $i^2 = a, j^2 = b, ij = -ji$ *for* $\mathrm{char}(K) \neq 2$ *and*
- $i^2 + i = a, j^2 = b, ij = j(i+1)$ *for* $\mathrm{char}(K) = 2$.

It is not hard to show, that any quaternion algebra over K is isomorphic to $\left(\frac{a,b}{K}\right)$ for some $a, b \in K$, see [Vi, Chapitere I.1] or [JS, Kapitel IX] for $\mathrm{char}(K) \neq 2$. Any $\gamma \in \left(\frac{a,b}{K}\right)$ can be uniquely written as $\gamma = \lambda_1 + \lambda_2 i + \lambda_3 j + \lambda_4 ij$ with $\lambda_i \in K$.
For $\mathrm{char}(K) \neq 2$ the anti-involution is given by $\bar{\gamma} = \lambda_1 - \lambda_2 i - \lambda_3 j - \lambda_4 ij$ and we compute $\mathrm{trd}(\gamma) = 2\lambda_1$ and $\mathrm{nrd}(\gamma) = \lambda_1^2 - a\lambda_2^2 - b\lambda_3^2 + ab\lambda_4^2$.
For $\mathrm{char}(K) = 2$ the anti-involution is given by $\bar{\gamma} = \lambda_1 + \lambda_2(i+1) + \lambda_3 j + \lambda_4 ij$ and we compute $\mathrm{trd}(\gamma) = \lambda_2$ and $\mathrm{nrd}(\gamma) = \lambda_1^2 + a\lambda_2^2 + b\lambda_3^2 + ab\lambda_4^2 + \lambda_1\lambda_2 + b\lambda_3\lambda_4$.
The norm map of the quaternion algebra $\left(\frac{a,b}{K}\right)$ gives us a quadratic form $Q_{a,b} : (\lambda_1, \ldots, \lambda_4) \mapsto \mathrm{nrd}(\lambda_1 + \lambda_2 i + \lambda_3 j + \lambda_4 ij)$.
Any quaternion algebra is either a division algebra or isomorphic to $M_2(K)$ (see [JS, Satz 1.4, IX]) and we have the following proposition:

Proposition 1.13 *Suppose* $\mathrm{char}(K) \neq 2$. *Then the following are equivalent:*

(a) $D := \left(\frac{a,b}{K}\right) \cong M_2(K)$

(b) There is an $x \in D$, $x \neq 0$, with $\mathrm{nrd}(x) = 0$.

(c) The quadratic form $Q_{a,b}$ is isotropic, i.e. there are $(x, y, v, w) \in K^4 \setminus \{(0,0,0,0)\}$ with $Q_{a,b}(x, y, v, w) = 0$.

(d) The equation $Z^2 - aX^2 - bY^2 = 0$ has a non-trivial solution over K.

(e) $a \in \mathrm{Image}(\mathrm{Norm}(K(\sqrt{b})/K)$

(f) $b \in \mathrm{Image}(\mathrm{Norm}(K(\sqrt{a})/K)$

Proof: See [JS, Satz 1.9, Chapter IX]. ∎

Now let K be a global field and $\mathfrak{p}$ a place of K.

Definition 1.14 *A quaternion algebra D over K is ramified at $\mathfrak{p}$ if and only if $D \otimes_K K_\mathfrak{p}$ is a division algebra.*

We define the Hilbert symbol of a pair $(a, b) \in K^2$ at a place $\mathfrak{p}$ as follows:

Definition 1.15

$$(a,b)_{K_\mathfrak{p}} := \begin{cases} +1 & \left(\frac{a,b}{K}\right) \text{ is unramified at } \mathfrak{p} \\ -1 & \left(\frac{a,b}{K}\right) \text{ is ramified at } \mathfrak{p}. \end{cases}$$

Now let K again be the field $k(T)$ where $k = \mathbb{F}_q$.

Definition 1.16 *Let a, ϖ be in $k[T]$ with ϖ irreducible. Define the Legendre symbol of a and ϖ as*

$$\left(\frac{a}{\varpi}\right) := \begin{cases} 1 & a \neq 0 \textit{ and } a \textit{ is a square modulo } \varpi \\ -1 & a \textit{ is a non-square modulo } \varpi \\ 0 & \varpi \textit{ divides } a. \end{cases}$$

The proof of the next proposition is the adaptation to the function-field situation of [Se2, Chapter III, Theorem 1].

Proposition 1.17 *Suppose q is odd. Write $\mathfrak{p} = (\varpi)$ and let $a = \varpi^\alpha u, b = \varpi^\beta v$ with $u, v \in O^\star_{K_\mathfrak{p}}, \alpha, \beta \in \mathbb{Z}$ and let $\varepsilon(\mathfrak{p}) := \frac{q-1}{2}\deg(\varpi) \pmod 2$. Then*

$$(a, b)_{K_\mathfrak{p}} = (-1)^{\alpha\beta\varepsilon(\mathfrak{p})} \left(\frac{u}{\varpi}\right)^\beta \left(\frac{v}{\varpi}\right)^\alpha.$$

Proof: In the proof we write (a, b) for $(a, b)_{K_\mathfrak{p}}$.
The right hand side of the equation clearly depends only on $\alpha \pmod 2$ and $\beta \pmod 2$. If $Q_{a,b}$ is isotropic, then so are $Q_{\varpi^2 a,b}, Q_{a,\varpi^2,b}$ and vice versa. Hence the left hand side also only depends on $\alpha \pmod 2$ and $\beta \pmod 2$. Because of symmetry we only need to consider the three cases $(\alpha, \beta) = (0, 0)$, $(\alpha, \beta) = (1, 0)$ and $(\alpha, \beta) = (1, 1)$.
Case one: $(\alpha, \beta) = (0, 0)$: Here the right hand side is 1, so we have to show that $Z^2 - uX^2 - vY^2$ has a solution in $K_\mathfrak{p}$. But $Z^2 - uX^2 - vY^2$ has a solution modulo ϖ, since all quadratic forms in at least three variables over a finite field have a non-trivial solution (see [Se2, Chapter I.2, Cor. 2]). Since $\mathrm{disc}(Z^2 - uX^2 - vY^2) \in O^\star_{K_\mathfrak{p}}$, this solution lifts to $O_{K_\mathfrak{p}}$ by Hensel's Lemma.
Case two: $(\alpha, \beta) = (1, 0)$: We must check that $(\varpi u, v) = \left(\frac{v}{\varpi}\right)$, From case one we know that $(u, v) = 1$, hence $u \in \mathrm{Image}(\mathrm{Norm}(K_\mathfrak{p}(\sqrt{v})/K_\mathfrak{p})$ and we have $\varpi \in \mathrm{Image}(\mathrm{Norm}(K_\mathfrak{p}(\sqrt{v})/K_\mathfrak{p})$ if and only if $u\varpi \in \mathrm{Image}(\mathrm{Norm}(K_\mathfrak{p}(\sqrt{v})/K_\mathfrak{p})$.
So $(\varpi u, v) = (\varpi, v)$ and we may assume $u = 1$. If $v = (v')^2$ is a square in $K_\mathfrak{p}$, then clearly $\left(\frac{v}{\varpi}\right) = 1$ and also $(v', 0, 1)$ is a non-trivial solution of $Z^2 - \varpi X^2 - vY^2 = 0$, so $(\varpi, v) = 1$. Let v be a non-square in $K_\mathfrak{p}$. Since $v \in O^\star_{K_\mathfrak{p}}$, this is equivalent to $\left(\frac{v}{\varpi}\right) = -1$. Suppose $Z^2 - \varpi X^2 - vY^2$ has a non-trivial solution (z, x, y). By normalizing we can assume that (z, x, y) is primitive, i.e. $(z, x, y) \in O_{K_\mathfrak{p}}$, and at least one of them is in $O^\star_{K_\mathfrak{p}}$. Suppose either $z \equiv 0 \pmod \varpi$ or $y \equiv 0 \pmod \varpi$. Then since $z^2 - vy^2 \equiv 0 \pmod \varpi$ and $v \not\equiv 0 \pmod \varpi$ we obtain both $z \equiv 0 \pmod \varpi$ and $y \equiv 0 \pmod \varpi$ and hence $\varpi x^2 \equiv 0 \pmod{\varpi^2}$, so $x \equiv 0 \pmod \varpi$. Therefore (z, x, y) was not primitive. So both z and y have to be non-zero modulo ϖ. Reducing $z^2 - \varpi x^2 - vy^2$ modulo ϖ we obtain $\left(\frac{v}{\varpi}\right) = 1$, which is a contradiction. So $Z^2 - \varpi X^2 - vY^2$ has no non-trivial solution, and hence $(\varpi, v) = -1$.
Case three: $(\alpha, \beta) = (1, 1)$: We must check that $(\varpi u, \varpi v) = (-1)^{\varepsilon(\mathfrak{p})} \left(\frac{u}{\varpi}\right)\left(\frac{v}{\varpi}\right)$. But since $Q_{\varpi u, -\varpi u}$ is isotropic we have

$$\varpi v \in \mathrm{Image}(\mathrm{Norm}(K_\mathfrak{p}(\sqrt{\varpi u})/K_\mathfrak{p}) \Leftrightarrow -\varpi^2 uv \in \mathrm{Image}(\mathrm{Norm}(K_\mathfrak{p}(\sqrt{\varpi u})/K_\mathfrak{p})$$

and hence

$$(\varpi u, \varpi v) = (\varpi u, -\varpi^2 uv) = (\varpi u, -uv),$$

so we can apply case two and see that

$$(\varpi u, \varpi v) = (\varpi u, -uv) = \left(\frac{-uv}{\varpi}\right) = \left(\frac{-1}{\varpi}\right)\left(\frac{u}{\varpi}\right)\left(\frac{v}{\varpi}\right) = (-1)^{\frac{q-1}{2}\deg(\varpi)}\left(\frac{u}{\varpi}\right)\left(\frac{v}{\varpi}\right).$$

∎

Let D be an indefinite quaternion algebra over K. Indefinite means that D is unramified at the place ∞, i.e. $D \otimes_K K_\infty \cong M_2(K_\infty)$. Let R denote the set of all ramified places of D.

Proposition 1.18 *The number of places in R is finite and even and D is up to isomorphism uniquely determined by R.*

Proof: See [Vi, Lemme III.3.1 and Theoreme III.3.1]. ∎

Let r be a monic generator of the ideal $\mathfrak{r} := \prod_{\mathfrak{p}\in R}\mathfrak{p}$. The ideal $\mathfrak{r}$ is called the discriminant of D.
An order of D is a free $k[T]$-submodule of rank 4 in D that is also a ring. An order Λ of D is called maximal if it is not properly contained in any other order of D. For any 4 elements $\gamma_1, \ldots, \gamma_4 \in D$ let $\mathrm{disc}(\gamma_1, \ldots, \gamma_4) := \det(\mathrm{trd}(\gamma_i\gamma_j))_{i,j=1,\ldots,4}$. For any order Λ of D the ideal of $k[T]$ generated by the set $\{\mathrm{disc}(\gamma_1, \ldots, \gamma_4) \mid \gamma_i \in \Lambda\}$ is a square (see [Vi, Lemme I.4.7], and we define the reduced discriminant $\mathrm{disc}(\Lambda)$ to be the square root of this ideal. Since $k[T]$ is a principal ideal domain, for any $k[T]$-basis $\{\gamma_1, \ldots, \gamma_4\}$ of Λ the element $\mathrm{disc}(\gamma_1, \ldots, \gamma_4)$ generates the ideal $\langle\{\mathrm{disc}(\gamma_1, \ldots, \gamma_4) \mid \gamma_i \in \Lambda\}\rangle_{k[T]}$. An order Λ of D is maximal if and only if $\mathrm{disc}(\Lambda) = \mathfrak{r}$, see [Vi, Corollaire III.5.3]. Since D is split at infinity and since K has class number 1, a maximal order Λ of D is unique up to conjugation, i.e. for any other maximal order Λ' we have $\Lambda' = \gamma\Lambda\gamma^{-1}$ for an $\gamma \in D^\star$, see [Vi, Corollaire III.5.7].
Let $\Gamma = \Gamma(\Lambda) = \{\gamma \in \Lambda \mid \mathrm{nrd}(\gamma) \in k^\star\}$. Since D is unramified at K_∞ we have $D \otimes_K K_\infty \cong M_2(K_\infty)$ and we obtain an embedding $\iota : D \hookrightarrow M_2(K_\infty)$. Via this embedding Γ is a subgroup of $\mathrm{SL}_2(K_\infty)\begin{pmatrix} k^\star & 0 \\ 0 & 1 \end{pmatrix} \subseteq \mathrm{GL}_2(K_\infty)$.
The following Proposition is well known. We give a proof for the sake of completeness.

Proposition 1.19 *Γ is a discrete subgroup of $\mathrm{GL}_2(K_\infty)$.*

Proof: The open sets $\{\pi^n M_2(O_\infty) \mid n \in \mathbb{N}\}$ form a basis of open neighbourhoods of 0 in $M_2(K_\infty)$. Hence it suffices to show that $\Lambda \cap \pi^n M_2(O_\infty)$ is finite for all $n \in \mathbb{N}$. To Λ we can associate a locally free coherent sheaf $\mathcal{D}$ over $\mathbb{P}^1_k$ with generic fibre D and such that for each open set $U \subset \mathbb{P}^1_k$ we have

$$\mathcal{D}(U) := \bigcap_{x\in U}((\Lambda \otimes_K K_x) \cap D)$$

with K_x the completion of K at x. Then

$$\mathcal{D}_x = (\Lambda \otimes_K K_x) \cap D$$

for all $x \in \mathbb{P}^1_k$ and

$$\Lambda \cap \pi^n M_2(O_\infty) = H^0(\mathbb{P}^1_k, \mathcal{D}(-n\infty)),$$

and since $\mathcal{D}(-n\infty)$ is a coherent vector bundle of rank 4 over $\mathbb{P}^k_1$ the dimension of $H^0(\mathbb{P}^1_k, \mathcal{D}(-n\infty))$ as a k-vector space is finite. ∎

We have a natural action of $\mathrm{GL}_2(K_\infty)$ and hence of Γ on $\mathcal{T}$. The goal of this chapter is to understand the structure of $\Gamma\backslash\mathcal{T}$ and to give an explicit algorithm to compute this quotient graph.

1.4 Facts about quaternion quotient graphs

In this section we gather some known results about the quotient graph $\Gamma\backslash\mathcal{T}$. The results are all taken from [Pa].

Lemma 1.20 *Let $v \in \mathrm{Ver}(\mathcal{T})$ and $\gamma \in \Gamma$. Than $d(v, \gamma v)$ is even.*

Proof: See [Se1, Corollary of Proposition II.1]. ∎

Proposition 1.21 *$\Gamma\backslash\mathcal{T}$ is a finite graph, meaning $\#\mathrm{Ver}(\mathcal{T})$ and $\#\mathrm{Edg}(\mathcal{T})$ are finite.*

Proof: See [Pa, Prop. 3.1]. ∎

Proposition 1.22 *Let $v \in \mathrm{Ver}(\mathcal{T})$ and $e \in \mathrm{Edg}(\mathcal{T})$. Then $\Gamma_v := \mathrm{Stab}_\Gamma(v)$ is either isomorphic to $\mathbb{F}_q^\star$ or $\mathbb{F}_{q^2}^\star$ and $\Gamma_e := \mathrm{Stab}_\Gamma(e)$ is isomorphic to $\mathbb{F}_q^\star$.*

Proof: See [Pa, Prop. 3.2]. ∎

We call a vertex v projectively stable if $\Gamma_v \cong \mathbb{F}_q^\star$ and a projectively unstable if $\Gamma_v \cong \mathbb{F}_{q^2}^\star$.

Corollary 1.23 *Let $v \in \mathrm{Ver}(\mathcal{T})$ be projectively unstable. Then Γ_v acts transitively on the vertices adjacent to v.*

Let

$$\mathrm{odd}(R) := \begin{cases} 0 & \text{if some place in } R \text{ has even degree,} \\ 1 & \text{otherwise} \end{cases}$$

and let

$$g(R) := 1 + \frac{1}{q^2-1}\prod_{\mathfrak{p}\in R}(q_\mathfrak{p} - 1) - \frac{q}{q+1}2^{\#R-1}\,\mathrm{odd}(R).$$

Let $\pi : \mathcal{T} \to \Gamma\backslash\mathcal{T}$ be the natural projection.

Theorem 1.24 *(a) The graph $\Gamma\backslash\mathcal{T}$ has no loops.*

(b) $h_1(\Gamma\backslash\mathcal{T}) = g(R)$.

(c) For $\bar{v} \in \Gamma\backslash\mathcal{T}$ and $v \in \pi^{-1}(\bar{v})$ we have: $\bar{v}$ is a terminal vertex if and only if v is projectively unstable and $\bar{v}$ has degree $q+1$ if and only if v is projectively stable.

(d) Let V_1 and V_{q+1} be the number of terminal and degree $q+1$ vertices of $\Gamma\backslash\mathcal{T}$. Then

$$V_1 = 2^{\#R-1}\,\mathrm{odd}(R) \text{ and } V_{q+1} = \frac{1}{q-1}(2g(R) - 2 + V_1).$$

Proof: See [Pa, Theorem 3.4] ∎

1.5 An algorithm to compute the quotient graph

In this and the following section we give an algorithm to compute the quotient graph $\Gamma\backslash\mathcal{T}$.

Remark 1.25 For any group G acting on a set X we can define a category $\mathcal{C}_G(X)$ with $\mathrm{Obj}(\mathcal{C}_G(X)) := X$ and

$$\mathrm{Hom}_G(x, y) := \{\gamma \in G \mid gx = y\} \subseteq G.$$

The composition of morphisms is given by multiplication in G. We will use this notation. Note that

$$\mathrm{End}_G(x) := \mathrm{Hom}_G(x, x) = \mathrm{Stab}_G(x).$$

In this section we assume that we can compute $\mathrm{Hom}_\Gamma(v, w)$ effectively for all $v, w \in \mathrm{Ver}(\mathcal{T})$. Under this assumption the following algorithm computes the quotient graph $\Gamma\backslash\mathcal{T}$ and even a fundamental domain for the action of Γ on $\mathcal{T}$. The algorithm also attaches labels to some vertices and edges, these labels will be needed for a reduction algorithm from $\mathcal{T}$ to the fundamental domain.

Algorithm 1.26

- *Start with any projectively stable vertex v and initialize a list* $\mathrm{CurrentVertList} := [(v, v_1), \ldots, (v, v_{q+1})]$ *where v_i are all adjacent vertices of v. Initialize a graph $\mathcal{G}$ with $\mathrm{Ver}(\mathcal{G}) = \{v\}$ and $\mathrm{Edg}(\mathcal{G}) = \varnothing$. Initialize* $\mathrm{NextVertList} := \varnothing$.
- *While* CurrentVertList *is not empty:*
- *For $i = 1$ to $\#\,\mathrm{CurrentVertList}$ do:*
  - ○ *Set $v_i := \mathrm{CurrentVertList}[i][2]$ and $v_i' := \mathrm{CurrentVertList}[i][1]$.*
  - ○ *If the vertex v_i is projectively unstable, then add the vertex v_i and an edge from v_i' to v_i to $\mathcal{G}$. This can be checked by testing whether $\#\,\mathrm{End}_\Gamma(x) = q^2 - 1$. We also store $\mathrm{End}_\Gamma(x)$ as a vertex label for v_i. Further remove (v_i', v_i) from* CurrentVertList.
  - ○ *If the vertex v_i is projectively stable, then check for all $j < i$ and $v_j := \mathrm{CurrentVertList}[j][2]$ whether $\Gamma v_j = \Gamma v_i$. This can be done by testing whether $\#\,\mathrm{Hom}_\Gamma(v_i, v_j) = q - 1$. If we found such a vertex v_j, then add an edge from v_i' to v_j to $\mathcal{G}$. We also store any element $\gamma \in \mathrm{Hom}_\Gamma(v_i, v_j)$ as an edge label for this edge (they only differ by $k^\star$). Remove (v_i', v_i) from* CurrentVertList. *Compute $\gamma v_i'$ using algorithm 1.8 and remove $(v_j, \gamma v_i')$ from* NextVertList. *If, after adding the edge to v_j, the degree of v_j is $q + 1$, then also remove (v_j', v_j) from* CurrentVertList *(where $v_j' := \mathrm{CurrentVertList}[j][1]$).*
  - ○ *If v_i is projectively stable and for all $j < i$ we have $\Gamma v_j \neq \Gamma v_i$, then add the vertex v_i and an edge from v_i' to v_i to $\mathcal{G}$. For all adjacent vertices $w \neq v_i'$ of v_i add (v_i, w) to* NextVertList.
- *If we are done with the for-loop set* $\mathrm{CurrentVertList} := \mathrm{NextVertList}$ *and* $\mathrm{NextVertList} := \varnothing$.

- *If* CurrentVertList *is empty return* $\mathcal{G}$.

Proposition 1.27 *Algorithm 1.26 computes the quotient graph* $\Gamma\backslash\mathcal{T}$.

Proof: Let $\mathcal{G}$ be the output of algorithm 1.26. We need to show that any two distinct vertices and edges in $\mathcal{G}$ are not Γ-equivalent and that for all $v \in \mathcal{T}$ there is a vertex $v' \in \mathcal{G}$ such that $\Gamma v = \Gamma v'$.
For the first assertion: Let $v_1, v_2 \in \mathrm{Ver}(\mathcal{G})$ and suppose $\gamma v_1 = v_2$ for $\gamma \in \Gamma$.
We distinguish two cases:
Case one: If v_1 is projectively unstable, then since

$$\mathrm{Stab}_\Gamma(v_2) = \gamma\,\mathrm{Stab}_\Gamma(v_1)\gamma^{-1} \tag{1}$$

v_2 also has to be projectively unstable. Hence both v_1 and v_2 are terminal vertices in $\mathcal{G}$. Let v_1' and v_2' be their unique adjacent vertices in $\mathcal{G}$. Since v_1' is adjacent to v_1, we see that $\gamma v_1'$ is adjacent to $\gamma v_1 = v_2$. We know that $\mathrm{Stab}_\Gamma(v_2)$ acts transitively on the vertices adjacent to v_2. Hence there is a matrix γ' in $\mathrm{Stab}_\Gamma(v_2)$ with $\gamma'\gamma v_1' = v_2'$, so v_1' and v_2' are Γ-equivalent. If v_1' and v_2' were also projectively unstable and therefore terminal vertices in $\mathcal{G}$, then since $\mathcal{G}$ is connected $\mathcal{G}$ would have to be the graph containing the two vertices v_1, v_2 and one edge connecting them. But then v_1 and v_2 have distance one, so by Lemma 1.20 they cannot be Γ-equivalent.
So v_1' and v_2' are projectively stable Γ-equivalent vertices and we can reduce this case to case two.
Case two:
If v_1 is projectively stable, then by equation (1) also v_2. Let v be the initial vertex of the algorithm and let $i_1 = d(v, v_1), i_2 = d(v, v_2)$. W.l.o.g. assume $i_1 \geq i_2$. We proof the assertion by induction over i_1: If $i_1 = 1$ then also $i_2 = 1$ ($i_2 = 0$ is not possible because of Lemma 1.20). Hence the vertices v_1 and v_2 both have the same distance 1 from v and since $\mathrm{Hom}_\Gamma(v_1, v_2) = q - 1$ they cannot be both in $\mathcal{G}$, which is a contradiction. The same reasoning rules out $i_1 = i_2$ for any $i_1, i_2 \geq 1$.
Suppose $i_1 > 1$. By Lemma 1.20 and the above observation we have $i_1 = i_2 + 2m$ for some $m \in \mathbb{N}_{\geq 1}$. For $j \in \{1, 2\}$ let v_j' be the vertex on the geodesic from v_j to v with $d(v, v_j') = i_j - 1$. Then by the construction of $\mathcal{G}$ we have $v_j' \in \mathcal{G}$. The vertex $\gamma v_1'$ is adjacent to $\gamma v_1 = v_2$. Hence $\gamma v_1'$ is either v_2' or an vertex v_2'' adjacent to v_2 with $d(v, v_2'') = i_2 + 1$.
We distinguish three cases:
Case I: $\gamma v_1' = v_2'$: In this case since $d(v, v_1') = i_1 - 1, \gamma v_1' = v_2'$ and $v_1', v_2' \in \mathcal{G}$ we can use the induction hypothesis to obtain a contradiction.
Case II: $d(v, \gamma v_1') = i_2 + 1$ and $\gamma v_1' \in \mathcal{G}$: In this case since $d(v, v_1') = i_1 - 1, d(v, \gamma v_1') = i_2 + 1 \leq i_1 - 1$ and $v_1', \gamma v_1' \in \mathcal{G}$ we can use the induction hypothesis to obtain a contradiction.
Case III: $d(v, \gamma v_1') = i_2 + 1$ and $\gamma v_1' \notin \mathcal{G}$: In this case, since $\gamma v_1'$ is adjacent to v_2 and $v_2 \in \mathcal{G}$, by construction of $\mathcal{G}$ there is a $\gamma' \in \Gamma$ such that $\gamma'\gamma v_1' \in \mathcal{G}$ and $d(v, \gamma'\gamma v_1') = i_2 + 1$. So we are reduced to case II.
We showed that any two vertices in $\mathcal{G}$ are not Γ-equivalent. But since for every edge e of $\mathcal{G}$ at least one of the vertices $\{o(e), t(e)\}$ has degree $q + 1$ (except for the case that $\mathcal{G}$ consist of only one edge), this also implies that two edges in $\mathcal{G}$ are not Γ-equivalent.

For the second assertion:

We already showed, that there are no Γ-equivalent vertices or edges in $\mathcal{G}$. Hence $\mathcal{G}$ is a subgraph of $\Gamma\backslash\mathcal{T}$. But since each vertex in $\mathcal{G}$ is either projectively unstable or has $q+1$ adjacent vertices in $\mathcal{G}$, we deduce that $\mathcal{G}$ is a connected component of $\Gamma\backslash\mathcal{T}$. But $\Gamma\backslash\mathcal{T}$ is connected, hence $\mathcal{G} = \Gamma\backslash\mathcal{T}$. ∎

We further need an algorithm to compute for any $v \in \mathrm{Ver}(\mathcal{T})$ a Γ-equivalent vertex $v' \in \mathcal{G}$. This can be done in time linear to the distance of v to $\mathcal{G}$. For this algorithm we only need the stabilizers of the terminal vertices of $\mathcal{G}$ and the elements $\gamma \in \mathrm{Hom}_\Gamma(v_i, v_j)$, which we both stored as vertex and edge labels during the computation of $\mathcal{G}$. We call this algorithm the reduction algorithm:

Algorithm 1.28 *Let $\mathcal{G}$ be the output of algorithm 1.26 with initial vertex v. Let v' be any vertex in $\mathrm{Ver}(\mathcal{T})$ and consider the geodesic $\mathcal{T}_0 : (v' = v_m, v_{m-1}, \ldots, v)$ from v' to v. Let v_i be the vertex of $\mathcal{T}_0 \cap \mathcal{G}$ closest to v. We call $r = m - i$ the distance from v to $\mathcal{G}$.*
If $r = 0$ we have $v' \in \mathcal{G}$. In this case return $(v', 1)$.
If $r > 0$ distinguish two cases:
Case I: If v_i is projectively unstable, then there is a matrix $\gamma \in \mathrm{Stab}_\Gamma(v_i)$ that maps v_{i+1} to a vertex of $\mathcal{G}$. The vertex γv then has shorter distance to $\mathcal{G}$ then v, since of the vertices $(\gamma v, \gamma v_{m-1}, \ldots, \gamma v_{i+1}, \gamma v_i = v_i)$ at least the last two belong to $\mathcal{G}$. Hence we can replace v by γv and apply the algorithm recursively to get some $(w, \tilde{\gamma})$. We then return $(w, \gamma\tilde{\gamma})$.
Case II: If v_i is projectively stable, then since v_{i+1} is not in $\mathcal{G}$ but adjacent to v_i, there has to be an edge in $\mathcal{G}$ connecting some v' and v_{i-1} in $\mathcal{G}$ which is labelled with a matrix $\gamma \in \Gamma$ such that $\gamma v' = v_{i+1}$. Then of the vertices $(\gamma^{-1}v, \gamma^{-1}v_{m-1}, \ldots, \gamma^{-1}v_{i+1} = v')$ at least $\gamma^{-1}v_{i+1}$ is in $\mathcal{G}$, so $\gamma^{-1}v$ has shorter distance to $\mathcal{G}$ then v, so again we apply the algorithm recursively on $\gamma^{-1}v$ to get some $(w, \tilde{\gamma})$. We then return $(w, \gamma^{-1}\tilde{\gamma})$.

Proposition 1.29 *Let v' in $\mathcal{T}$ and $\mathcal{G}$ the output of algorithm 1.26 with initial vertex v. Then algorithm 1.28 computes a Γ-equivalent vertex w of v' and an element $\gamma \in \Gamma$ with $\gamma v' = w$ in time $\mathcal{O}(n)$ where n is the distance of v' to $\mathcal{G}$.*

Proof: Since at each step of the algorithm the distance $d(v', \mathcal{G})$ gets smaller, the algorithm terminates and needs at most $d(v', \mathcal{G})$ steps. It is then clear that the algorithm returns an Γ-equivalent vertex $w \in \mathcal{G}$ and a matrix $\gamma \in \Gamma$ with $\gamma v' = w$. ∎

Example 1.30 In Figure 2 we give an example of the algorithm 1.26, where $k = \mathbb{F}_5$ and $r = T * (T+1) * (T+2) * (T+3)$. We start with $\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$ as the initial vertex v. The adjacent vertices are corresponding to the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is a terminal vertex, and the five vertices corresponding to $\begin{pmatrix} \pi^2 & \alpha\pi \\ 0 & 1 \end{pmatrix}$ with $\alpha \in k$. We compute that $\begin{pmatrix} \pi^2 & 0 \\ 0 & 1 \end{pmatrix}$ is the only projectively unstable vertex and

$$\#\,\mathrm{Hom}_\Gamma(\begin{pmatrix} \pi^2 & \pi \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \pi^2 & 4\pi \\ 0 & 1 \end{pmatrix}) = 4,$$

$$\#\,\mathrm{Hom}_\Gamma(\begin{pmatrix}\pi^2 & 2\pi\\ 0 & 1\end{pmatrix},\begin{pmatrix}\pi^2 & 3\pi\\ 0 & 1\end{pmatrix}) = 4.$$

This finishes the first step of the algorithm, as in the picture. In the second step we then continue with the eight indicated vertices of level 3 ...

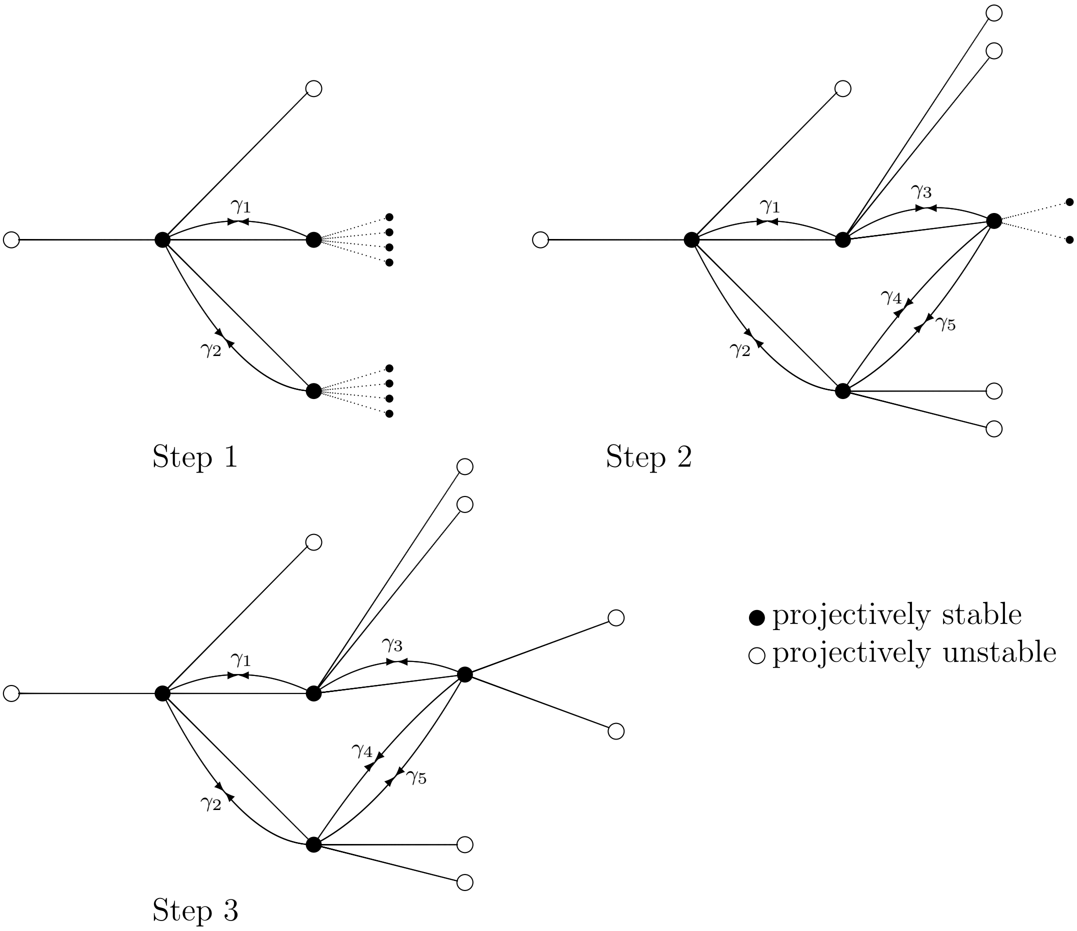


Figure 2: Example: $k = \mathbb{F}_5$, $r = T * (T+1) * (T+2) * (T+3)$

1.6 An algorithm to compute $\mathrm{Hom}_\Gamma(v, w)$

1.6.1 The case q odd, $\mathrm{odd}(R) = 1$

We first give an explicit description of the quaternion algebra D and its maximal order Λ.

Lemma 1.31 *Let $R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\}$ be a set of finite places of K with $\deg(\mathfrak{p}_i)$ odd for all i and l even, let r be a monic generator of the ideal $\mathfrak{r} = \prod_{i=1}^{l} \mathfrak{p}_i$ and let $\xi \in k^\star \backslash (k^\star)^2$. Then $\left(\frac{\xi, r}{K}\right)$ is ramified exactly at the places $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$.*

Proof: We compute the Hilbert symbols using Proposition 1.17. For $(\varpi) = \mathfrak{p} \notin R$ we have

$$(\xi, r)_{\mathfrak{p}} = (-1)^0 \left(\frac{\xi}{\varpi}\right)^0 \left(\frac{r}{\varpi}\right)^0 = 1$$

and for $(\varpi) = \mathfrak{p} \in R$ we have

$$(\xi, r)_{\mathfrak{p}} = (-1)^0 \left(\frac{\xi}{\varpi}\right)^1 \left(\frac{r/\varpi}{\varpi}\right)^0 = \left(\frac{\xi}{\varpi}\right) = \xi^{\frac{q-1}{2}\deg(\varpi)} = -1,$$

since $\deg(\varpi)$ is odd. ∎

From now on we set $D = \left(\frac{\xi, r}{K}\right)$ with $\xi \in k^\star \backslash (k^\star)^2$ fixed throughout these section.

Lemma 1.32

$$\Lambda := \langle 1, i, j, ij \rangle_A$$

is a maximal order.

Proof: Λ is clearly closed under multiplication and a lattice of rank 4. Hence Λ is an order. We have to check, that Λ is maximal. This is the ideal generated by

$$\det \begin{pmatrix} \operatorname{trd}(1) & \operatorname{trd}(i) & \operatorname{trd}(j) & \operatorname{trd}(ij) \\ \operatorname{trd}(i) & \operatorname{trd}(i^2) & \operatorname{trd}(ij) & \operatorname{trd}(i^2j) \\ \operatorname{trd}(j) & \operatorname{trd}(ji) & \operatorname{trd}(j^2) & \operatorname{trd}(jij) \\ \operatorname{trd}(ij) & \operatorname{trd}(iji) & \operatorname{trd}(ij^2) & \operatorname{trd}(ijij) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2\xi & 0 & 0 \\ 0 & 0 & 2r & 0 \\ 0 & 0 & 0 & -2\xi r \end{pmatrix} = -16\xi^2 r^2.$$

We see, that Λ has reduced discriminant $\mathfrak{r}$, and hence is a maximal order. ∎

Lemma 1.33 *The map $\iota : D \to M_2(K_\infty)$ defined by $i \mapsto \begin{pmatrix} 0 & 1 \\ \xi & 0 \end{pmatrix}$ and $j \mapsto \begin{pmatrix} \sqrt{r} & 0 \\ 0 & -\sqrt{r} \end{pmatrix}$ gives an isomorphism $D \otimes_K K_\infty \cong M_2(K_\infty)$.*

Proof: Since $r = \prod_{i=1}^{l} \varpi_i$ with $\varpi_i \in A$, l even and all $\deg(\varpi_i)$ odd, the degree of r is even, hence we have $\sqrt{r} \in K_\infty$. One checks that the given matrices $\iota(i)$ and $\iota(j)$ fulfil the relations $\iota(i)^2 = \xi, \iota(j)^2 = r$ and $\iota(i)\iota(j) = -\iota(j)\iota(i)$. This easily yields $\left(\frac{\xi, r}{K_\infty}\right) \cong M_2(K_\infty)$ under ι. The isomorphism $D \otimes_K K_\infty \cong \left(\frac{\xi, r}{K_\infty}\right)$ is obvious by construction of D. ∎

We can compute the first n coefficients of $\sqrt{r}$ in $K_\infty = k((\pi))$ in time $\mathcal{O}(n)$ by Newton iteration and using $\pi^{-l/2}$ as a first approximation.
Let $v_0 = [L(0,0)]$. Note that $\operatorname{Stab}_{\mathrm{GL}_2(K_\infty)}(v_0) = \mathrm{GL}_2(O_\infty) K_\infty^\star$. Hence

$$\operatorname{Stab}_\Gamma(v_0) = \mathrm{GL}_2(O_\infty) K_\infty^\star \cap \Gamma = \mathrm{GL}_2(O_\infty) \cap \Gamma$$

and

$$\mathrm{GL}_2(O_\infty) \cap \Gamma \supseteq \mathrm{GL}_2(k) \cap \Gamma = \{a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ \xi & 0 \end{pmatrix} \mid a, b \in k, (a,b) \neq (0,0)\}.$$

Hence the vertex v_0 is projectively unstable, $\mathrm{GL}_2(k) \cap \Gamma = \operatorname{Stab}_\Gamma(v_0)$ and $\pi(v_0)$ is a terminal vertex of $\Gamma \backslash \mathcal{T}$.

Let v_1 be the vertex $[L(1,0)]$. If v_1 is projectively unstable, then $\pi(v_1)$ is also a terminal vertex, and since v_0 and v_1 are adjacent in $\mathcal{T}$ this implies that $\Gamma\backslash\mathcal{T}$ is the graph containing two vertices and one edge connecting them. In that case $V_{q+1} = 0$. If $V_{q+1} \neq 0$, then v_1 has to be projectively stable. Hence we can use v_1 as the initial vertex for the algorithm 1.26. We already checked that v_0 is unstable. The other vertices adjacent to v_1 are $[L(2, \alpha\pi)]$ for $\alpha \in k$, see Lemma 1.9. These are the vertices we need to compare in the first step of the algorithm 1.26. Generally, Lemma 1.9 implies that in the n-th step of the algorithm we need to compare vertices of the form $[L(n, g(\pi))]$, where $g \in k[T]$ with $\deg(g) < n$ and $g(0) = 0$. The next Proposition proves that we can do this in time $\mathcal{O}(n^2)$.

Proposition 1.34 *Given $v = [L(n, g(\pi))]$ and $v' = [L(n, g'(\pi))]$ as above there is an algorithm that computes $\mathrm{Hom}_\Gamma(v', v)$ in time $\mathcal{O}(n^2)$.*

Proof: We have $\mathrm{Stab}_{\mathrm{GL}_2(K_\infty)}(v_0) = \mathrm{GL}_2(O_\infty)K_\infty^\star$ and since $\mathrm{GL}_2(K_\infty)$ acts transitively on $\mathcal{T}$ we conclude

$$\mathrm{Hom}_{\mathrm{GL}_2(K_\infty)}(v', v) = \gamma \mathrm{GL}_2(O_\infty)K_\infty^\star(\gamma')^{-1}$$

with $\gamma = \begin{pmatrix} \pi^n & g(\pi) \\ 0 & 1 \end{pmatrix}$ and $\gamma' = \begin{pmatrix} \pi^n & g'(\pi) \\ 0 & 1 \end{pmatrix}$ the matrices sending v_0 to v respectively v'. Hence

$$\mathrm{Hom}_\Gamma(v', v) = \gamma \mathrm{GL}_2(O_\infty)K_\infty^\star(\gamma')^{-1} \cap \Gamma = \gamma M_2(O_\infty)(\gamma')^{-1} \cap \Gamma.$$

We will give an algorithm to compute this set.
First observe that if we have any element $\tau \in \gamma M_2(O_\infty)(\gamma')^{-1} \cap \Lambda$, then taking determinants on both sides we obtain $\mathrm{nrd}(\tau) \in O_\infty \cap k[T] = k$, and since D is a quaternion algebra there are no non-zero elements of Λ having reduced norm zero. Hence

$$\gamma M_2(O_\infty)(\gamma')^{-1} \cap \Gamma = (\gamma M_2(O_\infty)(\gamma')^{-1} \cap \Lambda) \smallsetminus \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}.$$

Any element τ of Λ can be written as

$$\tau = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ \xi & 0 \end{pmatrix} + c\begin{pmatrix} \sqrt{r} & 0 \\ 0 & -\sqrt{r} \end{pmatrix} + d\begin{pmatrix} 0 & -\sqrt{r} \\ \xi\sqrt{r} & 0 \end{pmatrix}$$
$$= \begin{pmatrix} a + c\sqrt{r} & b - d\sqrt{r} \\ \xi(b + d\sqrt{r}) & a - c\sqrt{r} \end{pmatrix}$$

with $a, b, c, d \in k[T]$. Then $\tau \in \gamma M_2(O_\infty)(\gamma')^{-1}$ means that there are $v, w, x, y \in O_\infty$ such that

$$\tau = \begin{pmatrix} \pi^n & g(\pi) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} v & w \\ x & y \end{pmatrix}\begin{pmatrix} \pi^{-n} & -g'(\pi)\pi^{-n} \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} v + g(\pi)\pi^{-n}x & \pi^n w + g(\pi)y - g'(\pi)v - g(\pi)g'(\pi)\pi^{-n}x \\ \pi^{-n}x & y - g'(\pi)\pi^{-n}x \end{pmatrix}.$$

Comparing the entries of the two matrices we obtain the condition

$$B\begin{pmatrix} v \\ w \\ x \\ y \end{pmatrix} = A\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

with

$$A = \begin{pmatrix} 1 & 0 & \sqrt{r} & 0 \\ 0 & 1 & 0 & -\sqrt{r} \\ 0 & \xi & 0 & \xi\sqrt{r} \\ 1 & 0 & -\sqrt{r} & 0 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 1 & 0 & g(\pi)\pi^{-n} & 0 \\ -g'(\pi) & \pi^n & -g(\pi)g'(\pi)\pi^{-n} & g(\pi) \\ 0 & 0 & \pi^{-n} & 0 \\ 0 & 0 & -\pi^{-n}g'(\pi) & 1 \end{pmatrix}.$$

Hence

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = A^{-1}B \begin{pmatrix} v \\ w \\ x \\ y \end{pmatrix} = 1/2 \begin{pmatrix} v + y + (g(\pi) - g'(\pi))\pi^{-n}x \\ -g'(\pi)v + g(\pi)y + (\xi^{-1} - g(\pi)g'(\pi))\pi^{-n}x + \pi^n w \\ \rho v - \rho y + \rho(g(\pi) + g'(\pi))\pi^{-n}x \\ \rho g'(\pi)v - \rho g(\pi)y + \rho(g(\pi)g'(\pi) + \xi^{-1})\pi^{-n}x - \rho\pi^n w \end{pmatrix}$$

where $\rho = \sqrt{r}^{-1}$.
Since $a, b, c, d \in k[T]$, we can reduce the right hand side modulo πO_∞ to obtain

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \equiv 1/2 \begin{pmatrix} v_0 + y_0 + (g(\pi) - g'(\pi))\pi^{-n}x \\ (\xi^{-1} - g(\pi)g'(\pi))\pi^{-n}x \\ \rho(g(\pi) + g'(\pi))\pi^{-n}x \\ \rho(g(\pi)g'(\pi) + \xi^{-1})\pi^{-n}x \end{pmatrix} \pmod{\pi O_\infty}$$

where v_0 (resp. y_0) denotes the zeroth coefficient of v (resp. y).
Hence the tupel (a, b, c, d) depends only on $z_0 := v_0 + y_0$ and $x_0, \ldots, x_n$, where $x = \sum_{i=0}^{\infty} x_i \pi^i$.
Regarding $z_0, x_0, \ldots, x_n$ as indeterminates we obtain polynomials $a_{z_0,x_0,\ldots,x_n}, \ldots, d_{z_0,x_0,\ldots,x_n} \in k[T]$ whose coefficients are linear forms in $z_0, x_0, \ldots, x_n$. Moreover the above calculation shows that $\mathrm{Hom}_\Gamma(v', v)$ is in bijection to the solutions of

$$B^{-1}A \begin{pmatrix} a_{z_0,x_0,\ldots,x_n} \\ b_{z_0,x_0,\ldots,x_n} \\ c_{z_0,x_0,\ldots,x_n} \\ d_{z_0,x_0,\ldots,x_n} \end{pmatrix} \in O_\infty^4 \setminus \{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \}.$$

The expression on the left is a vector of Laurent series in $k((\pi))$. Thus the condition can be regarded as a linear system of equations in the coefficients of the principal parts of these series. The pole order of these series determines the number of equations to hold. Since we have $\deg(a_{z_0,x_0,\ldots,x_n}) \leq n - 1, \deg(b_{z_0,x_0,\ldots,x_n}) \leq n, \deg(c_{z_0,x_0,\ldots,x_n}) \leq n - 1 - \frac{1}{2}\deg(r)$ and $\deg(d_{z_0,x_0,\ldots,x_n}) \leq n - \frac{1}{2}\deg(r)$ and since the matrix $B^{-1}A$ has entries with valuation v_∞ greater or equal $-n$, we get at most $8n - 1$ linear equations over k in the variables $z_0, x_0, \ldots, x_n$. To obtain these equations we only need to know $B^{-1}A \mod \pi^n$, which means that we need to know an approximation of $\sqrt{r}$ up to $2n$ coefficients.
Solving these linear equations can be done in time $\mathcal{O}(n^2)$ using Gauss elimination. ∎

1.6.2 The case q odd, $\mathrm{odd}(R) = 0$

Again, we first need an explicit representation of D and Λ. Let $R = \{\mathfrak{p}_1 = (\varpi_1), \ldots, \mathfrak{p}_l = (\varpi_l)\}$ be a list of finite places of K with l even. Let $(r) = \mathfrak{r}$ be as above.

Lemma 1.35 *There is an irreducible monic polynomial $\alpha \in A$ of even degree such that*

$$\left(\frac{\alpha}{\varpi_i}\right) = -1 \textit{ for all } i \textit{ and } \left(\frac{r}{\alpha}\right) = 1.$$

Proof: Choose any $a \in A$ with

$$\left(\frac{a}{\varpi_i}\right) = -1$$

for all i. This can be done using the Chinese Remainder theorem. Now by the strong form of the analogue of Dirichlet's theorem ([Ro, Theorem 4.8]) the arithmetic progression $\{a + rb \mid b \in A\}$ contains an irreducible monic polynomial α of even degree. Since $\alpha \equiv a \pmod{\varpi_i}$ we also have

$$\left(\frac{\alpha}{\varpi_i}\right) = -1.$$

By quadratic reciprocity ([Ro, Theorem 3.3]) we then have

$$\left(\frac{\varpi_i}{\alpha}\right) = (-1)^{\frac{q-1}{2}\deg\alpha\deg\varpi_i}\left(\frac{\alpha}{\varpi_i}\right) = -1$$

since $\deg(\alpha)$ is even. But then

$$\left(\frac{r}{\alpha}\right) = \prod_{i=1}^{l}\left(\frac{\varpi_i}{\alpha}\right) = (-1)^l = 1.$$

∎

Remark 1.36 In practice we find α by the following method:

Step 1: Start with $m = 2$.

Step 2: Check for all monic irreducible polynomials α of degree m whether $\left(\frac{\alpha}{\varpi_i}\right) = -1$ for all $1 \leq i \leq l$.

Step 3: If we found an α with this property, then it fulfils the conditions of Lemma 1.35.

Step 4: Otherwise set $m := m + 2$ and go back to step 2.

Let α be as in Lemma 1.35 and define $D := \left(\frac{\alpha, r}{K}\right)$.

Proposition 1.37 *The quaternion algebra D is ramified exactly at R.*

Proof: We compute the Hilbert symbols using Proposition 1.17. For $(\varpi) = \mathfrak{p} \notin R$ and ϖ not equal to α we have

$$(\alpha, r)_{\mathfrak{p}} = (-1)^0 \left(\frac{\alpha}{\varpi}\right)^0 \left(\frac{r}{\varpi}\right)^0 = 1$$

and for $\mathfrak{p} = (\alpha)$ we have

$$(\alpha, r)_{\mathfrak{p}} = (-1)^0 \left(\frac{1}{\alpha}\right)^0 \left(\frac{r}{\alpha}\right)^1 = 1.$$

Finally for $(\varpi) = \mathfrak{p} \in R$ we have

$$(\alpha, r)_{\mathfrak{p}} = (-1)^0 \left(\frac{\alpha}{\varpi}\right)^1 \left(\frac{r/\varpi}{\varpi}\right)^0 = -1.$$

■

Since r is a square modulo α, there are $\varepsilon, \nu \in A$ with $\deg(\varepsilon) < \deg(\alpha)$ and $\varepsilon^2 = r + \nu\alpha$. Set

$$\Lambda := \langle e_1 = 1, e_2 = i, e_3 = j, e_4 = \frac{\varepsilon i + ij}{\alpha} \rangle_A.$$

Proposition 1.38 *The A-lattice Λ is a maximal order of D.*

Proof: We first check, that Λ is an order. Let

$$\gamma = a + bi + cj + d\frac{\varepsilon i + ij}{\alpha} = a + (b + \frac{d\varepsilon}{\alpha})i + cj + \frac{d}{\alpha}ij$$

with $a, b, c, d \in A$ be any element of Λ. Then $\mathrm{trd}(\gamma) = 2a$ and

$$\mathrm{nrd}(\gamma) = a^2 - \alpha(b + \frac{d\varepsilon}{\alpha})^2 - rc^2 + \alpha r(\frac{d}{\alpha})^2 = a^2 - rc^2 + \frac{rd^2}{\alpha} - \frac{b^2\alpha^2 + 2bd\varepsilon\alpha + d^2\varepsilon^2}{\alpha}$$

$$= a^2 - rc^2 - b^2\alpha - 2bd\varepsilon + d^2\frac{r - \varepsilon^2}{\alpha} = a^2 - rc^2 - b^2\alpha - 2bd\varepsilon + d^2\nu$$

are both in A. Since $\{e_1, e_2, e_3, e_4\}$ is an F-basis of D, we conclude that Λ is an A-lattice of D. To check that Λ is a ring, we compute

$$e_1 e_i = e_i e_1 = e_i,$$

$$e_2 e_3 = -e_3 e_2 = ij = \alpha e_4 - \varepsilon e_2,$$

$$e_2 e_4 = i\frac{\varepsilon i + ij}{\alpha} = \varepsilon + j = \varepsilon e_1 + e_3,$$

$$e_4 e_2 = \frac{\varepsilon i + ij}{\alpha} i = \varepsilon - j = \varepsilon e_1 - e_3,$$

$$e_3 e_4 = j\frac{\varepsilon i + ij}{\alpha} = -\frac{\varepsilon ij + ij^2}{\alpha} = -\frac{\varepsilon ij + ir}{\alpha}$$

$$= -\frac{\varepsilon ij + i(\varepsilon^2 - \alpha\nu)}{\alpha} = \nu i - \varepsilon\frac{\varepsilon i + ij}{\alpha} = \nu e_2 - \varepsilon e_4,$$

$$e_4e_3 = \frac{\varepsilon i + ij}{\alpha} j = -j \frac{\varepsilon i + ij}{\alpha} = -e_3e_4 = -\nu e_2 + \varepsilon e_4,$$

and

$$e_1^2 = e_1, e_2^2 = \alpha e_1, e_3^2 = re_1, e_4^2 = \frac{(\varepsilon i + ij)^2}{\alpha^2} = \frac{\varepsilon^2 i^2 - i^2 j^2}{\alpha^2} = \frac{\varepsilon^2 - r}{\alpha} = \nu e_1.$$

So Λ is closed under multiplication and hence an order. To check that Λ is maximal, we compute

$$\det(\operatorname{trd}(e_ie_j)_{i,j=1,\ldots,4}) = \det \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2\alpha & 0 & 2\varepsilon \\ 0 & 0 & 2r & 0 \\ 0 & 2\varepsilon & 0 & 2\nu \end{pmatrix} = 16r(\alpha\nu - \varepsilon^2) = -16r^2$$

and hence the ideal generated by $\det(\operatorname{trd}(e_ie_j)_{i,j=1,\ldots,4})$ is equal to (r^2). ∎

Lemma 1.39 *The map $\iota : D \to M_2(K_\infty)$ defined by $i \mapsto \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix}$ and $j \mapsto \begin{pmatrix} 0 & 1 \\ r & 0 \end{pmatrix}$ gives an isomorphism $D \otimes_K K_\infty \cong M_2(K_\infty)$.*

Proof: The degree of α is even, and so we have $\sqrt{\alpha} \in K_\infty$. For matrices $\iota(i)$ and $\iota(j)$ one verifies the relations $\iota(i)^2 = \alpha, \iota(j)^2 = r$ and $\iota(i)\iota(j) = -\iota(j)\iota(i)$ and concludes as in the proof of Lemma 1.33. ∎

Let $m = \deg(\alpha)$. Again we can compute the first n coefficients of $\sqrt{\alpha}$ in $K_\infty = k((\pi))$ in time $\mathcal{O}(n)$ by Newton iteration and using $\pi^{-m/2}$ as a first approximation.
Because of Theorem 1.24, we know that there are no projectively unstable vertices in this case. We use $v_0 = [O_\infty^2] = [L(0,0)]$ as the initial vertex for the algorithm. The vertices adjacent to v are $[L(1,\alpha)]$ for $\alpha \in k$ and $[L(-1,0)]$, see Lemma 1.9. These are the vertices we need to compare in the first step of the algorithm 1.26. Generally, Lemma 1.9 implies that in the n-th step of the algorithm we need to compare vertices of the form $[L(-n_1+n_2,g)]$, where $n_1, n_2 \in \mathbb{N}_0$ $n_1+n_2 = n$, $g \in K_\infty/\pi^{-n_1+n_2}O_\infty$ and with the conditions that if $n_2 = 0$ then $g = 0$ and if both $n_1, n_2 \neq 0$ then $v_\infty(g) = -n_1$ (see also Figure 1). The next Proposition proves that we can do this in time $O(n^2)$.

Proposition 1.40 *Given $v = [L(-n_1+n_2,g)]$ and $v' = [L(-n_1'+n_2',g')]$ with g, g' as above there is an algorithm that computes $\operatorname{Hom}_\Gamma(v',v)$ in time $\mathcal{O}(n^2)$.*

Proof: Let $\gamma = \begin{pmatrix} \pi^{-n_1+n_2} & g \\ 0 & 1 \end{pmatrix}$ and $\gamma' = \begin{pmatrix} \pi^{-n_1'+n_2'} & g' \\ 0 & 1 \end{pmatrix}$ the matrices sending v_0 to v respectively v'. Hence

$$\operatorname{Hom}_\Gamma(v',v) = \gamma \mathrm{GL}_2(O_\infty)K_\infty^\star(\gamma')^{-1} \cap \Gamma.$$

Since $v_\infty(\det(\gamma)) = -n_1+n_2, v_\infty(\det((\gamma')^{-1}) = n_1' - n_2'$ and $v_\infty(\det(\sigma)) = 0$ for all $\sigma \in \mathrm{GL}_2(O_\infty)$ we see that

$$\operatorname{Hom}_\Gamma(v',v) = \gamma \mathrm{GL}_2(O_\infty) \begin{pmatrix} \pi^{n_1-n_1'} & 0 \\ 0 & \pi^{n_1-n_1'} \end{pmatrix} (\gamma')^{-1} \cap \Gamma.$$

Again by taking determinants on both sides and the fact that $O_\infty \cap k[T] = k$, we see that this set equals

$$\gamma M_2(O_\infty)\begin{pmatrix}\pi^{n_1-n_1'} & 0\\ 0 & \pi^{n_1-n_1'}\end{pmatrix}(\gamma')^{-1} \cap \Lambda \setminus \{\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\}.$$

Any element $\tau \in \Lambda$ can be written as

$$\tau = a\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + b\begin{pmatrix}\sqrt{\alpha} & 0\\ 0 & -\sqrt{\alpha}\end{pmatrix} + c\begin{pmatrix}0 & 1\\ r & 0\end{pmatrix} + d\begin{pmatrix}\frac{\varepsilon}{\sqrt{\alpha}} & \frac{1}{\sqrt{\alpha}}\\ \frac{-r}{\sqrt{\alpha}} & \frac{-\varepsilon}{\sqrt{\alpha}}\end{pmatrix}$$

$$= \begin{pmatrix}a + b\sqrt{\alpha} + d\frac{\varepsilon}{\sqrt{\alpha}} & c + d\frac{1}{\sqrt{\alpha}}\\ r(c - d\frac{1}{\sqrt{\alpha}}) & a - b\sqrt{\alpha} - d\frac{\varepsilon}{\sqrt{\alpha}}\end{pmatrix}$$

for some $a, b, c, d \in k[T]$.

Then $\tau \in \gamma M_2(O_\infty)\begin{pmatrix}\pi^{n_1-n_1'} & 0\\ 0 & \pi^{n_1-n_1'}\end{pmatrix}(\gamma')^{-1}$ means that there are $v, w, x, y \in O_\infty$ such that

$$\tau = \begin{pmatrix}\pi^{-n_1+n_2} & g\\ 0 & 1\end{pmatrix}\begin{pmatrix}v & w\\ x & y\end{pmatrix}\begin{pmatrix}\pi^{n_1-n_1'} & 0\\ 0 & \pi^{n_1-n_1'}\end{pmatrix}\begin{pmatrix}\pi^{n_1'-n_2'} & -g'\pi^{n_1'-n_2'}\\ 0 & 1\end{pmatrix}$$

$$= \begin{pmatrix}\pi^{n_2-n_2'}v + g\pi^{n_1-n_2'}x & -g'\pi^{n_2-n_2'}v + \pi^{n_2-n_1'}w - gg'\pi^{n_1-n_2'}x + g\pi^{n_1-n_1'}y\\ \pi^{n_1-n_2'}x & -g'\pi^{n_1-n_2'}x + \pi^{n_1-n_1'}y\end{pmatrix}.$$

Comparing the entries of the two matrices we obtain the condition

$$B\begin{pmatrix}v\\ w\\ x\\ y\end{pmatrix} = A\begin{pmatrix}a\\ b\\ c\\ d\end{pmatrix}$$

with

$$A = \begin{pmatrix}1 & \sqrt{\alpha} & 0 & \frac{\varepsilon}{\sqrt{\alpha}}\\ 0 & 0 & 1 & \frac{1}{\sqrt{\alpha}}\\ 0 & 0 & r & \frac{-r}{\sqrt{\alpha}}\\ 1 & -\sqrt{\alpha} & 0 & \frac{-\varepsilon}{\sqrt{\alpha}}\end{pmatrix}$$

and

$$B = \begin{pmatrix}\pi^{n_2-n_2'} & 0 & g\pi^{n_1-n_2'} & 0\\ -g'\pi^{n_2-n_2'} & \pi^{n_2-n_1'} & -gg'\pi^{n_1-n_2'} & g\pi^{n_1-n_1'}\\ 0 & 0 & \pi^{n_1-n_2'} & 0\\ 0 & 0 & -g'\pi^{n_1-n_2'} & \pi^{n_1-n_1'}\end{pmatrix}.$$

Hence

$$\begin{pmatrix}a\\ b\\ c\\ d\end{pmatrix} = A^{-1}B\begin{pmatrix}v\\ w\\ x\\ y\end{pmatrix}$$

$$= 1/2\begin{pmatrix}\pi^{n_2-n_2'}v + (g-g')\pi^{n_1-n_2'}x + \pi^{n_1-n_1'}y\\ \frac{1+\varepsilon g'}{\sqrt{\alpha}}\pi^{n_2-n_2'}v - \frac{\varepsilon}{\sqrt{\alpha}}\pi^{n_2-n_1'}w + \frac{g+g'+\varepsilon(gg'+1/r)}{\sqrt{\alpha}}\pi^{n_1-n_2'}x + \frac{-1-\varepsilon g}{\sqrt{\alpha}}\pi^{n_1-n_1'}y\\ -g'\pi^{n_2-n_2'}v + \pi^{n_2-n_1'}w + (1/r - gg')\pi^{n_1-n_2'}x + g\pi^{n_1-n_1'}y\\ -\sqrt{\alpha}g'\pi^{n_2-n_2'}v + \sqrt{\alpha}\pi^{n_2-n_1'}w + \sqrt{\alpha}(-1/r - gg')\pi^{n_1-n_2'}x + \sqrt{\alpha}g\pi^{n_1-n_1'}y\end{pmatrix}.$$

Hence the tupel (a,b,c,d) depends only on $\underline{v} := v_0,\dots,v_{n-n_2+m/2}$, $\underline{w} := w_0,\dots,w_{n_1'-n_2+m/2}$, $\underline{x} := x_0,\dots,x_{n+m/2}$ and $\underline{y} := y_0,\dots,y_{n_1'+m/2}$ where $v = \sum_{i=0}^{\infty} v_i\pi^i$ (respectively w,x,y).
Regarding $\underline{v},\underline{w},\underline{x}$ and $\underline{y}$ as indeterminates we obtain polynomials $a_{\underline{v},\underline{w},\underline{x},\underline{y}}$, $b_{\underline{v},\underline{w},\underline{x},\underline{y}}$, $c_{\underline{v},\underline{w},\underline{x},\underline{y}}$ and $d_{\underline{v},\underline{w},\underline{x},\underline{y}}$ whose coefficients are linear forms in $\underline{v},\underline{w},\underline{x}$ and $\underline{y}$. Moreover the above calculation shows that $\mathrm{Hom}_\Gamma(v',v)$ is in bijection to the solutions of

$$B^{-1}A\begin{pmatrix} a_{\underline{v},\underline{w},\underline{x},\underline{y}} \\ b_{\underline{v},\underline{w},\underline{x},\underline{y}} \\ c_{\underline{v},\underline{w},\underline{x},\underline{y}} \\ d_{\underline{v},\underline{w},\underline{x},\underline{y}} \end{pmatrix} \in O_\infty^4 \smallsetminus \{\begin{pmatrix}0\\0\\0\\0\end{pmatrix}\}.$$

The expression on the left is a vector of Laurent series in $k((\pi))$. Thus the condition can be regarded as a linear system of equations in the coefficients of the principal parts of these series. The pole order of these series determines the number of equations to hold. Since we have $\deg(a_{\underline{v},\underline{w},\underline{x},\underline{y}}) \le n$, $\deg(b_{\underline{v},\underline{w},\underline{x},\underline{y}}) \le n+m/2$, $\deg(c_{\underline{v},\underline{w},\underline{x},\underline{y}}) \le n$ and $\deg(d_{\underline{v},\underline{w},\underline{x},\underline{y}}) \le m/2+n$ and since the matrix $B^{-1}A$ has entries with valuation v_∞ greater or equal $-(m/2+2n+\deg(r))$, we get at most $(4n+m)(m/2+2n+\deg(r))$ linear equations over k in $4n+m$ variables. To obtain these equations we only need to know $B^{-1}A \mod \pi^{m/2+n+1}$, which means that we need to know an approximation of $\sqrt{\alpha}$ up to $2n+m+1$ coefficients.
Solving these linear equations can be done in time $\mathcal{O}(n^2)$ using Gauss elimination.
∎

1.6.3 The case q even, general considerations

In the case q even we have to use a different representation for D, compare Definition1.12. However in this case if $D = \left(\frac{a,b}{K}\right)$ with $a,b \in K^\star$ then the subfield $K(\sqrt{b}) \subseteq D$ is an inseparable extension of K once $b \notin (K^\star)^2$ but $D \supseteq K(i)$ with $i^2+i+a=0$ is a separable Artin-Schreier extension of K. This asymmetry in the role of a and b indicates that a formula like Proposition1.17 for the ramification of D has to look quite different in this case.
The division algebra over K can be constructed in a systematic way as cyclic algebras, we quickly recall this construction here. Let $\mathrm{Br}(K)$ denote the Brauer group of K, that is the group of similarity-classes of finite-dimensional central simple algebras over K, where two such algebras A,B are similar if there are positive integers m and n such that $M_m(A) \cong M_n(B)$. We write $[A]$ for the similarity class of A. Multiplication in this group is defined by taking tensor products over K, the similarity class of K is the unit element, and since $A \otimes_K A^{\mathrm{op}} \cong M_n(K)$ with $n = \dim_K(A)$ we see that every element $[A]$ of $\mathrm{Br}(K)$ has $[A^{\mathrm{op}}]$ as an inverse.
Let F be an extension field of K. Then we have a natural map $\varphi : \mathrm{Br}(K) \to \mathrm{Br}(F)$ sending $[A]$ to $[A \otimes_K F]$. We define $\mathrm{Br}(K,F) := \mathrm{Kern}(\varphi)$.
Let F/K be a finite Galois extension of degree n with $G := \mathrm{Gal}(F/K)$ and let $\psi \in Z^2(G,F^\star)$ be a 2-cocycle. Let A be the F-algebra with basis $\{u_s \mid s \in G\}$ and multiplication

$$(\sum_{s\in G}\lambda_s u_s)(\sum_{s\in G}\mu_s u_s) = \sum_{s,t\in G}\psi(s,t)\lambda_s s(\mu_t)u_{st}. \qquad (2)$$

We write $A = (F,G,\psi)$ and call A the crossed product of F and G with respect to ψ.

Theorem 1.41 *$A = (F, G, \psi)$ is a central simple algebra over K of dimension n^2.*

Proof: See [Ja, Theorem 8.7]. ■

If F/K is a cyclic extension with $G = \langle s \rangle$, then we can choose ψ to be the map

$$\psi_\gamma(s^i, s^j) := \begin{cases} 1 & \text{if } 0 \leq i + j < n \\ \gamma & \text{if } n \leq i + j \leq 2n - 2. \end{cases}$$

for some $\gamma \in K^\star$, see [Ja, Section 8.5]. We write $A = (F, s, \gamma)$ and call A the cyclic algebra defined by F/K, the generator s of G and $\gamma \in K^\star$.

Theorem 1.42 *(a) $[A] = [(F, s, \gamma)]$ is independent of the choice of γ in $K^\star / \operatorname{Norm}_{F/K}(F^\star)$.*

(b) The map $\gamma \operatorname{Norm}_{F/K}(F^\star) \mapsto [(F, s, \gamma)]$ defines an isomorphism of $F^\star / \operatorname{Norm}_{F/K}(F^\star)$ with $\operatorname{Br}(K, F)$.

Proof: See [Ja, Theorem 8.14]. ■

Example 1.43 Let $a \in K^\star$ be any element such that $F := K[x]/(x^2 + x + a) \ncong K$. Then F/K is an Artin-Schreier extension, so it is cyclic of degree 2 and $G = \operatorname{Gal}(F/K)$ is generated by $s : r = \lambda_1 x + \lambda_2 \mapsto (\lambda_1 + 1)x + \lambda_2$. Choose any $b \in K^\star$. Then ψ_b is given by the following values:

	$(1,1)$	$(s,1)$	$(1,s)$	(s,s)
ψ_b	1	1	1	b

Let $A = (F, s, b)$. Then as an additive group

$$A = Fu_1 \oplus Fu_s \cong Ku_1 \oplus Ku_s \oplus Kxu_1 \oplus Kxu_s.$$

We compute a multiplication table using formula (2):

	u_1	u_s	xu_1	xu_s
u_1	u_1	u_s	xu_1	xu_s
u_s	u_s	bu_1	$xu_s + u_s$	$bxu_1 + bu_1$
xu_1	xu_1	xu_s	$xu_1 + au_1$	$xu_s + au_s$
xu_s	xu_s	bxu_1	au_s	abu_1

Hence the map given by $u_1 \mapsto 1$, $u_s \mapsto j$, $xu_1 \mapsto i$ and $xu_s \mapsto ij$ defines an isomorphism $A \cong \left(\frac{a,b}{K}\right)$.

We fix an $a \in K^\star$ such that $F := K[x]/(x^2 + x + a)$ is a cyclic degree 2 extension of K with Galois group $G = \{s\}$. Then by Example 1.43 for any $b \in K^\star$ we obtain the quaternion algebra $\left(\frac{a,b}{K}\right)$ as the cyclic algebra (F, s, b).
Let v be a finite place of K and let ϖ_v denote the corresponding monic irreducible in $k[T]$.

Proposition 1.44 *If F/K splits at v, then (F,s,b) is unramified at v.*

Proof: By Example 1.43 we have $D := (F,s,b) = \left(\frac{a,b}{K}\right)$. Hence $D_v := D \otimes_K K_v \cong \left(\frac{a,b}{K_v}\right)$. If F/K splits at v, then x^2+x+a has a solution over K_v. That means there is an $\alpha \in K_v$ such that $\alpha^2+\alpha+a=0$, and also $(\alpha+1)^2+\alpha+1+a=0$. Hence the map $\varphi : \left(\frac{a,b}{K_v}\right) \to M_2(K_v)$ defined by $i \mapsto \begin{pmatrix}\alpha & 0\\ 0 & \alpha+1\end{pmatrix}$ and $j \mapsto \begin{pmatrix}0 & 1\\ b & 0\end{pmatrix}$ provides an embedding of D_v into $M_2(K_v)$. Since both D_v and $M_2(K_v)$ are of dimension 4 over K_v we have $D_v \cong M_2(K_v)$ and hence D is unramified at v. ∎

Proposition 1.45 *If F/K is non-split at v, then (F,s,b) is unramified at v if and only if $b \in \mathrm{Norm}_{F_v/K_v}(F_v^\star)$.*

Proof: Let $D := (F,s,b)$. Since F/K is non-split at v, the extension F_v/K_v is a degree 2 Galois extension and it is clear from the construction of D that $D_v = (F_v,s,b)$. Theorem 1.42 applied to the extension F_v/K_v implies that $[D_v]=[K_v]$ if and only if $b \in \mathrm{Norm}_{F_v/K_v}(F_v^\star)$. If $[D_v]=[K_v]$ then there are $n,m \in \mathbb{N}$ such that $M_n(D_v) \cong M_m(K_v)$. But since D_v is central simple over K_v, we have $D_v \cong M_{n'}(\Delta)$ with Δ a division algebra over K_v. Hence $M_m(K_v) \cong M_n(D_v) \cong M_{nn'}(\Delta)$. This is only possible if $\Delta = K_v$. Since D_v is of dimension 4 over K_v this implies $D_v = M_2(K_v)$. On the other hand if $D_v \cong M_2(K_v)$ then clearly $[D_v]=[K_v]$. ∎

If F/K is non-split at v, then F_v/K_v is a degree 2 extension of local fields. If this extension is unramified, we have an easy criterion to decide whether some $b \in K_v^\star$ is in $\mathrm{Norm}_{F_v/K_v}(F_v^\star)$:

Proposition 1.46 *Suppose F/K is unramified at v. Then $b \in \mathrm{Norm}_{F_v/K_v}(F_v^\star)$ if and only if $v(b) \equiv 0 \pmod 2$.*

Proof: Since F_v/K_v is unramified it is an extension of residue fields. Hence we can assume w.l.o.g. that $K_v \cong \mathbb{F}_q((T))$ and $F_v \cong \mathbb{F}_{q^2}((T))$ for some prime power q. Then

$$\mathrm{Image}(\mathrm{Norm}_{F_v/K_v}(F_v^\star) = T^{2\mathbb{Z}}\mathbb{F}_q[[T]]^\star$$

which implies the Lemma. ∎

As a consequence to the above propositions we see that a cyclic algebra is only ramified at a finite number of places, a fact we already know by Proposition 1.18:

Corollary 1.47 *Let v be a finite place of K such that $v(a)=0=v(b)$. Then $\left(\frac{a,b}{K}\right)$ is unramified at v.*

Proof: Since $v(a)=0$, the extension F_v/K_v either splits or is unramified. In the first case by Proposition 1.44 we know that $\left(\frac{a,b}{K}\right)$ is unramified at v. In the second case we know by Proposition 1.46 that $b \in \mathrm{Norm}_{F_v/K_v}(F_v^\star)$ and hence by Proposition 1.45 that $\left(\frac{a,b}{K}\right)$ is unramified at v. ∎

Definition 1.48 *For $\varpi \in k[T]$ monic irreducible and $f \in k[T]$ we define the Artin-Schreier symbol*

$$[f, \varpi) := \begin{cases} 0 & \text{if } f \equiv x^2 + x \pmod{\varpi} \text{ for some } x \in k[T], \\ 1 & \text{otherwise.} \end{cases}$$

For $f \in k$ it is an easy task to evaluate the Artin-Schreier symbol $[f, \varpi)$:

Proposition 1.49 *For $f \in k$, $\varpi \in k[T]$ monic irreducible we have*

$$[f, \varpi) \equiv \mathrm{Trace}_{k/\mathbb{F}_2}(f) \deg(\varpi) \pmod 2.$$

We need to be able to decide whether F/K is split or non-split at a given place v. We fix an uniformizer π_v of K_v. Let α denote the Laurent series expansion in π_v of a at the place v. Then F/K is split at v if and only if the equation $x^2 + x = \alpha$ has a solution in K_v. Before we can give a criterion we need a Lemma:

Lemma 1.50 *Let $k \in \mathbb{N}$. Then $x^2 + x = \alpha + \pi^{-2k}$ has a solution in K_v if and only if $y^2 + y = \alpha + \pi^{-k}$ has a solution in K_v.*

Proof: Suppose there is an $x \in K_v$ such that $x^2 + x = \alpha + \pi^{-2k}$. Set $y := x + \pi^{-k}$. Then

$$y^2 + y = (x + \pi^{-k})^2 + x + \pi^{-k} = x^2 + x + \pi^{-2k} + \pi^{-k} = \alpha + \pi^{-k}.$$

∎

This Lemma allows us to replace α with an α' such that the principal part of α is 0 or $v(\alpha)$ is odd. The next two propositions treat these cases.

Proposition 1.51 *Let $\alpha \in K_v$ with principal part 0 and let α_0 denote the constant coefficient. Then $x^2 + x = \alpha$ has a solution in K_v if and only if $[\alpha_0, \varpi_v) = 0$.*

Proof: First suppose $\alpha_0 = 0$. Then by Proposition 1.49 we have $[0, \varpi_v) = 0$, hence we have to show that $x^2 + x = \alpha$ has a solution in K_v. Set $x := \sum_{n \geq 0} \alpha^{2^n}$. Because $v(\alpha) > 0$ this sum converges and $x^2 = \sum_{n \geq 1} \alpha^{2^n}$. Hence $x^2 + x = \alpha^{2^0} = \alpha$.
Now suppose $\alpha_0 \neq 0$. Let $\alpha' = \alpha - \alpha_0$. By the above there is an $y \in K_v$ such that $y^2 + y = \alpha'$. Hence $x^2 + x = \alpha$ has a solution in K_v if and only if $x^2 + x = \alpha_0$ has a solution in K_v. But this is equivalent to $[\alpha_0, \varpi_v) = 0$. ∎

Proposition 1.52 *Let $\alpha \in K_v$ with non-zero principal part and suppose $v(\alpha)$ is odd. Then $x^2 + x = \alpha$ has no solution in K_v.*

Proof: Suppose there is an $x \in K_v$ with $x^2 + x + \alpha = 0$ and let $v(\alpha) = 2m + 1$ with $m \leq 0$. Then $v(x^2 + x) = 2m + 1$, hence $v(x) = m + \frac{1}{2} \notin \mathbb{Z}$, which is a contradiction.
∎

1.6.4 The case q even, $\mathrm{odd}(R) = 1$

Again we first give an explicit description of the quaternion algebra D and its maximal order Λ.

Lemma 1.53 *Let $R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\}$ be a set of finite places of K with $\deg(\mathfrak{p}_i)$ odd for all i and l even, let r be a monic generator of the ideal $\mathfrak{r} = \prod_{i=1}^{l} \mathfrak{p}_i$ and let $\xi \in k^\star$ with $\mathrm{Trace}_{k/\mathbb{F}_2}(\xi) \neq 0$. Then $D := \left(\frac{\xi, r}{K}\right)$ is ramified exactly at the places $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$.*

Proof: Let $F := K[x]/(x^2+x+\xi)$. By Proposition 1.51 and Proposition 1.49 the extension F_v/K_v is split at every finite place v of even degree, hence by Proposition 1.44 we know that D is unramified at every finite place of even degree. At a finite place v of odd degree we know that F_v/K_v is non-split, but since $v(\xi) = 0$ we also know that F_v/K_v is unramified. Hence by Proposition 1.46 we have $r \notin \mathrm{Norm}_{F_v/K_v}(F_v^\star)$ if and only if v is one of the places $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$. So by Proposition 1.45 D has the claimed ramification property at all finite places.
At the infinite place D has to be unramified since by Proposition 1.18 the number of ramified places of D is even. ∎

Let $D := \left(\frac{\xi, r}{K}\right)$ as in the previous Lemma and $\Lambda := \langle e_1 := 1, e_2 := i, e_3 := j, e_4 := ij\rangle_A$ throughout this section.

Proposition 1.54 *Λ is a maximal order of D.*

Proof: It is clear that Λ is an order of D. We compute the square of the reduced discriminant of Λ as the ideal generated by

$$\det(\mathrm{trd}(e_i e_j)_{i,j=1,\ldots,4}) = \det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & r \\ 0 & 0 & r & 0 \end{pmatrix} = r^2.$$

Hence $\mathrm{disc}(\Lambda) = \mathfrak{r}$ and so Λ is maximal. ∎

Lemma 1.55 *Set $\varepsilon = T^{\deg(r)/2}\xi^{-q/2}$. Then there is an $\alpha \in K_\infty$ such that*

$$(\frac{\alpha}{\varepsilon})^2 + \frac{\alpha}{\varepsilon} + (\xi + \frac{r}{\varepsilon^2}) = 0.$$

Proof: Since $\deg(r)$ is even we have $\varepsilon \in K$. By the definition of ε we have $v_\infty(\xi + \frac{r}{\varepsilon^2}) \geq 1$, hence by Proposition 1.51 there is an $x \in K_\infty$ such that $x^2 + x = \xi + \frac{r}{\varepsilon^2}$ and hence $\alpha := x\varepsilon$ does the job. ∎

Fix α and ε as in the previous Lemma throughout this section.

Proposition 1.56 *The map $\iota : D \to M_2(K_\infty)$ defined by $i \mapsto \begin{pmatrix} 0 & \xi \\ 1 & 1 \end{pmatrix}$ and $j \mapsto \begin{pmatrix} \alpha & \xi\varepsilon + \alpha \\ \varepsilon & \alpha \end{pmatrix}$ gives an isomorphism of $D \otimes_K K_\infty \cong M_2(K_\infty)$.*

Proof: As in Lemma 1.33 we have to check that $\iota(i)$ and $\iota(j)$ fulfil the relations from Definition 1.12. We have

$$\iota(i)^2 = \begin{pmatrix} 0 & \xi \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} \xi & 0 \\ 0 & \xi \end{pmatrix} + \begin{pmatrix} 0 & \xi \\ 1 & 1 \end{pmatrix} = \xi\iota(1) + \iota(i)$$

and

$$\iota(j)^2 = \begin{pmatrix} \alpha & \xi\varepsilon + \alpha \\ \varepsilon & \alpha \end{pmatrix}^2 = \begin{pmatrix} \alpha^2 + \xi\varepsilon^2 + \alpha\varepsilon & 0 \\ 0 & \alpha^2 + \xi\varepsilon^2 + \alpha\varepsilon \end{pmatrix} = r\iota(j)$$

by the choice of α and ε. Finally we have

$$\iota(i)\iota(j) = \begin{pmatrix} 0 & \xi \\ 1 & 1 \end{pmatrix}\begin{pmatrix} \alpha & \xi\varepsilon + \alpha \\ \varepsilon & \alpha \end{pmatrix} = \begin{pmatrix} \xi\varepsilon & \xi\alpha \\ \alpha + \varepsilon & \xi\varepsilon \end{pmatrix} = \begin{pmatrix} \alpha & \xi\varepsilon + \alpha \\ \varepsilon & \alpha \end{pmatrix}\begin{pmatrix} 1 & \xi \\ 1 & 0 \end{pmatrix}$$

$$= \iota(j)(\iota(i) + \iota(1)).$$

∎

We can compute the first n coefficients of α in $K_\infty = k((\pi))$ in time $\mathcal{O}(n)$ by Newton iteration, or we can use the constructive proof of Proposition 1.51.
Let $v_0 := [L(0,0)]$. We have

$$\mathrm{Stab}_\Gamma(v_0) = \mathrm{GL}_2(O_\infty)K_\infty^\star \cap \Gamma \supseteq \{a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & \xi \\ 1 & 1 \end{pmatrix} \mid a, b \in k, (a,b) \neq (0,0)\}.$$

Hence the vertex v_0 is projectively unstable and $\pi(v_0)$ is a terminal vertex of $\Gamma\backslash\mathcal{T}$. Let $v_1 := [L(1,0)]$. As in the case of q odd and $\mathrm{odd}(R) = 1$ we distinguish the cases $V_{q+1} = 0$ or $V_{q+1} \neq 0$. In the first case v_1 is also projectively unstable, $\pi(v_1)$ a terminal vertex of $\Gamma\backslash\mathcal{T}$ and $\Gamma\backslash\mathcal{T}$ consists of one edge connecting two terminal vertices. In the other case v_1 is projectively stable and we use it as the initial vertex for the algorithm 1.26. Hence Lemma 1.9 tells us that in the n-th step of the algorithm we need to compare vertices of the form $[L(n, g(\pi))]$, where $g \in k[T]$ with $\deg(g) < n$ and $g(0) = 0$. We can do this in time $\mathcal{O}(n^2)$:

Proposition 1.57 *Given $v = [L(n, g(\pi))]$ and $v' = [L(n, g'(\pi))]$ as above there is an algorithm that computes $\mathrm{Hom}_\Gamma(v', v)$ in time $\mathcal{O}(n^2)$.*

Proof: Since the proof is very similar to that of Proposition 1.34, we only sketch the proof.
We have to compute the set

$$(\gamma M_2(O_\infty)(\gamma')^{-1}) \cap \Lambda) \setminus \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}$$

where

$$\gamma = \begin{pmatrix} \pi^n & g(\pi) \\ 0 & 1 \end{pmatrix}, \gamma' = \begin{pmatrix} \pi^n & g'(\pi) \\ 0 & 1 \end{pmatrix}.$$

Any element $\tau \in \Lambda$ can be written as

$$\tau = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & \xi \\ 1 & 1 \end{pmatrix} + c\begin{pmatrix} \alpha & \xi\varepsilon + \alpha \\ \varepsilon & \alpha \end{pmatrix} + d\begin{pmatrix} \xi\varepsilon & \xi\alpha \\ \alpha + \varepsilon & \xi\varepsilon \end{pmatrix}.$$

Then $\tau \in \gamma M_2(O_\infty)(\gamma')^{-1})$ means that there are $v, w, x, y \in O_\infty$ such that

$$\tau = \begin{pmatrix} v + \pi^{-n}g(\pi)x & g'(\pi)v + \pi^n w + \pi^{-n}g(\pi)g'(\pi)x + g(\pi)y \\ \pi^{-n}x & g'(\pi)\pi^{-n}x + y \end{pmatrix},$$

hence

$$B\begin{pmatrix} v \\ w \\ x \\ y \end{pmatrix} = A\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

with

$$A = \begin{pmatrix} 1 & 0 & \alpha & \xi\varepsilon \\ 0 & \xi & \xi\varepsilon + \alpha & \xi\alpha \\ 0 & 1 & \varepsilon & \alpha + \varepsilon \\ 1 & 1 & \alpha & \xi\varepsilon \end{pmatrix}$$

and

$$B = \begin{pmatrix} 1 & 0 & g(\pi)\pi^{-n} & 0 \\ g'(\pi) & \pi^n & g(\pi)g'(\pi)\pi^{-n} & g(\pi) \\ 0 & 0 & \pi^{-n} & 0 \\ 0 & 0 & \pi^{-n}g'(\pi) & 1 \end{pmatrix}.$$

Hence

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = A^{-1}B\begin{pmatrix} v \\ w \\ x \\ y \end{pmatrix}$$

and multiplying the matrices we see that the tupel (a, b, c, d) depends only on v_0, y_0 and $x_0, \ldots, x_n$ where x_i denotes the i-th coefficient of x (v_0, y_0 respectively). Regarding v_0, y_0 and $x_0, \ldots, x_n$ as indeterminates we get polynomials $a_{v_0,y_0,x_0,\ldots,x_n}, \ldots,$ $d_{v_0,y_0,x_0,\ldots,x_n} \in k[T]$ whose coefficients are linear forms in $v_0, y_0, x_0, \ldots, x_n$ and

$$\mathrm{Hom}_\Gamma(v', v) = B^{-1}A\begin{pmatrix} a_{v_0,y_0,x_0,\ldots,x_n} \\ b_{v_0,y_0,x_0,\ldots,x_n} \\ c_{v_0,y_0,x_0,\ldots,x_n} \\ d_{v_0,y_0,x_0,\ldots,x_n} \end{pmatrix} \in O_\infty^4 \setminus \{\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\}.$$

Since $B^{-1}A$ has entries with valuation greater or equal $-n - \deg(r)/2$ this leads to at most $8n + 2\deg(r)$ linear equations over k in $n + 3$ variables. To obtain this equations we need to know an approximation of α up to $2n + \deg(r)/2$ coefficients. Solving these linear equations can be done in time $\mathcal{O}(n^2)$ using Gauss elimination.

■

1.6.5 The case q even, $\mathrm{odd}(R) = 0$

1.7 Presentations of Γ and the word problem

From $\Gamma\backslash\mathcal{T}$ plus the labels on edges and projectively unstable vertices from algorithm 1.26 we can construct a presentation of Γ as an abstract group. This has been explained in [Se1, Chapter I.4] interpreting Γ as the amalgam of the stabilizers of the vertices of $\Gamma\backslash\mathcal{T}$ along the stabilizers of the edges connecting them. Compare also [Pa, Theorem 3.6].
We cite the facts we will use from [Se1] to construct a presentation of Γ.

Definition 1.58 *(a) A maximal subtree $\mathcal{S}$ of a graph $\mathcal{G}$ is a subgraph $\mathcal{S} \subset \mathcal{G}$ which is a tree and such that for any subgraph $\mathcal{S} \subsetneq \mathcal{G}' \subset \mathcal{G}$ we have $\mathcal{G}'$ is not a tree.*

(b) Let G be a group action on a graph $\mathcal{X}$. A tree of representatives of $\mathcal{X}$ $\pmod{G}$ is any subtree $\mathcal{S}$ of $\mathcal{X}$ which is the lift of a maximal subtree of $G\backslash\mathcal{X}$.

In our example Γ acts on the tree $\mathcal{T}$. If we remove any edge of $\Gamma\backslash\mathcal{T}$ labelled with an element of Γ, then we obtain a maximal subtree of $\Gamma\backslash\mathcal{T}$. This subtree can be lifted to a subtree $\mathcal{S}$ of $\mathcal{T}$ containing the initial vertex v. This lift is a tree of representatives of $\mathcal{T}$ $\pmod{G}$.

Lemma 1.59 *Let G be a group acting on a connected graph $\mathcal{X}$ and let $\mathcal{S}$ be a tree of representatives of $\mathcal{X}$ $\pmod{G}$. Let $\mathcal{Y}$ be a subgraph of $\mathcal{X}$ containing $\mathcal{S}$ such that the projection $\mathrm{Edg}(\mathcal{Y}) \to \mathrm{Edg}(G\backslash\mathcal{X})$ is a bijection and such that each edge $e \in \mathrm{Edg}(\mathcal{Y})$ has $t(e)$ or $o(e) \in \mathrm{Ver}(\mathcal{S})$. For each edge $e \in \mathrm{Edg}(\mathcal{Y})$ with $o(e) \in \mathcal{S}$ let g_e be an element of G with $g_e t(e) \in \mathrm{Ver}(\mathcal{S})$. Then G is isomorphic to the group generated by*

$$\{g_e \mid e \in \mathrm{Edg}(\mathcal{Y})\} \cup \{\mathrm{Stab}_G(v) \mid v \in \mathrm{Ver}(\mathcal{S})\}.$$

Proof: This is [Se1, Lemma I.4.4] ∎

Each edge $\bar{e} = (\bar{v}_1, \bar{v}_2)$ of $\Gamma\backslash\mathcal{T}$ which has a label is labelled with either a $\gamma \in \mathrm{Hom}_\Gamma(v_1, w_2)$ or $\gamma \in \mathrm{Hom}_\Gamma(w_1, v_2)$ where v_1 and v_2 are the lifts of $\bar{v}_1$ and $\bar{v}_2$ in $\mathcal{S}$ and w_1 and w_2 are adjacent vertices of v_1 and v_2 in $\mathcal{T}$. The subtree $\mathcal{Y}$ of $\mathcal{T}$ from the Lemma can then be obtain by adding the vertices w_i for each non-trivially labelled edge of $\Gamma\backslash\mathcal{T}$. The edge-label γ than maps w_i to some vertex of $\mathcal{S}$. Hence the Lemma implies that G is generated by the edge-labels plus the stabilizers of all vertices from the tree of representatives $\mathcal{S}$.
The relations these elements have to fulfil come from Theorem 13 of [Se1, Chapter I.5] and the construction of the fundamental group $\pi(\Gamma, \mathcal{Y}, \mathcal{S})$ on [Se1, Page 42]. In our case, since for all non-terminal vertices v of $\mathcal{S}$ we have $\mathrm{Stab}_\Gamma(v) = k^\star$, which commutes with all $\gamma \in \Gamma$, the relations are rather simple and we obtain the following:

Proposition 1.60 *Let $\Gamma\backslash\mathcal{T}$ be the output of algorithm 1.26. Fix a generator γ_v of $\mathrm{Stab}_\Gamma(v)$ for each terminal vertex of $\Gamma\backslash\mathcal{T}$ (these stabilizers have been attached to the vertices by the algorithm). Then Γ is isomorphic to the group generated by*

$$\{\sigma\} \cup \{\gamma_v \mid v \textit{ terminal in } \Gamma\backslash\mathcal{T}\} \cup \{\gamma \mid \gamma \textit{ appears as an edge-label of } \Gamma\backslash\mathcal{T}\}$$

subject to the relations

$$\sigma^{q-1} = 1,\ \gamma_v^{q+1} = \sigma \textit{ for all } v,\ [\sigma, \gamma] = 1 \textit{ for all } \gamma \textit{ in the edge-labels.}$$

In particular σ lies in the center of Γ, as it should.

Example 1.61 In the Example 1.30 the group Γ is generated by

$$\{\sigma, \gamma_{v_1}, \ldots, \gamma_{v_8}, \gamma_1, \ldots, \gamma_5\}$$

with relations

$$\sigma^4 = 1, \gamma_{v_i}^6 = \sigma, [\sigma, \gamma_i] = 1.$$

The word problem with respect to this set of generators was already solved by the reduction algorithm from algorithm 1.28.

References

[Co] **Keith Conrad:** Quadratic reciprocity in characteristic 2, *unpublished, http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/QRcharp.pdf*

[Ja] **Nathan Jacobson:** Basic algebra II, *Freeman* (1980)

[JS] **Jens Carsten Jantzen, Joachim Schwermer** Algebra, *Springer-Lehrbuch* (2006)

[Pa] **Mihran Papikian:** Trees, quaternion algebras and modular curves, *preprint* (2009)

[Ro] **Michael Rosen:** Number theory in function fields, *Springer Graduate Texts in Mathematics* (2000)

[Se1] **Jean-Pierre Serre:** Trees, *Springer Verlag* (1980)

[Se2] **Jean-Pierre Serre:** A course in arithmetic, *Springer Verlag, Graduate Texts in Mathematics, vol. 7* (1973)

[Vi] **Marie-France Vignéras:** Arithmétique des Algèbres de Quaternions, *Springer Verlag, Lecture Notes in Mathematics, vol. 800* (1980)