RAMIFICATION SEQUENCES AND BEZOUTIAN FORMS

KARIM JOHANNES BECHER AND MÉLANIE RACZEK

Abstract. We continue our study from [1] on the problem to bound the number of symbols needed to obtain an element of the second K-group of a rational function field with given ramification. Here we focus on the case of Milnor K-groups modulo 2 for fields of characteristic different from 2. To a given ramification sequence, we associate a quadratic form defined over the base field and study its properties. In particular, we relate the Witt index of the quadratic form to the minimal number of symbols necessary to represent the ramification sequence.

Keywords: Milnor K-theory, quadratic form, valuation, ramification

Classification (MSC 2010): 12E30, 12G05, 12Y05, 19D45

1. Introduction

Let K_1 and K_2 denote the functors associating to a field its first and second K-group. Let E be a field and let F be the function field of the projective line $\mathbb{P}^1_E$ over E. Let $\mathbb{P}^{1(1)}_E$ denote the set of closed points of $\mathbb{P}^1_E$.

Let $m \in \mathbb{N}$. There is a natural exact sequence

$$0 \longrightarrow K_2E/m \longrightarrow K_2F/m \xrightarrow{\partial} \bigoplus_{x\in\mathbb{P}^{1(1)}_E} K_1E(x)/m \longrightarrow K_1E/m \longrightarrow 0\,, \tag{1.1}$$

due to Tate (cf. [7, (2.3)]), where ∂ denotes the *ramification map*. By a ramification sequence we mean an element in the direct sum term whose image in K_1E/m is trivial and which therefore lies in the image of ∂. The group K_2F/m has a canonical set of generators, which are called *symbols*. Given a ramification sequence ρ one may ask how many symbols are needed to obtain an element $\xi \in K_2F/m$ such that $\partial(\xi) = \rho$. Without restrictions on E, in [1] for a ramification sequence ρ we constructed an element $\xi \in K_2F/m$ such that $\partial(\xi) = \rho$ and ξ is a sum of r symbols, where r is the integral part of the degree of ρ divided by two. We further gave examples where this bound is best possible.

We continue our investigation of the problem of bounding the number of symbols needed for representing a given ramification, but restricted to the case where $m = 2$ and $\mathrm{char}(E) \neq 2$. Thus we consider the K-group $k_2F = K_2F/2$ which by Merkurjev's Theorem is naturally isomorphic to $\mathrm{Br}_2(F)$, the 2-torsion part

Date: October 20, 2016.

of the Brauer group of F. Hence, the problem can be reinterpreted as a problem in terms of central simple algebras, where symbols correspond to quaternion algebras.

In this setting we relate the problem to quadratic form theory. The connection is made via pairs (f, g) of square-free coprime polynomials $f, g \in E[t]$. On the one hand, any ramification sequence can be represented by such a pair. On the other hand, any such pair gives rise to a quadratic form over E, closely related to the so-called *Bezoutian* of f and g introduced by Sylvester and Cayley.

In Section 2 we recall the necessary notions and statements from Milnor's K-theory involved in the above exact sequence (in the case of k_2). In Section 3 we study the properties of the Bezoutian of a pair of polynomials (f, g) as above in our setting. In particular, we characterise the isotropy of this form (Proposition 3.4) and we obtain a reciprocity law (Corollary 3.9), which together will be crucial in Section 5.

In Section 4 we consider a pair (f, g) coming from a specific representation of a symbol and show that the associated Bezoutian is hyperbolic provided that the symbol is unramified at ∞ (Proposition 4.4).

In Section 5, given a ramification sequence ρ we construct a sequence of polynomials which yields a representation of ρ as a sum of symbols. If ρ is given by the pair (f, g), we obtain an upper bound on the number of symbols needed to represent ρ in terms of the Witt index of the Bezoutian of (f, g) (Theorem 5.9). It refines the bound from [1, Theorem 3.10]: the larger the Witt index, the better the improvement.

The final section illustrates our study by results and examples for ramification sequences of small degree. In particular, we obtain a criterion for a ramification sequence of degree four to be represented by a symbol (Theorem 6.1). This generalises a result due to Sivatski in [8, Prop. 1.4], which inspired our investigation.

2. Preliminaries

Let F be a field. Let k_2F denote the abelian group generated by *symbols*, which are elements of the form $\{a, b\}$ with $a, b \in F^\times$, subject to the defining relations that the pairing

$$\{\cdot, \cdot\} : F^\times \times F^\times \longrightarrow k_2F$$

is bilinear, $\{a, 1-a\} = 0$ for any $a \in F^\times \setminus \{1\}$ and $\{a^2, b\} = 0$ for all $a, b \in F^\times$. It follows from the defining relations that k_2F is 2-torsion and that, for any $a, b \in F^\times$, we have $\{a, b\} = \{b, a\}$, and further $\{a, b\} = \{a+b, -ab\}$ provided that $b \neq -a$. Let k_1F denote the square class group $F^\times/F^{\times 2}$ in additive notation, where we write $\{a\} \in k_1F$ for the element given by the square class of $a \in F^\times$ and thus have $\{a\}+\{b\} = \{ab\}$ for $a, b \in F^\times$. Note that $k_iF = K_iF/2$ for $i = 1, 2$ in the notation used in the introduction.

By a *global field* we mean a field F that is either a finite extension of $\mathbb{Q}$ or a function field in one variable over a finite field.

2.1. **Proposition.** *If F is a global field then every element of k_2F is a symbol.*

Proof. This follows from the corresponding statement for K_2F. It was shown in [6] that every element of K_2F is a symbol, and as $k_2F = K_2F/2$ our statement follows. If $\mathrm{char}(F) \neq 2$ then one can argue alternatively that by the Hasse-Minkowski Theorem any quadratic form in six variables of determinant -1 is isotropic, which implies the statement. $\square$

By a $\mathbb{Z}$-*valuation* on a field we mean a valuation with value group $\mathbb{Z}$. Given a $\mathbb{Z}$-valuation v on F we denote by $\mathcal{O}_v$ its valuation ring and by κ_v its residue field. For $a \in \mathcal{O}_v$ let $\overline{a}$ denote the natural image of a in κ_v. By [7, (2.1)], for $n \geqslant 2$ and a $\mathbb{Z}$-valuation v on F, there is a unique homomorphism $\partial_v : k_2F \longrightarrow k_1\kappa_v$ such that

$$\partial_v(\{f,g\}) = v(f)\cdot\{\overline{g}\} \text{ in } k_1\kappa_v$$

for $f \in F^\times$ and $g \in \mathcal{O}_v^\times$. For $f,g \in F^\times$ we obtain that $f^{-v(g)}g^{v(f)} \in \mathcal{O}_v^\times$ and

$$\partial_v(\{f,g\}) = \{(-1)^{v(f)v(g)}\overline{f^{-v(g)}g^{v(f)}}\} \text{ in } k_1\kappa_v\,.$$

We turn to the situation where F is the function field of $\mathbb{P}^1_E$ over a field E. By the choice of a generator, we identify F with the rational function field $E(t)$ in the variable t over E. Let $\mathcal{P}$ denote the set of monic irreducible polynomials in $E[t]$. Any $p \in \mathcal{P}$ determines a $\mathbb{Z}$-valuation v_p on $E(t)$ that is trivial on E and such that $v_p(p) = 1$. There is further a unique $\mathbb{Z}$-valuation v_∞ on $E(t)$ such that $v_\infty(f) = -\deg(f)$ for any $f \in E[t]\setminus\{0\}$. We set $\mathcal{P}' = \mathcal{P}\cup\{\infty\}$. For $p \in \mathcal{P}'$ we write ∂_p for ∂_{v_p} and we denote by E_p the residue field of v_p. Note that, for $p \in \mathcal{P}$, E_p is naturally isomorphic to $E[t]/(p)$, and E_∞ is naturally isomorphic to E.

It follows from [7, Sect. 2] that the sequence

$$0 \longrightarrow k_2E \longrightarrow k_2E(t) \xrightarrow{\bigoplus \partial_p} \bigoplus_{p\in\mathcal{P}} k_1E_p \longrightarrow 0 \tag{2.2}$$

is split exact. We reformulate this fact and relate (2.2) to (1.1). We set

$$\mathfrak{R}_2'(E) = \bigoplus_{p\in\mathcal{P}'} k_1E_p\,.$$

(The index 2 is a reminiscence to the fact that we are working with Milnor K-groups modulo 2.)

For $p \in \mathcal{P}'$, the norm map of the finite extension E_p/E yields a group homomorphism $k_1E_p \longrightarrow k_1E$. Summation over these maps for all $p \in \mathcal{P}'$ yields a homomorphism $\mathrm{N} : \mathfrak{R}_2'(E) \longrightarrow k_1E$. Let $\mathfrak{R}_2(E)$ denote the kernel of N. We call $\partial = \bigoplus_{p\in\mathcal{P}'}\partial_p$ the *ramification map*. By [2, (7.2.4) and (7.2.5)] we obtain an exact sequence

$$0 \longrightarrow k_2E \longrightarrow k_2E(t) \xrightarrow{\partial} \mathfrak{R}_2'(E) \xrightarrow{\mathrm{N}} k_1E \longrightarrow 0\,. \tag{2.3}$$

In particular, $\mathfrak{R}_2(E)$ is equal to the image of $\partial : k_2E(t) \longrightarrow \mathfrak{R}_2'(E)$. The elements of $\mathfrak{R}_2(E)$ are therefore called *ramification sequences.*

The choice of the generator of F over E fixes a bijection $\phi : \mathbb{P}^{1(1)}_E \longrightarrow \mathcal{P}'$ and for any $x \in \mathbb{P}^{1(1)}_E$ a natural isomorphism between $E(x)$ and $E_{\phi(x)}$. This identifies $\bigoplus_{x\in\mathbb{P}^{1(1)}_E} k_1E(x)$ with $\mathfrak{R}'_2(E)$, and further the sequence (1.1) with (2.3). We will work with (2.3) in the sequel.

For a finite set $S \subseteq \mathcal{P}'$ we call $\sum_{p\in S}[E_p : E]$ the *degree of* S and denote it by $\deg(S)$. For $\rho = (\rho_p)_{p\in\mathcal{P}'} \in \mathfrak{R}'_2(E)$ we denote $\mathrm{Supp}(\rho) = \{p \in \mathcal{P}' \mid \rho_p \neq 0\}$ and $\deg(\rho) = \deg(\mathrm{Supp}(\rho))$, and we call this the *support* and the *degree of* ρ.

Given a ramification sequence $\rho \in \mathfrak{R}_2(E)$, we say that ρ *is represented by* $\xi \in k_2E(t)$ if $\partial(\xi) = \rho$. The problem at the centre of our study is to obtain a good upper bound on the smallest $n \in \mathbb{N}$ such that ρ is represented by a sum of n symbols in $k_2E(t)$.

2.4. **Example.** Assume that the field E is finite. Then by Proposition 2.1 every element of $k_2E(t)$ is a symbol. In particular, any ramification sequence in $\mathfrak{R}_2(E)$ is represented by a symbol.

For $x \in \mathbb{R}$ we set $\lfloor x\rfloor = \max\{z \in \mathbb{Z} \mid z \leqslant x\}$ and $\lceil x\rceil = \min\{z \in \mathbb{Z} \mid z \geqslant x\}$.

In [1, Theorem 3.10] we proved the following statement:

2.5. **Theorem.** *Any ramification sequence $\rho \in \mathfrak{R}_2(E)$ is represented by a sum of n symbols for $n = \lfloor \frac{\deg(\rho)}{2} \rfloor$.*

3. Bezoutians

From now on we assume that the field E has characteristic different from 2. We study a quadratic form given by two polynomials $f, g \in E[t]$ where g is square-free and f is coprime to g. This quadratic form is obtained by a transfer and it is closely related to the Bezoutian of the polynomials f and g, introduced by Sylvester and Cayley. We shall develop some rules of computation, including a reciprocity law (Theorem 3.8).

We start by recalling some basic concepts and terminology from quadratic form theory. For a non-degenerate quadratic form φ over E, we denote by $[\varphi]$ its Witt equivalence class, which we view as an element of the *Witt ring* WE.

For $\alpha \in WE$ we denote by $\mathrm{diman}(\alpha)$, the dimension of the unique anisotropic quadratic form φ over E such that $\alpha = [\varphi]$, and call this the *anisotropic dimension of* α. In other terms, given a quadratic form φ over E, we have

$$\dim(\varphi) = \mathrm{diman}([\varphi]) + 2i_W(\varphi)$$

where $\dim(\varphi)$ and $i_W(\varphi)$ are the dimension and the Witt index of φ. Unlike the dimension, the anisotropic dimension of a non-degenerate quadratic form depends only on its Witt equivalence class. Recall that the fundamental ideal IE consists of the classes $[\varphi]$ of even-dimensional quadratic forms φ over E. We denote by I^2E the square of this ideal. For $a \in E^\times$ we denote by $[a]$ the class in WE of the one-dimensional quadratic form $\langle a\rangle$ over E. Since quadratic forms over E are diagonalisable, WE is additively generated by the elements $[a]$ with $a \in E^\times$. Note that the unity in WE is the Witt equivalence class $[1]$, which we simply denote by 1. The element 0 in WE is given by the trivial quadratic form. A quadratic form over E is said to be *split* if it is either hyperbolic or Witt equivalent to a one-dimensional quadratic form. Recall that the discriminant of a quadratic form φ over E is defined as the class of $(-1)^{\frac{n(n-1)}{2}}\det(M)$ in $E^\times/E^{\times 2}$ where $n = \dim(\varphi)$ and where M is the matrix of φ with respect to an arbitrary E-basis. The discriminant is an invariant of the Witt equivalence class of a form.

Let $g \in E[t]$ be square-free. Let θ denote the class of t in $E_g = E[t]/(g)$, $n = \deg(g)$, and let $s_g : E_g \longrightarrow E$ be the E-linear form with $s_g(\theta^i) = 0$ for $i = 0, \dots, n-2$ and $s_g(\theta^{n-1}) = 1$.

3.1. **Proposition.** *Let $f, g \in E[t]$ be coprime and $\theta = t + (g)$ in E_g. The quadratic map*

$$q : E_g \longrightarrow E, x \mapsto s_g(f(\theta)x^2)$$

is non-degenerate. The quadratic form (E_g, q) has discriminant $\mathrm{N}_{E_g/E}(f(\theta))E^{\times 2}$. The Witt index of this form is at least $\lfloor \frac{\deg(g)-\deg(f)}{2} \rfloor$. In particular, if f is constant then (E_g, q) is split.

Proof. Set $n = \deg(g)$. Let $B = (b_{ij})_{i,j} \in \mathbb{M}_n(E)$ be given by

$$f(\theta)\theta^{j-1} = \sum_{i=1}^{n} b_{ij}\theta^{i-1}\,.$$

For $j, k = 1, \dots, n$ we obtain that

$$s_g(f(\theta)\theta^{j-1}\theta^{k-1}) = \sum_{i=1}^{n} b_{ij}s_g(\theta^{i-1}\theta^{k-1}).$$

With $C_1 = (s_g(\theta^{i-1}\theta^{j-1}))_{i,j} \in \mathbb{M}_n(E)$ and $C_f = (s_g(f(\theta)\theta^{i-1}\theta^{j-1}))_{i,j} \in \mathbb{M}_n(E)$ we obtain that $C_f = C_1 \cdot B$ and in particular

$$\det(C_f) = \det(C_1) \cdot \det(B)\,.$$

Note that $\mathrm{N}_{E_g/E}(f(\theta)) = \det(B)$ and

$$C_1 = \begin{pmatrix} 0 & \dots & 0 & 1 \\ \vdots & ⋰ & ⋰ & * \\ 0 & ⋰ & ⋰ & \vdots \\ 1 & * & \dots & * \end{pmatrix}$$

in view of the definition of s_g. Therefore

$$\det(C_f) = (-1)^{\lfloor \frac{n}{2} \rfloor} \cdot \mathrm{N}_{E_g/E}(f(\theta))\,.$$

As C_f is the matrix of the quadratic form q with respect to the basis $1, \theta, \dots, \theta^{n-1}$, this confirms that the quadratic form (E_g, q) is non-degenerate of discriminant $\mathrm{N}_{E_g/E}(f(\theta))E^{\times 2} \in E^\times/E^{\times 2}$.

Furthermore, for $k = \lfloor \frac{\deg(g)-\deg(f)}{2} \rfloor$ the vectors $1, \dots, \theta^{k-1}$ span a totally isotropic subspace of (E_g, q), so the Witt index of (E_g, q) is at least k. □

We call the quadratic form in Proposition 3.1 the *Bezoutian form of f modulo g*. We are indebted to J.-P. Tignol for pointing out to us a different way of obtaining this quadratic form.

3.2. **Proposition** (Tignol). *Let $f, g \in E[t]$ be coprime such that g is monic and square-free and $\deg(f) \leqslant \deg(g)$. Set $\theta = t + (g)$ in E_g. For $n = \deg(g)$ let $A = (a_{ij})_{i,j} \in \mathbb{M}_n(E)$ be the symmetric matrix given by*

$$\frac{g(X)f(Y) - f(X)g(Y)}{X - Y} = \sum_{i,j=1}^{n} a_{ij} X^{i-1} Y^{j-1}.$$

Then the quadratic forms

$$E_g \to E \colon x \mapsto s_g(f(\theta)x^2) \quad \textit{and} \quad E^n \to E \colon u \mapsto u^t A u$$

are isometric.

Proof. We factorize

$$g(X) = (X - \theta)h(X)$$

with $h(X) \in E_g[X]$. By definition of A we have

$$\sum_{i,j=1}^{n} a_{ij} X^{i-1} \theta^{j-1} = \frac{g(X)f(\theta) - g(\theta)f(X)}{X - \theta} = h(X)f(\theta).$$

We extend s_g to an $E[X]$-linear map $E_g[X] \to E[X]$. We can write

$$h(X) = X^{n-1} + h_1(\theta)X^{n-2} + \cdots + h_{n-2}(\theta)X + h_{n-1}(\theta)$$

with polynomials $h_1, \dots, h_{n-1} \in E[Y]$ of degree at most $n-1$. Since $g \in E[X]$ we obtain recursively for $i = 1, \dots, n-1$ that h_i is monic of degree i. Hence

$$s_g(h(X)) = s_g(h_{n-1}(\theta)) = 1\,.$$

For any positive integer k we have

$$\sum_{i,j=1}^{n} a_{ij} f(\theta)^{-1} X^{i-1} \theta^{j+k-2} = h(X)\theta^{k-1}.$$

If $1 < k \leqslant n$, then

$$(X^{k-1} - \theta^{k-1})h(X) = g(X)(X^{k-2} + X^{k-3}\theta + \ldots + X\theta^{k-3} + \theta^{k-2})$$

and s_g maps the right side to 0, showing that

$$\sum_{i,j=1}^{n} a_{ij} s_g(f(\theta)^{-1}\theta^{j+k-2}) X^{i-1} = s_g\left(h(X)\theta^{k-1}\right) = s_g\left(h(X)X^{k-1}\right) = X^{k-1}.$$

The last equality also holds for $k = 1$. Hence, for any $i, k \in \{1, \dots, n\}$, we have

$$\sum_{j=1}^{n} a_{ij} s_g(f(\theta)^{-1}\theta^{j+k-2}) = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k. \end{cases}$$

This shows that A is the inverse of $\left(s_g(f(\theta)^{-1}\theta^{i+j-2})\right)_{i,j}$, which is the representing matrix of q with respect to the E-basis $(f(\theta)^{-1}\theta^i)_{i=0}^{n-1}$ of E_g. Finally, since A is symmetric, it is congruent to A^{-1}. This proves the statement. □

More generally, for any two coprime polynomials $f, g \in E[t]$, denoting by n the maximum of $\deg(f)$ and $\deg(g)$ the matrix $A \in \mathbb{M}_n(E)$ given by the formula in Proposition 3.2 defines a non-degenerate n-dimensional quadratic form over E, called the *Hankel-Bezoutian of f and g*. This quadratic form has interesting properties and seems to have been studied considerably in the literature (cf. [3]). The Bezoutian form of f modulo g coincides with the Hankel-Bezoutian of f and g in the situation of Proposition 3.2. In general, the two concepts behave differently.

Given two polynomials $f, g \in E[t]$ with g square-free and prime to f, we write

$$\mathfrak{B}\left(\frac{f}{g}\right)$$

for the class in WE given by the Bezoutian form of f modulo g.

3.3. **Proposition.** *For any $a \in E^\times$ and $f, g, h \in E[t]$ with g square-free and coprime to fh, one has*

$$\mathfrak{B}\left(\frac{afh^2}{g}\right) = [a] \cdot \mathfrak{B}\left(\frac{f}{g}\right).$$

Proof. This follows directly from the properties of the transfer by which $\mathfrak{B}\left(\frac{*}{g}\right)$ is defined. □

3.4. **Proposition.** *Assume that the field E is infinite. Let $f, g \in E[t]$ be coprime with g monic and square-free. Let $\theta = t + (g)$ in E_g. The following are equivalent:*

(*i*) $\operatorname{diman}\left(\mathfrak{B}\left(\frac{f}{g}\right)\right) < \deg(g)$.

(*ii*) *There exists $f' \in E[t]$ such that* $\deg(f') \leqslant \deg(g) - 2$ *and* $f(\theta)f'(\theta) \in E_g^{\times 2}$.

(*iii*) *There exists $f' \in E[t]$ square-free such that* $\deg(f') \leqslant \deg(g) - 2$, $\deg(f') \equiv \deg(g) \bmod 2$ *and* $f(\theta)f'(\theta) \in E_g^{\times 2}$.

Proof. Let $n = \deg(g)$. Let $\widetilde{E}$ be an algebraic closure of E and $\widetilde{E}_g = \widetilde{E}[t]/(g)$. The equation

$$\alpha = \sum_{i=1}^{n} c_i(\alpha)\theta^{n-i} \text{ for } \alpha \in \widetilde{E}_g$$

determines $\widetilde{E}$-linear forms $c_1,\dots,c_n:\widetilde{E}_g\longrightarrow\widetilde{E}$. For $i=1,\dots,n$ we obtain a quadratic form $q_i:\widetilde{E}_g\longrightarrow\widetilde{E}, x\mapsto c_i(f(\theta)x^2)$. The quadratic space $(E_g,q_1|_{E_g})$ over E is non-degenerate and its Witt equivalence class is $\mathfrak{B}\left(\frac{f}{g}\right)$. Hence, Condition (i) is equivalent to saying that $(E_g,q_1|_{E_g})$ is isotropic. In particular, (ii) implies (i). Trivially (iii) implies (ii). It remains to show that (i) implies (iii).

Suppose that there exists $x\in E_g^\times$ with $q_1(x)=0\neq q_2(x)$. Then $\alpha=f(\theta)x^2\in E_g^\times$ and $c_1(\alpha)=0\neq c_2(\alpha)$, whereby $\alpha=h(\theta)$ for a polynomial $h\in E[t]$ coprime to g with $\deg(h)=n-2$. We write $h=f'\cdot\ell^2$ with $f',\ell\in E[t]$ such that f' is square-free. Then $f(\theta)f'(\theta)\in E_g^{\times 2}$ and $\deg(f')=n-2-2\deg(\ell)$, whereby $\deg(f')\leqslant\deg(g)-2$ and $\deg(f')\equiv\deg(g)\bmod 2$.

Hence, we are left with showing that the isotropy of $(E_g,q_1|_{E_g})$ implies the existence of $x\in E_g^\times$ with $q_1(x)=0\neq q_2(x)$.

Suppose first that $n=2$. We choose any $x\in E_g\setminus\{0\}$ with $q_1(x)=0$. As E_g is reduced and $f(\theta)\in E_g^\times$, it follows that $f(\theta)x^2\in E^\times$, whereby $x\in E_g^\times$ and $q_2(x)\neq 0$. Assume now that $n\geqslant 3$. Then q_1 is irreducible. Consider the affine quadrics $Q=\{x\in\widetilde{E}_g\mid q_1(x)=0\}$ and $Q'=\{x\in\widetilde{E}_g\mid q_2(x)=0\}$. It follows that Q is irreducible as a topological space. We choose $\beta\in\widetilde{E}_g$ with $c_1(\beta)=0\neq c_2(\beta)$. As $\widetilde{E}_g^\times=\widetilde{E}_g^{\times 2}$, there exists $y\in\widetilde{E}_g$ such that $\beta=f(\theta)y^2$, and then $q_1(y)=0\neq q_2(y)$. Hence $Q\not\subseteq Q'$, whereby $Q\setminus Q'$ is a non-empty Zariski open subset of Q. The complement of $\widetilde{E}_g^\times$ in $\widetilde{E}_g$ is a union of n affine hyperplanes, and therefore does not contain Q. Hence $\widetilde{E}_g^\times\cap Q$ is a non-empty Zariski open subset of Q. As Q is irreducible we conclude that $(Q\setminus Q')\cap(\widetilde{E}_g^\times\cap Q)=\widetilde{E}_g^\times\cap(Q\setminus Q')$ is also a non-empty Zariski open subset of Q. As (E_g,q_1) is isotropic, Q is rational over E. It follows that the set of E-rational points of Q is dense in Q. Hence $\widetilde{E}_g^\times\cap(Q\setminus Q')$ contains an E-rational point. In other words, there exists an element $x\in E_g^\times\cap(Q\setminus Q')$, and then $q_1(x)=0\neq q_2(x)$. □

In the sequel we give formulae for computing Bezoutians $\mathfrak{B}\left(\frac{f}{g}\right)$ where both $f,g\in E[t]$ are monic and square-free. Together with Proposition 3.3 this yields means of computation for more general situations.

3.5. **Proposition.** *For $f,g_1,g_2\in E[t]$ pairwise coprime and with g_1 and g_2 monic and square-free, we have that*

$$\mathfrak{B}\left(\frac{f}{g_1g_2}\right)=\mathfrak{B}\left(\frac{fg_2}{g_1}\right)+\mathfrak{B}\left(\frac{fg_1}{g_2}\right).$$

Proof. Set $g=g_1g_2$. Let θ, θ_1, θ_2 be the images of t in E_g, E_{g_1} and E_{g_2} respectively. Define the map $\Psi:E_{g_1}\oplus E_{g_2}\mapsto E_g$ by

$$\Psi(h_1(\theta_1)+h_2(\theta_2))=(h_1g_2+h_2g_1)(\theta).$$

Then Ψ is a E-vector space isomorphism. For $i = 1, 2$ one has

$$s_{g_i} = (s_g \circ \Psi)|_{E_i} .$$

We consider the quadratic maps

$$\begin{aligned} &q\colon E_g \to E\colon x \mapsto s_g(f(\theta)x^2) \quad \text{and} \\ &q_i\colon E_{g_i} \to E\colon x_i \mapsto s_{g_i}\big((fg_{3-i})(\theta_i)x_i^2\big) \quad \text{for } i = 1, 2. \end{aligned}$$

For $x_1 = h_1(\theta_1)$ and $x_2 = h_2(\theta_2)$ we have $\Psi(x_1) = (h_1g_2)(\theta)$, $\Psi(x_2) = (h_2g_1)(\theta)$ and $\Psi(x_1)\Psi(x_2) = 0$, and therefore

$$\begin{aligned} q(\Psi(x_1 + x_2)) &= s_g\big(f(\theta)(\Psi(x_1) + \Psi(x_2))^2\big) \\ &= s_g\big(f(\theta)\Psi(x_1)^2\big) + s_g\big(f(\theta)\Psi(x_2)^2\big) + 2s_g\big(f(\theta)\Psi(x_1)\Psi(x_2)\big) \\ &= s_g((fh_1^2g_2^2)(\theta)) + s_g((fh_2^2g_1^2)(\theta)) \\ &= (s_g \circ \Psi)\big((fg_2h_1^2)(\theta_1)\big) + (s_g \circ \Psi)\big((fg_1h_2^2)(\theta_2)\big) \\ &= s_{g_1}\big((fg_2)(\theta_1) \cdot x_1^2\big) + s_{g_2}\big((fg_1)(\theta_2) \cdot x_2^2\big) \\ &= q_1(x_1) + q_2(x_2). \end{aligned}$$

Hence Ψ is an isometry between $(E_{g_1}, q_1) \perp (E_{g_2}, q_2)$ and (E_g, q). $\square$

3.6. **Corollary.** *Let $n \in \mathbb{N}$ and $a_1, \dots, a_n \in E^\times$ pairwise distinct and $f \in E[t]$ such that $f(a_i) \neq 0$ for $i = 1, \dots, n$. Then*

$$\mathfrak{B}\left(\frac{f}{\prod_{i=1}^n (t - a_i)}\right) = \sum_{i=1}^n \Big[f(a_i) \prod_{j \neq i} (a_i - a_j)\Big].$$

Proof. For $g = \prod_{i=1}^n (t - a_i)$ we obtain by an iterative application of Proposition 3.5 that

$$\mathfrak{B}\left(\frac{f}{g}\right) = \sum_{i=1}^n \mathfrak{B}\left(\frac{f \prod_{j \neq i}(t - a_j)}{t - a_i}\right) = \sum_{i=1}^n \Big[f(a_i) \prod_{j \neq i} (a_i - a_j)\Big].$$

$\square$

3.7. **Corollary.** *Let $f_1, f_2, g_1, g_2 \in E[t]$ with g_1 and g_2 monic, square-free, relatively coprime and such that f_i is coprime to g_i for $i = 1, 2$. Then*

$$\mathfrak{B}\left(\frac{f_1}{g_1}\right) + \mathfrak{B}\left(\frac{f_2}{g_2}\right) = \mathfrak{B}\left(\frac{f_1g_2 + f_2g_1}{g_1g_2}\right) .$$

Proof. Let $h = f_1g_2 + f_2g_1$. For $i = 1, 2$ we have that $hg_{3-i} \equiv f_i\, g_{3-i}^2 \bmod g_i$. Using Proposition 3.5 and Proposition 3.3 we thus obtain that

$$\mathfrak{B}\left(\frac{h}{g_1g_2}\right) = \mathfrak{B}\left(\frac{hg_2}{g_1}\right) + \mathfrak{B}\left(\frac{hg_1}{g_2}\right) = \mathfrak{B}\left(\frac{f_1}{g_1}\right) + \mathfrak{B}\left(\frac{f_2}{g_2}\right) .$$

$\square$

The Bezoutians studied here satisfy a reciprocity law, which will turn out to be very useful in the sequel of the article.

3.8. **Theorem.** *Let $f, g \in E[t]$ be monic, square-free and relatively coprime. Then*

$$\mathfrak{B}\left(\frac{f}{g}\right) + \mathfrak{B}\left(\frac{g}{f}\right) = \begin{cases} 0 & \text{if } \deg(f) \equiv \deg(g) \bmod 2, \\ 1 & \text{if } \deg(f) \not\equiv \deg(g) \bmod 2. \end{cases}$$

Proof. It follows using Corollary 3.7 and Proposition 3.3 that

$$\mathfrak{B}\left(\frac{f}{g}\right) + \mathfrak{B}\left(\frac{g}{f}\right) = \mathfrak{B}\left(\frac{f^2+g^2}{fg}\right) = \mathfrak{B}\left(\frac{(f+g)^2}{fg}\right) = \mathfrak{B}\left(\frac{1}{fg}\right).$$

By Proposition 3.1 this element of WE is given by the split quadratic form of dimension $\deg(fg)$ and of trivial discriminant. This yields the statement. □

Given two elements $\alpha, \beta \in WE$, we write $\alpha \sim \beta$ if $\beta = c\alpha$ for some $c \in E^\times$, that is, if α and β are given by quadratic forms over E that are similar.

3.9. **Corollary.** *Let $f, g \in E[t]$ be square-free, relatively coprime and such that* $\deg(f) \equiv \deg(g) \bmod 2$. *Then*

$$\mathfrak{B}\left(\frac{f}{g}\right) \sim \mathfrak{B}\left(\frac{g}{f}\right).$$

Proof. Let $a, b \in E^\times$ and $f', g' \in E[t]$ monic such that $f = af'$ and $g = bg'$. Using Theorem 3.8 we obtain that

$$\mathfrak{B}\left(\frac{f}{g}\right) = [a] \cdot \mathfrak{B}\left(\frac{f'}{g'}\right) = [-a] \cdot \mathfrak{B}\left(\frac{g'}{f'}\right) = [-ab] \cdot \mathfrak{B}\left(\frac{g}{f}\right).$$

□

4. Bezoutians related to a symbol

We want to compute the Bezoutian of two coprime polynomials that come from a particular representation of a symbol.

4.1. **Proposition.** *Let σ be a symbol in $k_2E(t)$. Then there exist $f, g \in E[t]$ square-free, coprime and with g of even degree such that*

$$\sigma = \{f, g\}$$

and $\partial_p(\sigma) = 0$ for every prime factor p of f.

Proof. We choose $q, r, s \in E[t]$ square-free and pairwise coprime with $\sigma = \{qs, rs\}$. Then

$$\sigma = \{qs + rs, -qr\} = \{qs + rs - qr, (q+r)qrs\}.$$

We thus have $\sigma = \{f', g'\}$ for two coprime polynomials $f', g' \in E[t]$ such that g' is a multiple of qrs. We may assume that f', g' and $f'(1-g')$ are all different from 1, because otherwise $\sigma = 0$ and the statement holds trivially. Using now that $0 = \{f', 1-f'\} = \{1-g', g'\} = \{f'(1-g'), 1-f'(1-g')\}$, we rewrite

$$\sigma = \{f', g'\} = \{f', g'(1-f')\} = \{f'(1-g'), (1-f'(1-g'))g'\}\,.$$

At least one of the polynomials $g', g'(1-f')$ and $(1-f'(1-g'))g'$ has even degree. Hence, in any case we obtain a representation

$$\sigma = \{f'', g''\}$$

with $f'', g'' \in E[t]$ coprime and where g'' is of even degree and a multiple of qrs. We write $f'' = fh^2$ and $g'' = gh'^2$ with $f, g \in E[t]$ square-free and $h, h' \in E[t]$. Then f and g are coprime and square-free, g has even degree and

$$\sigma = \{f, g\}\,.$$

Furthermore, f is coprime to g'' and thus to qrs. Since $\sigma = \{qs, rs\}$ we conclude that $\partial_p(\sigma) = 0$ for every $p \in \mathcal{P}$ not dividing qrs, so in particular for every prime factor of f. $\square$

4.2. **Lemma.** *Let $f, g, h \in E[t]$ be monic, square-free and pairwise coprime, and let $a, b \in E^\times$ be such that $\partial_p(\{af, bgh\}) = 0$ for every $p \in \mathcal{P}$ not dividing g. Then*

$$\mathfrak{B}\left(\frac{af}{g}\right) = \begin{cases} 0 & \textit{if } (\deg(f), \deg(g), \deg(h)) \equiv (0,0,0) \bmod 2, \\ [b]-[ab] & \textit{if } (\deg(f), \deg(g), \deg(h)) \equiv (0,0,1) \bmod 2, \\ [a] & \textit{if } (\deg(f), \deg(g), \deg(h)) \equiv (0,1,0) \bmod 2, \\ [a]+[b]-[ab] & \textit{if } (\deg(f), \deg(g), \deg(h)) \equiv (0,1,1) \bmod 2, \\ [a]-[ab] & \textit{if } (\deg(f), \deg(g), \deg(h)) \equiv (1,0,0) \bmod 2, \\ [a]+[b] & \textit{if } (\deg(f), \deg(g), \deg(h)) \equiv (1,0,1) \bmod 2, \\ -[ab] & \textit{if } (\deg(f), \deg(g), \deg(h)) \equiv (1,1,0) \bmod 2, \\ [b] & \textit{if } (\deg(f), \deg(g), \deg(h)) \equiv (1,1,1) \bmod 2, \end{cases}$$

Furthermore, if $\partial_\infty(\{af, bgh\}) = 0$, then

$$\mathfrak{B}\left(\frac{af}{g}\right) = \begin{cases} 0 & \textit{if } \deg(g) \textit{ is even}, \\ [a]+[b]-[ab] & \textit{otherwise.} \end{cases}$$

Proof. We have

$$\mathfrak{B}\left(\frac{af}{g}\right) = [a]\cdot\mathfrak{B}\left(\frac{f}{g}\right) = -[a]\cdot\mathfrak{B}\left(\frac{g}{f}\right) + \begin{cases} 0 & \text{if } \deg(fg) \text{ is even,} \\ [a] & \text{otherwise.} \end{cases}$$

Set $\sigma = \{af, bgh\}$. For every $p \in \mathcal{P}$ dividing f we have $\{\overline{bgh}\} = \partial_p(\sigma) = 0$ in k_1E_p. Hence, bgh is a square modulo f, whereby

$$\mathfrak{B}\left(\frac{g}{f}\right) = [b]\cdot\mathfrak{B}\left(\frac{h}{f}\right) = -[b]\cdot\mathfrak{B}\left(\frac{f}{h}\right) + \begin{cases} 0 & \text{if } \deg(fh) \text{ is even,} \\ [b] & \text{otherwise.} \end{cases}$$

For every $p \in \mathcal{P}$ dividing h we have $\{af\} = \partial_p(\sigma) = 0$. Hence af is a square modulo h, whereby

$$\mathfrak{B}\left(\frac{f}{h}\right) = \mathfrak{B}\left(\frac{a}{h}\right) = \begin{cases} 0 & \text{if } \deg(h) \text{ is even,} \\ [a] & \text{otherwise.} \end{cases}$$

This together shows the first part of the statement.

Note further that

$$\partial_\infty(\sigma) = \begin{cases} 0 & \text{if } (\deg(f), \deg(gh)) \equiv (0,0) \bmod 2, \\ \{a\} & \text{if } (\deg(f), \deg(gh)) \equiv (0,1) \bmod 2, \\ \{b\} & \text{if } (\deg(f), \deg(gh)) \equiv (1,0) \bmod 2, \\ \{-ab\} & \text{if } (\deg(f), \deg(gh)) \equiv (1,1) \bmod 2. \end{cases}$$

Suppose now that $\partial_\infty(\sigma) = 0$. In each case where f or gh has odd degree, we conclude that at least one of a, b and $-ab$ is a square, that $\mathfrak{B}\left(\frac{af}{g}\right)$ is split of trivial discriminant and that $[1] - [a] - [b] + [ab] = [\langle 1, -a, -b, ab\rangle] = 0$. This yields the second part of the statement. $\square$

4.3. **Example.** Let $E = \mathbb{Q}_p$ for a prime number p with $p \equiv 5 \bmod 8$. Hence $-1 \in \mathbb{Q}_p^{\times 2}$ and $2 \notin \mathbb{Q}_p^{\times 2}$. For $a = 2$ and $b = p$, the polynomials $f = t(t-2)$, $g = (t-1)(t-p)(t+2p-2)$ and $h = t - p + 2$ satisfy the conditions in Lemma 4.2 with $(\deg(f), \deg(g), \deg(h)) \equiv (0,1,1) \bmod 2$. In this case $\mathfrak{B}\left(\frac{af}{g}\right)$ is given by the anisotropic quadratic form $\langle 2, 2p, p\rangle$.

4.4. **Proposition.** *Let $f, g, h \in E[t]$ be square-free and pairwise coprime with $\deg(g)$ even and such that $\partial_p(\{f, gh\}) = 0$ for all $p \in \mathcal{P}$ not dividing g as well as for $p = \infty$. Then*

$$\mathfrak{B}\left(\frac{f}{g}\right) = 0\,.$$

Proof. This follows from Lemma 4.2. $\square$

It follows from Proposition 4.1 that any symbol $\sigma \in k_2E(t)$ with $\partial_\infty(\sigma) = 0$ has representations $\sigma = \{f, g\} = \{f, gh\}$ with $f, g \in E[t]$ and $h = 1$ such that the conditions in Proposition 4.4 are satisfied.

5. Splitting sequences

Given ramification sequence ρ, we shall now construct a sequence of polynomials that yields a representation of ρ as the ramification of a sum of symbols. This leads to an improved bound on the length of such a representation of ρ.

Given $g \in E[t]$ monic and square-free and $f \in E[t]$ coprime to g, we denote by $\mathfrak{R}\left(\frac{f}{g}\right)$ the element $\rho \in \mathfrak{R}_2(E)$ defined by $\rho_p = \{\overline{f}\}$ for $p \in \mathcal{P}$ dividing g and by $\rho_p = 0$ for all other $p \in \mathcal{P}$.

For a finite subset $S \subseteq \mathcal{P}$ we set

$$\mathrm{P}_S = \prod_{p \in S} p \in E[t]$$

and observe that this polynomial is monic and square-free.

Consider a ramification sequence $\rho \in \mathfrak{R}_2(E)$. We fix a finite subset $S \subseteq \mathcal{P}$ such that $\mathrm{Supp}(\rho) \subseteq S \cup \{\infty\}$. We set $\deg(S) = \sum_{p\in S} \deg(p)$ and $g = \mathrm{P}_S$. Then $\mathfrak{R}\left(\frac{f}{g}\right) = \rho$ for a polynomial $f \in E[t]$ coprime to g which is determined by S up to a square modulo g. We set

$$\mathfrak{B}_S(\rho) = \mathfrak{B}\left(\frac{f}{g}\right).$$

The aim of this section is to relate ρ to $\mathfrak{B}_S(\rho)$.

5.1. **Proposition.** *We have the following:*
(a) The discriminant of $\mathfrak{B}_S(\rho)$ is the square class corresponding to $\rho_\infty \in k_1 E$.
(b) $\mathfrak{B}_S(\rho) \in IE$ if and only if $\deg(S)$ is even.
(c) $\mathfrak{B}_S(\rho) \in I^2 E$ if and only if $\deg(S)$ is even and $\rho_\infty = 0$.

Proof. Part (b) is obvious and (c) follows from (a) and (b) by using [5, Chap. II, Corollary 2.2]. It remains to show (a). Since $\rho \in \mathfrak{R}_2(E) = \ker(\mathrm{N})$, we obtain in $k_1 E$ that

$$0 = \mathrm{N}(\rho) = \sum_{p\in\mathrm{Supp}(\rho)} \mathrm{N}_{E_p/E}(\rho_p) = \rho_\infty + \sum_{p\in S} \mathrm{N}_{E_p/E}(\rho_p).$$

With $g = \mathrm{P}_S$ and $f \in E[t]$ coprime to g such that $\rho = \mathfrak{R}\left(\frac{f}{g}\right)$, it follows that

$$\rho_\infty = \sum_{p\in S} \mathrm{N}_{E_p/E}(f + (p)) = \mathrm{N}_{E_g/E}(f + (g)).$$

By Proposition 3.1 the last term is given by the discriminant of $\mathfrak{B}\left(\frac{f}{g}\right) = \mathfrak{B}_S(\rho)$. □

5.2. **Proposition.** *Let $r \in \mathbb{N}$, $f_0, \dots, f_r \in E[t]$ square-free with $f_r \in E^\times$ and such that, with $f_{r+1} = 1$, we have that f_{i-1} and f_i are relatively coprime and $f_{i-1}f_{i+1}$ is a square modulo f_i for $i = 1, \dots, r$. Then*

$$\mathfrak{R}\left(\frac{f_1}{f_0}\right) = \partial\left(\sum_{k=1}^{\lceil \frac{r}{2}\rceil} \{f_{2k-2}f_{2k}, f_{2k-1}\}\right).$$

Furthermore, for $s = |\{i \in \{1, \dots, r\} \mid \deg(f_i) \not\equiv \deg(f_{i-1}) \bmod 2\}|$ we have

$$\mathrm{diman}\left(\mathfrak{B}\left(\frac{f_1}{f_0}\right)\right) \leqslant s \leqslant r \quad \textit{and} \quad \mathrm{diman}\,\mathfrak{B}\left(\frac{f_1}{f_0}\right) \equiv s \bmod 2.$$

Proof. For $i = 1, \dots, r$ we have that $\mathfrak{R}\left(\frac{f_{i-1}f_{i+1}}{f_i}\right) = 0$ because $f_{i-1}f_{i+1}$ is a square modulo f_i. In particular $\mathfrak{R}\left(\frac{f_{r-1}}{f_r}\right) = \mathfrak{R}\left(\frac{f_{r+1}}{f_r}\right) = 0$, as $f_{r+1} = 1$.

With $n = \lceil \frac{r}{2} \rceil$ we obtain from the conditions that

$$\begin{aligned}
\partial\left(\sum_{k=1}^{n}\{f_{2k-2}f_{2k}, f_{2k-1}\}\right) &= \partial\left(\sum_{i=1}^{r}\{f_{i-1}, f_i\}\right)\\
&= \sum_{i=1}^{r}\left(\mathfrak{R}\left(\frac{f_{i-1}}{f_i}\right) + \mathfrak{R}\left(\frac{f_i}{f_{i-1}}\right)\right)\\
&= \sum_{i=1}^{r}\mathfrak{R}\left(\frac{f_{i-1}}{f_i}\right) + \sum_{i=0}^{r-1}\mathfrak{R}\left(\frac{f_{i+1}}{f_i}\right)\\
&= \mathfrak{R}\left(\frac{f_1}{f_0}\right) + \left(\sum_{i=1}^{r-1}\mathfrak{R}\left(\frac{f_{i-1}f_{i+1}}{f_i}\right)\right) + \mathfrak{R}\left(\frac{f_{r-1}}{f_r}\right)\\
&= \mathfrak{R}\left(\frac{f_1}{f_0}\right).
\end{aligned}$$

We prove the second part of the statement by induction on r. If $r = 0$ then $f_1 = 1$ and $\operatorname{diman}(\mathfrak{B}\left(\frac{f_1}{f_0}\right)) = \deg(f_0) = s = 0$ and the claim holds trivially. Suppose now that $r > 0$. For $s' = |\{i \in \{2,\dots,r\} \mid \deg(f_i) \not\equiv \deg(f_{i-1}) \bmod 2\}|$ we obtain by the induction hypothesis that

$$\operatorname{diman}\mathfrak{B}\left(\frac{f_2}{f_1}\right) \leqslant s' \leqslant r-1 \quad\text{and}\quad \operatorname{diman}\mathfrak{B}\left(\frac{f_2}{f_1}\right) \equiv s' \bmod 2\,.$$

If $\deg(f_0) \equiv \deg(f_1) \bmod 2$, then $s = s'$ and

$$\mathfrak{B}\left(\frac{f_1}{f_0}\right) \sim \mathfrak{B}\left(\frac{f_0}{f_1}\right) = \mathfrak{B}\left(\frac{f_2}{f_1}\right).$$

If $\deg(f_0) \not\equiv \deg(f_1) \bmod 2$, then $s = s' + 1$ and

$$\mathfrak{B}\left(\frac{f_1}{f_0}\right) \sim \mathfrak{B}\left(\frac{f_0}{f_1}\right) + [c] = \mathfrak{B}\left(\frac{f_2}{f_1}\right) + [c]\,,$$

for some $c \in E^\times$. In either case we conclude that

$$\operatorname{diman}\mathfrak{B}\left(\frac{f_1}{f_0}\right) \leqslant s \leqslant r \quad\text{and}\quad \operatorname{diman}\mathfrak{B}\left(\frac{f_1}{f_0}\right) \equiv s \bmod 2\,.$$

□

For $r \in \mathbb{N}$ and $f_0,\dots,f_r$ such as in Proposition 5.2 and with $\mathfrak{R}\left(\frac{f_1}{f_0}\right) = \rho$, we call $(f_0,\dots,f_r)$ a *splitting sequence of* ρ, and refer to the number r as its *length*. We say that the splitting sequence $(f_0,\dots,f_r)$ is *strictly decreasing* if we have $\deg(f_i) < \deg(f_{i-1})$ for $i = 1,\dots,r$.

5.3. **Corollary.** *Let r be the length of a splitting sequence of ρ. Then ρ is represented by a sum of n symbols for $n = \lceil \frac{r}{2} \rceil$.*

Proof. This is immediate from Proposition 5.2. □

One may ask whether any representation of ρ by a given number of symbols can be obtained from a splitting sequence via Proposition 5.2.

Having thus shown that a splitting sequence gives rise to a representation of ρ by a sum of symbols, we turn to the problem of constructing splitting sequences of small length. Recall that we are assuming throughout that $\mathrm{Supp}(\rho) \subseteq S \cup \{\infty\}$.

5.4. **Proposition.** *There exists a strictly decreasing splitting sequence of ρ starting with P_S. The length of any such splitting sequence is at most $\deg(S)$.*

Proof. We set $f_0 = \mathrm{P}_S$. If $f_0 = 1$ then (f_0) is the desired sequence. Otherwise $\deg(f_0) > 0$ and we choose $f_1 \in E[t]$ square-free and coprime to f_0 such that $\deg(f_1) < \deg(f_0)$ and $\mathfrak{R}\left(\frac{f_1}{f_0}\right) = \rho$. For $i \geqslant 1$ with $\deg(f_{i-1}) > 0$ we choose recursively $f_i' \in E[t]$ as the unique polynomial with $\deg(f_i') < \deg(f_{i-1})$ and $f_i' \equiv f_{i-2} \bmod f_{i-1}$ and then let f_i denote the square-free part of f_i', and we stop the process and set $r = i-1$ as soon as $\deg(f_{i-1}) = 0$. In this way we obtain a strictly decreasing splitting sequence of ρ starting with P_S.

Suppose now that $r \in \mathbb{N}$ is the length of a strictly decreasing splitting sequence of ρ starting with P_S, say $(f_0, \dots, f_r)$. As $\deg(f_{i-1}) - \deg(f_i) \geqslant 1$ for $i = 1, \dots, r$ and further $\deg(f_r) = 0$, we conclude that

$$\deg(S) = \deg(f_0) - \deg(f_r) = \sum_{i=1}^{r} (\deg(f_{i-1}) - \deg(f_i)) \geqslant r\,. \qquad \square$$

5.5. **Corollary.** *If* $\operatorname{diman} \mathfrak{B}_S(\rho) = \deg(S)$*, then the length of any strictly decreasing splitting sequence of ρ starting with* P_S *is equal to* $\deg(S)$*.*

Proof. Let $g = \mathrm{P}_S$ and choose $f \in E[t]$ coprime to g with $\mathfrak{R}\left(\frac{f}{g}\right) = \rho$. Let $r \in \mathbb{N}$ be the length of a strictly decreasing splitting sequence for ρ starting with g. As $\mathfrak{B}_S(\rho) = \mathfrak{B}\left(\frac{f}{g}\right)$ we obtain that $\operatorname{diman} \mathfrak{B}_S(\rho) \leqslant r \leqslant \deg(S)$ by Proposition 5.2 and Proposition 5.4. Hence, if $\operatorname{diman} \mathfrak{B}_S(\rho) = \deg(S)$ then $r = \deg(S)$. $\square$

We give an example where the hypothesis in Corollary 5.5 is satisfied for an arbitrary given degree.

5.6. **Example.** Let E_0 be a field, $d \geqslant 3$ and $a_1, \dots, a_d \in E_0^\times$ pairwise different. Let $b_1, \dots, b_{d-1}$ be indeterminates over E_0 and set $E = E_0(\!(b_1)\!) \dots (\!(b_{d-1})\!)$ and $b_d = b_1 \cdots b_{d-1}$. Consider

$$\xi = \textstyle\sum_{i=1}^d \{(1-a_i)t + a_i, b_i\}$$

in $k_2 E(t)$ and $\rho = \partial(\xi)$. Note that $\mathrm{Supp}(\rho) = \{t - \frac{a_i}{a_i - 1} \mid i = 1, \dots, d\}$ and thus $\deg(\rho) = d$. Using Corollary 3.6 we obtain for $S = \mathrm{Supp}(\rho)$ that

$$\mathfrak{B}_S(\rho) = \textstyle\sum_{i=1}^d [b_i c_i]$$

for certain $c_1, \dots, c_d \in E_0^\times$. It follows that $\operatorname{diman} \mathfrak{B}_S(\rho) = d = \deg(S)$.

5.7. **Lemma.** *Assume that E is infinite. Let $g \in E[t]$ be square-free and $f \in E[t]$ coprime to g. There exist $m \in \mathbb{N}$ and square-free polynomials $f_1, \dots, f_m \in E[t]$ such that, with $f_0 = g$ and $f_{-1} = f$ the following are satisfied for $i = 1, \dots, m$:*

- $\deg(f_i) \leqslant \deg(f_{i-1}) - 2$ *and* $\deg(f_i) \equiv \deg(g) \bmod 2$*;*
- *f_{i-1} and f_i are relatively coprime;*
- *$f_i f_{i-2}$ is a square modulo f_{i-1};*
- $\deg(f_m) = \operatorname{diman} \mathfrak{B}\left(\frac{f}{g}\right)$.

Furthermore, under these conditions

$$m \leqslant \tfrac{1}{2}\left(\deg(g) - \operatorname{diman} \mathfrak{B}\left(\frac{f}{g}\right)\right) \quad \textit{and} \ \mathfrak{B}\left(\frac{f_{i-1}}{f_i}\right) \sim \mathfrak{B}\left(\frac{f}{g}\right) \quad \textit{for } i = 1, \dots, m.$$

Proof. Assume $r \in \mathbb{N}$ and polynomials $f_0, \dots, f_r$ with $f_0 = g$ are given satisfying all of the given conditions not involving $\operatorname{diman} \mathfrak{B}\left(\frac{f}{g}\right)$. Then by Corollary 3.9 we have

$$\mathfrak{B}\left(\frac{f_{i-1}}{f_i}\right) \sim \mathfrak{B}\left(\frac{f_i}{f_{i-1}}\right) = \mathfrak{B}\left(\frac{f_{i-2}}{f_{i-1}}\right) \qquad \text{for } i = 1, \dots, r\,.$$

Thus $\mathfrak{B}\left(\frac{f_{i-1}}{f_i}\right) \sim \mathfrak{B}\left(\frac{f}{g}\right)$ and $\operatorname{diman} \mathfrak{B}\left(\frac{f_{i-1}}{f_i}\right) = \operatorname{diman} \mathfrak{B}\left(\frac{f}{g}\right)$ for $i = 1, \dots, r$. Furthermore, as $\deg(f_{i-1}) - \deg(f_i) \geqslant 2$ for $i = 1, \dots, r$ and $f_0 = g$ we obtain that

$$\deg(g) - \deg(f_r) = \left(\sum_{i=1}^{r} (\deg(f_{i-1}) - \deg(f_i))\right) \geqslant 2r.$$

As $\deg(f_r) \geqslant \operatorname{diman} \mathfrak{B}\left(\frac{f_{r-1}}{f_r}\right) = \operatorname{diman} \mathfrak{B}\left(\frac{f}{g}\right)$, we conclude that

$$r \leqslant \tfrac{1}{2}\left(\deg(g) - \operatorname{diman} \mathfrak{B}\left(\frac{f}{g}\right)\right)\,.$$

This shows the last part of the statement.

We now construct recursively a sequence of square-free polynomials as claimed. We set $f_{-1} = f$ and $f_0 = g$. For $i \geqslant 1$, as long as $\deg(f_{i-1}) > \operatorname{diman} \mathfrak{B}\left(\frac{f_{i-2}}{f_{i-1}}\right)$ holds, we use Proposition 3.4 to obtain a square-free polynomial $f_i \in E[t]$ coprime to f_{i-1} such that $\deg(f_i) \leqslant \deg(f_{i-1}) - 2$, $\deg(f_i) \equiv \deg(f_{i-1}) \bmod 2$ and $f_i f_{i-2}$ is a square modulo f_{i-1}. As soon as $\deg(f_{i-1}) = \operatorname{diman} \mathfrak{B}\left(\frac{f_{i-2}}{f_{i-1}}\right)$ holds, we stop and set $m = i - 1$. It follows from what we showed in the first part of the proof that the recursion terminates after finitely many steps. □

5.8. **Proposition.** *Assume that E is infinite. Set $d = \operatorname{diman} \mathfrak{B}_S(\rho)$. There exist $m \in \mathbb{N}$ and a strictly decreasing splitting sequence $(f_0, \dots, f_{d+m})$ of ρ starting with P_S such that* $\deg(f_i) \equiv \deg(f_{i-1}) \bmod 2$ *for $i = 1, \dots, m$ and* $\deg(f_{m+d-i}) = i$ *for $i = 0, \dots, d$.*

Proof. Let $f_0 = \mathrm{P}_S$ and $f_{-1} \in E[t]$ coprime to f_0 with $\mathfrak{R}\left(\frac{f_{-1}}{f_0}\right) = \rho$. We choose $m \in \mathbb{N}$ and $f_1, \dots, f_m \in E[t]$ as in Lemma 5.7. Then $\deg(f_m) = d = \operatorname{diman} \mathfrak{B}_S(\rho)$ and $\mathfrak{B}\left(\frac{f_{m-1}}{f_m}\right) \sim \mathfrak{B}\left(\frac{f_{-1}}{f_0}\right) = \mathfrak{B}_S(\rho)$. Set $\rho' = \mathfrak{R}\left(\frac{f_{m-1}}{f_m}\right)$. By Proposition 5.4 and Corollary 5.5 there exists a strictly decreasing splitting sequence of ρ' of length d starting with f_m, say $(f_m, \dots, f_{d+m})$. Then $(f_0, \dots, f_{d+m})$ has the required properties. $\square$

5.9. **Theorem.** *Any splitting sequence ρ with* $\operatorname{Supp}(\rho) \subseteq S \cup \{\infty\}$ *is represented by a sum of n symbols where* $n = \left\lceil \frac{\deg(S) + \operatorname{diman} \mathfrak{B}_S(\rho)}{4} \right\rceil$.

Proof. Set $d = \operatorname{diman} \mathfrak{B}_S(\rho)$. In view of Example 2.4 we may assume that E is infinite. Let $m \in \mathbb{N}$ and let $(f_0, \dots, f_{d+m})$ be a strictly decreasing splitting sequence of ρ starting with P_S and with the properties formulated in Proposition 5.8. We have $m \leqslant \frac{1}{2}(\deg(S) - d)$, whence $d + m \leqslant \frac{1}{2}(\deg(S) + d)$. The statement thus follows from Corollary 5.3. $\square$

5.10. **Remark.** By Theorem 2.5 the ramification sequence ρ is represented by a sum of n' symbols for $n' = \left\lfloor \frac{\deg(\rho)}{2} \right\rfloor$ symbols. Let us compare n' with the value of n in Theorem 5.9 that we obtain for $S = \operatorname{Supp}(\rho) \setminus \{\infty\}$. Obviously

$$\deg(S) = \begin{cases} \deg(\rho) & \text{if } \rho_\infty = 0, \\ \deg(\rho) - 1 & \text{if } \rho_\infty \neq 0. \end{cases}$$

and $\operatorname{diman} \mathfrak{B}_S(\rho) \leqslant \deg(S)$. We conclude that $n \leqslant n'$ except in the case where $\deg(S)$ is odd, $\operatorname{diman} \mathfrak{B}_S(\rho) = \deg(S)$ and $\rho_\infty = 0$.

Let us look more closely at this case. With $d = \deg(S) = \operatorname{diman}(\mathfrak{B}_S(\rho))$ we obtain that $n = \frac{d+1}{2} = n' + 1$. The strictly decreasing splitting sequence obtained from Lemma 5.7 which is used in the proof of Theorem 5.9 has length d. Denoting this sequence $(f_0, \dots, f_d)$, we have that $\deg(f_i) = d - i$ for $i = 1, \dots, d$. Applying Proposition 5.2 we obtain that $\rho = \partial(\sum_{k=1}^{n} \sigma_k)$ where $\sigma_k = \{f_{2k-2} f_{2k}, f_{2k-1}\}$ for $k = 1, \dots, n$ and $f_{d+1} = 1$. As $\deg(f_i) \equiv i + 1 \bmod 2$ for $i = 0, \dots, d$, it is easy to see that $\partial_\infty(\sigma_k) = 0$ for $k = 1, \dots, n-1$ and $\partial_\infty(\sigma_n) = \partial_\infty(\{f_{d-1}, f_d\}) = \{f_d\}$ in $k_1 E$. Hence, $\{f_d\} = \partial_\infty(\sum_{k=1}^{n} \sigma_k) = \rho_\infty = 0$, whereby $f_d \in E^{\times 2}$. This implies that $\sigma_n = \{f_{d-1}, f_d\} = 0$ in $k_2 E(t)$. We conclude that $\rho = \partial(\sum_{k=1}^{n-1} \sigma_k)$.

Hence, in each case our method applied as in the proof of Theorem 5.9 yields a representation of ρ by at most n' symbols.

Note finally that if $\deg(\rho)$ is odd and $\operatorname{diman} \mathfrak{B}_S(\rho) = \deg(\rho) - 4$, then $n' = n$. In particular, if $\deg(\rho) = 5$ and $\rho_\infty = 0$, then $n \geqslant n' = 2$, and we shall see in Example 6.3 that even in the case where $\mathfrak{B}_S(\rho)$ is split a single symbol may not be sufficient to represent ρ.

In relation to Theorem 5.9 one may ask the following:

5.11. **Question.** *Let $n \in \mathbb{N}$ be such that ρ is represented by a sum of n symbols. Set $S = \mathrm{Supp}(\rho) \setminus \{\infty\}$. Is there an upper bound on* $\mathrm{diman}\, \mathfrak{B}_S(\rho)$ *in terms of n?*

The following result answers Question 5.11 partially in the case where $n = 1$.

5.12. **Theorem.** *Set $S = \mathrm{Supp}(\rho) \setminus \{\infty\}$ and assume that* $\deg(\rho)$ *is even. If ρ is represented by a symbol, then $\mathfrak{B}_S(\rho)$ is split.*

Proof. By Proposition 4.1 there exist square-free coprime polynomials $f, g' \in E[t]$ such that $\sigma = \{f, g'\}$ and $\partial_p(\sigma) = 0$ for all p dividing f. It follows that $g' = gh$ with $g = P_S$ and $h \in E[t]$. Then $f, g, h \in E[t]$ are square-free and coprime and $\partial_p(\sigma) = 0$ holds for all p not dividing g. Then $\partial(\sigma) = \mathfrak{R}\left(\frac{f}{g}\right)$ and $\mathfrak{B}_S(\rho) = \mathfrak{B}\left(\frac{f}{g}\right)$. As $\deg(\rho)$ is even, the discriminant of $\mathfrak{B}_S(\rho)$ is trivial if and only if $\deg(g)$ is even. By Lemma 4.2 we have $(\deg(f), \deg(g), \deg(h)) \not\equiv (0, 1, 1) \bmod 2$ and if $\deg(g)$ is odd, then $\mathfrak{B}\left(\frac{f}{g}\right)$ is split. If $\deg(g)$ is even, whereby the discriminant of $\mathfrak{B}\left(\frac{f}{g}\right)$ is trivial, then Lemma 4.2 yields that $\mathfrak{B}\left(\frac{f}{g}\right) = 0$. $\square$

6. Ramification sequences of small degree

We conclude our study with a statement on ramification sequences of degree four followed by a series of examples of ramification sequences of small degree.

6.1. **Theorem.** *Assume that* $\deg(\rho) = 4$ *and set $S = \mathrm{Supp}(\rho) \setminus \{\infty\}$. Then ρ is represented by a symbol if and only if $\mathfrak{B}_S(\rho)$ is split.*

Proof. If E is infinite and $\mathrm{diman}\, \mathfrak{B}_S(\rho) \leqslant 1$ then we conclude by Theorem 5.9 that $\rho = \partial(\sigma)$ for a symbol $\sigma \in k_2E(t)$. If E is finite then the same conclusion holds trivially by Example 2.4. The converse follows from Theorem 5.12. $\square$

6.2. **Remark.** Assume that $\deg(\rho) = 4$ and let $S = \mathrm{Supp}(\rho) \setminus \{\infty\}$. If $\rho_\infty \neq 0$, then with $d \in E^\times$ such that $\rho_\infty = \{d\}$ in k_1E, it follows that $[1] - [d] \cdot \mathfrak{B}_S(\rho) = [\pi]$ for a 2-fold Pfister form π over E. Then π is hyperbolic if and only if $\mathfrak{B}_S(\rho)$ is split, and by Theorem 6.1 this is if and only if ρ is represented by a symbol. In the special case where S consists of three rational points, this characterisation was given in [8, Prop. 1.4] with an explicit construction of the form π, which can actually be retrieved from Corollary 3.6.

In the case where $\rho_\infty = 0$, the criterion in Theorem 6.1 can be reformulated in similar terms. In this case there is a unique 2-fold Pfister form π over E such that $\mathfrak{B}_S(\rho) \sim [\pi]$, and ρ is represented by a symbol if and only if π is hyperbolic.

Let $\rho \in \mathfrak{R}_2(E)$. The following example shows that Theorem 6.1 does not extend to the case where $\deg(\rho) = 5$.

6.3. **Example.** Set $\xi = \{(t-1)(t+1)(t-2)(t-3), -1\} + \{t(t-1), 7\}$ in $k_2\mathbb{Q}_7(t)$. Then $S = \mathrm{Supp}(\partial(\xi))$ consists of the polynomials $t - m$ with $m = -1, 0, 1, 2, 3$. By [4, Theorem 3.6] we have $\partial(\xi) \neq \partial(\sigma)$ for any symbol σ in $k_2\mathbb{Q}_7(t)$. Using Corollary 3.6 we obtain that $\mathfrak{B}_S(\partial(\xi)) = [1]$, whence $\mathfrak{B}_S(\partial(\xi))$ is split.

We are going to look at some examples where $\deg(\rho) = 6$ and $\rho_\infty = 0$ and where ρ is not represented by a symbol. In the first two examples we have that $\mathfrak{B}_S(\rho) = 0$ for $S = \mathrm{Supp}(\rho)$. In particular, the converse of the implication in Theorem 5.12 does not hold in general.

6.4. **Example.** We consider the field $E = \mathbb{Q}_p$ for a prime number $p \geqslant 7$. We find $\alpha, a, b \in \mathbb{Z} \setminus p\mathbb{Z}$ such that $a^2 + 1 \in \mathbb{Q}_p^{\times 2}$ and $\alpha, b^2 + 1 \notin \mathbb{Q}_p^{\times 2}$. Set

$$\xi = \{(t^2 - a^2)(t^2 - b^2), \alpha\} + \{t^2 + 1, p\} \in k_2\mathbb{Q}_p(t)\,.$$

By [4, Theorem 3.6] we have that $\partial(\xi) \neq \partial(\sigma)$ for all symbols $\sigma \in k_2\mathbb{Q}_p(t)$. We set $\rho = \partial(\xi)$. Set $S = \mathrm{Supp}(\rho)$ and note that S consists of the prime factors of $(t^2 - a^2)(t^2 - b^2)(t^2 + 1)$. Hence $\deg(S) = 6$. Computation yields that

$$\begin{aligned}
\mathfrak{B}_S(\rho) &= [\alpha] \cdot \mathfrak{B}\left(\frac{t^2+1}{(t^2-a^2)(t^2-b^2)}\right) + [p] \cdot \mathfrak{B}\left(\frac{(t^2-a^2)(t^2-b^2)}{t^2+1}\right) \\
&= [\langle -\alpha, p\rangle] \cdot \mathfrak{B}\left(\frac{(t^2-a^2)(t^2-b^2)}{t^2+1}\right) \\
&= [\langle -\alpha, p\rangle] \cdot \mathfrak{B}\left(\frac{(1+a^2)(1+b^2)}{t^2+1}\right) \;=\; 0
\end{aligned}$$

6.5. **Example.** Consider $E = \mathbb{Q}_p$ for a prime number $p \equiv \pm 3 \bmod 8$. Set

$$\xi = \{t(t-1)(t-2)(t-3), 2\} + \{t^2 + 1, p\} \in k_2\mathbb{Q}_p(t).$$

By [4, Theorem 3.6] we have that $\partial(\xi) \neq \partial(\sigma)$ for any symbol $\sigma \in k_2\mathbb{Q}_p(t)$. Note that $S = \mathrm{Supp}(\partial(\xi))$ is the set of prime factors of $g = t(t-1)(t-2)(t-3)(t^2+1)$ over $\mathbb{Q}_p$. Thus $\deg(S) = 6$. Using that $t(t-1)(t-2)(t-3) \equiv -10 \bmod t^2 + 1$ a similar computation as in Example 6.4 yields that $\mathfrak{B}_S(\partial(\xi)) = 0$.

By Theorem 5.9, assuming that $\deg(\rho) = 6$ and $\rho_\infty = 0$, the vanishing of $\mathrm{diman}\,\mathfrak{B}_S(\rho)$ implies that $\rho = \partial(\sigma_1 + \sigma_2)$ for two symbols σ_1 and σ_2 in $k_2E(t)$. The following example shows that the converse to this statement does not hold.

6.6. **Example.** Consider $\xi = \{(t^2 - 1)(t^2 - 2), -1\} + \{t(t-3), 11\}$ in $k_2\mathbb{Q}_{11}(t)$. Note that $S = \mathrm{Supp}(\partial(\xi))$ consists of the factors of $(t^2-1)(t^2-2)t(t-3)$ and thus has degree 6. A computation shows that $\mathfrak{B}_S(\partial(\xi)) = [\langle 1, 1, 11, 11\rangle] \neq 0$ in $W\mathbb{Q}_{11}$. Hence $\mathrm{diman}\,\mathfrak{B}_S(\partial(\xi)) = 4$.

Recall that $\mathcal{B}_S(\rho)$ lies in the fundamental ideal IE if and only if $\deg(S)$ is even. The following example illustrates that, in general, for finite subsets S_1 and S_2 of $\mathcal{P}$ with $\deg(S_1) \equiv \deg(S_2) \bmod 2$ and $\mathrm{Supp}(\rho) \subseteq S_1 \cap S_2$, we may have that $\mathcal{B}_{S_1}(\rho) \neq \mathcal{B}_{S_2}(\rho)$.

6.7. **Example.** Consider $\xi = \{t^4 - 1, -1\} + \{t^2 - t - 1, 3\} \in k_2\mathbb{Q}_3(t)$ and set $\rho = \partial(\xi)$ and $S = \mathrm{Supp}(\rho)$. We have $\rho_\infty = 0$, and since -1 is a square in the residue field of $t^2 + 1$, we also have $\rho_{t^2+1}(\xi) = 0$. It follows that S consists of the factors of $(t^2 - 1)(t^2 - t - 1)$. Hence $\deg(S) = 4$, and a computation yields that $\mathcal{B}_S(\rho) = [\langle 1,1,3,3\rangle] \neq 0$ in $k_2\mathbb{Q}_3$. In particular, ρ is not represented by a symbol, by Theorem 5.12. Another computation based on Theorem 3.8 further shows that

$$\mathfrak{B}\left(\frac{t^2-t-1}{t^4-1}\right) = \mathfrak{B}\left(\frac{t^4-1}{t^2-t-1}\right) = 0 \text{ in } k_2\mathbb{Q}_3\,.$$

For $S' = S \cup \{t^2+1\}$ we obtain that $\mathrm{Supp}(\rho) = S \subseteq S'$, $\deg(S') = 6$ and $P_{S'} = (t^4-1)(t^2-t-1)$. Since t^4-1 and t^2-t-1 are coprime, we conclude by Proposition 3.5 that

$$\mathcal{B}_{S'}(\rho) = \mathfrak{B}\left(\frac{-1(t^2-t-1)}{t^4-1}\right) + \mathfrak{B}\left(\frac{3(t^4-1)}{t^2-t-1}\right) = 0 \neq \mathcal{B}_S(\rho)\,.$$

6.8. **Question.** *Assume that* $\deg(\rho) = 6$ *and* $\rho_\infty = 0$. *Set* $S = \mathrm{Supp}(\rho)$. *Does any of the following two properties imply the other one?*

(*i*) $\rho = \partial(\sigma_1 + \sigma_2)$ *for two symbols* $\sigma_1, \sigma_2 \in k_2E(t)$.
(*ii*) $\mathrm{diman}\,\mathfrak{B}_S(\rho) \leqslant 4$.

Acknowledgments. This work was supported by the FWO Odysseus Programme (project *Explicit Methods in Quadratic Form Theory*), funded by the Fonds Wetenschappelijk Onderzoek – Vlaanderen. We would further like to express our gratitude to Jean-Pierre Tignol and to Chris Blondia for their supportive influence on this work.

References

[1] K.J. Becher, M. Raczek. On the second K-group of a rational function field. *Pacific J. Math.* **262** (2013): 1–9.
[2] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology.* Cambridge University Press (2006).
[3] G. Heinig, K. Rost. *Introduction to Bezoutians.* Numerical methods for structured matrices and applications, 25–118, *Oper. Theory Adv. Appl.*, 199, Birkhäuser Verlag, Basel, 2010.
[4] B.È. Kunyavskiĭ, L.H. Rowen, S.V. Tikhonov, V.I. Yanchevskiĭ. Bicyclic algebras of prime exponent over function fields. *Trans. Amer. Math. Soc.* **358** (2006): 2579–2610.
[5] T.Y. Lam. *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics, **67**, American Mathematical Society, Providence, RI, 2005.
[6] H.W. Lenstra Jr., K_2 of a global field consists of symbols. *Algebraic K-theory* (Proc. Conf., Northwestern Univ., Evanston, Ill., 1976), pp. 6973. *Lecture Notes in Math.*, Vol. 551, Springer, Berlin, 1976.
[7] J. Milnor. Algebraic K-theory and quadratic forms. *Invent. Math.* **9** (1970): 318–344.
[8] A. S. Sivatski. Faddeev invariants for central simple algebras over rational function fields. *Manuscripta Math.* **145** (2014): 71–88.

Universiteit Antwerpen, Departement Wiskunde–Informatica, Middelheimlaan 1, 2020 Antwerpen, Belgium.

E-mail address: karimjohannes.becher@uantwerpen.be, melanie.raczek@telenet.be