Journal of Algebra 361 (2012) 172–187

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Hilbert's Tenth Problem for rational function fields over p-adic fields

Claudia Degroote[1], Jeroen Demeyer[*,2]

Ghent University, Department of Mathematics, Krijgslaan 281, 9000 Gent, Belgium

ARTICLE INFO

Article history:
Received 24 June 2011
Available online 25 April 2012
Communicated by Laurent Moret-Bailly

Keywords:
Undecidability
Valuations
Quadratic forms

ABSTRACT

Let K be a p-adic field (a finite extension of some $\mathbb{Q}_p$) and let $K(t)$ be the field of rational functions over K. We define a kind of quadratic reciprocity symbol for polynomials over K and apply it to prove isotropy for a certain class of quadratic forms over $K(t)$. Using this result, we give an existential definition for the predicate "$v_t(x) \geqslant 0$" in $K(t)$. This implies undecidability of diophantine equations over $K(t)$.

1. Introduction

In [6], Kim and Roush proved undecidability for diophantine equations for rational function fields over a subfield of a p-adic field of odd residue characteristic. Our interest went out to improving their methods so they would also work in the case of residue characteristic 2. While the present paper follows some of the structure of Kim and Roush's proof, our proof is a general one that handles both p odd and $p = 2$. We also simplify many of the methods of Kim and Roush by working more in the context of the theory of quadratic forms. However, we only deal with p-adic fields (as opposed to subfields of p-adic fields).

This result fits in with other results concerning Hilbert's Tenth Problem. In his famous list of 23 problems, Hilbert asked for an algorithm that solves the following question: given a polynomial with integer coefficients in any number of unknowns, does this polynomial have an integer zero? In 1970 Matiyasevich proved, building on earlier work of Davis, Putnam and Robinson, that recursively enumerable sets are Diophantine (called the DPRM theorem). From this it follows that there is no algorithm to decide whether a polynomial over the integers has integer zeros. The undecidability of

[*] Corresponding author.
E-mail addresses: cdegroote@cage.ugent.be (C. Degroote), jdemeyer@cage.ugent.be (J. Demeyer).

[1] Ph.D. fellow of the Research Foundation — Flanders (FWO).

[2] Postdoctoral Fellow of the Research Foundation — Flanders (FWO).

0021-8693/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jalgebra.2012.03.039

diophantine equations has been shown for many other rings and fields, [9] gives an overview of what is known.

For rational function fields $K(t)$, to prove diophantine undecidability (i.e. a negative answer to Hilbert's Tenth Problem) it suffices to give an existential definition of the valuation ring at t. This method was first used by Denef [3] in characteristic zero, in general the result can be stated as follows:

Theorem 1.1. *(See [9, Theorem 2.3].) Let K be a field and let K_0 denote the prime subfield of K. Let t be a transcendental element over K. Suppose that there exists an existential formula $\psi(x)$ such that the following hold:*

1. *for every $x \in K_0(t)$ such that $v_t(x) \geqslant 0$, $\psi(x)$ holds;*
2. *for every $x \in K(t)$ such that $\psi(x)$ holds, we have $v_t(x) \geqslant 0$.*

Then the existential theory of $K(t)$ is undecidable.

Therefore, the aim of this paper is really to give an existential definition of the predicate "$v_t(x) \geqslant 0$" (we do not need to restrict to the prime field as in Theorem 1.1). This can easily be reduced to giving an existential definition of "$v_t(x)$ is even", this reduction is done implicitly in Theorem 5.3. We will use quadratic forms to define "$v_t(x)$ is even".

In Section 2 of this paper, we start with some basic definitions and theorems about quadratic forms, we give a refined Dirichlet density theorem for global fields and we introduce Newton polygons which immediately give the valuations of the zeros of a polynomial.

At various places in their proof, Kim and Roush take an element of $K(t)$ (where K is a p-adic field), apply a variable transformation which might live over a finite extension of K and then go the residue field (this is the rational function field over a finite field). The resulting functions are called "edge functions". They then reason with these functions and lift back to $K(t)$. Since our proof also needs to work for even residue characteristic and we want to work with quadratic forms, we cannot do this anymore. Instead, in Section 3, we define a kind of quadratic reciprocity symbol for polynomials over K. In the case of odd residue characteristic, this symbol can be defined completely in terms of the residue field. However, it is actually a lot more natural not to look at the residue field at all. We also prove a quadratic reciprocity law for this symbol. Section 4 contains our main result regarding quadratic forms: if $f \in K[t]$ has a particular Newton polygon, then certain quadratic forms over $K(t)$ involving f and an unknown function $s \in K(t)$ can be made isotropic. This is then used in Section 5 to give an existential definition of "$v_t(x) \geqslant 0$". Also in this last section, we use an elliptic curve to give an existential definition of the constants K in $K(t)$.

2. Definitions

We start with some definitions and properties of quadratic forms. We state Milnor's exact sequence, giving a local-global principle for the Witt ring $W(K(t))$ of a rational function field over a general base field K, and the well-known fact that a Pfister form is isotropic if and only if it is hyperbolic. We assume that the reader is familiar with the basic theory of quadratic forms, in particular the Witt ring. We refer to [7] or [10].

Definition 2.1. Let K be a field of characteristic $\neq 2$. For $\alpha_1, \dots, \alpha_n \in K^*$, the quadratic form

$$\bigotimes_{i=1}^{n} \langle 1, \alpha_i \rangle = \langle 1, \alpha_1, \alpha_2, \dots, \alpha_n, \alpha_1\alpha_2, \dots, \alpha_1\alpha_2 \cdots \alpha_n \rangle$$

is called an *n-fold Pfister form*.

Theorem 2.2. *(See [7, Ch. X, Theorem 1.7].) Let K be a field of characteristic $\neq 2$, φ a Pfister form over K. If φ is isotropic, then $\varphi = 0$ in the Witt ring $W(K)$.*

Let $p(t)$ be a monic, irreducible polynomial over K. An arbitrary quadratic form φ of dimension n over $K(t)$ can be written as $\varphi_1 \perp \langle p(t)\rangle\varphi_2$ with $\varphi_1 = \langle u_1, \dots, u_r\rangle$ and $\varphi_2 = \langle u_{r+1}, \dots, u_n\rangle$ where the $u_i(t)$ are polynomials coprime with $p(t)$. Denote the reduction of a polynomial $u(t)$ modulo $p(t)$ with $\overline{u(t)}$. Then $\overline{\varphi_1} = \langle \overline{u_1}, \dots, \overline{u_r}\rangle$ and $\overline{\varphi_2} = \langle \overline{u_{r+1}}, \dots, \overline{u_n}\rangle$ are called the *first* and *second residue forms of* φ. We denote the *second residue class map*

$$W\bigl(K(t)\bigr) \to W\bigl(K[t]/(p)\bigr) : \varphi \mapsto \overline{\varphi_2}$$

with δ_p.

Theorem 2.3 *(Milnor exact sequence). Let K be a field of characteristic $\neq 2$. Let i be the functorial map $W(K) \to W(K(t))$. Let $\delta = \bigoplus \delta_p$ where the direct sum extends over all monic irreducible polynomials $p(t) \in K[t]$. Then the following sequence of abelian groups is split exact:*

$$0 \to W(K) \xrightarrow{i} W\bigl(K(t)\bigr) \xrightarrow{\delta} \bigoplus_p W\bigl(K[t]/(p)\bigr) \to 0.$$

Proof. See [7, Ch. IX, Theorem 3.1]. □

At some point, we will construct a polynomial over a p-adic field K with certain properties. To do this, we will start from a polynomial in the reduction $k[t]$, where k is the (finite) residue field of K, which we will find using the following generalization of Dirichlet's density theorem:

Theorem 2.4. *(See [1, Theorem A.10 with $S_0 = \emptyset$].) Let F be a global field, S_∞ a finite non-empty set of primes of F, containing all archimedean primes when F is a number field. Let*

$$A = \bigl\{x \in F\colon\ v_{\mathfrak{p}}(x) \geqslant 0 \textit{ for all } \mathfrak{p} \notin S_\infty\bigr\}.$$

Suppose we are given $a, b \in A$ such that $aA + bA = A$ and for each $\mathfrak{p} \in S_\infty$ an open subgroup $V_{\mathfrak{p}} \subset F_{\mathfrak{p}}^*$ and an $x_{\mathfrak{p}} \in F_{\mathfrak{p}}^*$. Suppose also that $V_{\mathfrak{p}}$ has finite index in $F_{\mathfrak{p}}^*$ for at least one $\mathfrak{p} \in S_\infty$.

Then there exist infinitely many primes $\mathfrak{p}_0 \notin S_\infty$ such that there is a $c \in A$ satisfying

$$c \equiv a \mod b,$$
$$c \in x_{\mathfrak{p}} V_{\mathfrak{p}} \quad \textit{for all } \mathfrak{p} \in S_\infty,$$
$$cA = \mathfrak{p}_0.$$

Now we look at valued fields and we define the Newton polygon of a polynomial over a valued field. For the theory of valuations, we refer to [4]. Let K be a field with a discrete henselian valuation v. Let $\mathcal{O}$ denote the valuation ring. The fact that K is "henselian" means that the following holds:

Theorem 2.5 *(Hensel's Lemma). (See [4, Theorem 4.1.3].) For all $f \in \mathcal{O}[t]$ and $a \in \mathcal{O}$ such that $v(f(a)) > 2v(f'(a))$, there exists a $b \in \mathcal{O}$ such that $f(b) = 0$ and $v(b - a) > v(f'(a))$.*

Definition 2.6. Let $f(t) = a_0 + a_1 t + \cdots + a_d t^d$ be a polynomial over K with $a_0 a_d \neq 0$. The *Newton polygon* of f is the lower convex hull of the points $(i, v(a_i))$ in $\mathbb{R}^2$. A *vertex* of the Newton polygon is a point $(i, v(a_i))$ where two edges of a different slope meet. We call i the *degree* of the vertex $(i, v(a_i))$.

The Newton polygon of a polynomial consists of a sequence of edges with strictly increasing slopes, for which the following holds:

Theorem 2.7. *(See [8, II (6.3), II (6.4)].) Let K be a field with a discrete henselian valuation v. Let $f(t) = a_0 + a_1 t + \cdots + a_d t^d$ be a polynomial over K with $a_0 a_d \neq 0$. Denote the unique extension of v on the splitting field of f also by v. If $(r, v(a_r)) - (s, v(a_s))$ is an edge of the Newton polygon of f with slope m, then f has exactly $s - r$ roots $\alpha_1, \ldots, \alpha_{s-r}$ with valuation $v(\alpha_1) = \cdots = v(\alpha_{s-r}) = -m$. If the slopes of the Newton polygon of f are $m_1 < \cdots < m_k$ then*

$$f(t) = a_d \prod_{j=1}^{k} f_j(t), \tag{1}$$

with $f_j(t) = \prod_{v(\alpha_i) = -m_j} (t - \alpha_i) \in K[t]$.

Definition 2.8. We define *the factorization of f according to the slopes* to be the expression $a_d \prod_{j=1}^{k} f_j(t)$ in (1). Note that the polynomials $f_j(t)$ are not necessarily irreducible over K. The Newton polygon of each $f_j(t)$ has exactly one edge of slope m_j.

Lemma 2.9. *Let $a, b \in K^*$. If $v(b) > v(a) + v(4)$, then $a + b = x^2 a$ for some $x \in K^*$.*

Proof. By assumption, $v(a^{-1}b) > 0$, so $1 + a^{-1}b \in \mathcal{O}$. Let $f(t) = t^2 - (1 + a^{-1}b)$. Then $v(f(1)) = v(b) - v(a) > v(4) = 2v(f'(1))$. From Hensel's Lemma follows that $1 + a^{-1}b$ is a square. □

Lemma 2.10. *Let $f(t) = \sum_{k=0}^{d} b_k t^k$ be a monic polynomial (i.e. $b_d = 1$) whose Newton polygon has only one edge. Let $m := -v(b_0)/d$ be the slope. Let $\alpha \in K$. Then*

$$v\bigl(b_k \alpha^k\bigr) \geqslant k\bigl(m + v(\alpha)\bigr) - dm = (k - d)\bigl(m + v(\alpha)\bigr) + dv(\alpha).$$

Proof. This follows immediately from the fact that the Newton polygon of f has only one edge. □

Proposition 2.11. *Let K be a field with a discrete henselian valuation v and let $\alpha \in K$. Let f be a polynomial over K of even degree with $f(0) \neq 0$. Assume that the Newton polygon of f has only one edge, let m be the slope. Assume that $m \neq -v(\alpha)$ and let $N \in \mathbb{N}$ be such that*

$$N > \frac{v(4)}{|m + v(\alpha)|}. \tag{2}$$

Assume that f is of the form

$$f = a(t) + g(t)t^N + z(t)t^{2N + \deg g - \deg z},$$

where a, g and z are polynomials over K. Assume that $\deg(g)$ *and* $\deg(z)$ *are even and that* $\deg(a) < N$ *and* $\deg(z) < N$.

If $m < -v(\alpha)$, then $f(\alpha) = z(\alpha)$ in K^*/K^{*2}. If $m > -v(\alpha)$, then $f(\alpha) = a(\alpha)$ in K^*/K^{*2}.

Remark that we can always take $N = 1$ in (2) if the residue characteristic is different from 2.

Proof. Let $d = 2N + \deg(g)$ be the degree of f. Suppose first that the slope m of f is strictly smaller than $-v(\alpha)$. Let $c := z(\alpha)\alpha^{2N+\deg g-\deg z}$, whose leading term is the monomial of strictly lowest valuation in $f(\alpha)$. We then have that

$$c^{-1}f(\alpha) = c^{-1}a(\alpha) + c^{-1}g(\alpha)\alpha^N + 1.$$

Using Lemma 2.10, the inequality (2) implies

$$v\bigl(a(\alpha) + g(\alpha)\alpha^N\bigr) \geqslant (-N)\bigl(m + v(\alpha)\bigr) + dv(\alpha) = N\bigl|m + v(\alpha)\bigr| + v(c) > v(4) + v(c).$$

Therefore,

$$v\bigl(c^{-1}f(\alpha) - 1\bigr) > v(4).$$

By Hensel's Lemma applied to the polynomial $x^2 - (c^{-1}f(\alpha))$, we find that $c^{-1}f(\alpha)$ is a square. Since $\alpha^{2N+\deg g-\deg z}$ is a square, it follows that $z(\alpha)$ is in the same square class as $f(\alpha)$.

If the slope m of f is strictly bigger than $-v(\alpha)$, we let $c := a(\alpha)$. The constant term of c is the monomial of strictly lowest valuation in $f(\alpha)$. Note that $v(c) = -md$. We then have that

$$c^{-1}f(\alpha) = 1 + c^{-1}g(\alpha)\alpha^N + c^{-1}z(\alpha)\alpha^{d-\deg z}.$$

Using Lemma 2.10, the inequality (2) implies

$$v\bigl(g(\alpha)\alpha^N + z(\alpha)\alpha^{d-\deg z}\bigr) \geqslant N\bigl(m + v(\alpha)\bigr) - dm = N\bigl|m + v(\alpha)\bigr| + v(c) > v(4) + v(c).$$

Therefore,

$$v\bigl(c^{-1}f(\alpha) - 1\bigr) > v(4).$$

As before, we find that $c^{-1}f(\alpha)$ is a square; hence $f(\alpha)$ is in the same square class as $c = a(\alpha)$. □

3. A quadratic reciprocity symbol for polynomials

From now on, let K be a p-adic field, that is a finite extension of some $\mathbb{Q}_p$. Fix a uniformizer π of K, i.e. a generator of the maximal ideal in the valuation ring $\mathcal{O}$. We normalize the valuation on K and all its finite extensions such that $v(\pi) = 1$. This means for example that $v(\sqrt{\pi}) = 1/2$ in $K(\sqrt{\pi})$. Remark that v extends uniquely to the algebraic closure of K.

The structure of the Witt ring of p-adic fields is well known, in particular we know that $I^2(K) \cong \mathbb{Z}/2\mathbb{Z}$ and that $I^3(K) = 0$ (see [7, Ch. VI, Corollary 2.15]). In this section, we will define a kind of Legendre symbol for the function field $K(t)$. This symbol can be seen as the second residue map of a certain 3-fold Pfister form over $K(t)$, and takes two values according to the isotropy of this quadratic form. We will prove multiplicativity and a quadratic reciprocity law for this symbol.

Definition 3.1. Let $q(t)$ be a monic irreducible polynomial over K and let α be a root of q in the algebraic closure. For $p(t) \in K[t]$, coprime to $q(t)$, we define the Legendre symbol

$$\begin{aligned}\left(\frac{p}{q}\right) &= \delta_q\bigl(\langle 1, \pi\rangle\bigl\langle 1, -p(t)\bigr\rangle\bigl\langle 1, -q(t)\bigr\rangle\bigr)\\ &= \langle 1, \pi\rangle\bigl\langle 1, -p(\alpha)\bigr\rangle \in I^2\bigl(K(\alpha)\bigr) \cong \mathbb{Z}/2\mathbb{Z}.\end{aligned}$$

The second equality is justified because $\langle -1\rangle\varphi = \varphi$ for $\varphi \in I^2(L)$. We denote this symbol multiplicatively with values in $\{-1, 1\}$, despite the fact that the operation corresponds to addition of quadratic forms in the Witt ring. This symbol is well defined for $p(t) \in (K[t]/q(t))^*$.

For every $n \in \mathbb{Z}$, we have $(\frac{p}{q}) = (\frac{\pi^n p}{q})$ because of the factor $\langle 1, \pi\rangle$ in the definition of the Legendre symbol. For odd residue characteristic, this implies the following equivalent definition of the symbol:

$$\left(\frac{p}{q}\right) = 1 \quad \Longleftrightarrow \quad \pi^{-v(p(\alpha))} p(\alpha) \quad \text{is a square in } K(\alpha)^*,$$

where α is a root of $q(t)$. For even residue characteristic, we cannot give such an easy equivalence. Note that the symbol clearly depends on the choice of uniformizer π. To be consistent, we will work all the time with one fixed uniformizer.

Next, we prove multiplicativity of the symbol.

Proposition 3.2. *Let $q(t)$ be a monic irreducible polynomial over K. Let $p(t)$ and $r(t)$ be polynomials over K, coprime to $q(t)$. Then*

$$\left(\frac{pr}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{r}{q}\right). \tag{3}$$

Proof. Let α be a root of q. The statement (3) is equivalent to

$$\langle 1, \pi\rangle\langle 1, -p(\alpha)\rangle \perp \langle 1, \pi\rangle\langle 1, -r(\alpha)\rangle \perp -\langle 1, \pi\rangle\langle 1, -p(\alpha)r(\alpha)\rangle = 0.$$

We can simplify this to

$$\begin{aligned} \langle 1, \pi\rangle\langle 1, 1, -1, -p(\alpha), -r(\alpha), p(\alpha)r(\alpha)\rangle &= 0, \\ \langle 1, \pi\rangle\langle 1, -1\rangle \perp \langle 1, \pi\rangle\langle 1, -p(\alpha), -r(\alpha), p(\alpha)r(\alpha)\rangle &= 0, \\ \langle 1, \pi\rangle\langle 1, -p(\alpha)\rangle\langle 1, -r(\alpha)\rangle &= 0. \end{aligned}$$

Since 3-fold Pfister forms are hyperbolic over K, the last equality is always true. □

In order to further study this quadratic reciprocity symbol, we need to use transfers. See [10, Ch. 2, §5] for the definition and properties of the transfer map.

Proposition 3.3. *Let K be a p-adic field and L a finite extension of K. Let $s : L \to K$ be a non-zero K-linear map, $s_* : W(L) \to W(K)$ the corresponding transfer map. Then s_* induces an isomorphism $I^2(L) \xrightarrow{\sim} I^2(K)$.*

Proof. Recall that $I^2(L)$ and $I^2(K)$ have 2 elements, so it suffices to prove that the non-zero element of $I^2(L)$ maps to the non-zero element of $I^2(K)$. Let φ be a 4-dimensional anisotropic Pfister form over L, this means that $\varphi \neq 0$ in $I^2(L)$. From [10, Ch. 6, Theorem 4.4], it follows that $s_*(\varphi)$ is Witt equivalent to the unique anisotropic 4-dimensional quadratic form over K, so $s_*(\varphi) \neq 0$ in $W(K)$. □

Proposition 3.4. *Let $c \in K^*$ and $q \in K[t]$ be a monic irreducible polynomial. Then*

$$\left(\frac{c}{q}\right) = \left(\frac{c}{t}\right)^{\deg q}.$$

Proof. Let α be a root of q. Let $\varphi = \langle 1, \pi \rangle \langle 1, -c \rangle$ considered in $W(K(\alpha))$. Let $s : K(\alpha) \twoheadrightarrow K$ be a K-linear map. Proposition 3.3 says that $(\frac{c}{q}) = 1$ if and only if $s_*(\varphi) = 0$. By [10, Ch. 2, Theorem 5.6 and Lemma 5.8], we have

$$\begin{aligned} s_*(\varphi) &= \langle 1, \pi \rangle \langle 1, -c \rangle s_*\big(\langle 1 \rangle_L\big) \quad \big(\text{in } W(K)\big) \\ &= \begin{cases} \langle 1, \pi \rangle \langle 1, -c \rangle & (\deg q \text{ odd}), \\ 0 & (\deg q \text{ even}). \end{cases} \end{aligned}$$

This proves the proposition. □

Next, we want to find a quadratic reciprocity law. For p a monic irreducible polynomial of degree n we define the K-linear map

$$s_p : K[t]/(p) \to K$$

by $s_p(1) = s_p(t) = \cdots = s_p(t^{n-2}) = 0$, $s_p(t^{n-1}) = 1$. This map gives us the transfer homomorphism

$$(s_p)_* : W\big(K[t]/(p)\big) \to W(K).$$

For the prime at infinity, let $(s_\infty)_* = -id$. Then

Theorem 3.5. *(See [10, Ch. 6, Theorem 3.5].) Let K be a field of characteristic $\neq 2$. Let $\delta_p : W(K(t)) \to W(K[t]/(p))$ be the second residue class map with respect to the irreducible polynomial p or t^{-1} in case $p = \infty$ and let $(s_p)_*$ be the transfer homomorphism given above. For $\delta = \bigoplus \delta_p$ and $s_* = \sum (s_p)_*$ the following sequence is exact*:

$$W\big(K(t)\big) \xrightarrow{\delta} \bigoplus_{p,\infty} W\big(K[t]/(p)\big) \xrightarrow{s_*} W(K) \to 0.$$

In particular,

$$\sum (s_p)_* \delta_p(\varphi) = 0 \quad \big(\text{in } W(K)\big)$$

for every form $\varphi \in K(t)$.

Using this theorem, we can prove a reciprocity law for our symbol.

Theorem 3.6. *Let $p(t)$ and $q(t)$ be monic irreducible polynomials over K. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{t}\right)^{\deg p \deg q} \left(\frac{q}{p}\right). \tag{4}$$

Proof. Consider the quadratic form $\langle 1, \pi \rangle \langle 1, -p(t) \rangle \langle 1, -q(t) \rangle$. The second residue class map applied to this form is trivial, except possibly at p, q and ∞. In those cases we have that

$$\delta_p\big(\langle 1, \pi \rangle \big\langle 1, -p(t) \big\rangle \big\langle 1, -q(t) \big\rangle\big) = -\langle 1, \pi \rangle \big\langle 1, -q(\beta) \big\rangle,$$

where β is a root of p, and

$$\delta_q\big(\langle 1,\pi\rangle\big\langle 1,-p(t)\big\rangle\big\langle 1,-q(t)\big\rangle\big) = -\langle 1,\pi\rangle\big\langle 1,-p(\alpha)\big\rangle,$$

where α is a root of q. We claim that

$$\delta_\infty\big(\langle 1,\pi\rangle\big\langle 1,-p(t)\big\rangle\big\langle 1,-q(t)\big\rangle\big) = \langle 1,\pi\rangle\big\langle -1,(-1)^{\deg p\deg q}\big\rangle.$$

Indeed, we find

$$\begin{aligned}
&\delta_\infty\big(\langle 1,\pi\rangle\big\langle 1,-p(t)\big\rangle\big\langle 1,-q(t)\big\rangle\big) = 0 = \langle 1,\pi\rangle\langle -1,1\rangle \quad &&(\deg p \text{ even}, \deg q \text{ even}),\\
&\delta_\infty\big(\langle 1,\pi\rangle\big\langle 1,-p(t)\big\rangle\big\langle 1,-q(t)\big\rangle\big) = \langle 1,\pi\rangle\langle -1,1\rangle &&(\deg p \text{ odd}, \deg q \text{ even}),\\
&\delta_\infty\big(\langle 1,\pi\rangle\big\langle 1,-p(t)\big\rangle\big\langle 1,-q(t)\big\rangle\big) = \langle 1,\pi\rangle\langle -1,-1\rangle &&(\deg p \text{ odd}, \deg q \text{ odd}).
\end{aligned}$$

From Theorem 3.5, it follows that

$$(s_p)_*\big(\langle 1,\pi\rangle\big\langle 1,-q(\beta)\big\rangle\big) + (s_q)_*\big(\langle 1,\pi\rangle\big\langle 1,-p(\alpha)\big\rangle\big) - \langle 1,\pi\rangle\big\langle -1,(-1)^{\deg p\deg q}\big\rangle = 0.$$

By definition and multiplicativity of the symbol, we have that

$$\langle 1,\pi\rangle\big\langle 1,-(-1)^{\deg p\deg q}\big\rangle = \left(\frac{-1}{t}\right)^{\deg p\deg q}.$$

From Proposition 3.3 now follows

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{t}\right)^{\deg p\deg q}\left(\frac{q}{p}\right). \qquad \square$$

4. Isotropy of a certain class of quadratic forms

In this section, K denotes a p-adic field with fixed uniformizer π. Let $\mathcal{O}$ denote the valuation ring of K.

Lemma 4.1. *Let R be a ring and $x, y \in R$ such that $(x, y) = (1)$. Let $\rho \in R^*$ and $N \in \mathbb{N}$. Then $(x+\rho y^N, xy^N) = (1)$.*

Proof. Cubing the relation $(x, y) = (1)$, we get $(x^3, x^2y, xy^2, y^3) = (1)$. Clearly, $(x^3, x^2y, xy^2, y^3) \subseteq (x^2, y^2)$; therefore, $(x^2, y^2) = (1)$. We can continue this process by induction to get $(x^{2^n}, y^{2^n}) = (1)$ for all n, so also $(x^2, y^{2N}) = (1)$. Let $\mathcal{I} := (x + \rho y^N, xy^N)$. One can easily check that $x^2 = x(x + \rho y^N) - \rho xy^N \in \mathcal{I}$ and $y^{2N} = \rho^{-1}y^N(x + \rho y^N) - \rho^{-1}xy^N \in \mathcal{I}$. It follows that $(1) = (x^2, y^{2N}) \subseteq \mathcal{I}$, hence $\mathcal{I} = (1)$. $\square$

The following is the main theorem regarding isotropy of quadratic forms.

Theorem 4.2. *Let $\gamma \in K^*$. Let $g \in K[t]$ with $g(0) \neq 0$. If all the vertices of the Newton polygon of g have even degree, then there exists an $s \in K[t]$ such that both quadratic forms*

$$\langle 1,\pi\rangle\langle 1,-\gamma\rangle\langle 1,-s\rangle, \tag{5}$$

$$\langle 1,\pi\rangle\langle 1,tg\rangle\langle 1,-ts\rangle \tag{6}$$

are isotropic over $K(t)$.

Proof. Without loss of generality, we may assume that g is a square-free polynomial (we can divide out squared factors, this does not change the isotropy of (6)). Because of the factor $\langle 1, \pi \rangle$ appearing in (6), multiplying g with some power of π does not change the isotropy of that quadratic form. Therefore, we may assume that the leading coefficient ε of g has valuation zero.

Let $g = \varepsilon \prod_{i=1}^{n} g_i$ be the factorization according to the slopes of g. Write $g_i = \prod_j g_{ij}$, where the g_{ij} are monic and irreducible. Let n_i denote the degree of g_i, let $m_i = -v(g_i(0))/n_i$ denote the slope of g_i and d_i the denominator of $m_i \in \mathbb{Q}$. Then the degree of every g_{ij} must be a multiple of d_i.

Let N be an odd integer which is a multiple of all odd d_i and large enough such that

$$N > v(4)/\min_{i \neq j} |m_i - m_j| \quad \text{and} \quad N > \deg g.$$

In order to find s, we write $s = \varepsilon \prod_{i=1}^{n} \prod_j s_{ij}$ and define $s_i := \prod_j s_{ij}$. The chosen s_{ij} will satisfy the following properties:

(i) s_{ij} is coprime to tg.
(ii) s_{ij} is monic irreducible with slope m_i.
(iii) s_{ij} has even degree.
(iv) For all i, κ, λ with $i \neq \kappa$, the following equality holds:

$$\left(\frac{s_i}{g_{\kappa\lambda}}\right) = \left(\frac{g_i}{g_{\kappa\lambda}}\right). \tag{7}$$

By Theorem 2.3 it suffices to solve the quadratic forms (5) and (6) locally at primes associated with irreducible polynomials in $K[t]$ to solve them globally. Indeed, if all the second residue maps of such a quadratic form are zero, then this form is Witt equivalent to an anisotropic form φ over K. Since the dimension of φ is at most 4, the isotropy of (5) and (6) follows.

The second residue map of (5) is trivially zero, except at the irreducible factors s_{ij} of s. For each s_{ij}, this second residue form is $\langle 1, \pi \rangle \langle 1, -\gamma \rangle$ over $K[t]/(s_{ij})$. So property (iii) is sufficient to prove that (5) is isotropic: Proposition 3.4 implies that $(\frac{\gamma}{s_{ij}}) = 1$ for each irreducible factor s_{ij} of s.

To prove that $\langle 1, \pi \rangle \langle 1, tg \rangle \langle 1, -ts \rangle$ is isotropic over $K(t)$, we need to consider the second residue forms at t and at each g_{ij} and s_{ij}. The isotropy of these forms is equivalent to the following three conditions:

$$\left(\frac{sg}{t}\right) = 1, \tag{8}$$

$$\left(\frac{ts}{g_{ij}}\right) = 1 \quad \text{for all } i, j, \tag{9}$$

$$\left(\frac{-tg}{s_{ij}}\right) = 1 \quad \text{for all } i, j. \tag{10}$$

If conditions (9) and (10) are fulfilled, then (8) follows automatically (because we chose the leading coefficient of s to be equal to ε):

$$\begin{aligned}\left(\frac{sg}{t}\right) &= \left(\frac{\varepsilon}{t}\right) \prod_{i,j} \left(\frac{s_{ij}}{t}\right) \left(\frac{\varepsilon}{t}\right) \prod_{i,j} \left(\frac{g_{ij}}{t}\right) \\ &= \prod_{i,j} \left(\frac{-1}{t}\right)^{\deg s_{ij}} \left(\frac{t}{s_{ij}}\right) \prod_{i,j} \left(\frac{-1}{t}\right)^{\deg g_{ij}} \left(\frac{t}{g_{ij}}\right)\end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{-1}{t}\right)^{\deg s}\left(\frac{-1}{t}\right)^{\deg g}\prod_{i,j}\left(\frac{-g}{s_{ij}}\right)\prod_{i,j}\left(\frac{s}{g_{ij}}\right)\\
&= \prod_{i,j}\left[\left(\frac{-\varepsilon}{s_{ij}}\right)\prod_{\mu,\nu}\left(\frac{g_{\mu\nu}}{s_{ij}}\right)\right]\prod_{i,j}\left[\left(\frac{\varepsilon}{g_{ij}}\right)\prod_{\kappa,\lambda}\left(\frac{s_{\kappa\lambda}}{g_{ij}}\right)\right]\\
&= \prod_{i,j}\left[\left(\frac{-\varepsilon}{t}\right)^{\deg s_{ij}}\prod_{\mu,\nu}\left(\frac{-1}{t}\right)^{\deg g_{\mu\nu}\deg s_{ij}}\left(\frac{s_{ij}}{g_{\mu\nu}}\right)\right]\prod_{i,j}\left[\left(\frac{\varepsilon}{t}\right)^{\deg g_{ij}}\prod_{\kappa,\lambda}\left(\frac{s_{\kappa\lambda}}{g_{ij}}\right)\right] = 1
\end{aligned}
$$

since the degree of s and of g is even.

Using multiplicativity and property (7), we find

$$
\begin{aligned}
\left(\frac{ts}{g_{ij}}\right) = \left(\frac{\varepsilon t}{g_{ij}}\right)\prod_{\mu}\left(\frac{s_\mu}{g_{ij}}\right) &= \left(\frac{\varepsilon t}{g_{ij}}\right)\left(\frac{s_i}{g_{ij}}\right)\prod_{\mu\neq i}\left(\frac{g_\mu}{g_{ij}}\right)\\
&= \left(\frac{s_i}{g_{ij}}\right)\left(\frac{tg/g_i}{g_{ij}}\right).
\end{aligned}
$$

Since the degree of each s_{ij} is even, we have

$$
\left(\frac{-tg}{s_{ij}}\right) = \left(\frac{t}{s_{ij}}\right)\left(\frac{-\varepsilon}{s_{ij}}\right)\prod_{\kappa,\lambda}\left(\frac{g_{\kappa\lambda}}{s_{ij}}\right) = \left(\frac{s_{ij}}{t}\right)\prod_{\kappa,\lambda}\left(\frac{s_{ij}}{g_{\kappa\lambda}}\right).
$$

Therefore, the conditions (9) and (10) become

$$
\left(\frac{s_i}{g_{ij}}\right) = \left(\frac{tg/g_i}{g_{ij}}\right) \quad \text{for all } i,\ j, \tag{11}
$$

$$
\left(\frac{s_{ij}}{t}\right) = \prod_{\kappa,\lambda}\left(\frac{s_{ij}}{g_{\kappa\lambda}}\right) \quad \text{for all } i,\ j. \tag{12}
$$

Now we construct the s_i, satisfying properties (i)–(iv) and conditions (11) and (12). For this, we will have to distinguish two cases, according to the parity of d_i, the denominator of the slope m_i.

Case 1. d_i is odd.

In this case, we will have only one irreducible factor $s_i = s_{i1}$ with slope m_i. Using (7) and (11), we can rewrite the right-hand side of condition (12) as

$$
\begin{aligned}
\prod_{\kappa,\lambda}\left(\frac{s_i}{g_{\kappa\lambda}}\right) &= \prod_{\kappa\neq i,\lambda}\left(\frac{s_i}{g_{\kappa\lambda}}\right)\prod_{j}\left(\frac{s_i}{g_{ij}}\right)\\
&= \prod_{\kappa\neq i,\lambda,j}\left(\frac{g_{ij}}{g_{\kappa\lambda}}\right)\prod_{j}\left(\frac{tg/g_i}{g_{ij}}\right)\\
&= \prod_{\kappa\neq i,\lambda,j}\left(\frac{-1}{t}\right)^{\deg g_{\kappa\lambda}\deg g_{ij}}\left(\frac{g_{\kappa\lambda}}{g_{ij}}\right)\prod_{j}\left(\frac{tg/g_i}{g_{ij}}\right)
\end{aligned}
$$

$$= \prod_{\kappa \neq i} \left(\frac{-1}{t}\right)^{\deg g_\kappa \deg g_i} \prod_j \left(\frac{\varepsilon^{-1} g/g_i}{g_{ij}}\right) \prod_j \left(\frac{tg/g_i}{g_{ij}}\right)$$

$$= \prod_j \left(\frac{\varepsilon^{-1} t}{g_{ij}}\right) = \prod_j \left(\frac{\varepsilon^{-1}}{t}\right)^{\deg g_{ij}} \left(\frac{-1}{t}\right)^{\deg g_{ij}} \left(\frac{g_{ij}}{t}\right) = \left(\frac{g_i}{t}\right).$$

Therefore, condition (12) becomes

$$\left(\frac{s_i}{t}\right) = \left(\frac{g_i}{t}\right). \tag{13}$$

Let

$$R = \sum_{\{(\alpha,\beta) \in \mathbb{Z}^2 \mid \beta \geqslant 0 \wedge \alpha \geqslant m_i \beta\}} (\pi^\alpha t^\beta)\mathcal{O},$$

$$P = \sum_{\{(\alpha,\beta) \in \mathbb{Z}^2 \mid \beta \geqslant 0 \wedge \alpha > m_i \beta\}} (\pi^\alpha t^\beta)\mathcal{O}.$$

Clearly, R is an $\mathcal{O}$-module in $K[t]$, but one can check that it is actually a subring. Then P is a prime ideal in R. It is not hard to see that the usual Euclidean division for polynomials works in R, provided we divide by a polynomial whose leading term is not in P.

Let $u := \pi^{m_i d_i} t^{d_i}$ and $k = \mathcal{O}/(\pi)$. From now on, a line over an element of R denotes reduction modulo P. The quotient ring R/P is $k[\bar{u}]$ (the variable $\bar{u}$ is precisely the reduction of the element $u = \pi^{m_i d_i} t^{d_i}$). For a polynomial $f(\bar{u}) \in k[\bar{u}]$, we define $\deg^\dagger f := d_i \deg f$. This is chosen such that $\deg^\dagger \overline{f} = \deg f$ for all $f \in R$ with leading term not in P.

Define $h_i := \pi^{m_i n_i} g_i$. Since g_i is monic of degree n_i and slope m_i, it follows that $h_i \in R$. For g_μ with $m_\mu > m_i$, we have $\pi^{m_\mu n_\mu} g_\mu \in R$ and only the constant term of $\pi^{m_\mu n_\mu} g_\mu$ does not vanish modulo P. For g_μ with $m_\mu < m_i$, let $B_i \in 2d_i\mathbb{Z}$ such that $B_i \geqslant n_\mu = \deg g_\mu$. Then $\pi^{B_i m_i} t^{B_i - n_\mu} g_\mu \in R$ and only the leading term of $\pi^{B_i m_i} t^{B_i - n_\mu} g_\mu$ does not vanish modulo P. So we see that there exist $A, B \in \mathbb{Z}$ with B even such that $\pi^A t^B g/g_i = \varepsilon \pi^A t^B \prod_{\mu \neq i} g_\mu \in R \setminus P$. The reduction modulo P of $\pi^A t^B g/g_i$ is of the form $\rho \bar{u}^G$ with $\rho \in k^*$ and $G \geqslant 0$.

We want to construct s_i using the ring R. Since the conditions (11) and (13) do not change if we multiply s_i with a multiple of π, in reality we will construct $c := \pi^{m_i \deg s_i} s_i \in R$. We define

$$a := h_i + \pi^{m_i N + A} t^{N+B} g/g_i \in R,$$

$$b := h_i u^{N/d_i + G} = \pi^{m_i(N + d_i G)} t^{N + d_i G} h_i \in R.$$

We will construct c of the form $c = a + qb$ for some $q \in R$. Using the fact that $(\frac{t}{g_{ij}}) = (\frac{t^{N+B}}{g_{ij}})$ and $g_{ij} \mid h_i$, it is clear that $s_i := \pi^{-m_i \deg c} c = \pi^{-m_i \deg c}(a + qb)$ satisfies (11) and (13). At the same time, we will make sure that c is also of the form $r + \pi^{m_i e} t^e h_i$ for some $e \in 2d_i\mathbb{Z}$ and $r \in R$ with $\deg r \leqslant \deg h_i + e - N$. We claim that for such c, the following holds:

$$\left(\frac{c}{g_{\kappa\lambda}}\right) = \left(\frac{h_i}{g_{\kappa\lambda}}\right) \quad \text{for all } \kappa, \lambda \text{ with } i \neq \kappa. \tag{14}$$

Indeed, let α be a root of $g_{\kappa\lambda}$. If $m_i < m_\kappa = -v(\alpha)$, then by Proposition 2.11, the square class of $c(\alpha)$ in $K(\alpha)$ is the same as $\pi^{m_i e} h_i(\alpha)$. This implies (14). If $m_i > m_\kappa$, then the square class of $c(\alpha)$ in $K(\alpha)$

is the same as $a(\alpha)$. Since $(g/g_i)(\alpha)=0$, this also implies (14). Using $(\frac{s_i}{g_{\kappa\lambda}})=(\frac{c}{g_{\kappa\lambda}})$ and $h_i=\pi^{m_in_i}g_i$, it is clear that (14) implies (7).

The ideal $P+(u)$ in R contains all $\pi^{\alpha}t^{\beta}\in R$, except for π^0t^0. The constant term of h_i has valuation zero, therefore $(h_i)+P+(u)=(1)$. Note that $\bar a=\overline{h_i}+\rho\bar u^{N/d_i+G}$ and $\bar b=\overline{h_i}\bar u^{N/d_i+G}$. Since $(\overline{h_i},\bar u)=(1)$ in R/P, Lemma 4.1 implies $(\bar a,\bar b)=(1)$.

Let $N':=N/d_i$. We apply Theorem 2.4 to $k=R/(P+(u))$, $F=k(\bar u)$, $S_\infty=\{\mathfrak{p}_\infty\}$, then $A=k[\bar u]$. Take

$$\begin{aligned}V_\infty&=\left\{\bar u^{e'}+c_{e'-N'}\bar u^{e'-N'}+c_{e'-N'-1}\bar u^{e'-N'-1}+\cdots+c_0+c_{-1}\bar u^{-1}+\cdots\;\middle|\;e'\in 2\mathbb{Z}\right\}\\&\subseteq k\big(\big(\bar u^{-1}\big)\big)=k_\infty\end{aligned}$$

and $x_\infty=\overline{h_i}$.

Because of Theorem 2.4, there exist infinitely many $\overline{q_1}\in k[\bar u]$ such that $\bar c:=\bar a+\overline{q_1}\bar b\in k[\bar u]$ is irreducible and in $\overline{h_i}V_\infty$. There are infinitely many, so we may assume that $\deg^\dagger\bar c\geqslant N+\deg b$.

Since $\bar c\in\overline{h_i}V_\infty$, we can write $\bar c=\overline{h_i}(\bar u^{e'}+\overline{r_0})$, with $\overline{r_0}\in k((\bar u^{-1}))$ such that $\deg\overline{r_0}\leqslant e'-N'$. Let $\overline{r_1}=\overline{h_i}\overline{r_0}=\bar c-\overline{h_i}\bar u^{e'}\in k[\bar u]$, then $\deg^\dagger\overline{r_1}\leqslant n_i+e-N$, with $e=d_ie'$. Choose a lift $r_1\in R$ of $\overline{r_1}$ such that $\deg r_1=\deg^\dagger\overline{r_1}$. Now let $\tilde c=r_1+\pi^{m_ie}t^eh_i\in R$, then $\tilde c$ is a lift of $\bar c$.

Let $q_1\in R$ be a lift of $\overline{q_1}$. Lifting the equality $\bar c=\bar a+\overline{q_1}\bar b$ to R yields an error term which is in P, so there exists an $f\in P$ such that

$$\tilde c+f=a+q_1b. \tag{15}$$

Since the leading term of b is not in P, we can do Euclidean division of f by b: let $f=q_2b+r_2$ with $\deg r_2<\deg b$. Plugging this into (15) gives $\tilde c+r_2=a+(q_1-q_2)b$.

Reducing the equality $f=q_2b+r_2$ modulo P gives $0=\overline{q_2}\bar b+\overline{r_2}$. The leading term of b does not vanish modulo P, so $\deg^\dagger\overline{r_2}\leqslant\deg r_2<\deg b=\deg^\dagger\bar b$. Since $\overline{r_2}$ is a multiple of $\bar b$, it follows that $\overline{r_2}=0$.

Define $c:=\tilde c+r_2$, $q:=q_1-q_2$ and $r:=r_1+r_2$. Then

$$c=a+qb=r+\pi^{m_ie}t^eh_i,$$

which is of the required form. It remains to check that c is irreducible. Suppose c is reducible in $K[t]$, so $c=c_1c_2$ with $c_1,c_2\in K[t]$. Without loss of generality we can assume that $c_1(0)=1$. Since $c_2(0)=c(0)=h_i(0)$ is a unit and c_1 and c_2 have slope m_i, it follows that $c_1,c_2\in R$. Therefore, we can reduce modulo P to find $\bar c=\overline{c_1}\,\overline{c_2}$. Now the irreducibility of $\bar c$ together with $\deg^\dagger\bar c=\deg c$ implies that c is irreducible.

Case 2. d_i is even.

In this case, every g_{ij} has even degree. The previous method will not work because every odd degree monomial in R becomes zero in R/P. Instead we will find for each monic irreducible factor g_{ij} of g_i an irreducible s_{ij}. We set

$$s_{ij}=g_{ij}+p_{ij}$$

with $p_{ij}\in R$ with $\deg p_{ij}<\deg g_{ij}$ still to be determined. The coefficients of p_{ij} will be chosen to have large valuation. By [11, Ch. II, §2, Exercice 2], s_{ij} will be irreducible if the valuation of p_{ij} is sufficiently large (depending on g_{ij}).

Next, we want to check that

$$\left(\frac{g_{ij}+p_{ij}}{g_{\mu\nu}}\right)=\left(\frac{g_{ij}}{g_{\mu\nu}}\right)\qquad\text{for all }(\mu,\nu)\neq(i,j). \tag{16}$$

This follows from Lemma 2.9 if $v(p_{ij}(\alpha)) > v(g_{ij}(\alpha)) + v(4)$ for each root α of $g_{\mu\nu}$ with $(\mu, \nu) \neq (i, j)$. Since $g_{ij}(\alpha) \neq 0$ for each root α of $g_{\mu\nu}$ with $(\mu, \nu) \neq (i, j)$, we can enforce this condition by taking the coefficients of p_{ij} to have large enough valuation. Clearly, (16) implies that (7) is satisfied.

Using (16), we rewrite condition (11):

$$\prod_{\nu} \left(\frac{s_{i\nu}}{g_{ij}}\right) = \left(\frac{tg/g_i}{g_{ij}}\right),$$

$$\left(\frac{s_{ij}}{g_{ij}}\right) \prod_{\nu \neq j} \left(\frac{g_{i\nu}}{g_{ij}}\right) = \left(\frac{tg/g_i}{g_{ij}}\right),$$

$$\left(\frac{p_{ij}}{g_{ij}}\right) = \left(\frac{tg/g_{ij}}{g_{ij}}\right).$$

This condition will be satisfied if we choose p_{ij} such that $p_{ij} \equiv \pi^A tg/g_{ij} \pmod{g_{ij}}$ with $\deg p_{ij} < \deg g_{ij}$ for a large enough A. Using the fact that g_{ij} has even degree, the right-hand side of (12) becomes

$$\begin{aligned}\prod_{\kappa,\lambda} \left(\frac{s_{ij}}{g_{\kappa\lambda}}\right) &= \left(\frac{s_{ij}}{g_{ij}}\right) \prod_{(\kappa,\lambda)\neq(i,j)} \left(\frac{g_{ij}}{g_{\kappa\lambda}}\right) = \left(\frac{p_{ij}}{g_{ij}}\right) \prod_{(\kappa,\lambda)\neq(i,j)} \left(\frac{g_{\kappa\lambda}}{g_{ij}}\right) \\ &= \left(\frac{tg/g_{ij}}{g_{ij}}\right)\left(\frac{\varepsilon^{-1} g/g_{ij}}{g_{ij}}\right) = \left(\frac{\varepsilon^{-1}}{g_{ij}}\right)\left(\frac{t}{g_{ij}}\right) = \left(\frac{g_{ij}}{t}\right).\end{aligned}$$

Since $s_{ij}(0)$ and $g_{ij}(0)$ are in the same square class, this is equal to $(\frac{s_{ij}}{t})$, therefore (12) is satisfied. □

This easily implies the following corollary, which corresponds to [6, Theorem 17].

Corollary 4.3. *Let K be a p-adic field with uniformizer π and let $\gamma \in K^*$. Let $g \in K[t]$ with $g(0) \neq 0$. If all the vertices of the Newton polygon of g have even degree, then the quadratic form*

$$\langle 1, \pi\rangle\langle 1, -\gamma, -t, -g\rangle$$

is isotropic over $K(t)$.

Proof. It follows from Theorem 4.2 that there exists an $s \in K[t]$ such that the quadratic forms (5) and (6) are isotropic. By Theorem 2.2, these forms are zero in the Witt ring.

Therefore, in $W(K)$ we also have

$$0 = \langle 1, \pi\rangle\langle 1, -\gamma\rangle\langle 1, -s\rangle \perp \langle -t\rangle\langle 1, \pi\rangle\langle 1, tg\rangle\langle 1, -ts\rangle,$$

$$0 = \langle 1, \pi\rangle\langle 1, -\gamma, -s, \gamma s, -t, -g, s, tgs\rangle,$$

$$0 = \langle 1, \pi\rangle\langle 1, -\gamma, -t, -g\rangle \perp \langle 1, \pi\rangle\langle s\rangle\langle -1, \gamma, 1, tg\rangle.$$

This implies

$$\langle 1, \pi\rangle\langle 1, -\gamma, -t, -g\rangle = -\langle 1, \pi\rangle\langle s\rangle\langle \gamma, tg\rangle \quad \text{in } W(K).$$

Since the right-hand side has dimension 4 and the left-hand side dimension 8, it follows that the left-hand side is isotropic. □

5. Diophantine undecidability

In this section we will use the result of the previous section to give a diophantine definition of the predicate "$v_t(x) \geqslant 0$" in $K(t)$. By Theorem 1.1, this implies that the existential theory of $K(t)$ is undecidable.

As before, K denotes a p-adic field with fixed uniformizer π. From now on, fix $\gamma \in K^*$ such that the quadratic form $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over K (for the existence of such a γ, see for example [7, Ch. VI, Corollary 2.15]). Throughout this section, we work with the following system of two quadratic forms over $K(t)$:

$$\langle 1, \pi\rangle \ \langle 1, -\gamma, -t, -f\rangle, \tag{17}$$

$$\langle 1, \pi\rangle \ \langle 1, -\gamma, -t, -\gamma f\rangle \tag{18}$$

with $f \in K(t)$. First, we prove a theorem which is analogous to [6, Proposition 7]. The quadratic forms above are analogous[3] to the quadratic forms appearing in the cited proposition.

Theorem 5.1. *Let $f \in K(t)$ such that $v_t(f)$ is odd. Then one of the quadratic forms* (17) *or* (18) *is anisotropic over $K(t)$.*

Proof. Let $f_n t^n + f_{n+1} t^{n+1} + \cdots$ be the series expansion of f (with $f_n \neq 0$). By assumption, n is odd. The first and second residue class forms of (17) at t are $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ and $\varphi_1 := \langle 1, \pi\rangle\langle -1, -f_n\rangle$. The residue forms of (18) at t are $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ and $\varphi_2 := \langle 1, \pi\rangle\langle -1, -\gamma f_n\rangle$. By assumption $\langle 1, \pi\rangle\langle 1, -\gamma\rangle \neq 0$ in $W(K)$. Since

$$\begin{aligned}\varphi_2 - \varphi_1 &= \langle 1, \pi\rangle\langle -1, -\gamma f_n, 1, f_n\rangle \\ &= \langle f_n\rangle\langle 1, \pi\rangle\langle 1, -\gamma\rangle \neq 0 \quad \text{in } W(K),\end{aligned}$$

it follows that $\varphi_1 \neq 0$ or $\varphi_2 \neq 0$. Suppose that $\varphi_1 \neq 0$ (the argument for $\varphi_2 \neq 0$ is completely analogous). Since φ_1 is a Pfister form, it follows from Theorem 2.2 that φ_1 is anisotropic. Both residue forms of (17) are anisotropic, therefore (17) is anisotropic. □

We prove a consequence of Corollary 4.3. Roughly speaking, we start from a given rational function h and we construct a polynomial such that the vertices of its Newton polygon all have even degree. It is similar to [6, Theorem 9].

Theorem 5.2. *Let $h \in K(t)$ be such that $v_\infty(h) \geqslant -2$ and $v_t(h) = 0$. Then there exists $c \in K$ such that, if we let*

$$f := h + ct^2, \tag{19}$$

both quadratic forms (17) *and* (18) *are isotropic over $K(t)$.*

Proof. Since $v_\infty(h) \geqslant -2$ and $v_t(h) = 0$, we can write $h(t) = \frac{h_N(t)}{h_D(t)}$ with h_N and h_D polynomials such that $h_N(0)h_D(0) \neq 0$ and $\deg h_N \leqslant \deg h_D + 2$. Multiplying f with h_D^2 does not change the isotropy of (17) and (18). We want to apply Corollary 4.3 with $g = f h_D^2$, so

$$g = h_N h_D + ct^2 h_D^2.$$

[3] The letter b from Kim and Roush corresponds to our π; a corresponds to our γ; f corresponds to $t \cdot g$ and the forms are multiplied with a factor $\langle t\rangle$.

It is clear that $g(0) \neq 0$ and $\deg g = 2 + 2\deg h_D$. We can choose $c \in K$ such that $v(c)$ is very low (depending on the coefficients of h_N and h_D). Namely, we can choose $v(c)$ so low that the first edge of the Newton polygon of g has vertices of degree 0 and degree 2. Choosing $v(c)$ low enough, the remaining vertices of the Newton polygon of g are the vertices of the Newton polygon of $ct^2h_D^2$, and those also have even degree. So g satisfies the conditions of Corollary 4.3, and because multiplying g with an element of K^* does not change the degree of the vertices of g, the isotropy of (17) and (18) follows. □

We prove the next theorem similar to [2, Proposition 4.7], in which we relate the valuation at t to the isotropy of our system of quadratic forms.

Theorem 5.3. *Let $x \in K(t)$. Then $v_t(x) \geqslant 0$ if and only if there exists a $c \in K$ such that the quadratic forms* (17) *and* (18) *are isotropic with*

$$f := \frac{1 + t + t^2x^3}{1 + tx^3} + ct^2.$$

Proof. Define $h_N := 1 + t + t^2x^3$, $h_D := 1 + tx^3$ and $h := h_N/h_D$.

Assume first that $v_t(x) \geqslant 0$. Then $v_t(h_N) = 0$ and $v_t(h_D) = 0$ such that $v_t(h) = 0$. If $v_\infty(x) \geqslant 1$, then $v_\infty(h_N) = -1$ and $v_\infty(h_D) = 0$ such that $v_\infty(h) = -1$. If $v_\infty(x) \leqslant 0$, then $v_\infty(h_N) = -2 + 3v_\infty(x)$ and $v_\infty(h_D) = -1 + 3v_\infty(x)$ such that $v_\infty(h) = -1$. In short, if $v_t(x) \geqslant 0$, then $v_t(h) = 0$ and $v_\infty(h) = -1$. Theorem 5.2 gives us that there exists a $c \in K$ such that (17) and (18) are isotropic.

Conversely, assume that $v_t(x) \leqslant -1$. Then $v_t(h_N) = 2 + 3v_t(x)$ and $v_t(h_D) = 1 + 3v_t(x)$ such that $v_t(h) = 1$. It follows that $v_t(f) = 1$. By Theorem 5.1, for every $c \in K$, one of the quadratic forms (17) and (18) is anisotropic. □

Since quadratic forms being isotropic is a diophantine condition, the result in Theorem 5.3 is a diophantine definition of the valuation ring at t in $K(t)$, except for the part "there exists a $c \in K$". We now prove that the constants are diophantine in $K(t)$.

Proposition 5.4. *K is diophantine in $K(t)$.*

Proof. Let E be the elliptic curve over K given by the equation $y^2 = x^3 - x$. Let $y \in K$ with $v(y) > 0$. We claim that there is an $x \in K$ such that (x, y) lies on $E(K)$. Let $f(x) = x^3 - x - y^2 \in \mathcal{O}[x]$. Since $v(f(0)) = 2v(y) > 2v(f'(0)) = 0$, it follows from Theorem 2.5 that there exists a $b \in \mathcal{O}$ such that $f(b) = 0$. So

$$K = \bigl\{y_1/y_2 \bigm| (\exists x_1, x_2 \in K)\ \bigl((x_1, y_1) \in E(K) \wedge (x_2, y_2) \in E(K) \wedge y_2 \neq 0\bigr)\bigr\}.$$

By Hurwitz' Theorem [5, Ch. IV, Corollary 2.4], the curve $y^2 = x^3 - x$ admits no rational parametrization, so $E(K(t)) = E(K)$. This means

$$K = \bigl\{y_1/y_2 \bigm| \bigl(\exists x_1, x_2 \in K(t)\bigr)\ \bigl((x_1, y_1) \in E\bigl(K(t)\bigr) \wedge (x_2, y_2) \in E\bigl(K(t)\bigr) \wedge y_2 \neq 0\bigr)\bigr\};$$

hence K is diophantine in $K(t)$. □

Corollary 5.5. *In $K(t)$, the relation $v_t(x) \geqslant 0$ is diophantine.*

Proof. The result follows immediately from Theorem 5.3 and Proposition 5.4. □

Acknowledgment

The authors would like to thank Jan Van Geel for the many discussions together and the good suggestions he made, and for proofreading the paper.

References

[1] H. Bass, J. Milnor, J.-P. Serre, Solution of the congruence subgroup problem for SL_n $(n \geqslant 3)$ and Sp_{2n} $(n \geqslant 2)$, Inst. Hautes Études Sci. Publ. Math. 33 (1967) 59–137.
[2] Jeroen Demeyer, Diophantine sets of polynomials over number fields, Proc. Amer. Math. Soc. 138 (8) (2010) 2715–2728.
[3] Jan Denef, The Diophantine problem for polynomial rings and fields of rational functions, Trans. Amer. Math. Soc. 242 (1978) 391–399.
[4] Antonio Engler, Alexander Prestel, Valued Fields, Springer Monogr. Math., Springer, 2005.
[5] Robin Hartshorne, Algebraic Geometry, Grad. Texts in Math., vol. 52, Springer, 1977.
[6] Ki Hang Kim, Fred Roush, Diophantine unsolvability over p-adic function fields, J. Algebra 176 (1) (1995) 83–110.
[7] Tsit-Yuen Lam, Introduction to Quadratic Forms over Fields, Grad. Stud. Math., vol. 67, American Mathematical Society, 2005.
[8] Jürgen Neukirch, Algebraische Zahlentheorie, Springer, 1992.
[9] Thanases Pheidas, Karim Zahidi, Undecidability of existential theories of rings and fields: a survey, in: Denef, et al. (Eds.), Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, Ghent, 1999, in: Contemp. Math., vol. 270, 2000, pp. 49–105.
[10] Winfried Scharlau, Quadratic and Hermitian Forms, Grundlehren Math. Wiss., vol. 270, Springer, Berlin, 1985.
[11] Jean-Pierre Serre, Corps locaux, Actualités scientifiques et industrielles, Hermann, 1980.