Hilbert's Tenth Problem for function fields over valued fields in characteristic zero

Jeroen Demeyer*

2010–02–09

Abstract

Let K be a field with a valuation satisfying the following conditions: both K and the residue field k have characteristic zero; the value group is not 2-divisible; there exists a maximal subfield F in the valuation ring such that $\mathrm{Gal}(\bar{F}/F)$ and $\mathrm{Gal}(\bar{k}/k)$ have the same 2-cohomological dimension and this dimension is finite. Then Hilbert's Tenth Problem has a negative answer for any function field of a variety over K.

1 Introduction

Hilbert's Tenth Problem (from his well-known list of 23 problems presented in 1900) is the following: find an algorithm which, given a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$, decides whether or not f has a zero in $\mathbb{Z}^n$. It has been shown that such an algorithm does not exist by Matiyasevich (see [Mat70]), building on earlier work by Davis, Putnam and Robinson. See [Dav73] for a survey article with the proof of Hilbert's Tenth Problem.

Hilbert's Tenth Problem (HTP) can be generalized as follows: let $\mathcal{R}$ be a ring and $\mathcal{R}_0$ a finitely generated $\mathbb{Z}$-algebra in $\mathcal{R}$. Then Hilbert's Tenth Problem for $\mathcal{R}$ with coefficients in $\mathcal{R}_0$ is the question whether there exists an algorithm which can decide whether a polynomial $f \in \mathcal{R}_0[X_1, \ldots, X_n]$ has a solution in $\mathcal{R}^n$. If no such algorithm exists, we will say that $\mathcal{R}$ is *undecidable* with coefficients in $\mathcal{R}_0$.

Remark. Technically speaking we do not really need $\mathcal{R}_0$ to be finitely generated, but finitely generated rings have many nice properties. For more general rings, we would have to be more careful with our definition of Hilbert's Tenth Problem and diophantine models. Furthermore, all undecidability results so far (except for $\mathcal{R} = \mathbb{Z}$) work by giving a model or interpretation of $\mathbb{Z}$ over $\mathcal{R}$; this involves finitely many polynomials and hence it suffices to adjoin their coefficients to the ring $\mathcal{R}_0$.

---

*The author is a Postdoctoral Fellow of the Research Foundation – Flanders (FWO).

In this paper, $\mathcal{R}$ will always be a field. Then we might as well take coefficients in the fraction field of $\mathcal{R}_0$. So we can take $\mathcal{R}_0$ to be a finitely generated field.

This paper shows undecidability (in the sense of Hilbert's Tenth Problem) for function fields over valued fields, where both the valued field and the residue field have characteristic zero, the value group is not 2-divisible and some condition on Galois cohomology is satisfied (see Main Theorem 2).

Our Main Theorem generalizes a result by Kim and Roush (see [KR92]), who showed that $\mathbb{C}(Z_1, Z_2)$ is undecidable (with coefficients in $\mathbb{Q}(Z_1, Z_2)$). Eisenträger extended this to function fields of varietes of dimension ≥ 2 over $\mathbb{C}$ (see [Eis04]).

There are already a lot of results on HTP for function fields: Denef proved undecidability for rational function fields over real fields (see [Den78]), Moret-Bailly generalized this to function fields of varieties over real fields (see [MB05]). Kim and Roush proved the undecidability for rational function fields over p-adic fields (subfields of $\mathbb{Q}_p$, including all number fields). This was generalized to function fields of varieties independently by Moret-Bailly (see [MB05]) and Eisenträger (see [Eis07]). In positive characteristic, Pheidas proved undecidability for $\mathbb{F}_q(Z)$ (see [Phe91]) with q odd, Videla did the same for q even (see [Vid94]). This was generalized to function fields over finite fields by Shlapentokh (see [Shl96]) and Eisenträger (see [Eis03]). One of the biggest open questions regarding function fields is $\mathbb{C}(Z)$.

For our result, we consider function fields of curves over valued fields with residue characteristic zero. So we cannot apply our result to $\mathbb{Q}_p(Z)$ for example. One important application of our result where HTP was not known before is the field $\mathbb{C}((T))(Z)$.

Acknowledgements. A large part of this article was written during a stay at the Scuola Normale Superiore di Pisa, funded by the Research Foundation – Flanders (FWO). I thank the University of Ghent, the FWO and the Scuola Normale Superiore for giving me this possibility. I thank Karim Becher for discussing with me about the Milnor conjectures. I also thank Laurent Moret-Bailly and Angelo Vistoli for some helpful discussions regarding algebraic geometry.

2 Preliminaries

Before we can state the Main Theorem (see Section 4 and Section 5), we need some definitions regarding diophantine sets, valuations and quadratic forms.

2.1 Diophantine sets and diophantine models

The most important definition in the study of Hilbert's Tenth Problem is that of a diophantine set:

Definition 2.1. Let $\mathcal{R}_0 \subseteq \mathcal{R}$ be rings. Let $\mathcal{S}$ be a subset of $\mathcal{R}^n$. Then $\mathcal{S}$ is called *diophantine* over $\mathcal{R}$ with coefficients in $\mathcal{R}_0$ if and only if there exists a polynomial $f \in \mathcal{R}_0[A_1, \dots, A_n, X_1, \dots, X_m]$ for some $m \geq 0$ such that

$$\mathcal{S} = \{(a_1, \dots, a_n) \in \mathcal{R}^n \mid f(a_1, \dots, a_n, x_1, \dots, x_m) = 0 \text{ for some } (x_1, \dots, x_m) \in \mathcal{R}^m\}.$$

Next, we need to define a diophantine model of one ring $\mathcal{S}$ over a ring $\mathcal{R}$. This is a way of encoding the ring $\mathcal{S}$ as elements of $\mathcal{R}$ in a diophantine way.

Definition 2.2. Let $\mathcal{S}_0 \subseteq \mathcal{S}$ and $\mathcal{R}_0 \subseteq \mathcal{R}$ be rings. A *diophantine model* of $\mathcal{S}$ with coefficients in $\mathcal{S}_0$ over $\mathcal{R}$ with coefficients in $\mathcal{R}_0$ is an injective map $\phi : \mathcal{S} \hookrightarrow \mathcal{R}^m$ for some $m \geq 1$ such that the following sets are diophantine with coefficients in $\mathcal{R}_0$:

1. The image $\phi(\mathcal{S}) \subseteq \mathcal{R}^m$.
2. The graph of addition $\{(\phi(x), \phi(y), \phi(x+y)) \mid x, y \in \mathcal{S}\} \subseteq \mathcal{R}^{3m}$.
3. The graph of multiplication $\{(\phi(x), \phi(y), \phi(xy)) \mid x, y \in \mathcal{S}\} \subseteq \mathcal{R}^{3m}$.
4. Every singleton $\{\phi(x_0)\}$ with $x_0 \in \mathcal{S}_0$.

The reason for this definition is the following reduction, which is usually applied with $\mathcal{S}_0 = \mathcal{S} = \mathbb{Z}$ (in this case, condition 4 above follows from the other conditions):

Proposition 2.3. *Let $\mathcal{S}_0 \subseteq \mathcal{S}$ and $\mathcal{R}_0 \subseteq \mathcal{R}$ be rings such that $\mathcal{S}_0$ and $\mathcal{R}_0$ are finitely generated $\mathbb{Z}$-algebras. If $\mathcal{S}$ is undecidable with coefficients in $\mathcal{S}_0$, then also $\mathcal{R}$ is undecidable with coefficients in $\mathcal{R}_0$.*

2.2 Valuations

In this section we give definitions and properties of (Krull) valuations. We refer to [End72] and [EP05].

Definition 2.4. An *ordered abelian group* Γ is an abelian group with a total order $\leq$ such that $a \leq b$ implies $a + c \leq b + c$ for all $a, b, c \in \Gamma$.

Definition 2.5. A *valuation* v on a field K is a surjective map $v : K^* \twoheadrightarrow \Gamma$, where Γ is an ordered abelian group, satisfying the following conditions:

1. For all $x, y \in K^*$, $v(xy) = v(x) + v(y)$.
2. For all $x, y \in K^*$ such that $x + y \neq 0$, $v(x+y) \geq \min(v(x), v(y))$.

Γ is called the *value group* of the valuation. Usually one defines $v(0) = \infty$, which is consistent with the above axioms if ∞ is treated as an element greater than any element from Γ.

Every field has a *trivial valuation* with value group $\{0\}$. Then $v(x) = 0$ for $x \in K^*$ and $v(0) = \infty$.

If $v : K^* \twoheadrightarrow \Gamma$ is a valuation, the *valuation ring* $\mathcal{O}$ is the ring consisting of all elements of K having non-negative valuation:

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\}.$$

In $\mathcal{O}$, the elements with strictly positive valuation form a *maximal ideal* $\mathfrak{m}$. The field $k := \mathcal{O}/\mathfrak{m}$ is called the *residue field* of K with respect to v. We have a natural surjection $\pi : \mathcal{O} \twoheadrightarrow k$. The set of elements of valuation zero form the *unit group* $\mathcal{O}^*$. These are exactly the invertible elements of $\mathcal{O}$.

Proposition 2.6. *Let K be a field with a valuation v such that K and its residue field have characteristic zero. Let L be a finite extension of K and let $v_1, \ldots, v_n$ denote all the extensions of v to L. Let e_i denote the respective ramification indices and f_i the residue extension degrees. Then $\sum_{i=1}^n e_i f_i = [L : K]$.*

Proof. This follows from Corollary (20.23) and the definition of defectless at the beginning of §18 in [End72]. □

Remark. In general, without the hypothesis of charactertic zero, we have only an inequality $\sum_{i=1}^n e_i f_i \leq [L : K]$. However, if the value group is $\mathbb{Z}$, then the equality holds anyway if L/K is seperable.

Definition 2.7. With notations as above, a valued field K is called *henselian* if and only if the following property (called *Hensel's Lemma*) holds:

For every $P \in \mathcal{O}[Z]$ and $\alpha \in k$ such that α is a simple root of $P \bmod \mathfrak{m}$, there exists a $\beta \in \pi^{-1}(\alpha) \subseteq \mathcal{O}$ such that $P(\beta) = 0$ (the simple root α in the reduction can be lifted to a global root β).

If K is a field with valuation v, the *henselisation* K^{H} is the smallest extension of K which is henselian. This always exists and is an algebraic extension of K (it is usually defined as the fixed field of a certain subgroup of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$). The henselisation is an immediate extension, i.e. the value group Γ and the residue field k remain the same. All this follows from [EP05, Section 5.2].

If K is a valued field with $\operatorname{char} K = \operatorname{char} k = 0$, then clearly $\mathbb{Q} \subseteq \mathcal{O}$. By Zorn's Lemma, there is a *maximal subfield* $F \subseteq \mathcal{O}$. Saying that F is contained in $\mathcal{O}$ is equivalent to saying that the valuation is trivial on F. As a consequence, the projection π restricted to F is an embedding: we can always see F as a subfield of the residue field k.

Proposition 2.8. *Let K be a valued field with notations as above. Assume that* $\operatorname{char} K = \operatorname{char} k = 0$ *and let F be a maximal subfield of $\mathcal{O}$. Then k is an algebraic extension of $\pi(F)$. Moreover, if the valuation is henselian, then $\pi(F) = k$.*

Proof. For the Henselian case, see [CK77, Lemma 5.4.13 (ii)]. In the non-Henselian case, the part of that proof which excludes transcendental extensions $k/\pi(F)$ still works.

□

Definition 2.9. Let Γ be an abelian group. For a prime $p \in \mathbb{N}$, we say that Γ is *p-divisible* if every $x \in \Gamma$ can be written as py, with $y \in \Gamma$. In other words, if $p\Gamma = \Gamma$. We call Γ *divisible* if it is p-divisible for every prime p.

Definition 2.10. Let Γ be an abelian group. An element $g \in \Gamma$ is called *even* if $g \in 2\Gamma$, otherwise g is called *odd*.

Clearly, odd elements exist if and only if Γ is not 2-divisible.

We end this section by introducing the *composition* of valuations (see [EP05, Section 2.3, p. 45]). We will only use this in the examples (Section 7).

Proposition 2.11. *Let K be a field with a valuation v and residue field k_v. Assume u is a valuation on k_v, with residue field k_u. Then there exists a valuation w on K, called the composition of v with u, with residue field $k_w \cong k_u$ and such that the value groups form an exact sequence*

$$0 \longrightarrow \Gamma_u \longrightarrow \Gamma_w \longrightarrow \Gamma_v \longrightarrow 0. \tag{1}$$

From this exact sequence one can easily show that Γ_w is p-divisible if and only if both Γ_u and Γ_v are p-divisible (using the fact that we are dealing with *ordered* abelian groups).

2.3 Quadratic forms

Definition 2.12. A *quadratic form* Q over a field K is a polynomial over K in any number of variables, which is homogeneous of degree two.

In the case that $\operatorname{char} K \neq 2$ (for us this will always be the case), we can do a linear variable transformation such that Q becomes of the form

$$Q(x_1, x_2, \ldots, x_n) = a_1x_1^2 + \cdots + a_nx_n^2 \qquad (a_i \in K).$$

We write this as $Q = \langle a_1, \ldots, a_n \rangle$.

We define two operators on quadratic forms: the *orthogonal sum* ($\perp$) and *tensor product* ($\otimes$). Let $Q_1 = \langle a_1, a_2, \ldots, a_n \rangle$ and $Q_2 = \langle b_1, b_2, \ldots, b_m \rangle$. Then

$$\begin{aligned} Q_1 \perp Q_2 &= \langle a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \rangle, \\ Q_1 \otimes Q_2 &= \langle a_1b_1, a_1b_2, \ldots, a_1b_m, a_2b_1, a_2b_2, \ldots, a_2b_m, \ldots, a_nb_1, a_nb_2, \ldots, a_nb_m \rangle. \end{aligned}$$

With these operators, the set of quadratic forms over K becomes a semiring.

A quadratic form $\langle a_1, \ldots, a_n \rangle$ is called *isotropic* over K if and only if there exist $x_1, \ldots, x_n \in K$, not all zero, such that $a_1x_1^2 + \cdots + a_nx_n^2 = 0$. Otherwise, the quadratic form is called *anisotropic*.

An important special class of quadratic forms are the *Pfister forms*. These are the quadratic forms which can be written as

$$\langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle \otimes \cdots \otimes \langle 1, a_n \rangle.$$

The following propoposition will be crucial to prove the Main Theorem. It gives a way to reduce isotropicity of quadratic forms from a valued field K to the residue field k, provided that the value group is not 2-divisible.

Proposition 2.13. *Let K be a field with a valuation $v : K^* \twoheadrightarrow \Gamma$, and let k be its residue field. Assume $\operatorname{char} k \neq 2$. Let $t \in K$ have odd valuation (i.e. $v(t) \notin 2\Gamma$). Consider two quadratic forms $Q_1 = \langle a_1, \dots, a_n\rangle$ and $Q_2 = \langle b_1, \dots, b_m\rangle$ over K, such that all a_i's and b_j's have valuation 0. If $Q_1 \perp (\langle t\rangle \otimes Q_2)$ is isotropic over K, then either Q_1 or Q_2 is isotropic over the residue field k.*

Proof. Assume $a_1x_1^2 + \cdots + a_nx_n^2 + tb_1y_1^2 + \cdots + tb_my_m^2 = 0$. Consider an element from $\{x_1^2, \dots, x_n^2, ty_1^2, \dots, ty_m^2\}$ with minimal valuation. If x_i^2 has minimal valuation, then $a_1(x_1/x_i)^2 + \cdots + a_n(x_n/x_i)^2$ will be zero in the residue field. If ty_i^2 has minimal valuation, then $b_1(y_1/y_i)^2 + \cdots + b_n(y_m/y_i)^2$ will be zero in the residue field. □

If $Q_1 = Q_2$, we can formulate the proposition as follows:

Corollary 2.14. *Let K be a field with a valuation $v : K^* \twoheadrightarrow \Gamma$, and let k be its residue field. Assume $\operatorname{char} k \neq 2$. Let $t \in K$ have odd valuation. Consider a quadratic form $Q = \langle a_1, \dots, a_n\rangle$ over K, such that all a_i's have valuation 0. If $\langle 1, t\rangle \otimes Q$ is isotropic over K, then Q is isotropic over the residue field k.*

The converse of this proposition and corollary hold for henselian fields: if K is henselian, and either Q_1 or Q_2 is isotropic over the residue field, then $Q_1 \perp (\langle t\rangle \otimes Q_2)$ is isotropic over K.

3 Elliptic curves over function fields

Consider an elliptic curve E defined over a field K of characteristic zero. Such a curve can be defined by an affine equation of the form $Y^2 = f(X) = X^3 + a_2X^2 + a_4X + a_6$, where $f(X)$ has only simple zeros. There is exactly one point at infinity, which will be denoted by $\mathbf{0}$. The set of points $E(K)$ forms an abelian group with $\mathbf{0}$ as the neutral element.

3.1 Denef's method

Consider the rational function field $K(Z)$. Over $K(Z)$ we can define the following quadratic twist of E (sometimes called the *Manin–Denef curve*):

$$\mathcal{E} : f(Z)Y^2 = f(X). \tag{2}$$

Consider a point $(X, Y) \in \mathcal{E}(K(Z))$. We claim that such a point can be seen as a morphism from E to itself (morphism as a curve, $\mathbf{0}$ does not have to be mapped to $\mathbf{0}$). Define the action of $(X, Y) \in \mathcal{E}(K(Z))$ as follows:

$$\begin{aligned} &E(K) \to E(K) \\ &(x, y) \mapsto (X(x), Y(x)y). \end{aligned} \tag{3}$$

One can easily check that this is a well-defined morphism on $E(K)$. The identity is given by $(Z,1)$, and we denote its multiples $n \cdot (Z,1)$ by $(\mathrm{X}_n, \mathrm{Y}_n) \in \mathcal{E}(K(Z))$. This determines rational functions $\mathrm{X}_n, \mathrm{Y}_n \in K(Z)$, which obviously depend on the elliptic curve E.

The curve $\mathcal{E}$ was first used by Denef to prove existential undecidability for $\mathbb{R}(Z)$. The proof is based on the following theorem (see [Den78, Lemma 3.1]), where $\mathrm{End}_K(E)$ stands for the group of endomorphisms of E defined over K and $E[2](K)$ stands for the group of K-rational points on E having order dividing 2.

Theorem 3.1 (Denef)**.** *The group* $\mathcal{E}(K(Z))$ *is isomorphic to* $\mathrm{End}_K(E) \oplus E[2](K)$*. Under this isomorphism, the action* (3) *translates to an action of* $(\phi, T) \in \mathrm{End}_K(E) \oplus E[2](K)$ *on* E *by mapping* P *to* $\phi(P) + T$*.*

In our applications, we will take a curve without complex multiplication (i.e. $\mathrm{End}(E) \cong \mathbb{Z}$). Then $\mathcal{E}(K(Z)) \cong \mathbb{Z} \oplus E[2](K)$, hence $2 \cdot \mathcal{E}(K(Z)) \cong \mathbb{Z}$. This is how we will make our diophantine model of $\mathbb{Z}$ over $K(Z)$.

It turns out that we can easily describe the functions X_n and Y_n locally at Z^{-1}:

Proposition 3.2. *Let* $n \in \mathbb{Z} \setminus \{0\}$*. In the completion* $K((Z^{-1}))$*, the functions* X_n *and* Y_n *satisfy:*

$$\mathrm{X}_n(Z) = \frac{1}{n^2} Z + O(Z^0) \quad \text{and} \quad \mathrm{Y}_n(Z) = \frac{1}{n^3} + O(Z^{-1}).$$

(the notation $f(Z) = g(Z) + O(Z^{-n})$ *means* $v_{Z^{-1}}(f-g) \geq n$*.)*

Proof. Apply the following coordinate transformation on $\mathcal{E}$: $X = (f(Z)/Z^2)X'$ and $Y = (f(Z)/Z^3)Y'$. Using $f(X) = X^3 + a_2X^2 + a_4X + a_6$, we get

$$\mathcal{E}' : Y'^2 = X'^3 + a_2 \frac{Z^2}{f(Z)} X'^2 + a_4 \frac{Z^4}{f(Z)^2} X' + a_6 \frac{Z^6}{f(Z)^3} \tag{4}$$

Since f has degree 3, the coefficients of X'^2, X' and 1 in this equation have positive valuation at Z^{-1}.

Let P_1' be the point $(Z^3/f(Z), Z^3/f(Z))$ on $\mathcal{E}'$, this corresponds to $(Z,1)$ on $\mathcal{E}$. Let $P_n' := n \cdot P_1'$. Since $f(Z) = Z^3 + O(Z^2)$, we have to show that $P_n' := (1/n^2 + O(Z^{-1}), 1/n^3 + O(Z^{-1}))$.

It suffices to look at the reduction of $\mathcal{E}'$ modulo Z^{-1}. The reduction $\overline{\mathcal{E}'}$ is the cusp $\overline{Y'}^2 = \overline{X'}^3$. The group law on the set of non-singular points of $\overline{\mathcal{E}'}(K)$ is isomorphic to the additive group $K, +$ by the following correspondence (see [Sil86, III.2.5]):

$$\begin{aligned} \overline{\mathcal{E}'}(K) \setminus \{(0,0)\} &\to K, + \\ (X', Y') &\mapsto X'/Y' \end{aligned}$$

Using this, we get $\overline{P_n'} = n \cdot \overline{P_1'} = n \cdot (1,1) = (1/n^2, 1/n^3)$; hence $P_n' = (n^2 + O(Z^{-1}), 1/n^3 + O(Z^{-1}))$. □

3.2 Moret-Bailly's method

In [MB05], Moret-Bailly generalized Denef's method to make it work for function fields of curves (and then automatically also higher-dimensional varieties), as opposed to rational function fields. The idea is to take an embedding of $K(Z)$ into the function field $K(C)$ of a curve such that $\mathcal{E}(K(Z)) = \mathcal{E}(K(C))$.

In the theorem below, we will slightly generalize the main theorem by Moret-Bailly. This section assumes some familiarity with the paper [MB05]. However, the results are not needed for rational function fields.

We use the definition of *admissible function* from [MB05, Definition 1.5.2]. In that definition, there is set Q of closed points on C. This set does not matter for us, we can simply take any zero of the admissible function if necessary. Furthermore, we will always take $\Gamma = E$ (we will however vary the map $\pi : \Gamma \to \mathbb{P}^1$).

For our purposes, we can define an admissible function as follows:

Definition 3.3. Let C be a smooth projective geometrically connected curve over a field K of characteristic zero. Let E be an elliptic curve over K and $\pi : E \to \mathbb{P}^1$ a double cover. A function $g : C \to \mathbb{P}^1$ is called *admissible* for π if

(0) $\pi : E \to \mathbb{P}^1$ is étale above ∞ and ramified above 0 (see [MB05, 1.4.4]).

(i) g has no ramification index ≥ 3 (the ramification is simple).

(ii) g is étale above ∞ and the branch points of π.

Theorem 3.4. *Let K be a field of characteristic zero and E an elliptic curve $Y^2 = f(X)$ where $f(X) \in K[X]$ of degree 3. Assume that E has no complex multiplication. Let C be a smooth projective geometrically connected curve defined over K. Let $g : C \to \mathbb{P}^1$ be an admissible function for some $\pi : E \to \mathbb{P}^1$. Let $\bar{K}$ denote the algebraic closure of K.*

Let $\mathcal{S}$ be a finite set of tuples $(\alpha, \beta, \gamma, \delta, \varepsilon) \in K^5$ such that $f(\alpha) \neq 0$ and $\beta\varepsilon - \gamma\delta \neq 0$. Then there exist infinitely many $\lambda \in \mathbb{Q}$ such that for every $(\alpha, \beta, \gamma, \delta, \varepsilon) \in \mathcal{S}$ the set of $\bar{K}(C)$-points of the elliptic curve $f(\alpha + (\beta\lambda + \gamma)(\delta\lambda + \varepsilon)^{-1}g^{-1})Y^2 = f(X)$ is exactly

$$\mathbb{Z} \cdot \left(\alpha + \frac{\beta\lambda + \gamma}{(\delta\lambda + \varepsilon)g}, 1\right) \oplus E[2](\bar{K})$$

(the $\cdot$ denotes multiplication by an integer on the elliptic curve).

Proof. We need to adapt the method of Moret-Bailly to account for two things: first of all, we need several good functions (one for every element of $\mathcal{S}$). This works because intersections of Hilbert sets are still Hilbert sets. Second, we need to some kind of coordinate change $g^{-1} \leftrightarrow \alpha + (\beta\lambda + \gamma)(\delta\lambda + \varepsilon)^{-1}g^{-1}$.

For every $(\alpha, \beta, \gamma, \delta, \varepsilon) \in \mathcal{S}$, let π_α be the double cover

$$\begin{aligned} \pi_\alpha : \qquad & E \to \mathbb{P}^1 : \\ & (X, Y) \mapsto 1/(X - \alpha). \end{aligned}$$

Note that $\pi_\alpha^{-1}(0)$ is the point $\mathbf{0}$ on E and that $\pi_\alpha^{-1}(\infty)$ are the points on E with X-coordinate α. By assumption, these latter points are not 2-torsion. Hence, π_α is étale over ∞ and ramified over 0.

Let $\mathcal{B}$ be the union of all the branch points of these π_α, excluding 0. By assumption, g is admissible for some $\pi : E \longrightarrow \mathbb{P}^1$, therefore $g : C \to \mathbb{P}^1$ is étale above an open subset of $\mathbb{P}^1$, which includes 0 (a branch point of π) and ∞. It follows that, for almost all $\kappa \in K^*$, the function κg is étale above all points of $\mathcal{B}$. Choose such an $\kappa \in \mathbb{Q}^*$. Then $h := \kappa g$ is admissible for every given π_α (note that g and h are equal above 0 and ∞).

Now fix $(\alpha, \beta, \gamma, \delta, \varepsilon) \in \mathcal{S}$. Define the following elliptic curves, depending an a ξ which is an element of some extension of K.

$$\mathcal{E}_{\alpha,\xi} : f(\alpha + 1/\xi)Y^2 = f(X). \tag{5}$$

If we would strictly follow [MB05, 1.4.6], then we would have the equation $Y^2 = \xi^4 f(\alpha + 1/\xi)f(X)$. However, the equation (5) can be obtained by a coordinate change for the Y variable.

Write $K(Z)$ for the rational function field over K. Note that $K(\alpha + 1/Z) = K(Z)$. Because E does not have complex multiplication, Theorem 3.1 says that

$$\mathcal{E}_{\alpha,Z}(\bar{K}(Z)) = \mathbb{Z} \cdot (\alpha + 1/Z, 1) \oplus E[2](\bar{K}). \tag{6}$$

But we want to work over $\bar{K}(C)$ instead of $\bar{K}(Z)$. The function $h = \kappa g$ is admissible for π_α, so we can apply [MB05, Theorem 1.8]. Let K_0 be the field generated over $\mathbb{Q}$ by all the coefficients of elements of $\mathcal{S}$. There exists a Hilbert subset $\mathcal{H}_\alpha \subseteq K_0$ such that for all $\mu \in \mathcal{H}_\alpha$, we have

$$\begin{gathered} \mathcal{E}_{\alpha,Z}(\bar{K}(Z)) \cong \mathcal{E}_{\alpha,\mu h}(\bar{K}(C)) \\ Z \mapsto \mu h = \kappa\mu g. \end{gathered} \tag{7}$$

(see [FJ86, Section 11.1] for the definition of Hilbert sets, intuitively a Hilbert set contains 'most' elements of K_0). Note that we always have an embedding $\mathcal{E}_{\alpha,Z}(\bar{K}(Z)) \hookrightarrow \mathcal{E}_{\alpha,\mu h}(\bar{K}(C))$, but in general this is not surjective.

For $(\alpha, \beta, \gamma, \delta, \varepsilon) \in \mathcal{S}$, define $\mathcal{H}'_{(\alpha,\beta,\gamma,\delta,\varepsilon)}$ to be the set of all $\lambda \in K_0$ such that

$$\frac{\beta\lambda + \gamma}{\delta\lambda + \varepsilon} = \frac{1}{\kappa\mu} \text{ for some } \mu \in \mathcal{H}_\alpha. \tag{8}$$

Since $K_0((\beta Z + \gamma)/(\delta Z + \varepsilon)) = K_0(1/(\kappa Z))$, if follows from the definition of Hilbert sets that $\mathcal{H}'_{(\alpha,\beta,\gamma,\delta,\varepsilon)}$ is a Hilbert subset of K_0. Let $\mathcal{H}'$ be the intersection of all these $\mathcal{H}'_{(\alpha,\beta,\gamma,\delta,\varepsilon)}$. Since an intersection of finitely many Hilbert sets is still a Hilbert set and K_0 is finitely generated over the Hilbertian field $\mathbb{Q}$, it follows that $\mathcal{H}' \cap \mathbb{Q}$ is infinite. Now the result follows for all $\lambda \in \mathcal{H}'$ by putting together (6), (7) and (8). $\square$

4 First version of the Main Theorem

This whole section is devoted to the proof of the following theorem:

Main Theorem 1. *Let K be a field of characteristic zero with a valuation $v : K^* \twoheadrightarrow \Gamma$. Let $\mathcal{O}$ denote the valuation ring and k the residue field.*

Assume the following conditions are satisfied:

(i) The characteristic of the residue field k is zero.

(ii) The value group Γ is not 2-divisible.

(iii) Let F be a maximal field contained in $\mathcal{O}$. There is an integer $q \geq 0$ such that there exists a 2^q-dimensional Pfister form with coefficients in F which is anisotropic over k and such that every 2^{q+2}-dimensional Pfister form over a finite extension of $F(Z)$ is isotropic.

Let C be a smooth projective geometrically connected curve defined over K with a K-rational point and let $K(C)$ be its function field. Then $K(C)$ is undecidable with coefficients in some finitely generated subfield $\mathcal{L}_0$ of $K(C)$.

Remark. As Eisenträger notes in the introduction of [Eis07], this undecidability can be "trivial" in some cases, simply because of certain elements appearing in $\mathcal{L}_0$. For example, consider Tarski's proof that the theory of $\mathbb{R}$ in the language $\{0, 1, +, \cdot, \leq\}$ admits quantifier elimination (see [Tar51]). This immediately implies decidability for first-order sentences (in particular, diophantine equations). However, if we add some non-computable real α to the language, we still have quantifier elimination, but then atomic formulas (such as $2\alpha^3 - \alpha + 4 \geq 0$) are no longer decidable. This shows that undecidability can sometimes be a simple consequence of the language.

However, for a general field K, it is not at all clear what the natural language (or the corresponding field $\mathcal{L}_0$) should be. In Section 6, we will discuss the coefficient field $\mathcal{L}_0$. In the concrete examples in Section 7, we will see that this field $\mathcal{L}_0$ is the natural one which one would expect.

To prove the Main Theorem, we will construct a diophantine model of $\mathbb{Z}$ over $K(C)$. We do this using *two* elliptic curves, as in the proof of the undecidability of $\mathbb{C}(T, Z)$ by Kim and Roush ([KR92]) and of surfaces over $\mathbb{C}$ by Eisenträger ([Eis04]). The main problem however is that K might be much bigger than $F(T)$; it could be that there is no rank one elliptic curve over K.

Take an element $T \in K$ such that $v(T)$ is positive and odd (this is possible because of condition (ii)). We will identify $\mathbb{Z}$ with a subgroup of Γ by sending 1 to $v(T)$. An ordered abelian group is always torsion-free, so the map $\mathbb{Z} \hookrightarrow \Gamma : n \mapsto nv(T)$ is an embedding of ordered abelian groups.

4.1 The elliptic curve

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Choose an equation $Y^2 = f(X) = X^3 + a_2X^2 + a_4X + a_6$ for E with $a_2, a_4, a_6 \in \mathbb{Q}$ and $a_6 \neq 0$. Let $\pi : E \to \mathbb{P}^1 : (X,Y) \mapsto X^{-1}$. Since C was assumed to have a K-rational point, it follows from [MB05, 2.3.3] that there exists a function $g : C \to \mathbb{P}^1$ of odd degree which is admissible for π. Define Z to be g^{-1}. In what follows, we will see Z as an element of the function field $K(C)$. Then $K(C)$ is a finite extension of odd degree of the rational function field $K(Z)$.

Apply Theorem 3.4 with $\mathcal{S} = \{(0,1,T^{-2},0,1),(T^{-2},1,0,0,1)\}$ and let $\lambda \in \mathbb{Q}^*$ be such that the conclusion of that theorem holds. Define

$$A := (T^{-2} + \lambda)Z \quad \text{and} \quad B := T^{-2} + \lambda Z.$$

In the case of a rational function field, we can take $K(Z) = K(C)$ and then any $\lambda \in \mathbb{Q}^*$ works.

Define $L := K(C)(\sqrt{f(A)}, \sqrt{f(B)})$, which is a degree 4 extension of $K(C)$ (see Lemma 4.1 below). We assume that T and Z are in the field of coefficients $\mathcal{L}_0$. Both A and B are elements of $\mathbb{Q}(T,Z)$ and f has coefficients in $\mathbb{Q}$, therefore $f(A)$ and $f(B)$ are diophantine and we can make a diophantine model of L in $K(C)^4$.

Consider the following points on $E(L)$:

$$P_1 := (A, \sqrt{f(A)}) \quad \text{and} \quad P_2 := (B, \sqrt{f(B)})$$

Lemma 4.1. *The points P_1 and P_2 satisfy the following properties:*

1. *Let $\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$. The sets of multiples $\mathbb{Z}_0 \cdot P_1$ and $\mathbb{Z}_0 \cdot P_2$ are diophantine over L (as subsets of $\mathbb{A}^2(L) \cong L^2$).*
2. *P_1 and P_2 are independent points on $E(L)$.*
3. *Let $\bar{K}$ be the algebraic closure of K. Then the field $\bar{K}(C)(\sqrt{f(A)}, \sqrt{f(B)})$ is a degree 4 extension of $\bar{K}(C)$.*

Proof. Let $\mathcal{E}_A$ be the elliptic curve $f(A)Y^2 = f(X)$ and $\mathcal{E}_B$ be the elliptic curve $f(B)Y^2 = f(X)$, both defined over $K(C)$. According to Theorem 3.4, we have $\mathcal{E}_A(K(C)) = \mathbb{Z} \cdot (A,1) \oplus E[2](K)$ and $\mathcal{E}_B(K(C)) = \mathbb{Z} \cdot (B,1) \oplus E[2](K)$.

The set of multiples of $(A,1)$ on $\mathcal{E}_A(K(C))$ is diophantine because it can be written as

$$\{2 \cdot \mathcal{E}_A(K(C))\} \cup \{(A,1) + 2 \cdot \mathcal{E}_A(K(C))\}.$$

Since the $K(C)$-rational points of $\mathcal{E}_A$ are simply given by the elliptic curve equation, the above set is diophantine. We will use the affine equation, so we cannot get the point at infinity, we only get $\mathbb{Z}_0 \cdot (A,1)$. The coefficients of the equation for $\mathcal{E}_A$ lie in $\mathbb{Q}(T,Z)$, so we just need T and Z in $\mathcal{L}_0$ to make the diophantine definition.

Over $L = K(C)(\sqrt{f(A)}, \sqrt{f(B)})$, the curves $\mathcal{E}_A$ and E become isomorphic:

$$\begin{aligned} \theta : \mathcal{E}_A(L) &\xrightarrow{\sim} E(L) \\ (X, Y) &\mapsto (X, Y\sqrt{f(A)}). \end{aligned} \tag{9}$$

Now we can diophantinely define the set of non-zero multiples of $P_1 = (A, \sqrt{f(A)})$ on $E(L)$ by taking the multiples of $(A, 1)$ on $\mathcal{E}_A(L)$ and simply multiplying the y-coordinate by $\sqrt{f(A)}$. Analogously, the set $\mathbb{Z}_0 \cdot P_2$ is diophantine, which finishes the first point of the lemma.

To prove 2, first of all note that both P_1 and P_2 have infinite order in $E(L)$ because of Theorem 3.1. Assume we would have a relation $mP_1 = nP_2$ with $m \neq 0$ and $n \neq 0$. Since the x-coordinate of P_1 is A, it follows from Section 3.1 that the x-coordinate of mP_1 equals $\mathrm{X}_m(A)$. Similarly, the x-coordinate of nP_2 is $\mathrm{X}_n(B)$. So, we have $\mathrm{X}_m((T^{-2} + \lambda)Z) = \mathrm{X}_n(T^{-2} + \lambda Z)$. If we specialize the variable Z to T^{-1}, we get $\mathrm{X}_m(T^{-3} + \lambda T^{-1}) = \mathrm{X}_n(T^{-2} + \lambda T^{-1})$. But it follows from Proposition 3.2 that $v(\mathrm{X}_m(T^{-3} + \lambda T^{-1})) = -3$ and $v(\mathrm{X}_n(T^{-2} + \lambda T^{-1})) = -2$. This is a contradiction.

Finally, let us prove point 3. Assume that $\sqrt{f(A)}$ is in $\bar{K}(C)$. Then the isomorphism θ in (9) would be defined over $K(C)$. Since $E(\bar{K})$ contains n-torsion points for every n, $\mathcal{E}_A(\bar{K}(C))$ would also contain n-torsion points for every n. But by our construction, $\mathcal{E}_A(\bar{K}(C))$ has only 2-torsion points and points of infinite order. Therefore, $[\bar{K}(C)(\sqrt{f(A)}) : \bar{K}(C)] = 2$.

Now assume that $\sqrt{f(B)} \in \bar{K}(C)(\sqrt{f(A)})$. Then we can write $\sqrt{f(B)} = R + S\sqrt{f(A)}$ with R and S in $\bar{K}(C)$. Squared, we get

$$f(B) = R^2 + S^2 f(A) + 2RS\sqrt{f(A)} \in \bar{K}(C).$$

But $\sqrt{f(A)}$ does not lie in $\bar{K}(C)$, so we have two possibilities: either $R = 0$ or $S = 0$. If $S = 0$, then $\sqrt{f(B)} \in \bar{K}(C)$, which we can exclude as in the previous paragraph.

If $R = 0$, then $\sqrt{f(B)}$ is a $\bar{K}(C)$-multiple of $\sqrt{f(A)}$. Then $(B, \sqrt{f(B)}/\sqrt{f(A)})$ would be a point on $\mathcal{E}_A(\bar{K}(C))$. This means that 2 times this point is a multiple of $(A, 1)$. Applying the isomorphism θ, we find that $2 \cdot P_2$ is a multiple of P_1, in contradiction with the independence of P_1 and P_2. □

We have to make a technical remark about the point at infinity on the elliptic curve. We just defined $\mathbb{Z}_0 \cdot P_i$, the affine multiples of P_i. Instead of using coordinates (X, Y) in $\mathbb{A}^2$, we can use coordinates $(X, Y, 1)$ in $\mathbb{P}^2$. Then we can use coordinates $(0, 1, 0)$ for the point at infinity.

4.2 The model of $\mathbb{Z} \times \mathbb{Z}$

Consider the set $\mathbb{Z} \times \mathbb{Z}$ with the natural addition $(a, b) + (c, d) = (a + c, b + d)$. Define a binary relation $\mid$ on $\mathbb{Z} \times \mathbb{Z}$ which satisfies

$$a \text{ odd } \wedge \ b = 1 \implies \Big((a, b) \mid (c, d) \leftrightarrow (\exists r \in \mathbb{Z})\big((c, d) = (ra, rb)\big)\Big). \tag{10}$$

The truth of $(a,b) \mid (c,d)$ with a even or with $b \neq 1$ does not matter, we can define $\mid$ as we wish for such arguments. Note also that the existence of an r such that $(c,d) = (ra, r)$ is equivalent to $c = ad$.

If we embed $\mathbb{Z}$ into $\mathbb{Z} \times \mathbb{Z}$ by mapping n to $(n, 0)$, then we can existentially define the addition and multiplication on the image of $\mathbb{Z}$ in terms of the relations $+$ and $\mid$ on $\mathbb{Z} \times \mathbb{Z}$. For the addition, this is obvious since $a + b = c$ is equivalent to $(a,0) + (b,0) = (c,0)$. For the multiplication, we have:

Proposition 4.2. *Let $a, b, c \in \mathbb{Z}$. Then $ab = c$ if and only if there exists an $X \in \mathbb{Z} \times \mathbb{Z}$ such that the following relations are satisfied:*

$$(1,1) \mid X \tag{11}$$

$$(-1,1) \mid (X - 2(b,0)) \tag{12}$$

$$(2(a,0) + (1,1)) \mid (X + 2(c,0)) \tag{13}$$

Proof. First of all, note that these 3 relations all satisfy the left hand side of (10). If $ab = c$, then we can take $X = (b,b)$. Conversely, if the relations are satisfied, then X must be of the form (x,x) by (11). Now (12) says that $(-1,1) \mid (x - 2b, x)$. This implies that $b = x$. Using $X = (b,b)$, equation (13) becomes $(2a+1, 1) \mid (b + 2c, b)$ which implies $b + 2c = (2a+1)b$, hence $c = ab$. $\square$

We will apply this as follows: as shown in section 4.1, we can diophantinely define the sets $\mathbb{Z} \cdot P_1$ and $\mathbb{Z} \cdot P_2$, hence also $\mathbb{Z} \cdot P_1 + \mathbb{Z} \cdot P_2$ inside $E(L) \subseteq \mathbb{P}^2(L)$.

We identify $\mathbb{Z} \cdot P_1 + \mathbb{Z} \cdot P_2$ with $\mathbb{Z} \times \mathbb{Z}$ via $aP_1 + bP_2 \longleftrightarrow (a,b) \in \mathbb{Z} \times \mathbb{Z}$. Then the addition on $\mathbb{Z} \times \mathbb{Z}$ corresponds to addition on the elliptic curve, so it is diophantine. In section 4.3 we will show that also the relation $\mid$ is diophantine. This would show that the map $\mathbb{Z} \to E(L) : n \mapsto nP_1$ is a diophantine model of $\mathbb{Z}$. By Proposition 2.3, Main Theorem 1 would follow.

4.3 The quadratic form

The following theorem shows that the relation $\mid$ (see (10)) on $\mathbb{Z} \cdot P_1 + \mathbb{Z} \cdot P_2 \cong \mathbb{Z} \times \mathbb{Z}$ is diophantine.

Theorem 4.3. *Let Q be a 2^q-dimensional anisotropic Pfister form over k with coefficients in F, which exists by assumption. Let $m, n, r \in \mathbb{Z}$ with m odd. Then $n = mr$ if and only if $nP_1 + rP_2 = \mathbf{0}$ or*

$$\langle 1, y(mP_1 + P_2) \rangle \otimes \langle 1, y(nP_1 + rP_2) \rangle \otimes Q \tag{14}$$

is isotropic over L. ($y(P)$ stands for the y-coordinate of the point P.)

Remark. A quadratic form being isotropic is a diophantine condition if all the coefficients are diophantine. Therefore, the coefficients of Q must be elements of the field of coefficients $\mathcal{L}_0$.

Proof. The statement clearly holds if $n = r = 0$. For the rest of the proof, we assume this is not the case.

Assume $n = mr$ and set $P_3 := mP_1 + P_2$. Now (14) becomes

$$\langle 1, y(P_3)\rangle \otimes \langle 1, y(rP_3)\rangle \otimes Q. \tag{15}$$

Since $y(rP_3) = \mathrm{Y}_r(x(P_3))y(P_3)$, the coefficients of this quadratic form live in $L_0 := F(x(P_3), y(P_3))$. This field is isomorphic to the function field of E over F, so we can use condition (iii) from Main Theorem 1. The Pfister form (15) is 2^{q+2}-dimensional, therefore it is isotropic over $L_0 \subseteq L$.

Conversely, assume that (14) is isotropic over L. Let $s := n - mr$ and suppose that $s \neq 0$ in order to find a contradiction. Putting $P_3 := mP_1 + P_2$, we rewrite (14) as

$$\langle 1, y(P_3)\rangle \otimes \langle 1, y(sP_1 + rP_3)\rangle \otimes Q. \tag{16}$$

For the rest of this proof, we take the henselisation K^{H} as a base field, instead of K. Take any extension of the valuation v to K^{H}. By abuse of notation, we will still write v for this valuation. This extension is immediate, which means that the value group Γ and the residue field k remain the same. The henselisation is an algebraic extension, and K is relatively algebraically closed in L (because $K(C)$ is a function field over C and because of Lemma 4.1, item 3). Define

$$M := L \otimes_K K^{\mathrm{H}} = K^{\mathrm{H}}(C)(\sqrt{f(A)}, \sqrt{f(B)}).$$

Since (16) is isotropic over L, it is certainly isotropic over M. We just need the field M for this proof, we certainly do not need a diophantine model of M.

Recall that m is odd, in particular m is non-zero. The points mP_1 and P_2 have the following coordinates:

$$mP_1 = \big(\mathrm{X}_m(A), \mathrm{Y}_m(A)\sqrt{f(A)}\big), \tag{17}$$

$$P_2 = (B, \sqrt{f(B)}). \tag{18}$$

Consider $H(Z) := \mathrm{X}_m(A) - B \in K^{\mathrm{H}}(Z)$, we want to find a simple zero $\gamma \in K^{\mathrm{H}}$ of this rational function. Write the rational function $\mathrm{X}_m(\xi) \in \mathbb{Q}(\xi)$ as $R_m(\xi)/S_m(\xi)$ with $R_m(\xi), S_m(\xi) \in \mathbb{Q}[\xi]$. By Proposition 3.2, we can choose these such that R_m has leading term ξ^d and S_m has leading term $m^2\xi^{d-1}$ for some d. Keeping in mind that $A = (T^{-2}+\lambda)Z$ and $B = T^{-2} + \lambda Z$ with $\lambda \in \mathbb{Q}^*$, the following is a polynomial in the variable Z with coefficients in $\mathbb{Q}[T] \subseteq \mathcal{O}$:

$$G(Z) := T^{2d}S_m(A)H(Z) = T^{2d}R_m(A) - T^{2d}S_m(A)B. \tag{19}$$

We would like to apply Hensel's Lemma to find a root of $G(Z)$ in K^{H}. Modulo $\mathfrak{m}_v$ (the maximal ideal in $\mathcal{O}$ containing T), we have

$$\begin{aligned} G(Z) &\equiv (T^2A)^d - m^2(T^2A)^{d-1}(T^2B) \mod \mathfrak{m}_v \\ &\equiv Z^d - m^2Z^{d-1} \mod \mathfrak{m}_v. \end{aligned}$$

$$\begin{tikzcd}
& M = K^{\mathrm{H}}(C)(\sqrt{f(A)}, \sqrt{f(B)}) \arrow[dl, dash] \arrow[d, dash, "4"] \arrow[dr, dashed, "w"] & & \\
L = K(C)(\sqrt{f(A)}, \sqrt{f(B)}) \arrow[d, dash, "4"] & K^{\mathrm{H}}(C) \arrow[dl, dash] \arrow[r, dashed, "w"] \arrow[d, dash, "(\text{odd})"] & K^{\mathrm{H}\prime} \arrow[r, dashed, "v"] \arrow[d, dash, "f_w\ (\text{odd})"'] & k' \arrow[dd, dash, "f_v\ (\text{odd})"] \\
K(C) \arrow[d, dash, "(\text{odd})"] & K^{\mathrm{H}}(Z) \arrow[dl, dash] \arrow[r, dashed, "w"] & K^{\mathrm{H}} \arrow[d, dash] \arrow[dr, dashed, "v"] & \\
K(Z) & & K \arrow[r, dashed, "v"] & k
\end{tikzcd}$$

The various fields appearing in the proof of Theorem 4.3. A dashed arrow points from a valued field to its residue field, labeled by the valuation.

This equation has a simple zero $m^2 \mod \mathfrak{m}_v$, therefore Hensel's Lemma shows that $G(Z)$ has a simple root $\gamma \in K^{\mathrm{H}}$ with $\gamma \equiv m^2 \mod \mathfrak{m}_v$.

In order for γ to be a zero of the rational function $H(Z) = T^{-2d}G(Z)/S_m(A)$, it must not be a zero of $S_m(A) = S_m((T^{-2} + \lambda)Z)$. But S_m has coefficients in $\mathbb{Q}$, so the zeros of $S_m((T^{-2} + \lambda)Z)$ are of the form $\alpha/(T^{-2} + \lambda)$ with α algebraic over $\mathbb{Q}$. Since γ has valuation zero, it is clearly not of this form.

Define w as the discrete valuation on $K^{\mathrm{H}}(Z)$ at the point $Z = \gamma$. This means that $w(Z - \gamma) = 1$ and that w is trivial on K^{H}. Clearly, the residue field is K^{H}. We found γ as a simple zero of $H(Z) = \mathrm{X}_m(A) - B$, therefore

$$w(\mathrm{X}_m(A) - B) = 1. \tag{20}$$

We defined w as a valuation on $K^{\mathrm{H}}(Z)$, but we would like to extend w to the finite extension $M = K^{\mathrm{H}}(C)(\sqrt{f(A)}, \sqrt{f(B)})$. We use the notation $\tilde{x}$ for the reduction of x with respect to w, this gives a map $K^{\mathrm{H}}[Z]_{(Z-\gamma)} \to K^{\mathrm{H}}$. As we extend w to a finite extension, we keep the same notation.

Since $[K^{\mathrm{H}}(C) : K^{\mathrm{H}}(Z)]$ is odd, it follows from Proposition 2.6 that we can extend w to $K^{\mathrm{H}}(C)$ in such a way that both the ramification index e_w and the residue extension degree f_w are odd. Choose such an extension and write $K^{\mathrm{H}\prime}$ for the residue field of this extended valuation. The new value group is generated by $1/e_w$, we do not renormalize. Since algebraic extensions of henselian fields are again henselian (see [EP05, Section 4.1]), $K^{\mathrm{H}\prime}$ is also henselian (for the extension of v to $K^{\mathrm{H}\prime}$).

Now we still have to adjoin $\sqrt{f(A)}$ and $\sqrt{f(B)}$ to $K^{\mathrm{H}}(C)$. Note that $\tilde{A} = (T^{-2} + \lambda)\gamma$ and $\tilde{B} = T^{-2} + \lambda\gamma$ with $\lambda \in \mathbb{Q}^*$ and $\gamma \equiv m^2 \mod \mathfrak{m}_v$. It follows that $T^6 f(\tilde{A}) \equiv m^6 \mod \mathfrak{m}_v$ and $T^6 f(\tilde{B}) \equiv 1 \mod \mathfrak{m}_v$. Hensel's Lemma implies that $f(\tilde{A})$ and $f(\tilde{B})$ are squares in $K^{\mathrm{H}\prime}$. After extending w to $M = K^{\mathrm{H}}(C)(\sqrt{f(A)}, \sqrt{f(B)})$, the residue field remains $K^{\mathrm{H}\prime}$ and w does not ramify in this extension $M/K^{\mathrm{H}}(C)$.

Equation (20) implies that $m\tilde{P_1}$ and $\tilde{P_2}$ have the same x-coordinate (an element of K^{H}). This means that there are 2 possibilities: either they are the same point (equal

y-coordinates), or they are opposite points (opposite y-coordinates). But M has an involution σ mapping $\sqrt{f(B)}$ to $-\sqrt{f(B)}$, while fixing $K^{\mathrm{H}}(C)(\sqrt{f(A)})$ (this follows from Lemma 4.1). On the curve, $\sigma(P_1) = P_1$ but $\sigma(P_2) = -P_2$. We want $m\tilde{P_1}$ and $\tilde{P_2}$ to be opposite points. If this is not the case, replace w by the valuation $w \circ \sigma$. Then the points become opposite and

$$w\left(\mathrm{Y}_m(A)\sqrt{f(A)} - \sqrt{f(B)}\right) = 0. \tag{21}$$

We will now determine $w(y(P_3))$ using the fact that $P_3 = mP_1 + P_2$. We can do this with (20) and (21). The elliptic curve addition formula says that

$$\begin{aligned} x(P_3) &= -a_2 - x(mP_1) - x(P_2) + \left(\frac{y(mP_1) - y(P_2)}{x(mP_1) - x(P_2)}\right)^2 \\ &= -\underbrace{a_2}_{w \geq 0} - \underbrace{\mathrm{X}_m(A)}_{w=0} - \underbrace{B}_{w=0} + \underbrace{\left(\frac{\mathrm{Y}_m(A)\sqrt{f(A)} - \sqrt{f(B)}}{\mathrm{X}_m(A) - B}\right)^2}_{w=2(0-1)=-2}. \end{aligned}$$

We see that $w(x(P_3)) = -2$. The elliptic curve equation $y(P_3)^2 = f(x(P_3))$ implies that $w(y(P_3)) = -3$. This should indeed be negative because we already knew that $\tilde{P_3}$ is the point at infinity.

So far we determined the w-valuation of the coefficient $y(P_3)$ in the quadratic form (16). We claim that $w(y(sP_1 + rP_3)) = 0$. If $w(y(sP_1 + rP_3)) < 0$, then $s\tilde{P_1} + r\tilde{P_3} = s\tilde{P_1} = \mathbf{0}$; if $w(y(sP_1 + rP_3)) > 0$, then the y-coordinate of $s\tilde{P_1} + r\tilde{P_3} = s\tilde{P_1}$ is zero, hence $s\tilde{P_1}$ is 2-torsion. In any case, if $w(y(sP_1 + rP_3)) \neq 0$, then $\tilde{P_1}$ is a torsion point on E (here we need $s \neq 0$). But E has coefficients in $\mathbb{Q}$, hence all torsion is algebraic over $\mathbb{Q}$. The x-coordinate of $\tilde{P_1}$ is $\tilde{A} = (T^{-2} + \lambda)\gamma$ with $v(\tilde{A}) = -2$, therefore $\tilde{A}$ cannot be algebraic over $\mathbb{Q}$ and $\tilde{P_1}$ cannot be torsion.

We conclude $w(y(P_3)) = -3$ and $w(y(sP_1 + rP_3)) = 0$. We would like to apply Corollary 2.14 on (16). This works because -3 is odd in the value group of w; indeed the value group is $(1/e_w)\mathbb{Z}$ with e_w odd. So Corollary 2.14 gives us that

$$\langle 1, y(s\tilde{P_1})\rangle \otimes Q. \tag{22}$$

is isotropic over $K^{\mathrm{H}\prime}$.

Recall that $[K^{\mathrm{H}\prime} : K^{\mathrm{H}}] = f_w$ is odd. Since K^{H} is henselian, the valuation v on K^{H} can be extended to $K^{\mathrm{H}\prime}$ in a unique way. This extension has ramification index e_v and residue extension degree f_v which satisfy $e_v f_v = [K^{\mathrm{H}\prime} : K^{\mathrm{H}}] = f_w$, therefore both e_v and f_v are odd. Write k' for the new residue field.

The point $\tilde{P_1}$ has x-coordinate $\tilde{A} = (T^{-2} + \lambda)\gamma$ with $v(\tilde{A}) = -2$. The y-coordinate of $s\tilde{P_1}$ equals $\mathrm{Y}_s(\tilde{A})\sqrt{f(\tilde{A})}$. Proposition 3.2 implies that $v(\mathrm{Y}_s(\tilde{A})) = 0$; hence $v(y(s\tilde{P_1})) = v(f(\tilde{A}))/2 = -3$. Since e_v is odd, this -3 is an odd element of the value group of v on $K^{\mathrm{H}\prime}$. We can apply Corollary 2.14 on (22) to conclude that Q is isotropic over the residue field k'. Since $[k' : k] = f_v$ is odd and Q has coefficients in $F \subseteq k$, it follows from Springer's Theorem (see [Lam05, VII.2.7]) that Q is also isotropic over k. But Q was chosen to be anisotropic over k, so we have found a contradiction. □

5 The conditions of the Main Theorem

It turns out that we can simplify some of the conditions of Main Theorem 1. First of all, thanks to Voevodsky's work on the Milnor Conjectures (see [Pfi00] for a survey), we can replace condition (iii) in Main Theorem 1 by a simple condition on the 2-cohomological dimensions of $\mathrm{Gal}(\bar{F}/F)$ and $\mathrm{Gal}(\bar{k}/k)$. Second, the condition that the curve C has a rational point can be easily removed by going to a finite extension of K.

5.1 Galois Cohomology

We will recall some definitions and propositions from Galois cohomology, we refer to [Ser02] for background and proofs.

Throughout this section, let K be a characteristic zero field. Let $H^q(K, \mu_p)$ denote the q-th cohomology group of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ with coefficients in the group $\mu_p \subset \bar{K}^*$ of p-th roots of unity.

Definition 5.1. Let p be a prime number. The *p-cohomological dimension* of $\mathrm{Gal}(\bar{K}/K)$, denoted by $\mathrm{cd}_p(K)$, is the smallest integer q such that

$$H^{q+1}(L, \mu_p) = 0 \qquad \text{for all finite extensions } L \text{ of } K.$$

If there is no such q, then we define $\mathrm{cd}_p(K) = \infty$.

It turns out that we can describe how these cohomological dimensions behave with respect to field extensions:

Proposition 5.2 (see [Ser02, II.§ 4.2 Prop. 11])**.** *Let K be a characteristic zero field with $\mathrm{cd}_p(K) < \infty$, and let L be any extension of K. Then*

$$\mathrm{cd}_p(L) \leq \mathrm{cd}_p(K) + \mathrm{tr.\,deg}(L/K). \tag{23}$$

If L is finitely generated over K, the equality holds. In particular, cohomological dimensions remain the same under finite extensions, provided that $\mathrm{cd}_p(K) < \infty$.

The Milnor Conjectures, now proved by Voevodsky and others (see [Voe96] and [OVV07]) provide a connection between the Witt ring $W(K)$, the Galois cohomology groups $H^q(K, \mu_2)$ and Milnor's K-groups. For a survey article about this, see [Pfi00]. We need the following consequence of the Milnor conjectures:

Theorem 5.3. *([AE01] or [Pfi00]) Let I denote the fundamental ideal (generated by the 2-dimensional forms) in $W(K)$. Then $I^q/I^{q+1} \cong H^q(K, \mu_2)$.*

Using this, we know the possible dimensions of anisotropic Pfister forms over K:

Corollary 5.4. *There exists an anisotropic 2^q-dimensional Pfister form over K if and only if $H^q(K, \mu_2) \neq 0$.*

$$\begin{tikzcd}
 & & K' = K_1(\beta) \arrow[dl, dash] \arrow[d, dash] & \\
 & K_1 = K(\alpha) \arrow[dl, dash] \arrow[d, dash] & \mathcal{O}' \arrow[r, two heads] \arrow[dl, dash] \arrow[dr, dash, bend right] & k' \arrow[d, dash] \arrow[dl, equal] \\
K \arrow[d, dash] & \mathcal{O}_1 \arrow[r, two heads] \arrow[dl, dash] \arrow[dr, dash, bend right] & k_1 \arrow[dl, dash] \arrow[d, dash] & F' \arrow[dl, dash] \\
\mathcal{O} \arrow[r, two heads] \arrow[dr, dash, bend right] & k \arrow[d, dash] & F_1 = F(\beta) \arrow[dl, dash] & \\
 & F & &
\end{tikzcd}$$

Proof. If $H^q(K, \mu_2) = 0$, then $I^q/I^{q+1} = 0$. This implies that $I^q = I^{q+1}$, hence also $I^{q+1} = I^{q+2}$ and so on. The Arason–Pfister Hauptsatz (see [Lam05, X.5.1]) implies that $\bigcap_{n\geq 0} I^n = 0$, therefore $I^q = 0$. But I^q is generated by the 2^q-dimensional Pfister forms, therefore all 2^q-dimensional Pfister forms are hyperbolic (hence isotropic).

Conversely, if $H^q(K, \mu_2) \neq 0$, then $I^q \neq 0$. Therefore, there exists a non-hyperbolic Pfister form Q of dimension 2^q. But for Pfister forms, non-hyperbolic is the same as anisotropic. □

We can now change condition (iii) from Main Theorem 1:

Proposition 5.5. *Main Theorem 1 is still true if we replace condition* (iii) *by: "the* 2*-cohomological dimensions of F and k are equal and finite." We can do this without loss of generality.*

Note that this does *not* mean that condition (iii) from the Main Theorem is equivalent to "$\mathrm{cd}_2(F) = \mathrm{cd}_2(k) < \infty$", it just means that we can also prove the Main Theorem with the new condition instead of (iii). When we say "without loss of generality", it means that "$\mathrm{cd}_2(F) = \mathrm{cd}_2(k) < \infty$" always holds if (iii) is satisfied. We might need to extend the field $\mathcal{L}_0$ though.

Proof. Assume $q := \mathrm{cd}_2(F) = \mathrm{cd}_2(k)$ is finite and that conditions (i) and (ii) are satisfied. By definition of cohomological dimension, there is a finite extension k_1/k for which $H^q(k_1, \mu_2) \neq 0$.

By [End72, Theorem (27.1)], we can find an extension K_1/K such that v extended to K_1 has residue field k_1 and value group Γ. Choose α in the algebraic closure $\bar{K}$ such that $K_1 = K(\alpha)$.

Since $H^q(k_1, \mu_2) \neq 0$, Corollary 5.4 implies that there exists an anisotropic 2^q-dimensional Pfister form Q over k_1. The coefficients of Q are algebraic over F, since k_1/k and k/F are algebraic extensions.

Let $F_1 \subseteq k_1$ be the field obtained by adjoining the coefficients of Q to F. Choose $\beta \in F_1$ such that $F_1 = F(\beta)$. By Proposition 2.8, we can identify k_1 with a subfield of the henselisation K_1^{H}. So we have the following chain of field extensions: $F \subseteq F_1 \subseteq k_1 \subseteq K_1^{\mathrm{H}}$. Therefore, we can see β as an element of K_1^{H} and define $K' := K_1(\beta)$. Since K' is a subfield of K_1^{H}, the residue field $k' := k_1$ and value group Γ will remain the same if we take an extension of v to K'. Let $F' \supseteq F_1$ be a maximal subfield of K' on which v is trivial.

We claim that the conditions of Main Theorem 1 are satisfied for K', with maximal subfield F' and residue field k'. The residue field still has characteristic zero and the value group stayed the same, so conditions (i) and (ii) are still satisfied.

We have the quadratic form Q which is anisotropic over $k' = k_1$. We made sure that the coefficients of Q lie in $F_1 \subseteq F'$, by adjoining them.

By construction, k' is a finite extension of k, so we have $\mathrm{cd}_2(F) = \mathrm{cd}_2(k') = q$. Since k'/F' and F'/F are algebraic, we must also have $\mathrm{cd}_2(F') = q$.

On the other hand, from $\mathrm{cd}_2(F') = q$ it follows that $\mathrm{cd}_2(F'(Z)) = q + 1$. By definition of cohomological dimension, we have $H^{q+2}(L, \mu_2) = 0$ for all finite extensions L of $F'(Z)$, which implies that all Pfister forms over L of dimension 2^{q+2} will be isotropic.

Using Main Theorem 1, this would prove undecidability for $K'(C)$. However, $[K' : K]$ is finite, therefore one can make a model of $K'(C)$ in $K(C)^{[K':K]}$. So undecidability for the finite extension $K'(C)$ implies undecidability for $K(C)$.

Conversely, suppose that condition (iii) holds. The second part of this condition says that $H^{q+2}(L, \mu_2) = 0$ for all finite extentions L of $F(Z)$. This implies $\mathrm{cd}_2(F(Z)) \leq q + 1$, and Proposition 5.2 gives $\mathrm{cd}_2(F) = \mathrm{cd}_2(F(Z)) - 1 \leq q$.

The existence of an anisotropic 2^q-dimensional Pfister form over k implies that $H^q(k, \mu_2) \neq 0$ and $\mathrm{cd}_2(k) \geq q$. But k is algebraic over F, so by Proposition 5.2 we have the inequalities

$$q \leq \mathrm{cd}_2(k) \leq \mathrm{cd}_2(F) \leq q$$

which imply $\mathrm{cd}_2(F) = \mathrm{cd}_2(k) = q$, hence finite. □

Note that the inequality "$\mathrm{cd}_2(F) \geq \mathrm{cd}_2(k)$" is always satisfied, because k is an algebraic extension of F (see Proposition 2.8). So, it suffices to check that $\mathrm{cd}_2(F) \leq \mathrm{cd}_2(k)$.

5.2 The curve C

In Main Theorem 1, we assumed that C had a rational point. But we can easily get rid of this condition using field extensions.

Proposition 5.6. *The conclusion of Main Theorem 1 still holds if C does not have a K-rational point.*

Proof. We use the formulation of condition (iii) as in Proposition 5.5, so we assume that $\mathrm{cd}_2(F) = \mathrm{cd}_2(k) < \infty$.

Over an algebraically closed field, C must have a point so let $P \in C(\bar{K})$. Then P is actually defined over a finite extension K' of K. Take an extension of v to K' and let Γ' denote the new value group, k' the residue field and F' a maximal subfield of K' extending F.

We will now apply Main Theorem 1 for K'. The value group Γ' cannot be 2-divisible since $[\Gamma' : \Gamma]$ is finite. Since all extensions are finite, $\mathrm{cd}_2(F') = \mathrm{cd}_2(F)$ and $\mathrm{cd}_2(k') = \mathrm{cd}_2(k)$, therefore $\mathrm{cd}_2(F') = \mathrm{cd}_2(k') < \infty$, proving the new condition (iii). Now P is a K'-rational point, so Main Theorem 1 gives undecidability for $K'(C)$, hence also for $K(C)$. □

5.3 Second version of the Main Theorem

Applying the previous two sections, we can reformulate Main Theorem 1 as follows:

Main Theorem 2. *Let K be a field of characteristic zero with a valuation $v : K^* \twoheadrightarrow \Gamma$. Let $\mathcal{O}$ denote the valuation ring and k the residue field.*

Assume the following conditions are satisfied:

(i) The characteristic of the residue field k is zero.

(ii) The value group Γ is not 2-divisible.

(iii) Let F be a maximal field contained in $\mathcal{O}$. The 2-cohomological dimensions of F and k are equal and finite.

Let C be a smooth projective geometrically connected curve defined over K and let $K(C)$ be its function field. Then $K(C)$ is undecidable with coefficients in some finitely generated subfield $\mathcal{L}_0$ of $K(C)$.

If K is henselian, then we have $\mathrm{cd}_2(F) = \mathrm{cd}_2(k)$ by Proposition 2.8. So, in condition (iii) above we only need to check the finiteness of $\mathrm{cd}_2(k)$.

6 Coefficient field

So far, we have not really discussed the field $\mathcal{L}_0$ of coefficients for which we have undecidability of diophantine equations. We start from $\mathbb{Q}$ and add some constant symbols to make our diophantine model of $\mathbb{Z}$. There are four places in the proof where we need to enlarge $\mathcal{L}_0$:

1. To define the extension L and the points P_1 and P_2 on $E(L)$, $\mathcal{L}_0$ must at least contain T and Z. For T any element from K having positive odd valuation will do, Z is simply a transcendental element over K generating $K(Z)$.

2. To apply Proposition 5.5, we might need to extend our field K to a finite extension $K' = K(\alpha, \beta)$. So we need the coefficients of the minimal polynomial of α and β in $\mathcal{L}_0$. From the proof of Proposition 5.5, it can be seen that these are algebraic over F. So, if F happens to be finitely generated over $\mathbb{Q}$, we might as well include all of F into $\mathcal{L}_0$.
3. We have to express the coefficients of the quadratic form Q. These will also be algebraic over F.
4. Finally, we might need a finite extension to apply Proposition 5.6.

In concrete examples, one can usually specify the field $\mathcal{L}_0$ explicitly, see some of the examples below.

7 Examples

In this section we give some examples for which our theorem can be applied. We recover many known results. Whenever we use the word "undecidable" below, we mean that the existential theory is undecidable; in other words, Hilberts' Tenth Problem for that field has a negative answer.

The first example shows that we might as well take function fields of arbitrary varieties (of dimension ≥ 1) instead of curves.

Example 7.1. Let K be such that the conditions of Main Theorem 2 are satisfied for some curve C. Let L be a finitely generated extension of K, with transcendence degree at least 1. Then L is undecidable (with coefficients in some finitely generated field $\mathcal{L}_0$).

Proof. We consider two cases, according to the transcendence degree of L/K.

If the transcendence degree is exactly 1, then we let K' be the algebraic closure of K inside L. Then L is the function field of a curve over K', let $L = K'(C')$.

Let v be an extension of the given valuation to K'. The new value group Γ' might be larger than the original Γ, but in any case $[\Gamma' : \Gamma]$ is finite, so Γ' will still be non-2-divisible.

The maximal subfield $F' \supseteq F$ of $\mathcal{O}' \subseteq K'$ will be a finite extension of F, so $\mathrm{cd}_2(F') = \mathrm{cd}_2(F)$. The same is true for the new residue field k', so $\mathrm{cd}_2(F') = \mathrm{cd}_2(k') < \infty$.

If L has transdendence degree ≥ 2 over K, then we take a transcendence basis $\{Z_1, \ldots, Z_n\}$ of L/K. Let u be a valuation on $K(Z_1, \ldots, Z_{n-1})$ with residue field K. Let v be the given valuation on K. Let w be the composition of u with v (see Proposition 2.11 but with u and v swapped). We want to show that the conditions of Main Theorem 2 are satisfied for the base field $K(Z_1, \ldots, Z_{n-1})$ with valuation w and the curve $C = \mathbb{P}^1$. Then the statement for L will follow from the first part of this proof.

It is easy to see that $F \subseteq \mathcal{O}_v \subseteq K$ is also a maximal subfield of $\mathcal{O}_w$. Proposition 2.11 says that the residue field of w is k. So, clearly conditions (i) and (iii) are satisfied. Also condition (ii) is satisfied because of the exact sequence (1) and the fact that Γ_u is not 2-divisible. $\square$

To simplify the following examples, we will only consider rational function fields. However, because of the preceding example, everything still works for function fields of varieties. Moreover, considering only rational function fields makes the examples more concrete such that one can specify $\mathcal{L}_0$ in certain cases.

Example 7.2. If F is a characteristic zero field with $\mathrm{cd}_2(F)$ finite, then the 2-variable rational function field $F(Z_1, Z_2)$ is undecidable.

Proof. Apply the theorem with $K = F(Z_1)$ and v the discrete valuation associated to Z_1, which has residue field F. $\square$

Example 7.3. If F is a number field, then $F(Z_1, Z_2)$ is undecidable with $\mathcal{L}_0 = \mathbb{Q}(Z_1, Z_2)$. (see also [KR95]).

Proof. From the Theorem of Hasse–Minkowski it follows that all 4-dimensional quadratic forms over a non-real number field are isotropic. On the other hand, over a real field there are anisotropic Pfister forms of arbitrarily high dimension: take $\langle 1, 1\rangle \otimes \langle 1, 1\rangle \otimes \dots$. This implies that $\mathrm{cd}_2(F) = \infty$ if F is a real number field and $\mathrm{cd}_2(F) = 2$ otherwise. So in the non-real case we just have to apply Example 7.2.

If F is real, we can take the finite extension $F(\sqrt{-1})$. Then Main Theorem 2 gives undecidability for $F(\sqrt{-1})(Z_1, Z_2)$, which implies undecidability for $F(Z_1, Z_2)$. $\square$

Example 7.4. The fields $\mathbb{R}(Z_1, Z_2)$ and $\mathbb{C}(Z_1, Z_2)$ are undecidable with $\mathcal{L}_0 = \mathbb{Q}(Z_1, Z_2)$. (for $\mathbb{R}$ see also [Den78], for $\mathbb{C}$ see also [KR92]).

Example 7.5. Let F be a characteristic zero field with $\mathrm{cd}_2(F)$ finite. Then $F((T))(Z)$ is undecidable.

Proof. Let $K = F((T))$ and let v be the discrete valuation at T. The valuation ring $\mathcal{O} = F[[T]]$ has F as maximal subfield. This way, the conditions for Main Theorem 2 are satisfied. $\square$

This example can be generalized somewhat:

Example 7.6. Let K be a field for which the conditions of Main Theorem 2 are satisfied. Let K' be any extension of K, contained in the maximal completion $\hat{K}$ (for discrete valuations, this is "the" completion). Then $K'(Z)$ is undecidable.

Proof. Extend the given valuation v to a valuation on K'. The residue field and value group will remain the same ($\hat{K}$ is the maximal field with this property). In general, the maximal subfield F' of $\mathcal{O}'$ could be an extension of F, but still contained in k. Since $F \subseteq F' \subseteq k$ and k/F is algebraic, the extensions k/F' and F'/F are also algebraic. Hence

$$q = \mathrm{cd}_2(k) \leq \mathrm{cd}_2(F') \leq \mathrm{cd}_2(F) = q$$

from which $\mathrm{cd}_2(F') = \mathrm{cd}_2(k) = q$. $\square$

Example 7.7. Let F be a characteristic zero field for which $\mathrm{cd}_2(F)$ is finite. Let $\{X_i\}_{i\in I}$ be a set of algebraically independent variables, with $\#I \geq 2$. Then $F(\{X_i\}_{i\in I})$ is undecidable.

Proof. Choose a well-ordering $\preccurlyeq$ on I, this is a total order on I such that every non-empty subset of I has a minimal element (the existence of well-orderings is equivalent to the axiom of choice). I itself also has a smallest element i_0, let $Z := X_{i_0}$. We also define $I' := I \setminus \{i_0\}$ and $K := F(\{X_i\}_{i\in I'})$. We have to prove undecidability for $F(\{X_i\}_{i\in I}) = K(Z)$.

Let

$$\Gamma := \bigoplus_{i\in I'} \mathbb{Z}. \qquad \text{(direct sum of abelian groups)}$$

Since $\#I \geq 2$, this Γ is not 2-divisible.

We make this into an ordered abelian group $\Gamma, +, \leq$ by using the lexicographic ordering coming from $I, \preccurlyeq$. To define a valuation $v : K^* \twoheadrightarrow \Gamma$, we let v be trivial on F and define v for monomials:

$$v\left(\prod_{i\in I'} X_i^{m_i}\right) = \bigoplus_{i\in I'} m_i \in \Gamma.$$

Then the valuation of a polynomial is defined to be the minimal valuation of its terms. Finally, for rational functions we define $v(x/y) = v(x) - v(y)$. One can check that this does indeed satisfy the axioms of a valuation, and that the residue field is F (hence $\mathrm{cd}_2(k) = \mathrm{cd}_2(F) < \infty$). $\square$

Example 7.8. Let K be a field of characteristic zero containing an algebraically closed subfield. If K admits a valuation with non-2-divisible value group and residue characteristic zero, then $K(Z)$ is undecidable with $\mathcal{L}_0 = \mathbb{Q}(T, Z)$, where T can be any element with odd valuation.

Proof. Remark that K cannot be algebraically closed itself, because all valuations on algebraically closed fields have divisible value groups.

Write v for the given valuation with value group Γ_v, valuation ring $\mathcal{O}_v$, maximal subfield $F_v \subseteq \mathcal{O}_v$ and residue field k_v. Let C be an algebraically closed subfield of F_v (one can always take $C = \bar{\mathbb{Q}}$, since $\bar{\mathbb{Q}}$ has no non-trivial valuations with residue characteristic zero).

C is contained in F_v, so it is also contained in k_v. We would like to define a valuation u on k_v with C as residue field, we do this as follows: Choose a transcendence basis $\{X_i\}_{i\in I}$ for k_v over C. As in Example 7.7, we can construct a valuation u on $C(\{X_i\}_{i\in I})$ with residue field C. Extend this valuation to k_v. This extension is algebraic, so the new residue field is an algebraic extension of C, hence C itself.

Let w be the composite valuation of v and u, as defined in Proposition 2.11. We would like the apply the Main Theorem on K with valuation w. Since Γ_v is not 2-divisible, the exact sequence (1) ensures that Γ_w is not 2-divisible either.

We claim that C is a subfield of $\mathcal{O}_w$. We know that $C^* \subseteq \mathcal{O}_u^*$, and since π_v is an isomorphism on C, we also have $C^* \subseteq \pi_v^{-1}(\mathcal{O}_u^*) = \mathcal{O}_w^*$.

The residue field of w is C, so C must be a maximal subfield of $\mathcal{O}_w$. We have $\mathrm{cd}_2(C) = \mathrm{cd}_2(C) = 0$, so we can apply Main Theorem 2 with the valuation w. $\square$

References

[AE01] Jón Kr. Arason and Richard Elman, *Powers of the fundamental ideal in the Witt ring*, J. Algebra **239** (2001), no. 1, 150–160.

[CK77] Chen Chung Chang and Jerome Keisler, *Model theory*, North-Holland, 1977.

[Dav73] Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), no. 3, 233–269.

[Den78] Jan Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.

[Eis03] Kirsten Eisenträger, *Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific J. Math. **210** (2003), 261–281.

[Eis04] ———, *Hilbert's tenth problem for function fields of varieties over* $\mathbb{C}$, Int. Math. Res. Not. **59** (2004), 3191–3205.

[Eis07] ———, *Hilbert's tenth problem for function fields of varieties over number fields and p-adic fields*, J. Algebra **310** (2007), no. 2, 775–792.

[End72] Otto Endler, *Valuation theory*, Springer, 1972.

[EP05] Antonio Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer, 2005.

[FJ86] Michael Fried and Moshe Jarden, *Field arithmetic*, Springer, 1986.

[KR92] Ki Hang Kim and Fred Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, J. Algebra **150** (1992), no. 1, 35–44.

[KR95] ———, *Diophantine unsolvability over p-adic function fields*, J. Algebra **176** (1995), no. 1, 83–110.

[Lam05] Tsit-Yuen Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, no. 67, American Mathematical Society, 2005.

[Mat70] Yuri Matiyasevich, *Enumerable sets are Diophantine*, Soviet Math. Dokl. **11** (1970), 354–358.

[MB05] Laurent Moret-Bailly, *Elliptic curves and Hilbert's tenth problem for algebraic function fields over real and p-adic fields*, J. Reine und Angew. Math. **587** (2005), 77–143.

[OVV07] D. Orlov, A. Vishik, and V. Voevodsky, *An exact sequence for* $K_*^M/2$ *with applications to quadratic forms*, Ann. of Math. (2) **165** (2007), no. 1, 1–13.

[Pfi00] Albrecht Pfister, *On the Milnor conjectures: History, influence, applications*, Jber. d. Dt. Math.-Verein **102** (2000), 15–39.

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for rational function fields over finite fields*, Invent. Math. **103** (1991), 1–8.

[Ser02] Jean-Pierre Serre, *Galois cohomology*, Springer Monographs in Mathematics, Springer, 2002.

[Shl96] Alexandra Shlapentokh, *Diophantine undecidability over algebraic function fields over finite fields of constants*, J. Number Theory **58** (1996), 317–342.

[Sil86] Joseph Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer, 1986.

[Tar51] Alfred Tarski, *A decision method for elementary algebra and geometry*, University of California Press, 1951.

[Vid94] Carlos Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), 249–253.

[Voe96] Vladimir Voevodsky, *The milnor conjecture*, K-theory Preprint Archives, http://www.math.uiuc.edu/K-theory/0170/, 1996.