FIRST-ORDER DEFINITIONS IN FUNCTION FIELDS OVER ANTI-MORDELLIC FIELDS

BJORN POONEN AND FLORIAN POP

1. Introduction

Definition 1.1. A field k is anti-Mordellic (or large) if every smooth curve with a k-point has infinitely many k-points.

Separably closed fields, henselian fields, and real closed fields are examples of anti-Mordellic fields. An algebraic extension of an anti-Mordellic field is anti-Mordellic: see [Pop1996], Proposition 1.2.

Definition 1.2. Let k be a field. A function field over k is a finitely generated extension K of k with $\operatorname{trdeg}(K|k) > 0$.

Definition 1.3. The constant field of a field K finitely generated over k is the relative algebraic closure of k in K.

Theorem 1.4. *There exists a formula $\phi(t)$ that when interpreted in a field K finitely generated over an anti-Mordellic field k defines the constant field.*

Theorem 1.5. *For each of the following classes of fields, there is a sentence that is true for fields in that class and false for fields in the other five classes:*
1. *finite and anti-Mordellic fields*
2. *number fields*
3. *function fields over finite fields*
4. *function fields over anti-Mordellic fields of characteristic > 0*
5. *function fields over anti-Mordellic fields of characteristic 0*
6. *function fields over number fields*

Remark 1.6. It is impossible to distinguish finite fields from anti-Mordellic fields with a single sentence, since a nontrivial ultraproduct of finite fields is anti-Mordellic.

Finally, we have a few theorems characterizing algebraic dependence. Some of these require that the ground field k be "2-cohomologically well behaved" in the sense of Definition 5.1 in Section 5. The following theorems will be proved in Section 5.

Theorem 1.7. *There exists a formula $\phi_n(t_1, \dots, t_n)$ such that for every K finitely generated over a real closed or separably closed field k, and every $t_1, \dots, t_n \in K$, the formula holds if and only if $t_1, \dots, t_n$ are algebraically dependent over k.*

Date: February 20, 2006.

2000 *Mathematics Subject Classification.* Primary 11U09; Secondary 14G25.

Key words and phrases. First-order theory, finitely generated fields, anti-Mordellic fields.

B.P. was supported by NSF grant DMS-0301280 a Packard Fellowship, and the Miller Institute for Basic Research in Science. He thanks the Isaac Newton Institute for hosting a visit in the summer of 2005.

Theorem 1.8. *Let k be a 2-cohomologically well behaved field. Let $K|k$ be a finitely generated extension. Then there exists a first order formula (depending on K and k) with r free variables, in the language of fields augmented by a predicate for a subfield, that when interpreted for elements $t_1, \ldots, t_r \in K$ with the subfield being k holds if and only if the elements are algebraically independent over k.*

Corollary 1.9. *Let k be a finite field, a number field, or a 2-cohomologically well behaved anti-Mordellic field. Then there exists a first order formula (depending on K and k) with r free variables, in the language of fields, that when interpreted for elements $t_1, \ldots, t_r \in K$ holds if and only if the elements are algebraically independent over k.*

Proof. Theorem 1.4 of [Poonen2005-uniform-preprint] handles the case where k is finite or a number field. If k is anti-Mordellic, combine Theorems 1.4 and 1.8. □

Remark 1.10. We do not know if Theorem 1.8 and Corollary 1.9 can be made uniform in k and K, i.e., whether the formula can be chosen independent of k and K.

2. Defining the constants

In this section we prove Theorem 1.4.

Lemma 2.1. *Let k be an infinite field of characteristic p. Let S_0 be a finite subset of k, and let $S = \{s^{p^n} : s \in S_0, n \in \mathbb{N}\}$. Then $k - S$ is infinite.*

Proof. If k is algebraic over $\mathbb{F}_p$, then S is finite, so $k - S$ is infinite. Otherwise, choose $t \in k$ transcendental over $\mathbb{F}_p$; then for a given $s \in k$, the set $\{s^{p^n} : n \in \mathbb{N}\}$ contains at most one element of $\{t^\ell : \ \ell \text{ is prime}\}$, so $k - S$ is infinite. □

Lemma 2.2. *Let k be an infinite field. Let V be a k-variety. Let $\{C_a\}$ be a non-isotrivial family of curves of genus ≥ 2 over k with parameter a. Then there exist infinitely many $a \in k$ such that all rational maps from V to C_a are constant.*

Proof. Let p be the characteristic of k. A theorem of Severi [Samuel1966, Théorème 2] states that there are only finitely many fields L between k and the function field K of V such that L is the function field of a curve of genus ≥ 2 over k and K is separable over L. Thus the set S of $a \in k$ such that C_a admits a non-constant rational map from V is a finite set S_0 together with (if $p > 0$) the p^n-th powers of the elements of S_0 for all $n \in \mathbb{N}$. By Lemma 2.1, $k - S$ is infinite. □

Proof of Theorem 1.4. Without loss of generality we may assume that k is relatively algebraically closed in K. The discriminant of $x^5 + ax + 1$ (with respect to x) is $256a^5 + 3125$; if $\operatorname{char} k \notin \{2, 5\}$, this is a nonconstant squarefree polynomial in a, so the family of affine curves $C_a \colon y^2 = x^5 + ax + 1$ has both smooth and nodal curves, and is therefore non-isotrivial. If $\operatorname{char} k = 5$, the family $C_a \colon y^2 = x^7 + ax + 1$ is non-isotrivial for the same reason; and if $\operatorname{char} k = 2$, the family $C_a \colon y^2 + y = x^5 + ax$ is non-isotrivial, since a direct calculation (using the fact that the unique Weierstrass point must be preserved) shows that no two members of this family are isomorphic over an algebraic closure of k. The projection $x \colon C_a \to \mathbb{A}^1$ is étale above $0 \in \mathbb{A}^1(k)$.

For $a \in K$, define

$$S_a := \left\{ \frac{x_1}{x_2} : (x_1, y_1),\ (x_2, y_2) \in C_a(K) \text{ with } x_2 \neq 0 \right\}.$$

(A very similar definition was used in the proof of [Koenigsmann2002, Theorem 2].) We have

(1) If $a \in k$, then $k \subseteq S_a$. *Proof:* Let $f(x,y)=0$ is the equation of C_a in $\mathbb{A}^2$. Let $c \in k$. The map $(x_1,x_2)\colon C_a \times C_a \to \mathbb{A}^2$ is étale above $(0,0)$, so the point $(x_1,y_1,x_2,y_2) = (0,1,0,1)$ on the inverse image Y of the line $x_1 = cx_2$ in $C_a \times C_a$ is smooth. Since k is anti-Mordellic, Y has infinitely many other k-points, so $c \in S_a$.
(2) There exists $a_0 \in k$ such that $S_{a_0} = k$. *Proof:* Let V be an integral k-variety with function field K. Lemma 2.2 gives $a_0 \in k$ such that there is no nonconstant rational map $V \dashrightarrow C_{a_0}$ over k. Equivalently, $C_a(K) = C_a(k)$. So $S_{a_0} \subseteq k$, and we already know the opposite inclusion.
(3) If $a \in K - k$, then S_a is finite. *Proof:* By the function field analogue of the Mordell conjecture [Samuel1966, Théorème 4], $C_a(K)$ is finite, so $S_a(K)$ is finite.

Let A be the set of $a \in K$ such that S_a is a field containing a. Let $L := \bigcap_{a\in A} S_a$. Then L is uniformly definable by a formula. By (3), $A \subseteq k$ (a finite field cannot contain an element transcendental over k). Now by (1) and (2), $L = k$. □

Remark 2.3. Suppose K is finitely generated over a field k, and k is relatively algebraically closed in K. By the Weil conjectures applied to Y, there exists an explicit positive integer m such that (1) is true also in the case where k is a finite field of size $> m$. Let S'_a be the union of S_a with the set of zeros of $x^q - x$ in K for all $q \in \{2,3,\dots,m\}$. Let (1)', (2)', (3)' be the statements analogous to (1), (2), (3) but with S'_a in place of S_a. Then (1)', (2)', (3)' remain true for anti-Mordellic k, but now (1)' and (3)' hold also for finite k.

3. Some facts about quadratic forms

Proposition 3.1. *Let $q(x_1,\dots,x_n)$ be a quadratic form over a field K, and let L be a finite extension of K of odd degree. If q has a nontrivial zero over L, then q has a nontrivial zero over K.*

Proof. This is well known: see [LangAlgebra, Chapter V, Exercise 28]. □

Corollary 3.2. *Let K be a field of characteristic not 2. Let q be a quadratic form over K. Let L be a purely inseparable extension of K. If q has a nontrivial zero over L, then q has a nontrivial zero over K.*

Proof. If q has a nontrivial zero over L, the coordinates of this zero generate a finite purely inseparable extension of K, so we may assume $[L:K] < \infty$. Now the result follows from Proposition 3.1. □

For nonzero a, let $\langle\langle a\rangle\rangle$ denote the quadratic form $x^2 + ay^2$ and let $\langle\langle a_1,\dots,a_n\rangle\rangle = \langle\langle a_1\rangle\rangle \otimes \cdots \otimes \langle\langle a_n\rangle\rangle$ be the n-fold Pfister form.

Lemma 3.3. *Let k be a field, and let V be an integral k-variety with function field K. Suppose that v is a regular point on V, and that $t_1,\dots,t_m$ are part of a system of local parameters at v. Let q be a diagonal quadratic form over k having no nontrivial zero over the residue field of v. Then $q \otimes \langle\langle t_1,\dots,t_m\rangle\rangle_d$ has no nontrivial zero over K.*

Proof. This result is essentially contained in [Pop2002]. The proof is given again in Lemma A.5 in [Poonen2005-uniform-preprint]. □

Lemma 3.4. *Let ℓ be a field of characteristic not 2. Let L be a finitely generated extension of ℓ. Suppose that every 3-fold Pfister form $\langle\langle a, b, c\rangle\rangle$ over L has a nontrivial zero. Then*
(1) $\operatorname{trdeg}(L|\ell) \le 2$.
(2) *If moreover L admits a valuation that is trivial on $\ell^\times$ such that ℓ maps isomorphically to the residue field, and not every element of ℓ is a square in ℓ, then* $\operatorname{trdeg}(L|\ell) \le 1$.

Proof. (1) Let $t_1, \ldots, t_d$ be a transcendence basis for $L|\ell$. Let K be the maximal separable extension of $\ell(t_1, \ldots, t_d)$ contained in L. Let V be an integral variety over ℓ with function field K. Replacing V by an open subset if necessary, we may assume that $(t_1, \ldots, t_d)\colon V \to \mathbb{A}^n_\ell$ is étale. If ℓ is infinite, choose $(a_1, \ldots, a_d) \in \mathbb{A}^n(\ell)$ in the image of V; then by Lemma 3.3, $\langle\langle t_1 - a_1, \ldots, t_d - a_d\rangle\rangle$ has no nontrivial zero over K, and hence by Corollary 3.2, no nontrivial zero over L. If ℓ is finite, choose $(a_1, \ldots, a_d) \in \mathbb{A}^n(\ell')$ in the image of V for some $\ell'|\ell$ of odd degree, and repeat the previous argument with the minimal polynomial $P_{a_i}(t_i)$ of a_i over ℓ in place of $t_i - a_i$. In either case, this Pfister form contradicts the hypothesis if $d \ge 3$. Thus $d \le 2$.

(2) Suppose not. Then by (1), $\operatorname{trdeg}(L|\ell) = 2$. By the resolution of singularities for surfaces (see e.g. [Abhyankar1969]), we may choose a regular projective surface V over ℓ with function field L. The center of the given valuation on V is an ℓ-rational point $v \in V(\ell)$; hence v is actually a smooth point of V. Choose local parameters u_1, u_2 at v. Let $\alpha \in \ell$ be a non-square. By Lemma 3.3, $\langle\langle -\alpha, u_1, u_2\rangle\rangle$ has no nontrivial zero over L. This contradicts the hypothesis. □

Lemma 3.5. *Let X be a variety over an infinite field k. There exists an integer m such that the points on X of degree $\le m$ over k are Zariski dense in X.*

Proof. The desired property depends only on the birational class of X over $\overline{k}$. Therefore, enlarging k, we may reduce to the case where X is a geometrically integral closed hypersurface in $\mathbb{P}^n$. Choose $P \in (\mathbb{P}^n - X)(k)$. Projection from Q determines a generically finite rational map from X to $\mathbb{P}^{n-1}$, and the fibers above k-points in a Zariski dense open subset of $\mathbb{P}^{n-1}$ contain points of bounded degree. These points are Zariski dense in X. □

4. Distinguishing classes of fields

Proposition 4.1. *There is a sentence ϕ that is true for finite fields and anti-Mordellic fields, false for function fields over any field, and false for number fields.*

Proof. Let K be a field. Define S'_a as in Remark 2.3. Let ϕ be the sentence saying that $S'_a = K$ for all $a \in K$. This is true if K is finite or anti-Mordellic.

If K is a function field, then (3)' (whose proof is valid over any k) shows that for some a, the set S'_a is finite. If K is a number field, then S'_a is finite for all but finitely many a, by the Mordell conjecture [Faltings1983] applied to C_a. In both these cases, there exists $a \in K$ with $S'_a \ne K$. □

We can generalize Theorem 1.4 to include finitely generated extensions of finite fields:

Proposition 4.2. *There exists a formula that for K finitely generated over a finite or anti-Mordellic field k defines the constant field.*

Proof. We may assume that k is relatively algebraically closed in K. We use the notation of the proof of Theorem 1.4 and Remark 2.3. Let A' be the set of $a \in K$ such that S'_a is a field containing a. Let $k_1 := \bigcap_{a\in A'} S'_a$. Theorem 1.3 of [Poonen2005-uniform-preprint] gives a formula that defines the constant subfield if K is finitely generated over a finite field; over any field K, let k_2 be the subset it defines. Define

$$\tilde{k} := \begin{cases} k_1, & \text{if } S'_a \supseteq k_1 \text{ for every } a \in k_1, \\ k_2, & \text{otherwise.} \end{cases}$$

The subset $\tilde{k}$ is definable by a uniform formula; we claim that $\tilde{k} = k$.

If k is anti-Mordellic, then by the proof of Theorem 1.4, $k_1 = k$, and $\tilde{k} = k_1 = k$.

Now suppose k is finite, so $k_2 = k$. The set k_1 is a field (since it is an intersection of fields), and it contains k by Remark 2.3. If $k_1 = k$, then $\tilde{k} = k$. If $k_1 \supsetneq k$, and $a \in k_1 - k$, then by (3), S'_a is finite, so it cannot contain k_1; thus $\tilde{k} = k_2 = k$. □

Proposition 4.3. *There exists a sentence that is true for function fields over finite or anti-Mordellic fields and false for number fields and function fields over number fields.*

Proof. Use the sentence that says that the formula in Proposition 4.2 defines a field satisfying the sentence of Proposition 4.1. □

Proposition 4.4. *There is a sentence in the language of rings extended by a unary predicate that when interpreted in a function field K over a field k (not necessarily relatively algebraically closed) with the unary predicate defining k is true if and only if k is finite.*

Proof. By [Poonen2005-uniform-preprint, Remark 5.1], there is a formula $\phi(x, y)$ in the language of rings such that when it is interpreted in a function field K with finite constant field ℓ,

$$\{y \in K : \phi(x, y)\} = \ell[x]$$

for each $x \in K$. By [Rumely1980], there is a formula ψ defining a family of subsets that when interpreted in $\ell(x)$ for ℓ finite gives exactly the family of nontrivial valuation rings in $\ell(x)$ (possibly with repeats).

Now let K be a function field over an arbitrary field k. We claim that k is finite if and only if for some $x \in K$ the following hold:

(1) The set R defined by $\phi(x, \cdot)$ is a ring containing k and x.
(2) The family $\mathcal{F}$ defined by ψ interpreted over the fraction field L of R defines a set of nontrivial valuation rings in L, each containing k.
(3) The intersection of the valuation rings in $\mathcal{F}$ is a field ℓ.
(4) The element x is not in ℓ.
(5) The field ℓ maps isomorphically to the residue field of some valuation ring in $\mathcal{F}$.
(6) If $2 = 0$, then $[L : L^2] = 2$.
(7) If $2 \neq 0$, then every 3-fold Pfister form $\langle\langle a, b, c\rangle\rangle$ over L has a nontrivial zero, and some element of ℓ is not a square in ℓ.
(8) The intersection of the rings in $\mathcal{F}$ containing R equals R.
(9) Every ideal $aR + bR$ of R generated by two elements is principal.
(10) The elements $x - a$ for $a \in \ell$ are irreducible, and generate pairwise distinct ideals of R.
(11) There exists a nonzero $f \in R$ divisible in R by $x - a$ for all $a \in \ell$.

(These conditions can be expressed by a first order sentence in the language of rings with a predicate for k.)

If k is finite, and $x \in K$ is not in the constant field ℓ of K, then $R = \ell[x]$ for a finite field ℓ, and conditions (1)–(11) hold.

Conversely, suppose that conditions (1)–(11) hold for some $x \in K$. If $\operatorname{char} K = 2$, then (6) implies $\operatorname{trdeg}(L|\ell) \leq 1$. If $\operatorname{char} K \neq 2$, then (5) and (7) imply that $\operatorname{trdeg}(L|\ell) \leq 1$, by Lemma 3.4. Thus in every case, $\operatorname{trdeg}(L|\ell) \leq 1$. By (3), ℓ is an intersection of valuation rings, so it is relatively algebraically closed in L. By (4), $x \in L - \ell$, so $\operatorname{trdeg}(L|\ell) = 1$. Since L is a function field over k and $k \subseteq \ell$, L is a function field of transcendence degree 1 over ℓ. By (8), R is integrally closed in L; in particular it contains the integral closure R_0 of $\ell[x]$ in L. Thus R_0 is a Dedekind domain with fraction field L. Any ring between a Dedekind domain and its fraction field is itself a Dedekind domain, so R is a Dedekind domain. By (9), R is a principal ideal domain, and hence a unique factorization domain. Now (10) and (11) imply that ℓ is finite. So k is finite. □

Proposition 4.5. *There is a sentence that is true for function fields over finite fields and false for function fields over anti-Mordellic fields.*

Proof. Combine Propositions 4.2, and 4.4. □

Proposition 4.6. *There exists a sentence that for a function field K over a finite or anti-Mordellic field is true if and only if* $\operatorname{char} K = 0$.

Before beginning the proof of Proposition 4.6, we need a few definitions and a lemma. If M is an Abelian group and $n \geq 1$, let $M[n]$ be the kernel of the multiplication-by-n map $M \to M$. Also define $M_{\text{tors}} := \bigcup_{n \geq 1} M[n]$. If $E\colon y^2 = f(x)$ is an elliptic curve over a field K of characteristic $\neq 2$, and $t \in K$, then the twisted elliptic curve E_t is defined by $f(t)y^2 = f(x)$ over K. We will use the following, which is essentially a special case of a result of Moret-Bailly.

Lemma 4.7. *Let k be a field of characteristic* 0. *Let K be a function field over k. Let $E\colon y^2 = f(x)$ be an elliptic curve over k, where f is a cubic polynomial. Then there are infinitely many $t \in K$ with $f(t) \in K^\times - k^\times K^{\times 2}$ such that $E_t(K)$ is a finitely generated Abelian group with* $\operatorname{rk} E_t(K) = \operatorname{rk} \operatorname{End}_K(E)$.

Proof. We may enlarge k to assume that K is the function field of a geometrically irreducible curve over k. Replacing $f(x)$ by $f(x+c)$ for suitable $c \in k$, we may assume that $f(0) \neq 0$.

We use the terminology in [Moret-Bailly2005preprint, §1.5]. Let Γ be the smooth projective model of the $y^2 = x^4 f(1/x)$; cf. [Moret-Bailly2005preprint, 1.4.5(ii)]. By [Moret-Bailly2005preprint, 2.3.1], there exists $g \in K - k$ that is admissible for Γ. By [Moret-Bailly2005preprint, 1.8(ii) and 1.4.7], $\textsc{Good}(k) \cap \mathbb{Z}$ is infinite.

We claim that for any $\lambda \in \textsc{Good}(k) \cap \mathbb{Z}$, the value $t := \frac{1}{\lambda g}$ satisfies the required conditions. For such λ and t, we have $\lambda \in \operatorname{Good}(k)$ by [Moret-Bailly2005preprint, 1.5.4(i)]; thus $E'\colon (\lambda g)^4 f(\frac{1}{\lambda g}) y^2 = f(x)$ is an elliptic curve over K such that $E'(K)$ is finitely generated and $\operatorname{rk} E'(K) = \operatorname{rk} \operatorname{End}_K(E)$. By definition, E' is isomorphic to E_t.

Let $K\overline{k}$ be a compositum of K with an algebraic closure of $\overline{k}$ over k. If $f(t)$ were in $k^\times K^{\times 2}$, then E' would be isomorphic over $K\overline{k}$ to E, so $E'(K\overline{k}) \simeq E(K\overline{k}) \supseteq E(\overline{k})$ would not be finitely generated, contradicting the definition of $\textsc{Good}(k)$. □

Proof of Proposition 4.6. Use $\neg\phi$, where ϕ is a sentence equivalent to the following: $2 = 0$ or there exists an extension L of K with $[L : K] \leq 2$ such that for ℓ the subset defined in by the formula of Proposition 4.2 applied to L, there exist distinct $e_1, e_2, e_3 \in \ell$ such that if we write $f(x) := (x - e_1)(x - e_2)(x - e_3)$, then for all $t \in L$ with $f(t) \in L^\times - \ell^\times L^{\times 2}$, the twist E_t of $E\colon y^2 = f(x)$ satisfies $\# E_t(L)/2E_t(L) \geq 64$. For the K we are interested in, L is a function field over a finite or anti-Mordellic field, so ℓ is the constant field of L.

If $\operatorname{char} K = 2$, then ϕ is true. Now suppose K is a function field over an anti-Mordellic field of characteristic $p > 2$. Let L be a compositum of K with $\mathbb{F}_{p^2}$. Let E be an elliptic curve over $\mathbb{F}_p$ with $\# E(\mathbb{F}_p) = p+1$. Then the p^2-Frobenius endomorphism of E is multiplication by $-p$, so $\operatorname{rk} \operatorname{End}_{\mathbb{F}_{p^2}}(E) = 4$, and $E[2] \subseteq E(\mathbb{F}_{p^2})$. The curve $E_{\mathbb{F}_{p^2}}$ has an equation $y^2 = f(x)$ where $f(x) := (x - e_1)(x - e_2)(x - e_3)$ with distinct $e_1, e_2, e_3 \in \mathbb{F}_{p^2} \subseteq \ell$. Suppose $t \in L$ satisfies $f(t) \in L^\times - \ell^\times L^{\times 2}$. The restriction on t implies that E_t is not isomorphic over L to an elliptic curve over ℓ, so $E_t(L)$ is finitely generated. Quadratic twists of an elliptic curve have the same endomorphism ring, so the ring $\mathcal{O} := \operatorname{End}_L(E_t)$ is a maximal order in a non-split quaternion algebra $\mathbb{H}$ over $\mathbb{Q}$. Since $E_t(L) \otimes \mathbb{Q}$ is an $\mathbb{H}$-vector space, $4 \mid \operatorname{rk}_{\mathbb{Z}} E_t(L)$. The point $(t, 1) \in E_t(L)$ has infinite order, since under the $L(\sqrt{f(t)})$-isomorphism $E_t \to E$ mapping (x, y) to $(x, y\sqrt{f(t)})$ it corresponds to a point of E whose x-coordinate is transcendental over ℓ. Thus $\operatorname{rk}_{\mathbb{Z}} E_t(L) > 0$, so $\operatorname{rk}_{\mathbb{Z}} E_t(L) \geq 4$. Also, $E_t[2] \subseteq E_t(L)$, so $\# E_t(L)/2E_t(L) \geq 2^2 \cdot 2^4 = 64$.

Now suppose that K is a function field over an anti-Mordellic field of characteristic 0. Suppose L is an extension with $[L : K] \leq 2$, and $e_1, e_2, e_3 \in \ell$ are distinct. By Lemma 4.7 applied to L over ℓ, there exists $t \in L$ with $f(t) \notin \ell^\times L^{\times 2}$ such that $E_t(L)$ is finitely generated with $\operatorname{rk} E_t(L) = \operatorname{rk} \operatorname{End}_L(E)$. Since $\operatorname{rk} \operatorname{End}_L(E) \in \{1, 2\}$, and since $E_t(L)_{\text{tors}}$ is generated by at most 2 elements, we get $\# E_t(L)/2E_t(L) \leq 2^2 \cdot 2^2 = 16$. $\square$

Proof of Theorem 1.5. Taking $d = 0$ in the first claim of Theorem 1.5(3) of [Pop2002] gives a sentence that is true for number fields and false for function fields over number fields. Combining this with Propositions 4.1, 4.3, 4.5, and 4.6 gives the result. $\square$

5. Detecting algebraic dependence

We begin by recalling the following general facts: Let E be an arbitrary field of characteristic $\neq 2$. In particular, $\mu_2 = \{\pm 1\}$ is contained in E. We denote by G_E the absolute Galois group of E, and view μ_2 as a G_E-module.

1) Let $\operatorname{cd}_2^0(E) \in \mathbb{N} \cup \{\infty\}$ be the supremum over all the natural numbers n such that $\mathrm{H}^n(E, \mu_2) \neq 0$. Since the 2-cohomological dimension $\operatorname{cd}_2(E)$ is defined similarly, but the supremum is taken over all possible 2-torsion G_k-modules, one has

$$\operatorname{cd}_2^0(E) \leq \operatorname{cd}_2(E)\,.$$

Also define $\operatorname{vcd}_2(E) := \operatorname{cd}_2(E(\sqrt{-1}))$.

2) Recall the Milnor Conjecture (proved by Voevodsky et al.) It asserts that the n^{th} cohomological invariant $e_n\colon I_n(E)/I_{n+1}(E) \to \mathrm{H}^n(E, \mu_2)$, which maps each n-fold Pfister form $\langle\langle a_1, \ldots, a_n \rangle\rangle$ to the cup product $(-a_1) \cup \cdots \cup (-a_n)$, is a well defined isomorphism. Using the Milnor Conjecture one can describe $\operatorname{cd}_2^0(E)$ via the behavior of Pfister forms as follows: $n > \operatorname{cd}_2^0(E)$ if and only if every n-fold Pfister form over E represents 0 over E.

3) There exists a field E with $\operatorname{cd}_2^0(E) < \operatorname{cd}_2(E)$. For instance, let E be a maximal pro-2 Galois extension of a global or local field of characteristic $\neq 2$. Then every element of E is a square, so $\operatorname{cd}_2^0(E) = 0$. On the other hand, since the Sylow 2-groups of G_E are non-trivial, one has $\operatorname{cd}_2(E) > 0$ by [SerreGaloisCohomology, §I.3.3, Corollary 2].

Definition 5.1. A field E is said to be 2-cohomologically well behaved if $\operatorname{char} E \neq 2$ and for every finite extension $E'|E$ containing $\sqrt{-1}$ one has $\operatorname{cd}_2^0(E') = \operatorname{cd}_2(E') < \infty$.

Remark 5.2. If E is 2-cohomologically well behaved, then and $E'|E$ is a finite extension containing $\sqrt{-1}$, then

$$\operatorname{cd}_2^0(E') = \operatorname{vcd}_2(E') = \operatorname{vcd}_2(E),$$

since $\operatorname{cd}_2(E') = \operatorname{cd}_2(E(\sqrt{-1}))$ by [SerreGaloisCohomology, §II.4.2, Proposition 10].

Example/Fact 5.3. The following fields, when of characteristic $\neq 2$, are 2-cohomologically well behaved:

- separably closed fields (trivial),
- finite fields (follows from [SerreGaloisCohomology, II.§3]),
- local fields (follows from [SerreGaloisCohomology, II.§4.3]),
- number fields (follows from [SerreGaloisCohomology, II.§4.4]), and
- finitely generated fields (follows from the above and Proposition 5.4 below).

Proposition 5.4. *If E is 2-cohomologically well behaved, and E' is a function field over E, then E' is 2-cohomologically well behaved and* $\operatorname{vcd}_2(E') = \operatorname{vcd}_2(E) + \operatorname{trdeg}(E'|E)$.

Proof. We may assume $\sqrt{-1} \in E$. The case $\operatorname{trdeg}(E'|E) = 0$ follows from Remark 5.2. By induction on $\operatorname{trdeg}(E'|E)$, it will suffice to prove that $\operatorname{cd}_2^0(E') = \operatorname{vcd}_2(E) + 1$ for every extension $E'|E$ with $\operatorname{trdeg}(E'|E) = 1$. We may assume that E' is separably generated over E. Let X be a curve over E with function field E', let P be a smooth point on X, let κ be the residue field of P, and let $t \in E'$ be a uniformizer at P. Let $n = \operatorname{cd}_2^0(\kappa) = \operatorname{vcd}_2(E)$. By definition, there exists an n-fold Pfister form $\langle\langle \bar{a}_1, \dots, \bar{a}_n \rangle\rangle$ that does not represent 0 over κ. Lift each $\bar{a}_i$ to an a_i in the local ring at P. Then $\langle\langle a_1, \dots, a_n, t \rangle\rangle$ does not represent 0 over E'. Thus $\operatorname{cd}_2^0(E') \geq \operatorname{vcd}_2(E) + 1$. On the other hand, $\operatorname{cd}_2^0(E') \leq \operatorname{vcd}_2(E') = \operatorname{vcd}_2(E) + 1$ by [SerreGaloisCohomology, §II.4.2, Proposition 11], so we have equality. □

Proposition 5.5. *Let k be a field which is 2-cohomologically well behaved, and let $e =$* $\operatorname{vcd}_2(k)$. *Let $K|k$ be a finitely generated extension. Then the following hold:*

(1) *For each $n \in \mathbb{Z}_{\geq 0}$, there exists a sentence ϕ_n in the language of fields (depending on e) such that ϕ_n is true in K if and only if* $\operatorname{trdeg}(K|k) = n$.

One can take ϕ_n to be the following sentence: Every $(e+n+1)$-fold Pfister form over $K[\sqrt{-1}]$ represents 0, but there exist $(e+n)$-fold Pfister forms over $K[\sqrt{-1}]$ which do not represent 0.

(2) *For elements $t_1, \dots, t_r \in K^\times$, the following are equivalent:*
   (a) *$(t_1, \dots, t_r)$ are algebraically independent over k.*
   (b) *There exists a finite separable extension $l|k$ (depending on $t_1, \dots, t_r$) containing $\sqrt{-1}$ and elements $a_1, \dots, a_e, b_1, \dots, b_r \in l^\times$ such that $\langle\langle a_1, \dots, a_e, t_1 - b_1, \dots t_r - b_r \rangle\rangle$ does not represent 0 over Kl.*

Proof.

(1) By the discussion preceding Proposition 5.5 we have:

$$\operatorname{cd}_2^0(K[\sqrt{-1}]) = \operatorname{cd}_2^0(k[\sqrt{-1}]) + \operatorname{trdeg}(K|k) = e + \operatorname{trdeg}(K|k).$$

Now use the characterization of cd_2^0 in terms of Pfister forms.

(2), (b) $\Rightarrow$ (a): Suppose for the sake of obtaining a contradiction that $(t_1, \dots, t_r)$ is algebraically dependent over k. Let $L = l(t_1, \dots, t_r) \subset Kl$. Since $\sqrt{-1} \in l$, we have:

$$\mathrm{cd}_2(L) = \mathrm{cd}_2(l) + \mathrm{trdeg}(L|l) = e + \mathrm{trdeg}(L|l) < e + d$$

Thus by the discussion above, every $(e+d)$-fold Pfister form over L represents 0 over L. In particular, for all $(a_i)_i$ and $(b_j)_j$ as in (b), the resulting $(e+d)$-fold Pfister form $\langle\langle a_1, \dots, a_e, t_1-b_1, \dots t_r-b_r\rangle\rangle$ represents 0 over L. Since $L \subseteq Kl$, it follows that $\langle\langle a_1, \dots, a_e, t_1-b_1, \dots t_r-b_r\rangle\rangle$ represents 0 over Kl, a contradiction!

(2), (a) $\Rightarrow$ (b): The proof is an adaptation from and similar to [Pop2002], Section 1. By extending the list $\mathcal{T} := (t_1, \dots, t_r)$, we may assume that it is a transcendence basis for $K|k$. Let $K_0|k(\mathcal{T})$ be the relative separable closure of $k(\mathcal{T})$ in K. Thus $\mathcal{T}$ is a separable transcendence basis of $K_0|k$, and $K|K_0$ is a finite purely inseparable field extension. Further let R be the integral closure of $k[\mathcal{T}]$ in K_0, and let $X = \operatorname{Spec} R$. The k-embedding $k[\mathcal{T}] \hookrightarrow R$ defines a finite k-morphism $\phi\colon X \to \operatorname{Spec} k[\mathcal{T}] = \mathbb{A}^r_k$. Further, since $K_0|k(\mathcal{T})$ is separable, the k-morphism ϕ is generically étale. Therefore, ϕ is étale on a Zariski dense open subset $U \subset X'$. We choose a finite separable extension $l|k$ containing $\sqrt{-1}$ such that $U(l)$ is non-empty. Choose $x \in U(l)$, and let $b := (b_1, \dots, b_r) = \phi(x)$ be its image in $\mathbb{A}^r_k(l) = l^r$. Then $t_1 - b_1, \dots, t_r - b_r$ are local parameters at x. Since $\mathrm{cd}^0_2\, l = e$, we may choose $a_1, \dots, a_e \in l^\times$ such that $\langle\langle a_1, \dots, a_e\rangle\rangle$ has no nontrivial zero over l. Then by Lemma 3.3, $\langle\langle a_1, \dots, a_e, t_1 - b_1, \dots, t_r - b_r\rangle\rangle$ has no nontrivial zero over $K_0 l$. By Corollary 3.2, $\langle\langle a_1, \dots, a_e, t_1 - b_1, \dots, t_r - b_r\rangle\rangle$ has no nontrivial zero over Kl. $\square$

Proof of Theorem 1.8. Theorem 1.4 of [Poonen2005-uniform-preprint] handles the case where k is finite, so assume that k is infinite. By replacing k with a finite extension k' and simultaneously replacing K with Kk' (these extensions can be interpreted over (K, k)), we may assume that K is the function field of a geometrically integral variety X over k where $\sqrt{-1} \in k$, and by Lemma 3.5 we may assume that the points of degree $\le m$ on X are Zariski dense. Now, by the same proof as in Proposition 5.5(2), $t_1, \dots, t_r$ are algebraically independent over k if and only if there exists an extension $l|k$ of degree $\le m$ such that there exist $a_1, \dots, a_e, b_1, \dots, b_r \in l^\times$ such that $\langle\langle a_1, \dots, a_e, t_1 - b_1, \dots, t_r - b_r\rangle\rangle$ has no nontrivial zero over Kl. The preceding statement is expressible as a certain first order formula evaluated at $t_1, \dots, t_r$. $\square$

Unfortunately, in the case char $= 2$ we do not have at our disposal an easy way to relate $\mathrm{trdeg}(K|k)$ to (some) well understood invariants (say similar to the cohomological dimension). In the case k is separably closed, one can though employ the theory of $C_i^{(p)}$ fields. Recall that a field E is said to be a $C_i^{(p)}$ field, if every system of homogeneous forms

$$f_\rho(X_1, \dots, X_n) \quad (\rho = 1, \dots, r)$$

has a non-trivial common zero, provided the degrees d_ρ of the forms satisfy: $n > \sum_\rho d_\rho^i$ and $(p, d_\rho) = 1$ for all ρ.

The following are well known facts about $C_i^{(p)}$ fields, see e.g., [Pfister1995]:

1) Suppose that E is a p-field, i.e., every finite extension $E'|E$ has degree a power of p. Then E is a $C_0^{(p)}$ field.

2) If E is a $C_i^{(p)}$ field, then every finite extension $E'|E$ is again a $C_i^{(p)}$ field.

3) If E is a $C_i^{(p)}$ field, then the rational function field $E(t)$ in one variable over E is an $C_{i+1}^{(p)}$ field.

In particular, if k is a $C_i^{(p)}$ field, and $K|k$ is a function field with $\mathrm{trdeg}(K|k) = d$, then K is a $C_{i+d}^{(p)}$ field.

Now let $K|k$ be a function field. For every $\ell > 0$ and every system $\underline{t} = (t_1, \ldots, t_r)$ of elements of $K^\times$, let

$$q^{(\ell)}_{(t_1,\ldots,t_r)} = \sum_{\underline{i}} \underline{t}^{\underline{i}} X^\ell_{\underline{i}}$$

be the "generalized Pfister form" of degree ℓ in ℓ^r variables as introduced in [Pop2002], Section 1, p. 388. Here $\underline{i}$ is a multi-index $\underline{i} = (i_1, \ldots, i_r)$, with $0 \le i_j < \ell$.

Proposition 5.6. *Let k be a p-field. Let $K|k$ be a function field. For every $\ell \neq \mathrm{char}(K)$ that is relatively prime to p, and every system $(t_1, \ldots, t_r)$ of elements of $K^\times$, let $q^{(\ell)}_{(t_1,\ldots,t_r)}$ be the corresponding form of degree ℓ in ℓ^r variables over K. Then one has:*

1. *For every $r > \mathrm{trdeg}(K|k)$, and every $(t_1, \ldots, t_r)$, the resulting form $q^{(\ell)}_{(t_1,\ldots,t_r)}$ represents 0 over K.*
2. *For a given system $(t_1, \ldots, t_r)$ the following conditions are equivalent:*
   - (a) *$(t_1, \ldots, t_r)$ is algebraically independent over k.*
   - (b) *there exist $b_1, \ldots, b_r \in k$ such that $q^{(\ell)}_{(t_1-b_1,\ldots,t_r-b_r)}$ does not represent 0 over K.*
3. *In particular, for each $n \in \mathbb{Z}_{\ge 0}$ there exists a sentence in the language of fields that holds for K if and only if $\mathrm{trdeg}(K|k) = n$.*

Thus given algebraically independent elements $x_1, \ldots, x_r \in K$ over k, the relative algebraic closure L of $k(x_1, \ldots, x_r)$ in K is described by a predicate in one variable x as follows:

$$L = \{\, x \in K \mid (x_1, \ldots, x_r, x) \text{ is not algebraically independent over } k \,\}$$

Proof of Proposition 5.6.

(1): By the discussion above, K is a $C_d^{(p)}$ field for $d = \mathrm{trdeg}(K|k)$.

(2), (b) $\Rightarrow$ (a): Let $L = k(t_1, \ldots, t_r)$. If $t_1, \ldots, t_r$ are algebraically dependent, then $\mathrm{trdeg}(L|k) < r$, so by (1), any form $q^{(\ell)}_{(t_1-b_1,\ldots,t_r-b_r)}$ represents 0 over L, and hence represents 0 over K.

(2), (a) $\Rightarrow$ (b): The proof is very similar to the proof of the corresponding implication in Proposition 5.5. The relative separable closure K_0 of $k(t_1, \ldots, t_r)$ in K is the function field of an étale cover $U \to \mathbb{A}^r_k$ with the morphism being given by $(t_1, \ldots, t_r)$. Choose $(b_1, \ldots, b_n) \in \mathbb{A}^r(k)$ and a closed point $u \in U$ above it. If l is the residue field of u, then K_0 embeds into the iterated Laurent power series field $\Lambda := l((t_r - b_r)) \ldots ((t_1 - b_1))$, and K embeds into a purely inseparable finite extension Λ' of Λ. The field Λ has a natural valuation v whose value group is $\mathbb{Z}^r$ ordered lexicographically, generated by $v(t_i - b_i)$ for $1 \le i \le r$. The values of the coefficients of $q^{(\ell)}_{(t_1-b_1,\ldots,t_r-b_r)}$ are distinct modulo ℓ (they even a system of representatives for $\mathbb{Z}^r/\ell\mathbb{Z}^r$). If we extend v to a valuation v' on Λ', the value group G of v' contains $\mathbb{Z}^r$ with index prime to ℓ, so the v'-valuations of these coefficients have distinct images in $G/\ell G$. Now for any non-zero system of elements $\underline{x} = (x_{\underline{i}})_{\underline{i}}$ from $K \subseteq \Lambda'$, $q^{(\ell)}_{(t_1-b_1,\ldots,t_r-b_r)}(\underline{x})$ is a sum of elements having distinct v'-valuations (distinct even modulo ℓ). So $q^{(\ell)}_{(t_1-b_1,\ldots,t_r-b_r)}(\underline{x}) \neq 0$.

The remaining assertions of Proposition 5.6 are clear. $\square$

Proof of Theorem 1.7.

Case 1: $\mathrm{char}(k) \neq 2$.

If k is either real closed or separably closed, then $l := k[\sqrt{-1}]$ is the unique finite separable field extension of k containing $\sqrt{-1}$. Thus the result follows from Proposition 5.5 (2).

Case 2: $\mathrm{char}(k) = 2$.

Then k is a 2-field, so it is a $C(2)_0$ field. To conclude, one applies Proposition 5.6 with $p = 2$ and $\ell = 3$. $\square$

Acknowledgments

We thank Laurent Moret-Bailly for some discussions of his paper [Moret-Bailly2005preprint].

References

[Abhyankar1969] Shreeram Shankar Abhyankar, *Resolution of singularities of algebraic surfaces*, Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press, London, 1969, pp. 1–11. MR0257080 (41 #1734) ↑

[Faltings1983] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366. MR718935 (85g:11026a) (German) ↑

[Koenigsmann2002] Jochen Koenigsmann, *Defining transcendentals in function fields*, J. Symbolic Logic **67** (2002), 947–956. MR1925951 (2003f:03048) ↑

[LangAlgebra] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002, ISBN 0-387-95385-X. MR1878556 (2003e:00003) ↑

[Moret-Bailly2005preprint] Laurent Moret-Bailly, *Elliptic curves and Hilbert's tenth problem for algebraic function fields over real and p-adic fields*, October 2004, Preprint, to appear in *J. reine angew. Math.* ↑

[Pfister1995] Albrecht Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Mathematical Society Lecture Note Series, vol. 217, Cambridge University Press, Cambridge, 1995, ISBN 0-521-46755-1. MR1366652 (97c:11046) ↑

[Poonen2005-uniform-preprint] Bjorn Poonen, *Uniform first-order definitions in finitely generated fields*, December 2005, Preprint. ↑

[Pop1996] Florian Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), 1–34. MR1405941 (97h:12013) ↑

[Pop2002] ———, *Elementary equivalence versus isomorphism*, Invent. Math. **150** (2002), 385–408. MR1933588 (2003i:12016) ↑

[Rumely1980] R. S. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), 195–217. MR583852 (81m:03053) ↑

[Samuel1966] Pierre Samuel, *Compléments à un article de Hans Grauert sur la conjecture de Mordell*, Inst. Hautes Études Sci. Publ. Math. (1966), 55–62. MR0204430 (34 #4272) (French) ↑

[SerreGaloisCohomology] Jean-Pierre Serre, *Galois cohomology*, Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, ISBN 3-540-42192-0, Translated from the French by Patrick Ion and revised by the author. MR1867431 (2002i:12004) ↑

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu
URL: http://math.berkeley.edu/~poonen

Department of Mathematics, University of Pennsylvania, DRL, 209 S 33rd Street, Philadelphia, PA 19104. USA
E-mail address: pop@math.upenn.edu
URL: http://math.penn.edu/~pop