Collectanea Mathematica (electronic version): http://www.imub.ub.es/collect

Collect. Math. **58**, 1 (2007), 73–84

On $\emptyset$-definable elements in a field

Apoloniusz Tyszka

Technical Faculty, Hugo Kołłątaj University
Balicka 104, 30-149 Kraków, Poland
E-mail: rttyszka@cyf-kr.edu.pl

Received February 10, 2006. Revised April 25, 2006

Abstract

We develop an arithmetic characterization of elements in a field which are first-order definable by a parameter-free existential formula in the language of rings. As applications we show that in fields containing an algebraically closed field only the elements of the prime field are existentially $\emptyset$-definable. On the other hand, many finitely generated extensions of $\mathbb{Q}$ contain existentially $\emptyset$-definable elements which are transcendental over $\mathbb{Q}$. Finally, we show that all transcendental elements in $\mathbb{R}$ having a recursive approximation by rationals, are definable in $\mathbb{R}(t)$, and the same holds when one replaces $\mathbb{R}$ by any Pythagorean subfield of $\mathbb{R}$.

1. Introduction

Let $\mathcal{L}$ be an elementary language. Let $\mathcal{A}$ be any $\mathcal{L}$-structure and let R be any n-ary relation on $|\mathcal{A}|$. Svenonius' theorem ([15, 11, p. 184]) states that the following conditions are equivalent:

- R is $\emptyset$-definable in $\mathcal{A}$ by a formula of $\mathcal{L}$;
- for each elementary extension $(\mathcal{B}, S)$ of $(\mathcal{A}, R)$ each automorphism g of $\mathcal{B}$ satisfies $g(S) = S$.

Keywords: Algebraic function field in one variable over $\mathbb{Q}$ (over $\mathbb{R}$, over $\mathbb{Q}_p$), element transcendental over $\mathbb{Q}$ (over $\mathbb{R}$, over $\mathbb{Q}_p$), existentially $\emptyset$-definable element, Faltings' finiteness theorem, field finitely generated over $\mathbb{Q}$, Pythagorean subfield of $\mathbb{R}$, recursively approximable real number, subset of $\mathbb{R}$ which is implicitly $\emptyset$-definable in $(\mathbb{R}, +, \cdot, 0, 1)$.

MSC2000: 03C60, 12L12.

Applying this theorem for fields we conclude that for any field $\boldsymbol{K}$ and any $r \in \boldsymbol{K}$ the set $\{r\}$ is $\emptyset$-definable in $\boldsymbol{K}$ if and only if $g(r) = r$ for each field automorphism $g : \boldsymbol{L} \to \boldsymbol{L}$ and for each field $\boldsymbol{L}$ being an elementary extension of $\boldsymbol{K}$. In the next section we give another description of such elements r.

2. An arithmetic characterization of $\emptyset$-definable elements

Let $\boldsymbol{K}$ be a field and let A be a subset of $\boldsymbol{K}$. We say that a map $f : A \to \boldsymbol{K}$ is *arithmetic* if it satisfies the following conditions:

(1) if $1 \in A$ then $f(1) = 1$,
(2) if $a, b \in A$ and $a + b \in A$ then $f(a + b) = f(a) + f(b)$,
(3) if $a, b \in A$ and $a \cdot b \in A$ then $f(a \cdot b) = f(a) \cdot f(b)$.

Obviously, if $f : A \to \boldsymbol{K}$ satisfies condition (2) and $0 \in A$, then $f(0) = 0$. We call an element $r \in \boldsymbol{K}$ *arithmetically fixed* if there is a finite set $A(r) \subseteq \boldsymbol{K}$ (an *arithmetic neighbourhood* of r) with $r \in A(r)$ such that each arithmetic map $f : A(r) \to \boldsymbol{K}$ fixes r, i.e. $f(r) = r$. Note that any finite set containing an arithmetic neighbourhood or r is itself an arithmetic neighbourhood of r. We denote the set of arithmetically fixed elements of a field $\boldsymbol{K}$ by $\widetilde{\boldsymbol{K}}$.

Proposition ([16])

$\widetilde{\boldsymbol{K}}$ is a subfield of $\boldsymbol{K}$.

Proof. We set $A(0) = \{0\}$ and $A(1) = \{1\}$, so $0, 1 \in \widetilde{\boldsymbol{K}}$. If $r \in \widetilde{\boldsymbol{K}}$ then $-r \in \widetilde{\boldsymbol{K}}$, to see this we set $A(-r) = \{0, -r\} \cup A(r)$. If $r \in \widetilde{\boldsymbol{K}} \setminus \{0\}$ then $r^{-1} \in \widetilde{\boldsymbol{K}}$, to see this we set $A(r^{-1}) = \{1, r^{-1}\} \cup A(r)$. If $r_1, r_2 \in \widetilde{\boldsymbol{K}}$ then $r_1 + r_2 \in \widetilde{\boldsymbol{K}}$, to see this we set $A(r_1 + r_2) = \{r_1 + r_2\} \cup A(r_1) \cup A(r_2)$. If $r_1, r_2 \in \widetilde{\boldsymbol{K}}$ then $r_1 \cdot r_2 \in \widetilde{\boldsymbol{K}}$, to see this we set $A(r_1 \cdot r_2) = \{r_1 \cdot r_2\} \cup A(r_1) \cup A(r_2)$. □

Theorem 1

$\widetilde{\boldsymbol{K}} = \{x \in \boldsymbol{K} :$ $\{x\}$ *is existentially first-order definable in the language of rings without parameters*$\}$.

Proof. Let $r \in \boldsymbol{K}$ be arithmetically fixed, and let $A(r) = \{x_1, ..., x_n\}$ be an arithmetic neighbourhood of r with $x_i \neq x_j$ if $i \neq j$, and $x_1 = r$. We choose all formulae $x_i = 1$ $(i \in \{1, ..., n\})$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$ $(i, j, k \in \{1, ..., n\})$ that are satisfied in $A(r)$. Joining these formulae with conjunctions we get some formula Φ. Let $\mathcal{V}$ denote the set of variables in Φ, $x_1 \in \mathcal{V}$ since otherwise for any $s \in \boldsymbol{K} \setminus \{r\}$ the mapping $f := \mathrm{id}\,(A(r) \setminus \{r\}) \cup \{(r, s)\}$ satisfies conditions (1)-(3) and $f(r) \neq r$. The formula

$$\underbrace{\ldots\ \exists x_i\ \ldots}_{x_i \in \mathcal{V},\ i \neq 1} \quad \Phi$$

is satisfied in $\boldsymbol{K}$ if and only if $x_1 = r$. It proves the inclusion $\subseteq$. We begin the proof of the inclusion $\supseteq$. The proof presented here is formally a proof by induction on the complexity of the formula. We are going to use the following two algorithms.

ALGORITHM 1. In formulae Ψ of the language of rings, negations of atomic subformulae are replaced by atomic formulae. For the language of rings, each negation of an atomic

formula is equivalent to the formula of the form $W(y_1, ..., y_n) \neq 0$, where y_1, ..., y_n variables and $W(y_1, ..., y_n) \in \mathbb{Z}[y_1, ..., y_n]$. The algorithm selects a variable t which does not occur in Ψ, and instead of $W(y_1, ..., y_n) \neq 0$ introduces to Ψ the formula $W(y_1, ..., y_n) \cdot t - 1 = 0$. The received formula features one negation fewer and one variable more.

Algorithm 2. In formulae Ψ of the language of rings, some atomic subformulae are replaced by other atomic formulae or conjunctions of atomic formulae. Atomic subformulae of the form $y_i + y_j = y_k$, $y_i \cdot y_j = y_k$, $y_i = 1$, (y_i, y_j, y_k variables) are left without changes. Atomic subformulae of the form $y_i = 0$ (y_i is a variable) are replaced by $y_i + y_i = y_i$. Operation of the algorithm on other atomic subformulae will be explained on the example of subformula $1 + x + y^2 = 0$, which is replaced by

$$(t = 1) \wedge (t + x = u) \wedge (y \cdot y = z) \wedge (u + z = s) \wedge (s + s = s),$$

where variables t, u, z, s do not occur in Ψ. The above conjunction equivalently presents the condition $1 + x + y^2 = 0$ and is composed solely of the formulae of the form $y_i + y_j = y_k$, $y_i \cdot y_j = y_k$, $y_i = 1$, where y_i, y_j, y_k variables.

We start the main part of the proof. Let $r \in \boldsymbol{K}$, $\Gamma(x, x_1, ..., x_n)$ be a quantifier-free formula of the language of rings, and

$$\{r\} = \{x \in \boldsymbol{K} : \quad \boldsymbol{K} \models \exists x_1 ... \exists x_n \; \Gamma(x, x_1, ..., x_n)\}.$$

We may assume that $\Gamma(x, x_1, ..., x_n)$ has the form $\Lambda_1 \vee ... \vee \Lambda_l$, where each of the formulae Λ_1, ..., Λ_l is the conjunction of atomic formulae and negations of atomic formulae. We want to prove that $r \in \widetilde{\boldsymbol{K}}$. After an iterative application of Algorithm 1 to the formula $\Gamma(x, x_1, ..., x_n)$ we receive a quantifier-free formula $\Omega(x, x_1, ..., x_m)$ for which: $\Omega(x, x_1, ..., x_m)$ has the form $\Xi_1 \vee ... \vee \Xi_l$, and each of the formulae Ξ_1, ..., Ξ_l is the conjunction of atomic formulae, and

$$\{r\} = \{x \in \boldsymbol{K} : \quad \boldsymbol{K} \models \exists x_1 ... \exists x_m \; \Omega(x, x_1, ..., x_m)\},$$

where $m - n$ is the number of negations in the formula $\Gamma(x, x_1, ..., x_n)$. After an iterative application of Algorithm 2 to the formula $\Omega(x, x_1, ..., x_m)$ we receive a quantifier-free formula $\Delta(x, x_1, ..., x_p)$ for which: $\Delta(x, x_1, ..., x_p)$ has the form $\Pi_1 \vee ... \vee \Pi_l$, and each of the formulae Π_1, ..., Π_l is the conjunction of atomic formulae of the form $y_i + y_j = y_k$, $y_i \cdot y_j = y_k$, $y_i = 1$, where y_i, y_j, y_k variables, and

$$\{r\} = \{x \in \boldsymbol{K} : \; \boldsymbol{K} \models \exists x_1 ... \exists x_p \; \Delta(x, x_1, ..., x_p)\}.$$

Since

$$\begin{aligned}\{r\} &= \{x \in \boldsymbol{K} : \quad \boldsymbol{K} \models \exists x_1 ... \exists x_p \; \Delta(x, x_1, ..., x_p)\} \\ &= \bigcup_{i=1}^{l} \Big\{x \in \boldsymbol{K} : \; \boldsymbol{K} \models \underbrace{... \exists x_s ...}_{x_s \in \mathrm{Fr}(\Pi_i) \setminus \{x\}} \; \Pi_i(x, \; ..., \; x_s, \; ...)\Big\},\end{aligned}$$

for some $i \in \{1, ..., l\}$ the condition

$$\{r\} = \Big\{x \in \boldsymbol{K} : \; \boldsymbol{K} \models \underbrace{... \exists x_s ...}_{x_s \in \mathrm{Fr}(\Pi_i) \setminus \{x\}} \; \Pi_i(x, \; ..., \; x_s, \; ...)\Big\}$$

is satisfied. For indices s for which x_s is a variable in Π_i, we choose $w_s \in \boldsymbol{K}$ for which $\boldsymbol{K} \models \Pi_i[x \to r, \ ..., \ x_s \to w_s, \ ...]$. Then $A(r) = \{1, r, ..., w_s, ...\}$ is an arithmetic neighbourhood of r, so $r \in \widetilde{\boldsymbol{K}}$. □

Let $\boldsymbol{K}$ be a field extending $\mathbb{Q}$. R.M. Robinson proved in [12]: if each element of $\boldsymbol{K}$ is algebraic over $\mathbb{Q}$ and $r \in \boldsymbol{K}$ is fixed for all automorphisms of $\boldsymbol{K}$, then there exist $U(y), V(y) \in \mathbb{Q}[y]$ such that $\{r\}$ is definable in $\boldsymbol{K}$ by the formula

$$\exists y \, (U(y) = 0 \land x = V(y))\,.$$

Corollary 2

If a field $\boldsymbol{K}$ extends $\mathbb{Q}$ and each element of $\boldsymbol{K}$ is algebraic over $\mathbb{Q}$, then

$$\widetilde{\boldsymbol{K}} = \bigcap_{\sigma \,\in\, \mathrm{Aut}(\boldsymbol{K})} \{x \in \boldsymbol{K} : \ \sigma(x) = x\}\,.$$

For a more general theorem and its proof, see [9, Proposition 1]. Let $\mathbb{R}^{\rm alg} := \{x \in \mathbb{R} : \ x \text{ is algebraic over } \mathbb{Q}\}$ and $\mathbb{Q}_p^{\rm alg} := \{x \in \mathbb{Q}_p : \ x \text{ is algebraic over } \mathbb{Q}\}$. By Corollary 2, $\widetilde{\mathbb{R}^{\rm alg}} = \mathbb{R}^{\rm alg}$ and $\widetilde{\mathbb{Q}_p^{\rm alg}} = \mathbb{Q}_p^{\rm alg}$. It gives $\widetilde{\mathbb{R}} = \mathbb{R}^{\rm alg}$ and $\widetilde{\mathbb{Q}_p} = \mathbb{Q}_p^{\rm alg}$, see [16].

Theorem 3

Let $\boldsymbol{K}$ be a field extending $\mathbb{Q}$, $\phi(x, x_1, ..., x_n)$ is a quantifier-free formula of the language of rings, and $\boldsymbol{K} \models \exists x \exists x_1 ... \exists x_n \phi(x, x_1, ..., x_n)$. Then there exist a prime number p and $U(y), V(y) \in \mathbb{Q}[y]$ such that

$$\{x \in \mathbb{Q}_p : \quad \mathbb{Q}_p \models \exists x_1 ... \exists x_n \exists y \, (\phi(x, x_1, ..., x_n) \land U(y) = 0 \land x = V(y))\} = \{b\}$$

for some $b \in \mathbb{Q}_p^{\rm alg}$.

Proof. We choose $a, a_1, ..., a_n \in \boldsymbol{K}$ such that $\boldsymbol{K} \models \phi(a, a_1, ..., a_n)$, so $\mathbb{Q}(a, a_1, ..., a_n) \models \exists x \exists x_1 ... \exists x_n \phi(x, x_1, ..., x_n)$. There is a prime number p such that $\mathbb{Q}(a, a_1, ..., a_n)$ embeds in $\mathbb{Q}_p$, see [1, Theorem 1.1 in Chapter 5]. By this, $\mathbb{Q}_p \models \exists x \exists x_1 ... \exists x_n \phi(x, x_1, ..., x_n)$. Since $\mathbb{Q}_p^{\rm alg}$ is an elementary subfield of $\mathbb{Q}_p$ ([10]), there exists $b \in \mathbb{Q}_p^{\rm alg}$ such that $\mathbb{Q}_p^{\rm alg} \models \exists x_1 ... \exists x_n \phi(b, x_1, ..., x_n)$. By Robinson's theorem there exist $U(y), V(y) \in \mathbb{Q}[y]$ such that $\{b\}$ is definable in $\mathbb{Q}_p^{\rm alg}$ by the formula $\exists y \, (U(y) = 0 \land x = V(y))$. Thus,

$$\{x \in \mathbb{Q}_p : \quad \mathbb{Q}_p \models \exists x_1 ... \exists x_n \exists y \, (\phi(x, x_1, ..., x_n) \land U(y) = 0 \land x = V(y))\}$$
$$= \{x \in \mathbb{Q}_p^{\rm alg} : \quad \mathbb{Q}_p^{\rm alg} \models \exists x_1 ... \exists x_n \exists y \, (\phi(x, x_1, ..., x_n) \land U(y) = 0 \land x = V(y))\} = \{b\} \quad \square$$

3. Fields with algebraically closed subfields

We use below "bar" to denote the algebraic closure of a field. It was proved in [16] that $\widetilde{\mathbb{C}} = \mathbb{Q}$. Similarly, $\widetilde{\overline{\mathbb{Q}}} = \mathbb{Q}$.

Theorem 4

If $\boldsymbol{K}$ is a field and some subfield of $\boldsymbol{K}$ is algebraically closed, then $\widetilde{\boldsymbol{K}}$ is the prime field in $\boldsymbol{K}$.

Proof. For any field $\boldsymbol{K}$ of non-zero characteristic $\widetilde{\boldsymbol{K}}$ is the prime field in $\boldsymbol{K}$, see [16]. Let $\mathrm{char}(\boldsymbol{K}) = 0$. We may assume that $\boldsymbol{K}$ extends $\mathbb{Q}$. By the assumption of the theorem $\boldsymbol{K}$ extends $\overline{\mathbb{Q}}$. By the Proposition $\widetilde{\boldsymbol{K}} \supseteq \mathbb{Q}$. We want to prove $\widetilde{\boldsymbol{K}} \subseteq \mathbb{Q}$ in a constructive way without the use of Theorem 1. Let $r \in \widetilde{\boldsymbol{K}}$, and let $A(r) = \{x_1, ..., x_n\}$ be an arithmetic neighborhood of r, $x_i \neq x_j$ if $i \neq j$, and $x_1 = r$. We choose all formulae $x_i = 1$ $(i \in \{1, ..., n\})$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$ $(i, j, k \in \{1, ..., n\})$ that are satisfied in $A(r)$. Joining these formulae with conjunctions we get some formula Φ. Let $\mathcal{V}$ denote the set of variables in Φ, $x_1 \in \mathcal{V}$ since otherwise for any $s \in \boldsymbol{K} \setminus \{r\}$ the mapping $f := \mathrm{id}\,(A(r) \setminus \{r\}) \cup \{(r, s)\}$ satisfies conditions (1)-(3) and $f(r) \neq r$. Since $A(r)$ is an arithmetic neighbourhood of r, the formula

$$\underbrace{... \exists x_i ...}_{x_i \in \mathcal{V},\ i \neq 1} \quad \Phi \tag{4}$$

is satisfied in $\boldsymbol{K}$ if and only if $x_1 = r$. Since $\overline{\boldsymbol{K}}$ extends $\boldsymbol{K}$,

$$\overline{\boldsymbol{K}} \models \underbrace{... \exists x_i ...}_{x_i \in \mathcal{V},\ i \neq 1} \quad \Phi[x_1 \to r]$$

$\overline{\mathbb{Q}}$ is an elementary subfield of $\overline{\boldsymbol{K}}$ ([6, p. 306]), so there exists $r_1 \in \overline{\mathbb{Q}}$ satisfying

$$\overline{\mathbb{Q}} \models \underbrace{... \exists x_i ...}_{x_i \in \mathcal{V},\ i \neq 1} \quad \Phi[x_1 \to r_1] \tag{5}$$

$\boldsymbol{K}$ extends $\overline{\mathbb{Q}}$, so by (4) there is a unique $r_1 \in \overline{\mathbb{Q}}$ satisfying (5) and this r_1 equals r. Thus, $r \in \overline{\mathbb{Q}}$ and the formula

$$\underbrace{... \exists x_i ...}_{x_i \in \mathcal{V},\ i \neq 1} \quad \Phi$$

is satisfied in $\overline{\mathbb{Q}}$ if and only if $x_1 = r$. Hence $r \in \widetilde{\overline{\mathbb{Q}}} = \mathbb{Q}$. □

Corollary 5

Let $\boldsymbol{K}$ be an arbitrary field. Then no subfield of $\widetilde{\boldsymbol{K}}$ is algebraically closed.

Theorem 6

If a field $\boldsymbol{K}$ extends $\mathbb{Q}$ and $r \in \widetilde{\boldsymbol{K}}$, then $\{r\}$ is definable in $\boldsymbol{K}$ by a formula of the form $\exists x_1 ... \exists x_m T(x, x_1, ..., x_m) = 0$, where $m \in \{1, 2, 3, ...\}$ and $T(x, x_1, ..., x_m) \in \mathbb{Z}[x, x_1, ..., x_m]$.

Proof. From the definition of $\widetilde{\boldsymbol{K}}$ it follows that $\{r\}$ is definable in $\boldsymbol{K}$ by a finite system **(S)** of polynomial equations of the form $x_i + x_j - x_k = 0$, $x_i \cdot x_j - x_k = 0$, $x_i - 1 = 0$, cf. the proof of the inclusion $\subseteq$ inside the proof of Theorem 1. If $\overline{\mathbb{Q}} \subseteq$

$\boldsymbol{K}$, then by Theorem 4 each element of $\widetilde{\boldsymbol{K}}$ is definable in $\boldsymbol{K}$ by a single equation $w_1 \cdot x + w_0 = 0$, where $w_0 \in \mathbb{Z}$, $w_1 \in \mathbb{Z} \setminus \{0\}$. If $\overline{\mathbb{Q}} \not\subseteq \boldsymbol{K}$, then there exists a polynomial

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x] \qquad (n \geq 2,\ a_n \neq 0)$$

having no root in $\boldsymbol{K}$. By this, the polynomial

$$B(x,y) := a_n x^n + a_{n-1} x^{n-1} y + ... + a_1 x y^{n-1} + a_0 y^n$$

satisfies

$$\forall u, v \in \boldsymbol{K}\ ((u = 0 \land v = 0) \Longleftrightarrow B(u,v) = 0)\,, \tag{6}$$

see [3, pp. 363–364] and [14, p. 108], cf. [2, p. 172]. Applying (6) to **(S)** we obtain that **(S)** is equivalent to a single equation $T(x, x_1, ..., x_m) = 0$, where $m \in \{1,2,3,...\}$ and $T(x, x_1, ..., x_m) \in \mathbb{Z}(x, x_1, ..., x_m)$. □

Theorem 6 remains true if $\mathrm{char}(\boldsymbol{K}) = p \neq 0$. In this case $\widetilde{\boldsymbol{K}}$ is the prime field in $\boldsymbol{K}$ ([16]), so each element of $\widetilde{\boldsymbol{K}}$ is definable by the equation $w_1 \cdot x + w_0 = 0$ for some $w_0 \in \{0, 1, ..., p-1\}$, $w_1 \in \{1, ..., p-1\}$.

4. Transcendental elements in finitely generated fields

It is known ([7]) that for any field $\boldsymbol{K}$ there is a function field $\boldsymbol{F}/\boldsymbol{K}$ in one variable containing elements that are transcendental over $\boldsymbol{K}$ and first-order definable in the language of rings with parameters from $\boldsymbol{K}$. We present similar results with quite different proofs.

Theorem 7

Let w be transcendental over $\mathbb{Q}$ and a field $\boldsymbol{K}$ be finitely generated over $\mathbb{Q}(w)$. Let $g(x,y) \in \mathbb{Q}[x,y]$, there exists $z \in \boldsymbol{K}$ with $g(w,z) = 0$, and the equation $g(x,y) = 0$ defines an irreducible algebraic curve of genus greater than 1. We claim that some element of $\widetilde{\boldsymbol{K}}$ is transcendental over $\mathbb{Q}$.

Proof. By Faltings' finiteness theorem ([4], cf. [8, p. 12], formerly Mordell's conjecture) the set

$$P := \{u \in \boldsymbol{K} :\ \ \exists s \in \boldsymbol{K}\ g(u,s) = 0\}$$

is finite, $w \in P$. Let $P = \{u_1, ..., u_n\}$, $u_i \neq u_j$ if $i \neq j$, and

$$t_k(x_1, ..., x_n) := \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} x_{i_1} x_{i_2} ... x_{i_k} \qquad (k \in \{1, ..., n\})$$

denote the basic symmetric polynomials. We claim that

$$t_1(u_1, ..., u_n), ..., t_n(u_1, ..., u_n) \in \widetilde{\boldsymbol{K}} \tag{7}$$

and $t_i(u_1, ..., u_n)$ is transcendental over $\mathbb{Q}$ for some $i \in \{1, ..., n\}$. We want to prove (7) in a constructive way without the use of Theorem 1. To prove (7) we choose $z_k \in \boldsymbol{K}$ $(k \in \{1, ..., n\})$ that satisfy $g(u_k, z_k) = 0$. There exist $m \in \{1,2,3,...\}$ and

$$h : \{0, ..., m\} \times \{0, ..., m\} \to W(m) := \{0\} \cup \left\{\frac{c}{d} :\ \ c, d \in \{-m, ..., -1, 1, ..., m\}\right\}$$

such that

$$g(x,y) = \sum_{i,j \in \{0,...,m\}} h(i,j) \cdot x^i \cdot y^j \,.$$

Let

$$M_k := \{u_{i_1} u_{i_2} ... u_{i_k} : \;\; 1 \le i_1 < i_2 < ... < i_k \le n\} \qquad (k \in \{1,...,n\})$$

$$N := \left\{ b \cdot u_k^i \cdot z_k^j : \;\; b \in W(m), \; i,j \in \{0,...,m\}, \; k \in \{1,...,n\} \right\}$$

$$T := \left\{ \sum_{a \in S} a : \; \emptyset \neq S \subseteq N \cup \bigcup_{k=1}^{n} M_k \right\}$$

$$\cup \left\{ u_i - u_j, \frac{1}{u_i - u_j} : \;\; i,j \in \{1,...,n\}, \; i \neq j \right\}.$$

Since $M_k \subseteq T$ for each $k \in \{1,...,n\}$,

$$t_k(u_1,...,u_n) = \sum_{a \in M_k} a \in T$$

for each $k \in \{1,...,n\}$. We claim that T is an arithmetic neighbourhood of $t_k(u_1,...,u_n)$ for each $k \in \{1,...,n\}$. To prove it assume that $f : T \to \boldsymbol{K}$ satisfies conditions (1)-(3). Since $T \supseteq N \supseteq W(m)$, f is the identity on $W(m)$. For any $k \in \{1,...,n\}$ and any non-empty $L \subsetneq \{0,...,m\} \times \{0,...,m\}$ the elements

$$\sum_{(i,j) \in L} h(i,j) \cdot u_k^i \cdot z_k^j$$

and

$$\sum_{(i,j) \in (\{0,...,m\} \times \{0,...,m\}) \setminus L} h(i,j) \cdot u_k^i \cdot z_k^j$$

belong to T. By these facts and by induction

$$0 = f(0) = f(g(u_k, z_k)) = f\left(\sum_{i,j \in \{0,...,m\}} h(i,j) \cdot u_k^i \cdot z_k^j \right)$$

$$= \sum_{i,j \in \{0,...,m\}} f\left(h(i,j) \cdot u_k^i \cdot z_k^j\right) = \sum_{i,j \in \{0,...,m\}} h(i,j) \cdot f(u_k)^i \cdot f(z_k)^j = g(f(u_k), f(z_k))$$

for any $k \in \{1,...,n\}$. Thus, $f(u_k) \in P$ for each $k \in \{1,...,n\}$. Since

$$1 = f(1) = f\left((u_k - u_l) \cdot \frac{1}{u_k - u_l} \right) = (f(u_k) - f(u_l)) \cdot f\left(\frac{1}{u_k - u_l} \right),$$

we conclude that $f(u_k) \neq f(u_l)$ if $k \neq l$. Therefore, f permutes the elements of $\{u_1,...,u_n\}$. By this,

$$t_k(u_1,...,u_n) = t_k(f(u_1),...,f(u_n)) = \sum_{1 \le i_1 < i_2 < ... < i_k \le n} f(u_{i_1}) f(u_{i_2}) ... f(u_{i_k})$$

$$= \sum_{1 \le i_1 < i_2 < ... < i_k \le n} f(u_{i_1} u_{i_2} ... u_{i_k}) = f\left(\sum_{1 \le i_1 < i_2 < ... < i_k \le n} u_{i_1} u_{i_2} ... u_{i_k} \right)$$

$$= f(t_k(u_1,...,u_n))$$

for any $k \in \{1,...,n\}$. We have proved that T is an arithmetic neighbourhood of $t_k(u_1,...,u_n)$ for each $k \in \{1,...,n\}$, so $t_k(u_1,...,u_n) \in \widetilde{\boldsymbol{K}}$ for each $k \in \{1,...,n\}$.

We prove now that $t_i(u_1,...,u_n)$ is transcendental over $\mathbb{Q}$ for some $i \in \{1,...,n\}$. Assume, on the contrary, that all $t_k(u_1,...,u_n)$ $(k \in \{1,...,n\})$ are algebraic over $\mathbb{Q}$. Since $u_1,...,u_n$ are the roots of the polynomial

$$x^n - t_1(u_1,...,u_n)x^{n-1} + t_2(u_1,...,u_n)x^{n-2} - ... + (-1)^n t_n(u_1,...,u_n),$$

we conclude that $u_1,...,u_n$ are also algebraic over $\mathbb{Q}$. It is impossible, because among elements $u_1,...,u_n$ is w that is transcendental over $\mathbb{Q}$. □

In the proof of Theorem 7 for each $k \in \{1,...,n\}$ the set $\{t_k(u_1,...,u_n)\}$ is existentially $\emptyset$-definable in $\boldsymbol{K}$ by the formula $\exists u_1 \exists s_1 ... \exists u_n \exists s_n$

$$(g(u_1,s_1)=0 \wedge ... \wedge g(u_n,s_n)=0 \ \wedge \ \underbrace{... \wedge u_i \neq u_j \wedge ...}_{1 \le i<j \le n} \ \wedge \ v = t_k(u_1,...,u_n)) \qquad (8)$$

Applying Theorem 1 we obtain $t_k(u_1,...,u_n) \in \widetilde{\boldsymbol{K}}$ for each $k \in \{1,...,n\}$, unfortunately, without a direct description of any arithmetic neighbourhood of $t_k(u_1,...,u_n)$. This gives a non-constructive proof of Theorem 7.

Formula (8) has a form

$$\exists u_1 \exists s_1 ... \exists u_n \exists s_n \phi(v,u_1,s_1,...,u_n,s_n),$$

where $\phi(v,u_1,s_1,...,u_n,s_n)$ is quantifier-free. By Theorem 3 there exist a prime number p and $U(y), V(y) \in \mathbb{Q}[y]$ such that the formula

$$\exists u_1 \exists s_1 ... \exists u_n \exists s_n \exists y \, (\phi(v,u_1,s_1,...,u_n,s_n) \wedge U(y)=0 \wedge v = V(y))$$

defines in $\mathbb{Q}_p$ an element that is algebraic over $\mathbb{Q}$.

The proof of Theorem 7 gives an element of $\widetilde{\boldsymbol{K}}$ that is transcendental over $\mathbb{Q}$. Let $\boldsymbol{K}$ be a field extending $\mathbb{Q}$ and $v \in \widetilde{\boldsymbol{K}}$ is transcendental over $\mathbb{Q}$. Since $\widetilde{\boldsymbol{K}}$ is a subfield of $\boldsymbol{K}$, $\mathbb{Q}(v) \setminus \mathbb{Q} \subseteq \widetilde{\boldsymbol{K}}$. Obviously, each element of $\mathbb{Q}(v) \setminus \mathbb{Q}$ is transcendental over $\mathbb{Q}$.

There exists a function field $\boldsymbol{K}/\mathbb{Q}$ in one variable such that

$$\widetilde{\boldsymbol{K}} = \boldsymbol{K} \supsetneq \mathbb{Q} = \{x \in \boldsymbol{K} : \ x \text{ is algebraic over } \mathbb{Q}\}.$$

It follows from Proposition 3 in [9].

Theorem 7 admits a more general form. Let the fields $\boldsymbol{K}$ and $\boldsymbol{L}$ be finitely generated over $\mathbb{Q}$ such that $\boldsymbol{L}$ extends $\boldsymbol{K}$. Let $w \in \boldsymbol{L}$ be transcendental over $\boldsymbol{K}$, $g(x,y) \in \mathbb{Q}[x,y]$, there exists $z \in \boldsymbol{L}$ with $g(w,z)=0$, and the equation $g(x,y)=0$ defines an irreducible algebraic curve of genus greater than 1. Analogously as in the proof of Theorem 7 we conclude that there is an element of $\widetilde{\boldsymbol{L}}$ that is transcendental over $\boldsymbol{K}$.

Let p be a prime number, $\mathbb{R}(x,y)$ $(\mathbb{Q}_p(x,y))$ denote the function field defined by $px^4+p^2y^4=-1$. The genus of the extension $\mathbb{R}(x,y)/\mathbb{R}$ $(\mathbb{Q}_p(x,y)/\mathbb{Q}_p)$ is greater than 1. By the results in [7, p. 952, item 3 inside the proof of Theorem 1] the sets

$$\{(u,v) \in \mathbb{R}(x,y) \times \mathbb{R}(x,y) : \ \ pu^4 + p^2v^4 = -1\} \setminus \{(u,v) \in \mathbb{R} \times \mathbb{R} : \ \ pu^4 + p^2v^4 = -1\}$$

$$\{(u,v) \in \mathbb{Q}_p(x,y) \times \mathbb{Q}_p(x,y) : \ \ pu^4 + p^2v^4 = -1\} \setminus \{(u,v) \in \mathbb{Q}_p \times \mathbb{Q}_p : pu^4 + p^2v^4 = -1\}$$

are finite. Since

$$\{(u,v) \in \mathbb{R} \times \mathbb{R} : \ \ pu^4 + p^2v^4 = -1\} = \emptyset$$

and

$$\{(u,v) \in \mathbb{Q}_p \times \mathbb{Q}_p : \ \ pu^4 + p^2v^4 = -1\} = \emptyset,$$

the sets

$$\{(u,v) \in \mathbb{R}(x,y) \times \mathbb{R}(x,y) : \ \ pu^4 + p^2v^4 = -1\}$$

and

$$\{(u,v) \in \mathbb{Q}_p(x,y) \times \mathbb{Q}_p(x,y) : \ \ pu^4 + p^2v^4 = -1\}$$

are finite. Analogously as in the proof of Theorem 7 we conclude that there is an element of $\widetilde{\mathbb{R}(x,y)}$ ($\widetilde{\mathbb{Q}_p(x,y)}$) that is transcendental over $\mathbb{R}$ ($\mathbb{Q}_p$).

5. Recursively defined transcendentals in function fields over archimedean pythagorean fields

A real number r is called recursively approximable, if there exists a computable sequence of rational numbers which converges to r, see [17]. Let $\omega := \{0,1,2,...\}$, $\boldsymbol{K}$ be a subfield of $\mathbb{R}$. $\boldsymbol{K}$ is said to be Pythagorean if

$$\forall x \in \boldsymbol{K} \ (0 \leq x \Rightarrow \exists y \in \boldsymbol{K} \ \ x = y^2)\,.$$

Our next theorem is inspired by Cherlin's example in [7, p. 949].

Theorem 8

If $\boldsymbol{K}$ is a Pythagorean subfield of $\mathbb{R}$, t is transcendental over $\boldsymbol{K}$, and $r \in \boldsymbol{K}$ is recursively approximable, then $\{r\}$ is ∅-definable in $(\boldsymbol{K}(t), +, \cdot, 0, 1)$.

Proof. It follows from [13, p. 280] that there is a formula $\mathcal{N}(x)$ in the language of rings such that

$$\{x \in \boldsymbol{K}(t) : \ \boldsymbol{K}(t) \models \mathcal{N}(x)\} = \omega\,. \tag{9}$$

Let $\mathcal{M}(x)$ abbreviate $\exists y \ 1 + x^4 = y^2$. It is known that

$$\{x \in \boldsymbol{K}(t) : \ \boldsymbol{K}(t) \models \mathcal{M}(x)\} = \boldsymbol{K},$$

for the proof see [6, p. 34]. Assume that $r \geq 0$, the proof in case $r \leq 0$ goes analogically. There exist recursive functions $f : \omega \to \omega$ and $g : \omega \to \omega \setminus \{0\}$ such that $\lim\limits_{n\to\infty} \frac{f(n)}{g(n)} = r$. Since f and g are recursive there exist formulae $F(s,t)$ and $G(s,t)$ (both in the language of rings) for which

$$\forall n, m \in \omega \ (m = f(n) \Longleftrightarrow \omega \models F(n,m))$$

and

$$\forall n, m \in \omega \ (m = g(n) \Longleftrightarrow \omega \models G(n,m))$$

By (9) we can find formulae $\widetilde{F}(s,t)$ and $\widetilde{G}(s,t)$ for which

$$\forall s, t \in \boldsymbol{K}(t) \ ((s \in \omega \wedge t \in \omega \wedge t = f(s)) \Longleftrightarrow \boldsymbol{K}(t) \models \widetilde{F}(s,t))$$

and

$$\forall s, t \in \boldsymbol{K}(t) \ ((s \in \omega \wedge t \in \omega \wedge t = g(s)) \Longleftrightarrow \boldsymbol{K}(t) \models \widetilde{G}(s,t)\,.$$

Let $a < b$ abbreviate

$$a \neq b \wedge \mathcal{M}(a) \wedge \mathcal{M}(b) \wedge \exists c \ (\mathcal{M}(c) \wedge a + c^2 = b)\,.$$

The formula

$$\begin{aligned}\mathcal{M}(x) \wedge \forall \varepsilon \ (0 < \varepsilon \Rightarrow \exists z \exists s \exists u \exists v \ (z \neq x \ \wedge \ x < z + \varepsilon \ \wedge \ z < x + \varepsilon \ \wedge \\ \mathcal{N}(s) \wedge \mathcal{N}(u) \wedge \mathcal{N}(v) \wedge \widetilde{F}(s,u) \wedge \widetilde{G}(s,v) \wedge z \cdot v = u))\end{aligned}$$

defines r in $(\boldsymbol{K}(t), +, \cdot, 0, 1)$. □

Let $\mathcal{L}$ be an elementary language, let M be an $\mathcal{L}$-structure, and let U be an n-ary relation on M. We say that U is implicitly $\emptyset$-definable in M if there exists a sentence Φ in the language $\mathcal{L} \cup \{\mathcal{U}\}$ with an additional n-ary predicate symbol $\mathcal{U}$, such that for all n-ary relations U^* on M, $(M, U^*) \models \Phi$ if and only if $U^* = U$, see the introductory part of [5].

Theorem 9

If a real number r is recursively approximable, then $\{r\}$ is existentially $\emptyset$-definable in $(\mathbb{R}, +, \cdot, 0, 1, U)$ for some unary predicate U which is implicitly $\emptyset$-definable in $(\mathbb{R}, +, \cdot, 0, 1)$.

Proof. If r is a rational number then $\{r\}$ is existentially $\emptyset$-definable in $(\mathbb{R}, +, \cdot, 0, 1)$. At this moment we assume that r is an irrational number. We may assume without loss of generality that $r < 0$, so there exists an integer $i < r$. There exist recursive functions $f : \omega \to \omega$ and $g : \omega \to \omega \setminus \{0\}$ such that $\lim\limits_{n \to \infty} -\frac{f(n)}{g(n)} = r$, we may assume without loss of generality that $-\frac{f(n)}{g(n)} \in (i, 0)$ for each $n \in \omega$. Since f and g are recursive, there exist formulae $F(s,t)$ and $G(s,t)$ (both in the language of rings) for which

$$\forall n, m \in \omega \ (m = f(n) \Longleftrightarrow \omega \models F(n,m))$$

and

$$\forall n, m \in \omega \ (m = g(n) \Longleftrightarrow \omega \models G(n,m))\,.$$

Let

$$U := \{r + i\} \cup \{-\frac{f(n)}{g(n)} : \quad n \in \omega\} \cup \omega$$

and $\mathcal{U}$ be a unary predicate symbol for membership in U. Let $x \leq y$ abbreviate

$$\exists s \ x + s^2 = y,$$

$x < y$ abbreviate

$$x \leq y \wedge x \neq y,$$

$\mathrm{succ}(x, y)$ abbreviate

$$x < y \wedge \mathcal{U}(x) \wedge \mathcal{U}(y) \wedge \forall z \ ((x < z \wedge z < y) \Rightarrow \neg\mathcal{U}(z)),$$

$\mathrm{accum}(x)$ abbreviate

$$\forall \varepsilon \ (0 < \varepsilon \Rightarrow \exists z \ (z \neq x \wedge x < z + \varepsilon \wedge z < x + \varepsilon \wedge \mathcal{U}(z)))\,.$$

We have:

$$\forall x \in \mathbb{R} \ (x \in \omega \Longleftrightarrow \mathbb{R} \models (0 \leq x \wedge \mathcal{U}(x)))\,.$$

Therefore, extending the language of rings with predicate symbol $\mathcal{U}$ for membership in U we can find formulae $\widetilde{F}(s, t)$ and $\widetilde{G}(s, t)$ for which

$$\forall s, t \in \mathbb{R} \ ((s \in \omega \wedge t \in \omega \wedge t = f(s)) \Longleftrightarrow \mathbb{R} \models \widetilde{F}(s, t))$$

and

$$\forall s, t \in \mathbb{R} \ ((s \in \omega \wedge t \in \omega \wedge t = g(s)) \Longleftrightarrow \mathbb{R} \models \widetilde{G}(s, t))\,.$$

The sentence

$$\begin{gathered}
\mathcal{U}(0) \wedge \forall x \ ((0 \leq x \wedge \mathcal{U}(x)) \Rightarrow \mathrm{succ}(x, x+1)) \\
\wedge \forall x \ ((0 \leq x + \underbrace{1 + ... + 1}_{|i|-\text{times}} \wedge \ x < 0) \Longleftrightarrow \exists s \exists u \exists v \\
(0 \leq s \wedge \mathcal{U}(s) \wedge 0 \leq u \wedge \mathcal{U}(u) \wedge 0 \leq v \wedge \mathcal{U}(v) \wedge \widetilde{F}(s, u) \wedge \widetilde{G}(s, v) \wedge u + x \cdot v = 0)) \\
\wedge \forall x \ ((0 < x + \underbrace{1 + ... + 1}_{2|i|-\text{times}} \ \wedge \ x + \underbrace{1 + ... + 1}_{|i|-\text{times}} < 0) \\
\Rightarrow (\mathcal{U}(x) \Longleftrightarrow \mathrm{accum}(x + \underbrace{1 + ... + 1}_{|i|-\text{times}}))) \\
\wedge \forall x \ (x + \underbrace{1 + ... + 1}_{2|i|-\text{times}} \leq 0 \Rightarrow \neg\mathcal{U}(x))
\end{gathered}$$

is valid in $\mathbb{R}$ if and only if $\mathcal{U}(x)$ means $x \in U$, so U is implicitly ∅-definable in $\mathbb{R}$. The formula

$$\exists t \exists y \ (x + t^2 = 0 \wedge x = y + \underbrace{1 + ... + 1}_{|i|-\text{times}} \ \wedge \ \mathcal{U}(y))$$

defines r in $(\mathbb{R}, +, \cdot, 0, 1, U)$. □

Acknowledgement. The author wishes to thank the anonymous referee for valuable suggestions.

References

1. J.W.S. Cassels, *Local Fields*, London Mathematical Society Student Texts 3, Cambridge University Press, Cambridge, 1986.

2. D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag, New York, 1997.
3. M. Davis, Y. Matijasevič, and J. Robinson, Hilbert's tenth problem, Diophantine equations: positive aspects of a negative solution, *Mathematical developments arising from Hilbert problems*, Proc. Sympos. Pure Math. **28**, Part 2, Amer. Math. Soc. 323–378, 1976; reprinted in: The collected works of Julia Robinson, Amer. Math. Soc. 269–324, 1996.
4. G. Faltings, Endlichkeitssätze für abelsche varietäten über zahlkörpern, *Invent. Math.* **73** (1983), 349–366.
5. K. Fukuzaki and A. Tsuboi, Implicit definability of subfields, *Notre Dame J. Formal Logic* **44** (2003), 217–225.
6. C.U. Jensen and H. Lenzing, *Model Theoretic Algebra: with Particular Emphasis on Fields, Rings, Modules*, Gordon and Breach Science Publishers, New York, 1989.
7. J. Koenigsmann, Defining transcendentals in function fields, *J. Symbolic Logic* **67** (2002), 947–956.
8. S. Lang, *Number Theory III: Diophantine Geometry*, Encyclopaedia of Mathematical Sciences **60**, Springer-Verlag, Berlin, 1991.
9. G. Lettl, Finitely arithmetically fixed elements of a field, 9 pages, to appear in *Arch. Math. (Basel)*, Presented at 70th Workshop on General Algebra, Institute of Discrete Mathematics and Geometry, Vienna University of Technology, May 26–29, 2005.
10. A. Macintyre, Twenty years of p-adic model theory, *Logic Colloquium '84 (Manchester, 1984), 121–153*, Stud. Logic Found. Math., 120, North-Holland, Amsterdam, 1986.
11. B. Poizat, *A Course in Model Theory: An Introduction to Contemporary Mathematical Logic*, Springer-Verlag, New York, 2000.
12. R.M. Robinson, Arithmetical definability of field elements, *J. Symbolic Logic* **16** (1951), 125–126.
13. R.M. Robinson, The undecidability of pure transcendental extensions of real fields, *Z. Math. Logik Grundlagen Math.* **10** (1964), 275–282.
14. A. Shlapentokh, Hilbert's tenth problem over number fields, a survey, *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, 107–137, Contemp. Math., 270, Amer. Math. Soc., Providence, RI, 2000.
15. L. Svenonius, A theorem on permutations in models, *Theoria (Lund)* **25** (1959), 173–178.
16. A. Tyszka, A discrete form of the theorem that each field endomorphism of $\mathbb{R}$ ($\mathbb{Q}_p$) is the identity, *Aequationes Math.* **71** (2006), 100–108.
17. X. Zheng, Recursive approximability of real numbers, *MLQ Math. Log. Q.* **48** (2002), 131–156.