Some Undecidable Field Theories

Martin Ziegler

Introduction

We will construct in this paper a sequence of fields, in each of which the ring of integers can be interpreted.[1]

As consequences we obtain:

A finitely axiomatizable theory, which has [either[2]] an algebraically closed field, $\mathbf{R}$(the field of real numbers) or one of the p-adic fields $\mathbf{Q_p}$, as a model, is undecidable. In particular we have: (case $\mathbf{R}$)

The theory of Euclidean fields is undecidable.

The theory of Pythagorean fields is undecidable.

(A formally-real field is *Euclidean*, if each of its elements is either a square or the negative of a square, and *Pythagorean*, if each sum of squares is a square.)

The question of the decidability of Euclidean fields was posed by Tarski in 1950. ([T]). The case $\mathbf{R}$ of our theorem stated above was conjectured in [T].

Tarski's problem was until now treated on by K. Hauschild ([H1]), ([H2]). His proof for the undecidability of Pythagorean fields is however mistaken and irreparable (see [C], [F]). Our construction adapts a fundamental idea of Hauschild's: "q-th roots",

I thank A. Prestel and U. Henschel for their support.

1 Discussion of the results

Let F_p be the field with p elements. Let L_p be the algebraic closure of the rational function field $F_p[t]$.

We show in sections 2-5 the

Theorem 1 *Let q be a prime number, A a countable structure, L one of the fields L_p with $p \neq q$, $\mathbf{C}$, $\mathbf{R}$, or $\mathbf{Q_p}$. There there exists a field $K \subset L$ such that*

(1) A can be interpreted [defined] in K

(2) If the intermediate field $H \subset L$ is finite over K, then the degree $[H : K]$ is equal to 1 or divisible by q.

If L has characteristic 0 and $A = (\mathbf{Z}, +, \cdot)$, then $\mathbf{Z}$ is a definable subset of K.

Corollary 1 *Every finite subtheory of the theory of L is undecidable.*

[1] Beeson (translator): I think he means "defined", but he says "interpreted". All footnotes in this paper have been inserted by the translator–there are no footnotes in the original. My apologies for the defects of the translation. I am not a native speaker of German.

[2] phrases in brackets, like this one, were inserted by Beeson and are not present in the original.

Proof [of the corollary]. Let T be a finite subtheory of $Th(L)$. Let P be the set of all primes different from the characteristic of L. For each $q \in P$, we choose [by the theorem] a field K_q for which (2) holds and in which $(\mathbf{Z}, +, \cdot)$ is interpretable. We choose a non-principal ultrafilter U on P. Define

$$K = \frac{\prod_{q \in P} K_q}{U}.$$

Then K is relatively algebraically closed in K^P/U.[3]

From this it follows that $K \equiv L$.[4] (The theory and model theory of algebraically closed, real-closed, and p-adically closed fields that we have used here can be found in [CK], [M], [K], [AK].)

K is therefore a model of T. Consequently also one of the fields K_q is a model of T, since T is finite. T thus has a model, in which the ring of whole numbers is interpretable. Then the conclusion follows from [TMR].

In order to derive further consequences from our theorem, we define a sequence of elementary theories. The verification that these theories really are "elementary" is left to the reader. (One observes that the "p-valuation" in models of $T^H_{p,q}$ is elementarily definable.)

$T^A_{p,q}$ = the theory of fields of characteristic p, in which the degree of each irreducible polynomial is 1 or divisible by q. (p is prime or 0.)

T^R_Z = the theory of formally real fields, in which the degree of each irreducible polynomial is 1 or even.

T^R_q = the theory of formally real fields such that

(a) the degree of each irreducible polynomial, that has a zero in a formally real extension, is 1 or divisible by q.

(b) the field is closed in its real closure ($q \neq 2$).

$T^H_{p,q}$ = the theory of formal p-adic fields such that

(a) the degree of each irreducible polynomial, that has a zero in a formally p-adic extension, is 1 or divisible by q.

(b) the field is closed in its p-adic closure ($q \neq 2$).

One can easily verify that each of these theories (whereby for $T^A_{p,q}$ we still assume $p \neq q$) has one of the fields K given in the theorem [sic] as a model.[5]

Corollary 2 *The theories $T^A_{p,q}(p \neq q)$, T^R_q, $T^H_{p,q}$ are undecidable.*

Without proof we append a sequence of remarks:

Each finite theory that has one of the mentioned fields L as a model, is for sufficiently large q a subtheory of one of theories $T^A_{p,q}$, T^R_q, T^H_q [sic][6] The theory of euclidean fields is contained in T^R_q for $q \neq 2$.

A field K of characteristic p is a model of $T^A_{p,q}$ if and only if each polynomial in $K[X]$ whose degree is not divisible by q has a zero in K, if and only if the degree of each finite extension of K is a power of q.

---

[3]The original has a typo K^p/U, but what is meant here is the ultrapower $K^P/U = \frac{\prod_{u \in U} K}{U}$. Here is the proof: Given a polynomial $f \in K[x]$, which has a root $\alpha \in \prod_{p \in U} L$, we have to show that $\alpha_p \in K_p$ except for finitely many p. If $\alpha \notin K_p$ then $[K_p[\alpha_p] : K_p$ is divisible by p. This can happen only for those finitely many p that divide the degree of f.

[4]He means by $\equiv$, elementary equivalence.

[5]It is not clear what is meant by "one of the fields K given in the theorem as a model." The theories under discussion are not finitely axiomatizable, so he is not attempting to derive this from the previous corollary, but from the theorem itself.

[6]T^H_q has not been defined, only $T^H_{p,q}$.

A formally real field is a model of T_2^R if and only each each polynomial of odd degree has a zero, if and only if each formally real extension is a power of 2. [7]

Suppose $(R, <)$ is closed in a real closed field $(L, <)$. Then R is a model of T_q^R if and only if the degree of each irreducible polynomial with alternating signs is equal to 1 or is divisible by q.

Suppose that the valued field (H, w) is closed in the p-adically closed field (L, v) with $w \subset v$. Then H is a model of $T_{p,q}^H$ if and only if the degree of each irreducible polynomial fulfilling the hypotheses of Hensel's lemma is either 1 or divisible by q.

Open Questions:

$T_{q,q}^A$ is a subtheory of the (decidable) theory of separable closed fields of characteristic q (see [E]). Is either $T_{q,q}^A$ or $T_{q,q}^A + \forall x \exists y\ y^q = x$ decidable?

For $q_1 \neq q_2$, $T_{p,q_1}^A + T_{p,q_2}^A$ is the theory of algebraically closed fields of characteristic p. For $q \neq 2$, $T_2^R + T_q^R$ is the theory of real closed fields. For different q_i, $n \geq 1$, are the theories $T_{p,q_0}^H + \ldots + T_{p,q_n}^H$ and $(q_i \neq 2)$ $T_{q_0}^R + \ldots T_{q_n}^R$ decidable?

K is essentially quadratically closed, when each algebraic extension of K is quadratically closed. The theory of essentially quadratically closed fields of characteristic p is, as a subtheory of $T_{p,q}^A$ for $q \neq 2$, undecidable. Is the theory of essentially euclidean fields decidable?

2 Construction of M

From now on, we fix q, A, and L as in the hypotheses of the theorem. Let F be the relative algebraic closure of the prime field of L.

Lemma 0 *There is a subset M of F, such that A is interpretable in (F, M) and*
(3) $0 \in M$; the index of M considered as an additive subgroup of F is infinite.

Proof. First we remark that F is an infinite extension of its prime field. In the case that $A = (\mathbf{Z}, +, \cdot)$ and L has characteristic 0, take $M = \mathbf{Z}$ [and the proof is finished]. Otherwise we can assume that $A = (A, R)$, with R symmetric and irreflexive, because each structure can be interpreted in a graph. Let A be enumerated without repetition as $a_0, a_1, \ldots$. Consider F as a vector space over its prime field. Let $B = b_0, b_1, \ldots$ be a basis of an infinite-dimensional subspace of infinite codimension. Define S by $S(b_i, b_j)$ if and only if $R(a_i, a_j$. Then $(A, R) \cong (B, S)$. Let c_1 and c_2 be linearly independent over B. We now define

$$\begin{aligned} M &= \{0\} \cup B \cup \{c_1 + b_i \mid i \in \mathbf{N}\} \\ &\quad \cup \{c_2 + b_i \mid i \in \mathbf{N}\} \cup \{b_i + b_j | S(b_i, b_j)\} \end{aligned}$$

Then we can define B and S (with parameters c_1, c_2):

$$\begin{aligned} B &= \{b \in M \mid c_1 + b \in M, c_2 + b \in M\} \\ S &= \{(b, c) \mid b\ \in B, c \in B, b + c \in M, b \neq c\} \end{aligned}$$

[7] He must mean "has degree a power of 2".

3 Construction of K

Let $t \in L$ be transcendent over F. Let $F^* = F - \{0\}$.

We want to construct $K \subset L$ as an algebraic extension of $F(t)$ in such a way that besides (2) we have[8]

$$F = \{a \in K \mid \forall b \in L^q (1 + b \in K^q \wedge a^q + b^{-1} \in K^q \rightarrow b \in K^q)\}$$

and

$$M = \{r \in F \mid \forall r_1, r_2 \in F(r_1 \neq r_2 \& r_1 + r_2 = r \rightarrow (t^q - r_1 \in F^* \cdot K^q \vee t^q - r_2 \in F^* \cdot K^q))\}$$

We will construct K as the union of a sequence

$$F(t) = E_0 \subset E_1 \subset E_2 \subset \ldots \subset L$$

of finite extensions of $F(t)$. In order to control the q-th powers, we choose at the same time a sequence

$$\phi = S_0 \subset S_1 \subset S_2 \ldots$$

of finite subsets $S_i \subset E_i \cap L^q$ with the goal that

$$(K \cap L^q) \backslash K^q = (\cup_{i \in \mathbf{N}} S_i)$$

In order not to make the desired relation between M and $(K \cap L^q) \backslash K^q$ impossible already through the wrong choice of (E_i, S_i), we require for all i that

(4) There is a family $(v_s)_{s \in S_i}$ of valuations $v_s : E_i \rightarrow G_{v_s}$[9] with v_s trivial on F, such that

(4.1) (in G_{v_s}) $v_s(s)$ is not divisible by q, for $s \in S_i$.

(4.2) for all $r_1, r_2 \in F$, $r_1 + r_2 \in M$, $r_1 \neq r_2$:
$\forall s \in S_i q$ divides $v_s(t^q - r_1)$ or $\forall s \in S_i q$ divides $v_s(t^q - r_2)$

We begin with an enumeration $a_0, a_1, \ldots$ of all $a \in L$ that are algebraic over $F(t)$. Each element of this sequence should be repeated infinitely often.

Suppose (E_i, S_i) are already constructed. We distinguish four cases[10]

(Case 1). $i = 4n$. Then there are two subcases.

(a) q divides $[E_i(a_n) : E_i]$. Then define $(E_{i+1}, S_{i+1}) = (E_i, S_i)$.

(b) q does not divide $[E_i(a_n) : E_i]$. Then define $(E_{i+1}, S_{i+1}) = (E_i(a_n), S_i)$.

In the verification of (4) we will use the following lemma.

Lemma 1 *Let H_2 be a finite extension of the field H_1, with q not dividing $[H_2 : H_1]$. Let $v : H_1 \rightarrow G_{v_1}$ be a discrete valuation. Then there is an extension v_2 of v_1 to H_2 with q not dividing $(G_{v_2} : G_{v_1})$.*

[8] The final right parenthesis in the formula is misplaced in the original, but is correctly placed here. The notation L^q means the set of q-th powers of elements of L.

[9] Although G_{v_s} is not defined, it must stand for the value group of the valuation v_s.

[10] Numbering of the cases added by Beeson. The four cases occupy three full pages in the original paper and several lemmas are proved in between the cases of this definition. We retain this latter confusing feature in the interest of accurate translation, but at least we mark the four cases of the definition clearly. The idea is that four successive values of i will be used to deal with each a_n, namely $i = 4n$,$4n+1$, $4n+2$, and $4n+3$. The first value of i (Case 1) will (possibly) add a_n to E_i to get E_{i+1}. The next value of i (Case 2) will either add $\sqrt[q]{a_n}$ to E_i or it will add a_n to S_i, indicating our intention *never* to add $\sqrt[q]{a_n}$ to any E_i in the future. In Cases 3 and 4, we either add the q-th roots of certain quantities to E_i (in Case 3) or we add the quantities themselves to S_i (in Case 4).

Proof. We can assume that H_2 is separable or purely inseparable over H_1. In the separable case we have[11]

$$[H_2 : H_1] = \sum_i (G_{v_2^i} : G_{v_1}) f_i$$

where v_2^i runs over all extensions of v_1 to H_2 and f_i is the degree of the valued quotient field extension. Therefore q cannot divide all the $(G_{v_2}^i : G_{v_1})$.

If H_2 is purely inseparable over H_1, then there is exactly one extension v_2. $(G_{v_2}^i : G_{v_1})$ is a power of p, where $p \neq q$. [That proves the lemma.]

If now the $v_s : E_i \to G_{v_s}$, $s \in S_i$, satisfy (4.1) and (4.2), then we choose extensions $\bar{v}_s : E_{i+1} \to G_{\bar{v}_s}$ with q not dividing $(G_{\bar{v}_s} : G_{v_s})$. The $\bar{v}_s$ for $s \in S_i$ again satisfy (4.1) and (4.2).

(Case 2) $i = 4n + 1$. There are three cases.

(a) $a_n \notin E_i$ or $a_n \notin L^q$. Then we define $(E_{i+1}, S_{i+1}) = (E_i, S_i)$. [End of Case 1a. The next sentence must be meant to apply to both Cases 1b and 1c, although it occurs before the indicated beginning of either case.]

If $a_n \in E_i \cap L^q$. we choose $v_s : E_i \to G_{v_s}$, $s \in S_i$ by (4).

(b) There is some $s \in S_i$ for which q does not divide $v_s(a_n)$. In this case define

$$(E_{i+1}, S_{i+1}) = (E_i, S_i \cup \{a_n\}).$$

Then (4) holds, if we take v_s for v_{a_n}.

(c) q divides all $v_s(a_n)$, $s \in S_i$. We define

$$(E_{i+1}, S_{i+1}) = (E_i(\sqrt[q]{a_n}), S_i),$$

whereby $\sqrt[q]{a_n} \in E_i$ in case $a_n \in E_i^q$. That (4) holds follows from

Lemma 2 *Let q be different from the characteristic of the quotient field (translation?) of the valued field (H, v). Let $a \in H \backslash H^q$ and $v(a)$ divisible by q. Then there exists an extension w of v to $H(\sqrt[q]{a})$ with $G_w = G_v$.*

Proof. First note that $q = [H(\sqrt[q]{a}) : H]$. There is $c \in H$ with $v(c^q) = v(a)$. If the class of $c^q a^{-1}$ in the quotient class field is not a q-th power, then $G_w = G_v$ for all extensions w of v (Gradungleichung). Otherwise the q-th root of $c^q a^{-1}$ lies in the henselian hull of (H, v). We get w through the embedding of $H(\sqrt[q]{a})$ in the henselian hull.

(Case 3) $i = 4n + 2$ There are two cases

(a) $a_n \notin E_i$ or $a_n \in F$. Then we define $(E_{i+1}, S_{i+1}) = (E_i, S_i)$.

(b) $a_n \in E_i \backslash F$.

Then there is a valuation v on E_i, trivial on F, for which $v(a_i)$ is negative. Let (4) be satisfied by $(v_s)_{s \in S_i}$. First we extend E_i to a field E, for which (4.2) holds for $v, v_s, (s \in S_i)$:

If (4.2) already holds in E_i for $v, v_s, (s \in S_i)$, we just take $E = E_i$. Otherwise there must be an $r \in F$ such that q does not divide $v(t^q - r)$ and for all $s \in S_i$, $q \mid v_s(t^q - r)$. One observes: there is at most one $r \in F$, for which q does not divide $v(t^q - r)$. We still need

Lemma 3 *$L = L^q \cdot F$.*

[11] He uses v_2^i as a variable indexed by i. It's a bit strange to use a superscript for an index. One could more conventionally have written w_i.

Proof. Let $a \in L$. We seek $b \in F^*$ with $ab^{-1} \in L^q$.[12] If L is algebraically closed or real-closed, we will find b in $\{1, -1\}$. In case $L = \mathbf{Q_p}$, we note that c is a q-th power in $\mathbf{Q_p}$ if $w(c - d^q) \geq w(c) + 3$ (Hensel's lemma, w is the p-adic valuation on Q_p.) We thus choose $b \in F$ so that $w(a-b) \geq w(a)+3$. Then we have $w(ab^{-1} - 1) \geq w(ab^{-1}) + 3$.

The lemma delivers a $d \in F^*$ with $d(t^q - r) \in L^q$. We define

$$E = E_i(\sqrt[q]{d(t^q - r)}).$$

Let $\bar{v}$ be any extension of v to E of v, the extensions $\bar{v}_s$ of the v_s being chosen by Lemma 2. Then (E_i, S_i) satisfy (4) and (4.2) holds for $\bar{v}$, $\bar{v}_s$, $(s \in S_i)$.

Finally we specify a $b \in E$ such that

$$b, 1 + b, a_n^q + b^{-1} \in L^q$$

$$c \text{ divides } \bar{v}(1 + b), \bar{v}(a_n^q + b^{-1}), \bar{v}_s(1 + b), \bar{v}_s(a_n^q + b^{-1}), (s \in S_i)$$

$$\bar{v}(b) \text{ is the smallest positive element of } G_{\bar{v}}$$

and define

$$(E_{i+1}, S_{i+1}) = (E(\sqrt[q]{1 + b}, \sqrt[q]{a_n^q + b^{-1}}, S_i \cup \{b\}).$$

If we extend $\bar{v}, \bar{v}_s$ using Lemma 2[13] then we see that (4) holds. ((4.2) is satisfied by the choice of E.)

It still remains to find b.

The valuations $\bar{v}$, $\bar{v}_s$ are independent. The Approximation Theorem delivers us then a b such that

$$q \text{ divides } \bar{v}_s(b), \bar{v}_s(b) < 0, -\bar{v}_s(a_n^q), (s \in S_i, \bar{v} \neq \bar{v}_s)$$

$$\bar{v}(b) = \text{ the smallest positive element of } G_{\bar{v}}$$

Now one easily calculates that all values $\bar{v}(1+b), \bar{v}(a_n^q + b^{-1}), \bar{v}_s(1+b), \bar{v}_s(a_n^q + b^{-1})$ are divisible by q. If $L = L_p$, $\mathbf{C}$, or $q \neq 2$ and $L = \mathbf{R}$, it is also clear that b, $1 + b$, $a_n^q + b^{-1} \in L^q$. In the other cases we must specify b still more precisely:

$L = \mathbf{R}$, $q = 2$: We choose b so that in addition $b > 0$.

$L = \mathbf{Q_p}$: Let w be the p-adic valuation on L, and $d \in Q^q$ with $w(d) \geq 3$ and $w(a_n^q d) \geq 3$. By the Approximation Theorem, we choose b so that in addition $w(d - b) \geq w(d) + 3$. Then we have

$$w(b - d) \geq w(b) + 3 \Rightarrow b \in L^q$$

$$w((1 + b) - 1) = w(d) \geq 3 \Rightarrow 1 + b \in L^q$$

$$w((a_n^q + b^{-1}) - b^{-1}) \geq w(b^{-1}) + 3 = w(a_n^q + b^{-1}) + 3 \Rightarrow a_n^q + b^{-1} \in L^q$$

Case(4) $i = 4n + 3$. We distinguish two cases:

(a) $a_n \in M$ or $a_n \notin F$. Here we define $(E_{i+1}, S_{i+1}) = (E_i, S_i)$.

(b) $a_n \in F \backslash M$.

Let (4) be satisfied by $(v_s)_{s \in S_i}$. We observe that

$$B = \{r \in F \mid \exists s \in S_i \; q \text{ does not divide } v_s(t^q - r)\}$$

[12] The text has L^φ, which must be a misprint.

[13] Beeson: $\bar{v}$ and $\bar{v}_s$ are defined on E, an extension of E_i, and now we need to extend them to E_{i+1}, which is obtained from E by throwing in two more q-th roots.

is finite.

For $r \in F^*$, $t^q - r$ has multiple factors (in $F[t]$). There also exists a valuation $\bar{v}_r$ on $F(t)$, trivial on F, for which $\bar{v}_r(t^q - r)$ is the smallest positive element of $G_{\bar{v}_r}$. We choose for each r an extension w_r of $\bar{v}_r$ to E_i. Then we have $G_{\bar{v}_r} = G_{w_r}$ for almost all r. The set

$$C = \{r \in F^* \mid q \ \text{ divides } w_r(t^q - r)\}$$

is thus finite. We remark that $w_r(t^q - r') = 0$, if $r \neq r'$. We now choose $r_1 \in F$ so that $r_1 \neq 0$, a_n, $2r_1 \neq a_n$ and r_1 do not lie in any of the sets

$$C, a_n - C, M - G, a_n - (M - B).$$

Let $r_2 = a_n - r_1$. Lemma 3 delivers us $s_i \in F^*$ with $s_i(t^q - r_i) \in L^q$. We define

$$(E_{i+1}, S_{i+1}) = (E_i, S_i \cup \{s_1(t^q - r_1), s_2(t^q - r_2)\}).$$

We still have to prove (4). Because q does not divide $w_{r_1}(t^q - r_1)$ and $w_{r_2}(t^q - r_2)$, (4.2) holds for the valuations w_{r_1}, w_{r_2}, and $v_s (s \in S_i)$. In order to show (4.2), let $\bar{r}_1 \neq \bar{r}_2 \in F$, with $\bar{r}_1 + \bar{r}_2 \in M$ given. Then for example, for all $s \in S_i$, $v_s(t^q - \bar{r}_1)$ is divisible by q. If also $w_{r_1}(t^q - \bar{r}_1)$ and $w_{r_2}(t^q - \bar{r}_1)$ are divisible by q, we are done. Suppose also for example that q does not divide $w_{r_1}(t^q - \bar{r}_1)$. Then we have $r_1 = \bar{r}_1$, $r_1 \neq \bar{r}_2$, and $\bar{r}_2 \in M - r_1$. Consequently $w_{r_i}(t^q - \bar{r}_2) = 0$, and all the $v_s(t^q - \bar{r}_2)$ for $s \in Si$ are divisible by q.

With this, the construction of K is complete.

4 The properties of K

We show in this section (2) and

$$(K \cap L^q) \backslash K^q = \left(\cup_{i \in N} S_i \right) \tag{5}$$

$$K \backslash F^* \cdot K^q = F^* \cdot \left(\cup_{i \in N} S_i \right)$$

$$F = \{a \in K \mid \forall b \in L^q \ \ (1 + b \in K^q \wedge a^q + b^{-1} \in K^q) \Rightarrow b \in K^q\} \tag{6}$$

$$F = \{a \in K \mid \forall b \in K \ \ (1 + b \in K^q \wedge a^q + b^{-1} \in K^q) \Rightarrow b \in F^* \cdot K^q\}$$

$$M = \{r \in F \mid \forall r_1, r_2 \in F \ \ (r_1 \neq r_2 \wedge r_1 + r_2 = r) \Rightarrow$$
$$(t^1 - r_1 \in F^* \cdot K^q \vee t^1 - r_2 \in F^* \cdot K^q)\} \tag{7}$$

Proof of (2). Let $K \subset H \subset L$ and H finite over K. We want to show that q divides the degree $[H : K]$. We can suppose $H = K(a)$. For arbitrarily large n we have $a = a_n$. Choose n so large, that

$$[E_{4n}(a) : E_{4n}] = [K(a) : K].$$

In the construction when $i = 4n$ the subcase (a) applies. Thus q divides $E_{4n}(a) : E_{4n}$.

Proof of (5) and the equation after (5):

"$\supset$" Let $a \in F^* \cdot K^q$. For all sufficiently large i we have $a \in F^* \cdot E_i^q$ and $v(a)$ is divisible by q for all v that are trivial on F. Because of (4.1), a does not lie in $F^* \cdot S_i$.

"$\subset$" Let $a \in K \backslash F^* \cdot K^q$. According to Lemma 3, we can choose $f \in F^*$ with $\bar{a} = af \in L^q$. We now have $\bar{a} \in (K \cap L^q) \backslash K^q$.

Let $a_n = \bar{a}$ and n so large, that $\bar{a} \in E_{4n+1}$. In the construction, under the case $i = 4n+1$ the subcase (b) applies. Then $\bar{a} \in S_{i+1}$. From this it follows that $a \in F^* \cdot S_{i+1}$.

Proof of (6) and the equation after (6):

"$\supset$" Let $a \in F$. For some $b \in K$ suppose $1 + b \in K^q$ and $a^q + b^{-1} \in K^q$. Let i be so large that $1 + b \in E_i^q$ and $a^q + b^{-1} \in E_i^q$. Let v be a valuation on E_i that is trivial on F. If $v(b) > 0$, then $v(b) = -v(a^q + b^{-1})$ is divisible by q. If $v(b) < 0$, then $v(b) = v(1 + b)$ is divisible by q. Because then $v(b)$ is always divisible by q, it follows from (4) that $b \notin F^* \cdot S_i$. Then by the equation after (5), we ahve $b \in F^* \cdot K^q$. If $b \in L^q$, it follows from (5) that $b \in K^q$.

"$\subset$" Let $a \in K \backslash F$. Let n be so large that $a \in E_{4n+2}$, and let $a = a_n$. In the construction, under $i = 4n + 2$ the subcase (b) applies. In S_{i+1} there is therefore a b with $1 + b$ and $a^q + b^{-1} \in E_{i+1}^q$. We then have

$$b \in L^q, 1 + b \in K^q, a^q + b^{-1} \in K^q, b \notin F^* \cdot K^q.$$

Proof of (7).

"$\supset$" Let $r_1 + r_2 \in M$, $r_1 \neq r_2$. If $t^q - r_i$ are both[14] not in $F^* \cdot K^q$, then because of the equation after (5), we have $t^q - r_1, t^q - r_2 \in F^* \cdot S_i$ for sufficiently large i. However, that contradicts (4).

"$\subset$" Let $r = a_n \in F \backslash M$. In the construction under the case $i = 4n + 3$, the subcase (b) applies. There there exist $r_1 \neq r_2 \in F$, $r_1 + r_2 = r$ and $s_i \in F^*$, for which $s_1(t^q - r_1), s_2(t^q - r_2) \in S_{i+1}$. Then because of the equation after (5) $t^q - r_1, t^q - r_2 \notin F^* \cdot K^q$.

5 Proof of the theorems

We still have to show, that A is interpretable in K. Because of (7), it suffices to show that F is definable in K. We distinguish three cases:

Case 1: $L = L_p$, $\mathbf{C}$, or $q \neq 2$ and $L = \mathbf{R}$. Then $K \subset L^p$ and by (6) we have

$$F = \{a \in K \mid \forall b \in K(1 + b \in K^q \wedge a_q + b^{-1} \in K^q) \Rightarrow b \in K^q\}$$

Case 2: $L = \mathbf{R}$, $q = 2$. Then $F^* \cdot K^q\ K^q \cup -K^q\}$, and we have because of the equation after (6),

$$F = \{a \in K \mid \forall b \in K(1 + b \in K^q \wedge a^q + b^{-1} \in K^q) \Rightarrow b \in K^q \cup -K^q\}$$

Case 3: $L = Q_p$. We receive from (6) a definition of F, if we can define $K \cap K^q$ in K. But because Q is closed in $\mathbf{Q_p}$, because of Hensel's lemma we have $c \in L^q$ if and only if there exists $d \in K$ (or: $\mathbf{Q}$) with $w(c - d^q) \geq w(c) + 3$.[15] It suffics then to give an elementary definition of the p-adic valuation w in K: If r is relatively prime to p, then for all $c \in L$ we have $w(c) \geq 0$ if and only if $1 + pc^r \in L^r$. If r is a prime number different from q and p, we have by (2) that for all $c \in K$, $w(c) \geq 0$ if and only if $q + pc^r \in K^r$.

6 References

[AK] Ax, Kochen. Diophantine problems over local fields, I, II, III., *Amer. J. of Math.* **87, 88** (1965, 1966).

[C] Cherlin, G. *Mathematical Reviews* **50** (1975) (Review of H1].

[CK] Chang-Keisler *Model Theory.* Amsterdam (1973).

[14] Beeson: He has $t^q - r_1$ but in view of "both" he must mean r_i, not r_1.

[15] Again, d^ϕ is certainly a misprint for d^q.

[E] Ershov, Ju. L. Fields with a solvable theory. *Doklady Akademii Nauk SSSR* **174** (1967), 19–20. English translation, *Soviet math.* **8** (1967), 575–576.

[F] Ficht, H. *Zur Theorie der pythagoräischen Körper*, Diplomarbeit, Konstanz (1979).

[H1] Hauschild, K. Rekursive Unentscheidbarkeit der Theorie der pythagoräischen Körper, *Fundamenta Math.* **82** (1974), 191–197.

[H2] Hauschild, K., Addendum, betreffend dei rekursive Unentscheidbarkeit der Theorie der pythagoräischen Körper, *preprint*, Berlin (1977).

[K] Kochen, S. Integer valued rational functions over the p-adic numbers. A p-adic analogue of the theory of real fields. *Proc. Symp. pure Math. XII) (Number theory)* (1969(, 57–73.

[TMR] Tarski, Mostowski, Robinson, *Undecidable Theories*, Amsterdam (1953).

[M] Macintyre, A. Definable subsets of p-adic fields, *Journal of Symbolic Logic* **41** (1976).