Annals of Pure and Applied Logic 41 (1989) 27–32
North-Holland

COUNTABLE VALUED FIELDS IN WEAK SUBSYSTEMS OF SECOND-ORDER ARITHMETIC

Kostas HATZIKIRIAKOU and Stephen G. SIMPSON*
Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA

Communicated by A. Nerode
Received 28 September 1987

0. Introduction

This paper is part of the program of reverse mathematics. We assume the reader is familiar with this program as well as with RCA_0 and WKL_0, the two weak subsystems of second-order arithmetic we are going to work with here. (If not, a good place to start is [2].)

In [2], [3], [4], many well-known theorems about countable rings, countable fields, etc. were studied in the context of reverse mathematics. For example, in [2], it was shown that, over the weak base theory RCA_0, the statement that every countable commutative ring has a prime ideal is equivalent to weak König's Lemma, i.e. the statement that every infinite $\{0, 1\}$ tree has a path.

Our main result in this paper is that, over RCA_0, Weak König's Lemma is equivalent to the theorem on extension of valuations for countable fields. The statement of this theorem is as follows: "Given a monomorphism of countable fields $h : L \to K$ and a valuation ring R of L, there exists a valuation ring V of K such that $h^{-1}(V) = R$."

In [5], Smith produces a recursive valued field (F, R) with a recursive algebraic closure $\tilde{F}$ such that R does not extend to a recursive valuation ring $\tilde{R}$ of $\tilde{F}$. However, there is little or no overlap between the contents of the present paper and [5].

1. Countable valued fields in RCA_0

1.1. Definition (RCA_0). A *countable valued field* consists of a countable field F together with a countable linearly ordered abelian group G and a function $\mathrm{ord} : F \to G \cup \{\infty\}$ satisfying:

(i) $\mathrm{ord}(a) = \infty$ iff $a = 0$,

(ii) $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) + \mathrm{ord}(b)$,

* Simpson's research was partially supported by NSF grant DMS-8701481.

(iii) $\operatorname{ord}(a+b) \geqslant \min(\operatorname{ord}(a), \operatorname{ord}(b))$.
Such a function is called a *valuation* on F.

1.2. Definition (RCA_0). A subring V of a countable field F is called a *valuation* ring of F iff for any $x \in F^* = F \setminus \{0\}$ either $x \in V$ or $x^{-1} \in V$.

1.3. Theorem (RCA_0). *A valuation ring V of a countable field F is a local ring, i.e. it has a unique maximal ideal M_V consisting of all non-units of V.*

Proof. The set of non-units of V, $M_V = \{a \in V: a^{-1} \notin V\}$, exists by Δ_1^0 comprehension, an axiom scheme that RCA_0 includes. We prove that M_V is an ideal. Let $x, y \in M_V$. We can assume $x \cdot y^{-1} \in V$. Then $1 + x \cdot y^{-1} = (x+y)/y \in V$. If $x+y$ were not in M_V, then $1/(x+y)$ would belong to V, whence $y^{-1} \in V$ and this would contradict the fact that $y \in M_V$. Now, let $x \in M_V$ and $y \in V$. Then $x \cdot y \in M_V$. If not, $(x \cdot y)^{-1} \in V$, i.e. $y^{-1} \cdot x^{-1} \in V$, whence $x^{-1} \in V$ which contradicts the fact that $x \in M_V$. Hence M_V is an ideal which clearly is the unique maximal ideal of V. □

1.4. Theorem (RCA_0). *Every valuation on a countable field F gives rise to a valuation ring of F and, conversely, every valuation ring of a countable field F gives rise to a valuation on F.*

Proof. Suppose ord is a valuation on F. The set $V = \{a \in F: \operatorname{ord}(a) \geqslant 0\}$ exists by Δ_1^0 comprehension and it is a valuation ring of F; the unique maximal ideal of V is $M_V = \{a \in F: \operatorname{ord}(a) > 0\}$. Conversely, let V be a valuation ring of F. Let $V^* = \{a \in V: a^{-1} \in V\}$. This set exists by Δ_1^0 comprehension. V^* is a subgroup of the multiplicative group $F^* = F \setminus \{0\}$, so we may form the quotient group $G = F^*/V^*$. The elements of G are those $a \in F^*$ such that $\forall b\ ((b < a$ and $b \in F^*) \rightarrow a \cdot b^{-1} \notin V^*)$, i.e. minimal representatives of the equivalence classes under the equivalence relation $a \sim b$ iff $a \cdot b^{-1} \in V^*$. (Here, minimal refers to the ordering of $\mathbb{N}$, assuming that $F \subseteq \mathbb{N}$; see Section 2 in [2].) Thus, G is an abelian multiplicative countable group and on G we can define the linear ordering $\forall a, b \in G\ a <_G b$ iff $a^{-1} \cdot b \in V \setminus V^*$. This ordering exists by Δ_1^0 comprehension, and $(G, <_G)$ is an ordered abelian group. Hence, we can now define a valuation $\operatorname{ord}: F \rightarrow G \cup \{\infty\}$ via

$$\operatorname{ord}(a) = \begin{cases} \text{the least (in the sense of } <_{\mathbb{N}}) \ c \text{ such} & \\ \quad \text{that } c \in F^* \text{ and } c \cdot a^{-1} \in V^*, & \text{if } a \neq 0, \\ \infty & \text{if } a = 0. \end{cases} \qquad \square$$

The previous theorem allows the following equivalent definition of a countable valued field.

1.5. Definition (RCA_0). A *countable valued field* consists of a countable field F and a valuation ring V of F. We write (F, V).

1.6. Definition (RCA_0). An *extension* $h:(F, R)\to(K, V)$ of countable valued fields is a field monomorphism $h: F\to K$ such that $h^{-1}(V)=R$.

1.7. Remark. Suppose $h:(F, R)\to(K, V)$ is an extension of countable valued fields as above. Let $\mathrm{ord}_F: F^*\to G_F$ and $\mathrm{ord}_K: K^*\to G_K$ be the valuations associated with (F, R) and (K, V) as in Theorem 1.4. Then, there is an obvious monomorphism $\hat{h}: G_F\to G_K$ such that the following diagram commutes:

$$\begin{array}{ccc} F & \xrightarrow{h} & K \\ {\scriptstyle \mathrm{ord}_F}\downarrow & & \downarrow{\scriptstyle \mathrm{ord}_K} \\ G_F & \xrightarrow{\hat{h}} & G_K \end{array}$$

Conversely, given any such commutative diagram, there is a corresponding extension of countable valued fields. These facts can be proved in RCA_0.

2. Proof of the main theorem

To prove our main theorem, we need the following two lemmas.

2.1. Lemma (WKL_0). *Let K be a countable field, R a countable commutative ring, I an ideal of R, and $h: R\to K$ a ring monomorphism. Then there exists a valuation ring V of K such that $h(R)\subseteq V\subseteq K$ and $h(I)\subseteq M_V\subset V$.*

Proof. We argue in WKL_0. The method is similar to the one used in the construction of a prime ideal of a countable commutative ring. (See Theorem 3.1 in [2].) Let $a_0, a_1, \ldots$ be an enumeration of K. Let $b_0, b_1, \ldots$ be an enumeration of $h(R)$. Let $c_0, c_1, \ldots$ be an enumeration of $h(I)$. Note that $h(R)$ and $h(I)$ are defined by Σ^0_1 formulas and, hence, they can be enumerated within RCA_0.

We define a tree T by induction on $s=\mathrm{lh}(\sigma)$ and simultaneously we define finite sets $X_\sigma\subseteq K$, $\sigma\in T$, with the property that $\sigma\subset\tau$ implies $X_\sigma\subseteq X_\tau$. At stage s, $T_s=\{\sigma\in T: \mathrm{lh}(\sigma)=s\}$ is defined. For $s=0$, let $T_0=\{\emptyset\}$ and $X_\emptyset=\emptyset$. Assume T_{s-1} is defined and let $\sigma\in T_{s-1}$. The construction splits into the following 5 cases. For convenience assume that $s=5m+r$, $0\leq r<5$.

$r=0$. For each $\sigma\in T_{s-1}$, put $\sigma 0\in T_s$ and let $X_{\sigma 0}=X_\sigma\cup\{b_m\}$.

$r=1$. For each $\sigma\in T_{s-1}$, put $\sigma 0\in T_s$ and let $X_{\sigma 0}=X_\sigma$, unless $m=(i, j, k)$ (every natural number encodes a triple of natural numbers) and $a_i, a_j\in X_\sigma$ in which case let $X_{\sigma 0}=X_\sigma\cup\{a_i+a_j\}$.

$r=2$. For each $\sigma\in T_{s-1}$, put $\sigma 0\in T_s$ and let $X_{\sigma 0}=X_\sigma$, unless $m=(i, j, k)$ and $a_i, a_j\in X_\sigma$ in which case let $X_{\sigma 0}=X_\sigma\cup\{a_i\cdot a_j\}$.

$r=3$. For each $\sigma\in T_{s-1}$, put $\sigma 0\in T_s$ and let $X_{\sigma 0}=X_\sigma$, unless $m=(i, j, k)$ and $a_i\cdot a_j=1$ in which case put $\sigma 0$, $\sigma 1\in T_s$ and let $X_{\sigma 0}=X_\sigma\cup\{a_i\}$ and $X_{\sigma 1}=X_\sigma\cup\{a_j\}$.

$r=4$. For each $\sigma\in T_{s-1}$, put $\sigma 0\in T_s$ and let $X_{\sigma 0}=X_\sigma$, unless $m=(i, j, k)$ and

$a_i \in X_\sigma$ and $a_i \cdot c_j = 1$ in which case put neither $\sigma 0$ nor $\sigma 1 \in T_s$ and do not define $X_{\sigma 0}$ and $X_{\sigma 1}$.

Claim (RCA_0). *T is infinite.*

Proof. Consider the Π^0_1 formula

$$\psi(s) \equiv \exists \sigma \in T_s\, (1 \notin I_\sigma),$$

where I_σ is the ideal generated by I inside the ring $R[X_\sigma]$, i.e. the ring generated by $R \cup X_\sigma$ inside K. (Note that I_σ and $R[X_\sigma]$ are defined by Σ^0_1 formulas; we do not assume that they exist as sets.)

Now, $\psi(0)$ holds since I is an ideal of R. Assume that $\psi(s-1)$ holds, $\sigma \in T_{s-1}$ and $1 \notin I_\sigma$. If $r = 0$, 1, 2, or 4, then clearly $I_{\sigma 0} = I_\sigma$ and so $\psi(s)$ holds. If $r = 3$, then, either only $\sigma 0$ was thrown into T_s, whence $X_{\sigma 0} = X_\sigma$ and $I_{\sigma 0} = I_\sigma$ and so $\psi(s)$ holds, or both $\sigma 0$, $\sigma 1 \in T_s$ and $X_{\sigma 0} = X_\sigma \bigcup \{a\}$, $X_{\sigma 1} = X_\sigma \cup \{a^{-1}\}$, for some $a \in K$. In this case assume that $1 \in I_{\sigma 0}$ and $1 \in I_{\sigma 1}$. Then, we have:

(I) $1 = \alpha_0 + \alpha_1 \cdot a + \cdots + \alpha_n \cdot a^n, \quad \alpha_i \in I_\sigma,\ i = 1, \ldots, n.$
(II) $1 = \beta_0 + \beta_1 \cdot a^{-1} + \cdots + \beta_m \cdot a^{-m}, \quad \beta_i \in I_\sigma,\ i = 1, \ldots, m.$

By the Σ^0_1 least element principle we may assume that m, n are chosen as small as possible and, by symmetry, we may assume that $n \geqslant m$. Now, we have:

$$\begin{aligned}
\text{(II)} \;&\Rightarrow\; a^n = \beta_0 \cdot a^n + \cdots + \beta_m \cdot a^{n-m} \\
&\Rightarrow\; (1-\beta_0) \cdot a^n = \beta_1 \cdot a^{n-1} + \cdots + \beta_m \cdot a^{n-m}, \\
\text{(I)} \;&\Rightarrow\; (1-\beta_0) = (1-\beta_0) \cdot \alpha_0 + \cdots + \alpha_n \cdot \beta_1 \cdot a^{n-1} + \cdots + \alpha_n \cdot \beta_m \cdot a^{n-m}, \\
&\text{i.e. } 1 = \beta_0 + (1-\beta_0) \cdot \alpha_0 + \cdots + \alpha_n \cdot \beta_1 \cdot a^{n-1} + \cdots + \alpha_n \cdot \beta_m \cdot a^{n-m},
\end{aligned}$$

so 1 can be written as a polynomial in a of degree smaller than n with coefficients in I_σ. (The above computation is taken from the standard textbook proof of the extension of valuations theorem; see, for instance, Lemma 9.1, Section II, in [1].) This is a contradiction. Hence, either $1 \notin I_{\sigma 0}$ or $1 \notin I_{\sigma 1}$ and so $\psi(s)$ holds. Since RCA_0 includes Π^0_1 induction (see Lemma 1.1 in [2]), we have that $\psi(s)$ holds for all $s \in \mathbb{N}$. Hence, T is infinite. □ (Claim)

Now, by Weak König's Lemma let f be a path through T. Let $V_0 = \bigcup_{\sigma \subset f} X_\sigma$. Then, V_0 is a valuation ring of K (because of cases $r = 1, 2, 3$) and $h(R) \subseteq V_0$ (because of case $r = 0$). Moreover, every element of $h(I)$ is a non-unit of V_0 (because of case $r = 4$). However, V_0 is defined by a Σ^0_1 formula and, so, may not exist. Hence, consider the following tree S of all sequences $\sigma \in \mathrm{Seq}_2$ satisfying:

For all $i, j, k < \mathrm{lh}(\sigma)$:
(i) $a_i = b_j \Rightarrow \sigma(i) = 1$,
(ii) $\sigma(i) = \sigma(j)$ and $a_i + a_j = a_k \Rightarrow \sigma(k) = 1$,
(iii) $\sigma(i) = \sigma(j)$ and $a_i \cdot a_j = a_k \Rightarrow \sigma(k) = 1$,
(iv) $a_i \cdot a_j = 1 \Rightarrow \sigma(i) = 1$ or $\sigma(j) = 1$,
(v) $a_i = c_j$ and $a_i \cdot a_k = 1 \Rightarrow \sigma(k) = 0$.

To see that S is an infinite tree, let $s \in \mathbb{N}$. Then let $X = \{i < s : \forall n\ (a_i \in X_{f[n]})\}$. X exists by bounded Σ_1^0 comprehension (see Lemma 1.6 in [2]). So, define $\sigma \in 2^s$ by

$$\sigma(i) = \begin{cases} 1 & \text{if } i \in X, \\ 0 & \text{if } i \notin X. \end{cases}$$

Then, σ exists and $\sigma \in S$ since V_0 is a valuation ring of K, $h(R) \subseteq V_0$, and every element of $h(I)$ is a non-unit of V_0. So, S is infinite and hence there is a path g through it. Let $V = \{a_i : g(i) = 1\}$. Then, this set exists by Δ_1^0 comprehension and it is a valuation ring of K (conditions (ii), (iii), (iv)), such that $h(R) \subseteq V$ (condition (i)). By condition (v), all elements of $h(I)$ are non-units, hence $h(I) \subseteq M_V$, where M_V is the maximal ideal of V which exists by Δ_1^0 comprehension (Theorem 1.3). $\square$

2.2. Lemma (RCA_0). *Lemma* 2.1 *implies the theorem on extension of valuations for countable fields*: "*Given a monomorphism of countable fields $h : L \to K$ and a valuation ring R of L, there exists a valuation ring V of K such that $h^{-1}(V) = R$.*"

Proof. Assume Lemma 2.1. Then, given the monomorphism $h : L \to K$ and the valuation ring R of L, there is a valuation ring V of K such that $h(R) \subseteq V \subseteq K$ and $h(M_R) \subseteq M_V \subset V$. We need to prove that $h^{-1}(V) = R$. Let $a \in R$, then $h(a) \in h(R)$, hence $h(a) \in V$ and so $a \in h^{-1}(V)$. Let $a \in h^{-1}(V)$, then $h(a) \in V$. Then, if $h(a) = 0$, we have $a = 0$, hence $a \in R$. If $h(a) \neq 0$, then $a \neq 0$ and if $a \notin R$ then $a^{-1} \in M_R$, whence $h(a^{-1}) \in h(M_R) \subseteq M_V$. Hence, $1/h(a) \in M_V$, whence $1 \in M_V$, a contradiction. So $a \in R$. $\square$

Now, we are ready to prove the following:

2.3. Theorem (RCA_0). *The following are equivalent*:
(i) *Weak König's Lemma.*
(ii) *The theorem on extension of valuations for countable fields.*

Proof. (i) $\Rightarrow$ (ii) follows from Lemmas 2.1 and 2.2.

(ii) $\Rightarrow$ (i). Assume (ii). Let $f, g : \mathbb{N} \to \mathbb{N}$ be two 1–1 functions such that $f(n) \neq g(m)$, $\forall n, m \in \mathbb{N}$. Consider the field $K = \mathbb{Q}(x_n : n \in \mathbb{N})$ and the field $L = \mathbb{Q}(y_n, z_n : n \in \mathbb{N})$. Let $h : L \to K$ be the field monomorphism defined via $h(y_n) = x_{f(n)}$ and $h(z_n) = x_{g(n)}$, $\forall n \in \mathbb{N}$. Let G be the direct sum of countably many copies of $\mathbb{Z}$; so, a typical element of G is $\boldsymbol{a} = (a_0, a_1, \ldots, a_k, \ldots)$ where $a_k \in \mathbb{Z}$ and $a_k = 0$ for all but a finite number of indices k. G is an ordered abelian group under the lexicographical ordering: $\boldsymbol{a} <_G \boldsymbol{b}$ if and only if $a_l <_{\mathbb{Z}} b_l$ where l is the least k such that $a_k \neq b_k$. We define a valuation ord: $L \to G \cup \{\infty\}$ as follows: For any monomial $y_1^{m_1} \cdot z_1^{n_1} \cdots y_r^{m_r} \cdot z_r^{n_r}$, $m_i \geq 0$, $n_i \geq 0$ for $i = 1, \ldots, r$ define:

$$\mathrm{ord}(y_1^{m_1} \cdot z_1^{n_1} \cdot \cdots \cdot y_r^{m_r} \cdot z_r^{n_r}) = (m_1, -n_1, \ldots, m_r, -n_r, 0, 0, \ldots) \in G.$$

Then, for $p \in \mathbb{Q}[y_n, z_n : n \in \mathbb{N}]$, say $p = \sum_{i=1}^{s} c_i w_i$, where w_i is a monomial and $c_i \in \mathbb{Q} - \{0\}$, $i = 1, \ldots, s$, define $\mathrm{ord}(p) = \min \mathrm{ord}\, w_i$. We define $\mathrm{ord}(0) = \infty$. Now, for $a = p/q \in L = \mathbb{Q}(y_n, z_n : n \in \mathbb{N})$, define $\mathrm{ord}(a) = \mathrm{ord}(p) - \mathrm{ord}(q)$. It is easy to verify that ord is a valuation. Let $R = \{a : a \in L \text{ and } \mathrm{ord}(a) \geq 0\}$. Then, by (ii), there is a valuation ring V of K such that $h^{-1}(V) = R$. Let $X = \{n : x_n \in V\}$. For $m \in N$ we have $x_{f(m)} \in V$ (since $h^{-1}(x_{f(m)}) = y_m \in R$) and $x_{g(m)} \notin V$ (since $h^{-1}(x_{g(m)}) = z_m \notin R$). Hence, $f(m) \in X$ and $g(m) \notin X$, $\forall m \in \mathbb{N}$. So, by assuming (ii), we proved (over RCA_0) the statement: "If $f, g: \mathbb{N} \to \mathbb{N}$ are 1–1 functions and $f(n) \neq g(m)$ $\forall n, m \in \mathbb{N}$, then $\exists X \forall m\, (f(m) \in X$ and $g(m) \notin X)$." But, over RCA_0, this is equivalent to Weak König's lemma (see Lemma 3.2 in [2]), and, hence, we are done. □

References

[1] O. Endler, Valuation Theory (Springer, Berlin, 1972).

[2] H. Friedman, S. Simpson and R. Smith, Countable algebra and set existence axioms, Ann. Pure Appl. Logic 25 (1983) 141–181; Addendum 27 (1983) 319–320.

[3] S. Simpson and R. Smith, Factorization of polynomials and Σ_1^0 induction, Ann. Pure Appl. Logic 31 (1986) 289–306.

[4] S. Simpson, Ordinal numbers and the Hilbert Basis Theorem, J. Symbolic Logic 53 (1988) 961–974.

[5] R. Smith, Splitting algorithms and effective valuation theory, in: J.N. Crossley, ed., Aspects of Effective Algebra (Upside Down A Book Company, 1980) 232–245.