Extensions of Commutative Rings in Subsystems of Second Order Arithmetic

Kostas Hatzikiriakou
Department of Elementary Education
University of Thessaly
Argonafton & Fillelinon, GR-382 21 Volos, Greece
kxatzkyr@uth.gr

Abstract. We prove that the existence of the integral closure of a countable commutative ring $R$ in a countable commutative ring $S$ is equivalent to Arithmetical Comprehension (over $RCA_0$). We also show that i) the Lying Over ii) the Going Up theorem for integral extensions of countable commutative rings and iii) the Going Down theorem for integral extensions of countable domains $R \subset S$, with $R$ normal, are provable in $WKL_0$.

1 Introduction

This paper is a contribution to the program of Reverse Mathematics that currently develops mathematics in subsystems of second order arithmetic and attempts to classify key theorems of mathematics according to their logical strength in a relatively small number of classes that have emerged in the course of the above development, see [3,6].

In this paper we use three subsystems of second order arithmetic: $RCA_0$, $WKL_0$ and $ACA_0$. The reader who is not familiar with these systems should consult [2] or [6]. The basic theory of integral ring extensions can be found in [1, 4, 5]. All the rings considered in this paper are commutative and countable. More precisely, a countable commutative ring $R$ is a subset of $\mathbb{N}$ (the set of natural numbers), together with binary operations $+,-, \cdot$ a unary operation $-$ and distinguished elements 0, 1 such that the system $(R, +,-, \cdot, 0, 1)$ obeys the usual commutative ring axioms. We also assume that whenever $R \subset S$, the unit element of the two rings is the same.

2 Integral closure and Arithmetic Comprehension

Definition 1 ($RCA_0$) Let $R$ and $S$ be rings with $R \subset S$. An element $s$ of $S$ is called integral over $R$ if and only if $s$ is a root of a monic polynomial of $R[x]$, i.e. if and only if $s^n + r_{n-1} \cdot s^{n-1} + \ldots + r_1 \cdot s + r_0 = 0$, for $r_i \in R$, $i = 0, \ldots, n - 1$. If all the elements of $S$ are integral over $R$, then the extension $R \subset S$ is called integral.

⋆ I am grateful to S. G. Simpson for his advice in putting together this paper.
Lemma 2 ($ACA_0$) Let $R$ and $S$ be rings with $R \subset S$. The integral closure of $R$ in $S$ exists.

**Proof.** The integral closure of $R$ in $S$ is the $\Sigma^0_1$ definable set $K = \{ s \in S : \exists r_0 \ldots \exists r_{n-1} (r_0 \in R \land \ldots r_{n-1} \in R \land s^n + r_{n-1} \cdot s^{n-1} + \ldots + r_1 \cdot s + r_0 = 0) \}$ and thus it exists by Arithmetical Comprehension, an axiom scheme included in $ACA_0$.

Theorem 3 ($RCA_0$) The following are equivalent:
1. Arithmetical Comprehension
2. Given countable rings $R,S$ with $R \subset S$, the integral closure of $R$ in $S$ exists.
3. Given countable fields $K,L$ with $K \subset L$, the relative algebraic closure of $K$ in $L$ exists.

**Proof.** 1)$$2)$ by Lemma 1. $2)$ $$3)$ Trivial. $3)$$1)$ It suffices to prove that given any one-to-one function $f : \mathbb{N} \to \mathbb{N}$, its range exists (see [6]). We are going to use an idea of Fröhlich and Shepherdson that is also used in [2] to show that if $F \subset K$ are countable fields, the existence of a transcendental basis for $K$ over $F$ is equivalent to Arithmetical Comprehension. Let $R = \mathbb{Q}[x_0, x_1, \ldots]$ and let $P$ be the ideal of $R$ generated by $x_{f(n)} - x_0$, for $n > 0$ (for simplicity, assume that $f(0) = 0$). In $RCA_0$, we can prove that this ideal exists and it is prime (see [2]). Thus $R/P$ exists and it is a domain, hence let $L$ be its field of fractions. Let $K$ be $\mathbb{Q}(x_0)$. By 3), the relative algebraic closure of $K$ in $L$ exists and obviously $m$ belongs to the range of $f$ if and only if $x_m$ belongs to the relative algebraic closure of $K$ in $L$.

3  $WKL_0$ and the Lying Over, the Going Up and the Going Down Theorem

In the theory of integral ring extensions there are three prominent theorems, the Lying Over, The Going Up and the Going Down (due to Cohen-Seidenberg). We show that all of them can be proved in $WKL_0$. The main tool in proving these theorems in $WKL_0$ is a form of Krull’s theorem, which we state and prove.

Proposition 4 ($WKL_0$) Let $R$ be a countable ring, let $I$ be a $\Sigma^0_1$ ideal of $R$ and let $M$ be a $\Sigma^0_1$ multiplicative set disjoint from $I$, ($1 \in M$). Then there is a prime ideal $P$ of $R$, which contains $I$ and is disjoint from $M$.

**Proof.** Let $a_0 = 0, a_1 = 1, \ldots$ be an enumeration of $R$, let $b_0 = 0, b_1 = 1, \ldots$ be an enumeration of $I$ and let $c_0 = 0, c_1 = 1, \ldots$ be an enumeration of $M$ (Lemma II.3.7 in [6]). We define a tree $T \subseteq Seq_2$ by induction on $s = lh(\sigma)$ and simultaneously we define finite sets $X_\sigma \subseteq S$, with the property that if $\sigma$ is an initial segment of $\tau$, then $X_\sigma \subseteq X_\tau$. At stage $s$, $T_s = \{ \sigma \in T : lh(\sigma) = s \}$ is defined. For $s = 0$, $T_0 = \{0\}$ and $X_{<s} = \{0\}$. Now assume that $T_{s-1}$ has been defined. The definition of $T_s$ splits into 5 cases. Let $s = 5 \cdot m + r$, $0 \leq r > 5$ and
assume that $m$ encodes a triple of natural numbers $(i, j, k)$. Assume $\sigma \in T_{s-1}$.

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

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

Case 3. $r = 2$. 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 $a_i \in X_\sigma$, in which case let $X_{\sigma 0} = X_\sigma \cup \{a_i + a_j\}$.

Case 4. $r = 3$. 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 $a_i, a_j \in X_\sigma$, in which case put $\sigma 0, \sigma 1$ in $T_s$ and let $X_{\sigma 0} = X_\sigma \cup \{a_i\}$ and $X_{\sigma 1} = X_\sigma \cup \{a_j\}$.

Case 5. $r = 4$. 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 $a_i = c_j$, 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 $H_1$ 0 formula $\psi(s) = \exists \sigma \in T_s(I_\sigma \cap M = \emptyset)$, where $I_\sigma$ is the ideal generated by $I \cup X_\sigma$ in $R$. Then $\psi(0)$ holds, since $I$ and $M$ are disjoint.

Now assume that $\psi(s - 1)$ holds and that $\sigma \in T_{s-1}$ and $I_\sigma \cap M = \emptyset$. Then, in cases 1, 2, 3 and 5, $I_{\sigma 0} = I_\sigma$, and so $\psi(s)$ holds. In case 4, either only $\sigma 0$ was put in $T_s$ and $X_{\sigma 0} = X_\sigma$ and $I_{\sigma 0} = I_\sigma$, or both $\sigma 0$ and $\sigma 1$ were put in $T_s$ and $X_{\sigma 0} = X_\sigma \cup \{a_i\}$ and $X_{\sigma 1} = X_\sigma \cup \{a_j\}$ and $a_i, a_j \in I_\sigma$. Assume then, towards a contradiction, that $I_{\sigma 0} \cap M \neq \emptyset$ and $I_{\sigma 1} \cap M \neq \emptyset$. Hence there exist $m_1, m_2$ in $M$ such that $m_1 = b \cdot r \cdot a_i$ and $m_2 = d \cdot s \cdot a_j$, where $b, d \in I_\sigma$ and $r, s \in R$. Then $m_1 \cdot m_2 = b \cdot d + b \cdot r \cdot a_i + d \cdot s \cdot a_i + r \cdot s \cdot a_i \cdot a_j$. This means that $m_1, m_2 \in I_\sigma \cap M$, contradiction. So, at least one of the that $I_{\sigma 0} \cap M = \emptyset$ and $I_{\sigma 1} \cap M = \emptyset$ holds and so $\psi(s)$ holds. Since $RCA_0$ includes $H_1^0$ induction (see Corollary II.3.10 in [6]), $\psi(s)$ holds for all $s \in \mathbb{N}$. Hence $T$ is infinite. □

So by Weak König’s Lemma, the defining set existence axiom of $WKL_0$,

let $f$ be a path through $T$. Let $P_0 = \cup_s X_\sigma$, where $\sigma$ ranges over all finite initial segments of $f$. Then $P_0$ is a prime ideal (because of 2, 3, 4), it contains 1 (because of 1) and it is disjoint from $M$ (because of 5). However, $P_0$ is defined by a $\Sigma^0_1$ formula and thus it may not exist. So consider the following tree $S$ of all sequences of $\Sigma_1$, such that for all $i, j, k > lh(\sigma)$:

i) $a_i = b_j \rightarrow \sigma(i) = 1$

ii) $\sigma(i) = \sigma(j) = 1$ and $a_i + a_j = a_k \rightarrow \sigma(k) = 1$

iii) $\sigma(i) = 1$ and $a_i \cdot a_j = a_k \rightarrow \sigma(k) = 1$

iv) $\sigma(i) = \sigma(j) = 0$ and $a_i \cdot a_j = a_k \rightarrow \sigma(k) = 0$

v) $a_i = c_j \rightarrow \sigma(i) = 0$.

Claim ($RCA_0$). $S$ is infinite.

Proof. To see that $S$ is an infinite tree, let $s$ be a natural number. Then let $X = \{i < s : \exists \sigma(a_i \in X_{\sigma[i,n]}\}$). Now $X$ exists by bounded $\Sigma^0_1$ comprehension (Theorem II.3.9 in [6]) and so we can define $\sigma \in 2^s$ by $\sigma(i) = 1$ if $i \in X$ and $\sigma(i) = 0$ if $i \notin X$. Thus $\sigma$ exists and $\sigma \in X$, since $P_0$ is a prime ideal which contains $I$ and is disjoint from $M$. □
By Weak König’s Lemma, let $g$ be a path through $S$. Then let $P = \{a_i : g(i) = 1\}$. This set exists by $\Delta^0_1$ comprehension and it is the required prime ideal.

**Remark.** Proposition 3.1 is basically Exercise IV.6.6 in [6] and its proof is similar to the proof of Theorem IV.6.2 in [6].

**Proposition 5 (WKL₀)** The Lying Over Theorem: Let $R$ and $S$ be rings such that $R \subseteq S$ and the extension is integral. Let $P$ be a prime ideal of $R$. Then there exists a prime ideal $Q$ of $S$ that lies over $P$, i.e. $Q \cap R = P$.

**Proof.** Let $I = PS$ be the ideal generated by $P$ in $S$ and let $M = R - P$. Then $I$ is a $\Sigma^0_1$ ideal of $S$ and $M$ a multiplicative set of $S$. By Proposition 3.1, it suffices to prove that $I \cap M = \emptyset$. Given that the extension is integral, we can prove that if $m \in PS$, then $m^n + p_{n-1} \cdot m^{n-1} + \ldots + p_1 \cdot m + p_0 = 0$, for some $n > 0$, $p_i \in P$; $i = 0, \ldots, n - 1$. Hence, if $m \in I \cap R - P = \emptyset$, then in particular $m \in R$, so $m^n \in P$ and hence $m \in P$, contradiction. [The details of this proof, as it is given for example in Proposition 2.10 in [5], go through in RCA₀.]

**Proposition 6 (RCA₀)** The Lying Over Theorem implies the Going Up Theorem for integral extensions, i.e. the theorem whose statement is: “Given two rings $R \subseteq S$, such that the extension is integral, and given two prime ideals $P_1 \subseteq P_2$ in $R$ and $Q_1$ a prime ideal in $S$, such that $Q_1 \cap R = P_1$, there exists a prime ideal $Q_2$ in $S$ such that $Q_1 \subseteq Q_2$ and $Q_2 \cap R = P_2$.”

**Proof.** We argue in RCA₀. $R/P_1 = R/Q_1 \cap R$ exists in RCA₀ and it is a subring of $S/Q_1$. It is easy to prove in RCA₀ that if $R \subseteq S$ is integral extension than the extension $R/P_1 \subseteq S/Q_1$ is integral, too. Now $P_2/P_1$ is a prime ideal in $R/P_1$ (since $P_1 \subseteq P_2$ are prime ideals in $R$). Thus by the Lying Over Theorem there exists a prime ideal $Q_2/Q_1$ in $S/Q_1$ such that $Q_2/Q_1 \cap R/P_1 = P_2/P_1$. Hence $Q_2 \cap R = P_2$.

**Proposition 7 (WKL₀)** The Going Down theorem: Let $R$ be a normal domain (i.e. integrally closed in its field of fractions), $S$ a domain and $R \subseteq S$ an integral extension. If $P_1 \subseteq P_2$ are two prime ideals in $R$ and $Q_2$ a prime ideal in $S$, such that $Q_2 \cap R = P_2$, there exists a prime ideal $Q_1$ in $S$ such that $Q_1 \subseteq Q_2$ and $Q_1 \cap R = P_1$.

**Proof.** Let $I = P_1 S$ be the ideal generated by $P_1$ in $S$ and let $M_1 = R - P_1$, $M_2 = S - Q_2$ and $M = M_1M_2 = \{r \cdot s : r \in M_1 \text{ and } s \in M_2\}$. Then $I$ is a $\Sigma^0_1$ ideal of $S$ and $M$ is a $\Sigma^0_1$ multiplicative subset of $S$ containing $I$. Also, $I$ and $M$ are disjoint. The proof, as it is given for example in Proposition 2.16 in [5], goes through in RCA₀. Hence, by Proposition 3.1, we get a prime ideal $Q_1$ disjoint from $M$ and containing $P_1$ and this is the required prime ideal.

**Open Question.** Are all of any of the Lying Over, Going Up and Going Down theorems equivalent to Weak König’s Lemma over RCA₀?
References