Annals of Pure and Applied Logic 31 (1986) 289–306
North-Holland

FACTORIZATION OF POLYNOMIALS AND Σ_1^0 INDUCTION*

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

Rick L. SMITH
Department of Mathematics, University of Florida, Gainesville, FL 32611, USA

Communicated by A. Nerode
Received 19 March 1985

0. Introduction (for algebraists)

In the body of this paper we use the apparatus of mathematical logic to investigate the role of induction in algebraic reasoning. We show that a surprisingly strong form of induction is needed in order to prove certain very basic and simple algebraic lemmas.

The purpose of this section is to explain one of our results in an intuitive way making no use of mathematical logic. We shall construct a 'counterexample' to the assertion that every polynomial over a field has an irreducible factor. The polynomial occurring in our 'counterexample' is the cyclotomic polynomial $x^{2^n}+1$ where $n=2^{1000}$.

Let I be the set of positive integers i having the property that i grains of sand do not constitute a heap of sand. Obviously 1 belongs to I. Furthermore, it is impossible to change a non-heap into a heap by adding one grain of sand. Thus for any $i \in I$ we see that $i+1$ also belongs to I. On the other hand $n=2^{1000}$ clearly does not belong to I. (This counterexample to induction was known to the ancient Greeks as the *paradox of the heap*.) For each $i \in I$ let K_i be the splitting field of $x^{2^i}+1$ over the rational field $\mathbb{Q}=K_0$. Let K be the union of the tower $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_i \subseteq \cdots$ $(i \in I)$. Thus K is a countable field.

We claim that $x^{2^n}+1$ has no irreducible factor over the field K. Suppose that $p(x)$ were such a factor. There must be an $i \in I$ such that all the coefficients of $p(x)$ belong to K_i. Thus $p(x)=x^{2^{n-i}}-\alpha$ where $\alpha^{2^i}+1=0$. But then $p(x)$ factors in K_{i+1} as $(x^{2^{n-i-1}}+\beta)(x^{2^{n-i-1}}-\beta)$ where $\beta=\sqrt{\alpha}$. This is a contradiction since $K_{i+1} \subseteq K$.

In Section 3 below we convert the above line of reasoning into a rigorous

* Research partially supported by NSF grants MCS-8107867 and MVS-8301622.

argument. We show that a certain strong form of induction (known as Σ^0_1 induction) is necessary for any proof of the following lemma: every polynomial over a countable field has an irreducible factor. On the other hand, it was shown in [1] that this same form of induction is sufficient for the development of a certain large portion of countable algebra. Combining these results we have a precise characterization of what form of induction is needed for that portion of algebra.

1. Introduction (for logicians)

In [1] familiar theorems of countable algebra were classified according to the set existence axioms which are needed to prove them. Many theorems of countable algebra turned out in [1] to be equivalent to such axioms, the equivalence being provable over the weak base theory RCA_0. In the present work, we consider refinements of the results of [1] which are obtained by weakening the base theory.

All of the formal theories in [1] and in the present paper are in the language of second order arithmetic. The theory RCA_0 consists of addition, multiplication, Δ^0_1 comprehension and Σ^0_1 induction. The presence of Σ^0_1 induction allows one to define functions from natural numbers to natural numbers by primitive recursion. In particular RCA_0 proves the existence of the exponential function $\exp(m, n) = m^n$.

In the present paper, we study the weaker system RCA_0^* consisting of addition, mutiplication, exponentiation, Δ^0_1 comprehension, and Σ^0_0 induction. Thus RCA_0 is equivalent to RCA_0^* plus Σ^0_1 induction. It is known that RCA_0^* is properly weaker than RCA_0. It turns out that some but not all of the results of [1] which were proved in RCA_0 can be proved in RCA_0^*. For instance, it appears that RCA_0^* is sufficient to prove Theorems 3.5, 4.1, 4.4, 4.5, 5.4, and 6.4 of [1]. The proofs would be essentially the same as in [1] except that Lemma 1.5 of [1] must be replaced by Lemma 2.4 below. We do not know whether Theorems 2.5, 2.12, 3.1, 3.3, and 4.3 of [1] are provable in RCA_0^*. Lemma 2.4 of [1] is definitely not provable in RCA_0^*.

Our main purpose in the present paper is to show that RCA_0^* is not strong enough to prove certain basic lemmas about polynomials in one variable over a countable field. Specifically, let $f(x)$ be any polynomial with integer coefficients in one variable, and let K be any countable field. We show that RCA_0^* is not strong enough to prove any of the following assertions:

(1) $f(x)$ has at least one factor over K which is irreducible over K.

(2) $f(x)$ has a factorization into polynomials over K each of which is irreducible over K.

(3) The set of roots of $f(x)$ in K is finite.

Furthermore, we show that each of the assertions (1), (2) and (3) is equivalent over RCA_0^* to Σ_1^0 induction. Thus no theory in the language of second-order arithmetic, which contains RCA_0^* but does not contain RCA_0, can suffice to prove these assertions.

The results which we have just described constitute a contribution to the program of Reverse Mathematics as described in [1], [2], [3] and [4]. The purpose of Reverse Mathematics is to determine which set existence axioms are needed to prove specific theorems of ordinary mathematics. In the present paper, the ordinary mathematical theorems which we have in mind are assertions (1), (2) and (3) above. The set existence axiom which we have in mind is *bounded Σ_1^0 comprehension*, i.e. the scheme

$$\forall m\, \exists X\, \forall i\, (i \in X \leftrightarrow (i < m \wedge \phi(i)))$$

where $\phi(i)$ is any Σ_1^0 formula in which X does not occur. We shall show in Section 2 that bounded Σ_1^0 comprehension is equivalent to Σ_1^0 induction.

In an unpublished abstract [5], Friedman has announced another result of the above type. Namely, according to Friedman, Σ_1^0 induction is equivalent to the assertion that every finitely generated vector space over the rational numbers (or over any countable field) has a basis. We do not know of any other results of this type, in which theorems of ordinary mathematics are equivalent to Σ_1^0 induction. However, we suspect that there are many such results waiting to be discovered.

2. The formal system RCA_0^*

The language of RCA_0^* is the language of second-order arithmetic augmented by a binary function symbol exp denoting exponentiation. There are *number variables* $i, j, k, m, n, \ldots$ and *set variables* $X, Y, Z, \ldots$ The number variables are intended to range over the set ω of natural numbers, while the set variables are intended to range over subsets of ω. *Numerical terms* are the number variables, the constant symbols 0 and 1, and $t_1 + t_2$, $t_1 \cdot t_2$, $t_1^{t_2}$ ($= \exp(t_1, t_2)$) where t_1 and t_2 are numerical terms. Atomic formulas are $t_1 = t_2$, $t_1 < t_2$, and $t_1 \in X$ where t_1 and t_2 are numerical terms. *Formulas* are built up from atomic formulas by means of propositional connectives, number quantifiers $\forall n$ and $\exists n$, and set quantifiers $\forall X$ and $\exists X$.

The axioms of RCA_0^* include the following *basic axioms*:

$$\begin{array}{ll}
m+1 \neq 0, & m \cdot (n+1) = m \cdot n + m, \\
m+1 = n+1 \rightarrow m = n, & m^0 = 1, \\
m+0 = m, & m^{n+1} = m^n \cdot m, \\
m+(n+1) = (m+n)+1, & \sim m < 0, \\
m \cdot 0 = 0, & m < n+1 \leftrightarrow (m = n \vee m < n).
\end{array}$$

If t is any numerical term and ϕ is any formula, we write $(\forall m<t)\,\phi$ (respectively $(\exists m<t)\,\phi$) as an abbreviation for $\forall m\,(m<t\rightarrow\phi)$ (respectively $\exists m\,(m<t\wedge\phi)$). The quantifiers $\forall m<t$ and $\exists m<t$ are known as *bounded number quantifiers*. A formula is called Σ^0_0 if it is built up from atomic formulas, propositional connectives, and bounded number quantifiers. A formula is called Σ^0_1 (respectively Π^0_1) if it has the form $\exists m\,\phi$ (respectively $\forall m\,\phi$) where ϕ is Σ^0_0. For $k=0$, 1, Σ^0_k *induction* is the scheme

$$(\phi(0)\wedge\forall n\,(\phi(n)\rightarrow\phi(n+1)))\rightarrow\forall n\,\phi(n)$$

where ϕ is Σ^0_k. Also Σ^0_k *comprehension* is the scheme

$$\exists X\,\forall n\,(n\in X\leftrightarrow\phi(n))$$

where ϕ is Σ^0_k and X does not occur in ϕ. Finally Δ^0_1 *comprehension* is the scheme

$$\forall n\,(\phi(n)\leftrightarrow\psi(n))\rightarrow\exists X\,\forall n\,(n\in X\leftrightarrow\phi(n))$$

where ϕ is Σ^0_1, ψ is Π^0_1, and X does not occur in ϕ.

The system RCA_0^* consists of the basic axioms plus Δ^0_1 comprehension plus Σ^0_0 induction. The system RCA_0 consists of the basic axioms plus Δ^0_1 comprehension plus Σ^0_1 induction. Trivially RCA_0 is equivalent to RCA_0^* plus Σ^0_1 induction.

We now sketch a development of some results about sets and functions within RCA_0^*. Ordered pairs of natural numbers are encoded as $(m,n)=(m+n)^2+m$. We use $\mathbb{N}$ to denote the set of all natural numbers as defined within (any model of) RCA_0^*. For any sets X and Y we write $X\times Y=\{(m,n):m\in X\wedge n\in Y\}$. Also N^k is the set of all (natural numbers which are codes for) sequences of natural numbers of length k. Functions $f:X\rightarrow Y$ are identified with sets of (codes for) ordered pairs. The following lemma says that the universe of total functions is closed under Kleene's μ-operator.

2.1. Lemma (RCA_0^*). *Suppose that $g:\mathbb{N}^k\times\mathbb{N}\rightarrow\mathbb{N}$ has the property that $\forall \boldsymbol{m}\,\exists n\,(g(\boldsymbol{m},n)=0)$. Then there is a unique function $f:\mathbb{N}^k\rightarrow\mathbb{N}$ defined by $f(\boldsymbol{m})=$ least n such that $g(\boldsymbol{m},n)=0$.*

Proof. Immediate by Δ^0_1 comprehension. □

The next lemma says that the universe is closed under *bounded primitive recursion*.

2.2. Lemma (RCA_0^*). *Suppose $g:\mathbb{N}^k\rightarrow\mathbb{N}$, $b:\mathbb{N}\times\mathbb{N}^k\rightarrow\mathbb{N}$, $h:\mathbb{N}\times\mathbb{N}\times\mathbb{N}^k\rightarrow\mathbb{N}$. Then there is a unique function $f:\mathbb{N}\times\mathbb{N}^k\rightarrow\mathbb{N}$ defined by $f(0,\boldsymbol{m})=g(\boldsymbol{m})$ and $f(n+1,\boldsymbol{m})=\min(b(n,\boldsymbol{m}),\,h(f(n,\boldsymbol{m}),n,\boldsymbol{m}))$.*

Proof. Fix $\boldsymbol{m}\in\mathbb{N}^k$ and put $b(n)=b(n,\boldsymbol{m})$. We first prove the lemma under the assumption that b is *monotone*, i.e. $b(i)\leqslant b(j)$ whenever $i\leqslant j$. Put $c(n)=b(n)^n$.

Then each function from $\{0, 1, \ldots, n-1\}$ into $\{0, 1, \ldots, b(n-1)\}$ is encoded by a unique integer less than $c(n)$. Using Σ_0^0 induction and Δ_1^0 comprehension we can prove by induction on n that the sequence

$$\langle f(1, \boldsymbol{m}), f(2, \boldsymbol{m}), \ldots, f(n, \boldsymbol{m})\rangle$$

is encoded by some integer less than $c(n)$. Then f itself exists by Δ_1^0 comprehension.

Suppose now that b is not monotone. Using the special case of the lemma which has already been proved, define a function $j: \mathbb{N} \rightarrow \mathbb{N}$ by $j(0) = 0$, $j(n+1) = j(n)$ if $b(n+1) \leqslant b(j(n))$, $j(n+1) = n+1$ otherwise. By Δ_1^0 comprehension define $b'(n) = b(j(n)) = \max\{b(i) : i \leqslant n\}$. Then b' is monotone and we can repeat the previous argument using $c'(n) = b'(n)^n$ instead of $c(n)$. This completes the proof of Lemma 2.2. $\square$

A set X is *bounded* if $\exists n\, \forall m\, (m \in X \rightarrow m < n)$. Let $\langle p_m : m \in \mathbb{N}\rangle$ be the enumeration of the prime numbers in increasing order. A set X is *finite* if it is encoded by a single number, i.e. if $\exists n\, \forall m\, (m \in X \leftrightarrow p_m$ divides $n)$.

2.3. Lemma (RCA$_0^*$). *Every bounded set is finite.*

Proof. Given X, use bounded primitive recursion to define $f: \mathbb{N} \rightarrow \mathbb{N}$ by $f(0) = 1$, $f(m+1) = f(m) \cdot p_m$ if $m \in X$, $f(m+1) = f(m)$ if $m \notin X$. Thus $f(n) = \Pi\{p_m : m < n \wedge m \in X\}$. If X is bounded by n, then X is encoded by $f(n)$. $\square$

2.4. Lemma (RCA$_0^*$). *Let $\phi(n)$ be any Σ_1^0 formula. There exist a set $X \subseteq \mathbb{N}$ and a one-to-one function $f: X \rightarrow \mathbb{N}$ such that $\forall n\, (\phi(n) \leftrightarrow \exists m\, (m \in X \wedge f(m) = n))$.*

Proof. Let $\phi(n) = \exists j\, \theta(j, n)$ where θ is Σ_0^0. By Σ_0^0 comprehension let $X = \{(j, n) : \theta(j, n) \wedge \sim(\exists i < j)\, \theta(i, n)\}$. Define $f: X \rightarrow N$ by $f((j, n)) = n$.

2.5. Lemma (RCA$_0^*$). *The following are pairwise equivalent:*

(a) *Σ_1^0 induction.*

(b) *The universe of total functions is closed under primitive recursion.*

(c) *For any infinite set X there exists a principal function $\pi_X: \mathbb{N} \rightarrow X$ which enumerates the elements of X in increasing order.*

(d) *Bounded Σ_1^0 comprehension.*

(e) *If $\phi(i)$ is Σ_1^0 and $\forall i\, (\phi(i) \rightarrow i < n)$ and $\forall i\, \forall j\, ((\phi(j) \wedge i < j) \rightarrow \phi(i))$, then $\exists m\, \forall i\, (\phi(i) \leftrightarrow i < m)$.*

Proof. The implications (a) to (b) to (c) to (d) are proved in [1]. The implication from (d) to (e) is obvious. To prove that (e) implies Σ_1^0 induction, assume $\psi(0) \wedge \forall k\, (\psi(k) \rightarrow \psi(k+1)) \wedge \sim\psi(n)$ where ψ is Σ_1^0. Put $\phi(i) = \exists k\, (i \leqslant k < n \wedge \psi(k))$. Then by (e) there exists m such that $\forall i\, (\phi(i) \leftrightarrow i < m)$. Then $\psi(m) \wedge \sim(m+1)$, a contradiction. This completes the proof. $\square$

In order to orient the reader, we shall now give an example of a model of RCA_0^* in which Σ_1^0 induction fails. For more results on models of RCA_0^*, see Section 4 below.

2.6. Example. Let M be any nonstandard model of first-order Peano arithmetic. Let $a \in |M|$ be any nonstandard integer and define a sequence $b_0 = a$, $b_{n+1} = b_n^{b_n}$, $n \in \omega$. Let $|I|$ be the set of all $b \in |M|$ such that $b <^M b_n$ for some $n \in \omega$. Clearly $|I|$ is a proper initial segment of $|M|$. Let I be the submodel of M whose universe is $|I|$. Then I is a model of the first-order part of RCA_0^*. If we let the set variables range over subsets of $|I|$ of the form $X \cap |I|$ where X is M-finite, then I becomes a model of RCA_0^*. Note that the set of standard integers is a proper Σ_1^0 initial segment of I, so we have an explicit failure of 2.5(e).

3. Algebra in RCA_0^*

A *countable field* is a set $F \subseteq \mathbb{N}$ with operations $+, -, \cdot$ defined on F and constants $0, 1$ where the usual field axioms are satisfied. A Σ_1^0 formula $\phi(v)$ *defines a* Σ_1^0 *subfield of* F if $\phi(0)$ and $\phi(1)$ hold and $\forall x\,(\phi(x) \rightarrow x \in F)$ and $\forall x, y\,((\phi(x) \wedge \phi(y) \wedge y \neq 0) \rightarrow (\phi(x+y) \wedge \phi(x-y) \wedge \phi(x \cdot y) \wedge \phi(x \div y)))$. These definitions can be extended in the obvious way to algebraic structures other than fields. The next lemma is useful in showing that many results in [1] which were proved in RCA_0 can be proved in RCA_0^*.

3.1. Lemma (RCA_0^*). *Let F be a countable field and suppose that $\phi(v)$ defines a Σ_1^0 subfield of F. Then there is a field K and a monomorphism $f: K \rightarrow F$ such that $\forall x\,(\phi(x) \leftrightarrow \exists y \in K\,(f(y) = x))$. Thus, every Σ_1^0 subfield is the range of a monomorphism.*

Proof. By Lemma 2.4 there is a set X and a one-to-one $f: X \rightarrow F$ such that $\forall x\,(\phi(x) \leftrightarrow \exists y \in X\,(f(y) = x))$. Define field operations on X in the unique way so that f is a monomorphism. $\square$

Other, more common, methods of constructing fields are also available to us. For example, given a ring R and indeterminates $x_0, x_1, \ldots$ we may construct the polynomial ring $R[x_0, x_1, \ldots]$ or, if R is a domain, we have the rational functions $R(x_0, x_1, \ldots)$ over R. These constructions can be found in [9]. If R is a ring and I is an ideal of R, then R/I can be represented by a set of coset representatives where the least element of each coset is chosen.

While these constructions work well in RCA_0^*, other techniques require Σ_1^0 induction. The troublesome techniques arise when we introduce the structure of the nature numbers into the field. This is done when we study polynomials of arbitrary degree or when we define the 'characteristic homomorphism' $f:\mathbb{Z}\to F$ by $f(1)=1$. (Here $\mathbb{Z}$ is the ring of integers.)

To illustrate, let us consider the characteristic homomorphism. We can define $\phi:\mathbb{N}\to F$ by the primitive recursion $\phi(0)=0$ and $\phi(n+1)=\phi(n)+1$. This is not a bounded primitive recursion, since the $+$ on the right hand side is a field operation. Furthermore, the existence of a function ϕ which satisfies this recursion is equivalent to Σ_1^0 induction. We capture this in the next definition and theorem.

3.2. Definition. A countable field F is an *evaluation field* if for each $n\in\mathbb{N}$ there is a function $E:\mathbb{Z}[x_0,\ldots,x_{n-1}]\times F^n\to F$ which satisfies these clauses for $\boldsymbol{a}=(a_0,\ldots,a_{n-1})$:

(1) $E(0,\boldsymbol{a})=0$ and $E(1,\boldsymbol{a})=1$,

(2) $E(x_i,\boldsymbol{a})=a_i$,

(3) $E(f+g,\boldsymbol{a})=E(f,\boldsymbol{a})+E(g,\boldsymbol{a})$,

(4) $E(f\cdot g,\boldsymbol{a})=E(f,\boldsymbol{a})\cdot E(g,\boldsymbol{a})$.

We call E the *evaluation function.*

This definition can be made for other algebraic structures by evaluating arbitrary terms in the language of the structure.

3.3. Theorem (RCA_0^*). *Σ_1^0 induction is equivalent to the statement "Every countable field is an evaluation field".*

Proof. Since an evaluation function E can be obtained by primitive recursion it is clear that Σ_1^0 induction implies that every countable field is an evaluation field.

Suppose conversely, that Σ_1^0 induction fails. By Lemma 2.5(e) there is an $n\in\mathbb{N}$ and a Σ_1^0 formula $\phi(x)$ such that

$$\forall x\,(\phi(x)\to x\leqslant n)\wedge\forall x,y\,(x<y\leqslant n\wedge\phi(y)\to\phi(x)),$$

but there is no $m\leqslant n$ with $\forall x\,(\phi(x)\leftrightarrow x\leqslant m)$. Notice that $\forall x\,(\phi(x)\to\phi(x+1))$, but we assume more by considering the formula $\psi(x)\leftrightarrow\exists z\leqslant n\,(\phi(z)\wedge x\leqslant 2^{2^z})$. We see that $\forall x,y\,((\psi(x)\wedge\psi(y))\to(\psi(x+y)\wedge\psi(x\cdot y)))$, and there is no $m\leqslant 2^{2^n}$ such that $\forall x\,(x\leqslant m\leftrightarrow\psi(x))$. Thus we will assume that ϕ is closed under $+$ and $\cdot$.

By Lemma 2.4 there is a set X and a one-to-one function $f:X\to\mathbb{N}$ such that $\forall x\,(\phi(x)\leftrightarrow\exists y\in X\,(f(y)=x))$. Through f, X acquires the structure of $+$, $\cdot$ and $<$. By the usual algebraic constructions there is an ordered field F and an order-preserving monomorphism $g:X\to F$. The field F is minimal in the sense that if $h=g\circ f^{-1}$, then

$$\forall x\in F\,\exists k\,(\phi(k)\wedge x\leqslant h(k)).$$

We claim that F is not an evaluation field. In fact, we claim that $p(x)=n\cdot x$

cannot be evaluated at $x=1$. If $n\cdot 1\in F$, then there is a $k\leqslant n$ such that $\phi(k)$ and $n\cdot 1\leqslant h(k)$. But $h^{-1}(n\cdot 1)=n$ so that $n=k$ and n is a maximal element for ϕ which is a contradiction. □

We cannot expect a field to be an evaluation field when working in RCA_0^*, but many of our favorite fields are evaluation fields. We are taking special care to use only evaluation fields to prove our principal results about polynomials. The next few lemmas are to provide us with a stock of evaluation fields.

A ring with an evaluation function will be called an *evaluation ring*. We say a ring R has a *sum* and *product* if there are functions S and P on finite sequences of elements of R into R which satisfy these recurrence relations:

$$S(\langle a\rangle)=a, \qquad S(\langle a_1,\ldots,a_n,a_{n+1}\rangle)=S(\langle a_1,\ldots,a_n\rangle)+a_{n+1},$$

and

$$P(\langle a\rangle)=a, \qquad P(\langle a_1,\ldots,a_n,a_{n+1}\rangle)=P(\langle a_1,\ldots,a_n\rangle)\cdot a_{n+1}.$$

3.4. Lemma (RCA_0^*). *If R has a sum and product, then R is an evaluation ring.*

Proof. This is a simple substitution using Δ_1^0 comprehension. □

3.5. Lemma (RCA_0^*). *The field of rational numbers, $\mathbb{Q}$, is an evaluation field.*

Proof. First observe that $\mathbb{N}$ has a sum and product by bounded primitive recursion. For example, we may obtain $P(\langle a_0,\ldots,a_n\rangle)=f(\langle a_0,\ldots,a_n\rangle,n)$ where f is given by

$$f(m,0)=\begin{cases} a, & \text{if } m=\langle a\rangle,\\ 0, & \text{otherwise,}\end{cases}$$

$$f(m,n+1)=\begin{cases} f(k,n)\cdot a, & \text{if } m=\langle k,a\rangle \text{ and } k \text{ has length } n+1,\\ 0, & \text{otherwise.}\end{cases}$$

$f(m,n)$ is bounded by m^n. A sum and product for $\mathbb{Z}$ and $\mathbb{Q}$ can now be easily defined. □

3.6. Lemma (RCA_0^*). *Let $t_0,\ldots,t_k$ be indeterminates, then $\mathbb{Q}[t_0,\ldots,t_k]$ is an evaluation ring.*

Proof. $\mathbb{Q}[t_0,\ldots,t_k]$ inherits a sum directly from $\mathbb{Q}$. As for the product, consider the coefficient c of a monomial $m=t_0^{i_0}\cdots t_k^{i_k}$ occurring in the product of $f_0,\ldots,f_n$. Now $c=\sum_\sigma(\prod_{i=0}^n\sigma(i))$ where σ runs over all sequences with $\sigma(i)$ the coefficient of m_i occurring in f_i and $\prod_{i=0}^n m_i=m$. Clearly, the set of these σ is bounded and hence, by Lemma 2.3, is finite. We may now apply the sum and product from $\mathbb{Q}$ to obtain c. This can be done uniformly for all coefficients in the product of $f_0,\ldots,f_n$. □

3.7. Lemma (RCA_0^*). *Let $R = \mathbb{Q}[t_0, \ldots, t_n]$ and let M be a maximal ideal in R, then R/M is an evaluation field.*

Proof. Immediate from Lemma 3.6 and the definition of R/M. □

This concludes our discussion of evaluation fields. As mentioned above, our principal theorems will be proven using evaluation fields. We now show, with the aid of Σ_1^0 induction, that the assertions (1), (2) and (3) given in the introduction hold.

3.8. Lemma (RCA_0). *Let F be a countable field and $f(x) \in F[x]$. Then*
(1) *$f(x)$ has an irreducible factor.*
(2) *$f(x)$ has a finite factorization into irreducible polynomials over F.*
(3) *$f(x)$ has only finitely many roots in F.*

Proof. Since (1) and (3) follow easily from (2) we need only prove (2). Define

$$\phi(n) \leftrightarrow \exists m \geqslant n\ \exists g_1, \ldots, g_m \in F[x]\ (f(x) = g_1(x) \cdots g_m(x)).$$

Notice that $\forall n\ (\phi(n) \to n \leqslant \deg(f))$, so by Σ_1^0 induction (in the form of Lemma 2.5(e)) there is an $m \leqslant \deg(f)$ such that $\forall n\ (\phi(n) \to n \leqslant m)$ and $\phi(m)$. Thus if $f(x) = g_1(x) \cdots g_m(x)$ each $g_i(x)$ is irreducible. □

While we not particularly interested in the uniqueness of factorizations, we note that uniqueness can also be shown in RCA_0. These results can be extended to multivariate polynomials.

3.9. Theorem (RCA_0^*). *The following are pairwise equivalent:*
(a) *Σ_1^0 induction.*
(b) *For each countable field F and every polynomial $f(x) \in F[x]$, $f(x)$ has only finitely many roots in F.*
(c) *Same as* (b) *with 'field' replaced by 'evaluation field'.*

Proof. (a) implies (b) by Lemma 3.8 and (b) implies (c) trivially. We use Lemma 2.5(d) to show (c) implies (a). Let $\phi(x)$ be a Σ_1^0 formula and $n \in \mathbb{N}$. We want to show that $\{m \leqslant n : \phi(m)\}$ exists.

Let $R = \mathbb{Q}[t_0, \ldots, t_n]$ and $M = \langle t_k^2 - p_k : k \leqslant n \rangle$ where $p_0, p_1, \ldots$ is an enumeration of the primes. At this stage we have not yet shown that M exists and is maximal. We first show M is maximal by showing that every element of R has an inverse modulo M. Every element of R can be written as a $\mathbb{Q}$-linear combination of monomials $t_{i_1} \cdots t_{i_k}$, modulo M. Furthermore, we can write an element in the form $a + bt_k$ where t_k does not occur in either a or b. We can now explicitly define the inverse by bounded primitive recursion, viz.

$$i(a) = a^{-1} \quad \text{if } a \in \mathbb{Q} \text{ and } a \neq 0,$$

$$i(a + bt_k) = \begin{cases} i(a) & \text{if } a \neq 0 \text{ and } b = 0, \\ i(bp_k)t_k & \text{if } a = 0 \text{ and } b \neq 0, \\ a \cdot i(a^2 - b^2 p_k) - b \cdot i(a^2 - b^2 p_k)t_k & \text{if } a, b \neq 0. \end{cases}$$

It is easily checked by Σ_0^0 induction that $(a + bt_k) \cdot i(a + bt_k) = 1$ if a and b are not both 0. Thus M is maximal. M exists by Δ_1^0 comprehension, since $f \notin M \leftrightarrow \exists g \in R\ (f \cdot g - 1 \in M)$. By Lemma 3.7 R/M is an evaluation field.

Let $\psi(x)$ be the Σ_1^0 formula which asserts that x is in the subfield of R/M generated by those t_k, $k \leq n$ and $\phi(k)$. By Lemma 3.1 there is a field F and a monomorphism $g: F \to R/M$ such that $\psi(x) \leftrightarrow \exists y \in F\ (g(y) = x)$. The restriction of the evaluation function on R/M to F is an evaluation function on F.

Let $f(x) = \prod_{i=0}^{n} (x^2 - p_i)$ and suppose that $\{\alpha \in F : f(\alpha) = 0\}$ is finite. Thus $\{m \leq n : \exists \alpha \in F\ (f(\alpha) = 0 \wedge g(\alpha) = p_m)\}$ is finite, but this is clearly the same as $\{m \leq n : \phi(m)\}$. □

3.10. Theorem (RCA$_0^*$). *The following are pairwise equivalent:*

(a) *Σ_1^0 induction.*

(b) *For every countable field and every polynomial $f(x) \in F[x]$, $f(x)$ has a finite factorization into irreducible polynomials over F.*

(c) *Same as* (b) *with 'field' replaced by 'evaluation field'.*

Proof. We show (c) implies (a). Let F be the field constructed in Theorem 3.9. Suppose $f(x) = \prod_{i=0}^{n} (x^2 - p_i)$ has a finite factorization into irreducibles, $f(x) = g_1(x) \cdots g_m(x)$. Thus

$$\{\alpha \in F : f(\alpha) = 0\} = \{\alpha \in F : \exists i \leq m\ (x - \alpha = g_i(x))\}$$

is a finite set, and following the proof of Theorem 3.9 we see that Σ_1^0 induction holds. □

3.11. Theorem (RCA$_0^*$). *The following are pairwise equivalent:*

(a) *Σ_1^0 induction.*

(b) *For every countable field F and every polynomial $f(x) \in F[x]$, $f(x)$ has an irreducible factor.*

(c) *Same as* (b) *with 'field' replaced by 'evaluation field'.*

Proof. We show (c) implies (a) by using 2.5(e). Let $\phi(v)$ be Σ_1^0 and $n \in \mathbb{N}$ and suppose that $\forall k < l \leq n\ (\phi(l) \to \phi(k)) \wedge \forall k\ (\phi(k) \to k \leq n)$. We want to find an $m \leq n$ such that $\forall k\ (\phi(k) \leftrightarrow k \leq m)$. The proof uses the splitting fields K_m of the cyclotomic polynomials $g_m(x) = x^{2^m} + 1$. The next lemma has the basic facts about these fields.

3.12. Lemma (RCA_0^*). *For each $m \in \mathbb{N}$:*

(1) *K_m exists and is an evaluation field.*

(2) *If $l < m$, then $K_l \subset K_m$.*

(3) *$[K_m : \mathbb{Q}] = 2^m$ and $[K_n : K_m] = 2^{n-m}$.*

(4) *If $p(x) \in K_m[x]$ is an irreducible factor of $g_n(x)$, then $p(x) = x^{2^{n-m}} - \omega$ for some $\omega \in K_m$ a root of $g_m(x)$.*

Proof. Let $R_m = \mathbb{Q}[t_1, \ldots, t_m]$ and M_m the ideal generated by $t_1^2 + 1$, $t_2^2 - t_1, \ldots, t_m^2 - t_{m-1}$. Using the same methods as in Theorem 3.9 we see that M_m exists and is a maximal ideal. We claim $K_m = R_m/M_m$ is the splitting field of $g_m(x)$. By Lemma 3.7 K_m is an evaluation field.

For each $s \in 2^m$ we define $\omega_s \in K_m$, a root of $g_m(x)$. This is done by bounded primitive recursion. For $m = 1$, $\omega_0 = \sqrt{-1} = t_1$, and $\omega_1 = -\omega_0$. If ω_s is defined, $\omega_{s0} = \sqrt{\omega_s}$ and $\omega_{s1} = -\sqrt{\omega_s} = -\omega_{s0}$. By Σ_0^0 induction, $\omega_s \in K_m$ if $s \in 2^m$ and $g_m(\omega_s) = 0$. Furthermore, if $s \neq t$, then $\omega_s \neq \omega_t$, and $\omega_s = t_m$ if $s = (0, \ldots, 0) \in 2^m$. Now K_m is generated by t_m, contains all roots of $g_m(x)$, and hence K_m is the splitting field of $g_m(x)$. This proves (1) and (2).

Given $s, t \in 2^m$ we can define by bounded primitive recursion a $\mathbb{Q}$-automorphism $\theta : K_m \to K_m$ such that $\theta(\omega_s) = \omega_t$. This is possible since $x^2 - \omega_s$ is irreducible over K_l for $s \in 2^l$. By the classical Kronecker factorization algorithm [6, p. 82], t_m has an irreducible polynomial $h(x)$ over $\mathbb{Q}$. Since $h(\theta(t_m)) = 0$, we see that $h(x)$ has 2^n distinct roots, and thus $h(x) = x^{2^m} + 1$ and $[K_m : \mathbb{Q}] = 2^m$. The standard proof shows that $[K_n : \mathbb{Q}] = [K_n : K_m] \cdot [K_m : \mathbb{Q}]$ so that $[K_n : K_m] = 2^{n-m}$. This proves (3).

Let $\omega \in K_m$ be a root of $g_m(x)$, so that $\omega = \omega_s$ for some $s \in 2^m$. Now every root of $x^{2^{n-m}} - \omega$ in K_n is a root of $x^{2^n} + 1$, so by counting, $x^{2^n} + 1 = \prod_{s \in 2^m} (x^{2^{n-m}} - \omega_s)$. We claim that $x^{2^{n-m}} - \omega$ is irreducible. Let $v \in K_n$ be a root of $x^{2^{n-m}} - \omega$, then v is a root of $x^{2^n} + 1$ and hence $\mathbb{Q}(v) = K_n$. Thus $x^{2^{n-m}} - \omega$ splits completely on the adjunction of a single root, it follows that $x^{2^{n-m}} - \omega$ is irreducible. This proves (4) and concludes the proof of Lemma 3.12. □

Let $\psi(x) \leftrightarrow \exists m \leq n\, (\phi(m) \wedge x \in K_m)$. Clearly $\psi(x)$ defines a Σ_1^0 subfield of K_n, so by Lemma 3.1 there is a field F and a monomorphism $f : F \to K_n$ such that $\forall x\, (\psi(x) \leftrightarrow \exists y \in F\, (f(y) = x))$. The restriction of the evaluation function on K_n is an evaluation function on F. Thus F is an evaluation field.

Suppose that $g_n(x)$ has an irreducible factor $p(x) \in F[x]$. We may assume that $p(x) \in K_m[x]$ for some $m \leq n$ where $\phi(m)$ holds. Also $p(x)$ is irreducible over $K_m[x]$, so by Lemma 3.12(4), $p(x) = x^{2^{n-m}} - \omega$ for some $\omega \in K_m$. Now if $\phi(m+1)$ holds, then $p(x)$ is irreducible over K_{m+1} also, and hence $p(x) = x^{2^{n-m-1}} - v$ for some $v \in K_{m+1}$, which is impossible. Thus m is maximal and by Lemma 2.5(e), Σ_1^0 induction holds. $\square$

4. Models of $\mathbf{RCA}_0^*$

The purpose of this section is to study logical properties of the formal system RCA_0^*. Our method is to prove theorems concerning models of RCA_0^*. From these model-theoretic results we deduce proof-theoretic corollaries.

Let L_2 be the language of RCA_0^*, i.e. the language of second-order arithmetic augmented by a binary function symbol $\exp(m, n) = m^n$. A *model for* L_2 is an ordered 8-tuple

$$M = (|M|, \mathcal{S}^M, +^M, \cdot^M, \exp^M, <^M, 0^M, 1^M)$$

where $|M|$ is a set; $\mathcal{S}^M$ is a collection of subsets of $|M|$; $+^M$, $\cdot^M$, and $\exp^M$ are functions from $|M| \times |M|$ into $|M|$; $<^M$ is a subset of $|M| \times |M|$; and 0^M and 1^M are distinguished elements of $|M|$. Let T be any theory in the language L_2. We say the *M satisfies T* or *is a model of T* if the axioms of T are universally true in M when the number variables range over $|M|$, the set variables range over $\mathcal{S}^M$, and $+$, $\cdot$, exp, $<$, 0, 1, are interpreted in the obvious way. All of the models we consider will satisfy the basic axioms plus Σ_0^0 induction (cf. Section 2).

The *first-order part of M* is the ordered 7-tuple obtained from the ordered 8-tuple M by omitting $\mathcal{S}^M$. We shall now characterize the first-order parts of models of RCA_0^*.

By Σ_1^0 *collection* we mean the scheme

$$\forall i\, \exists j\, \phi(i, j) \rightarrow \forall m\, \exists n\, \forall i < m\, \exists j < n\, \phi(i, j)$$

where $\phi(i, j)$ is any Σ_1^0 formula in which m and n do not occur.

4.1. Lemma. RCA_0^* *proves* Σ_1^0 *collection.*

Proof. We reason in RCA_0^*. Assume $\forall i\, \exists j\, \phi(i, j)$. Let $\phi(i, j) = \exists k\, \theta(i, j, k)$ where θ is Σ_0^0. Write $(j, k) = (j + k)^2 + j$. Using Σ_0^0 induction and Δ_1^0 comprehension, we get a function $f: \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(i) =$ least (j, k) such that $\theta(i, j, k)$ holds. Using bounded primitive recursion, define $g: \mathbb{N} \rightarrow \mathbb{N}$ by $g(0) = f(0)$, $g(m + 1) = g(m)$ if $f(m + 1) \leq f(g(m))$, $g(m + 1) = m + 1$ otherwise. By Δ_1^0 comprehension define $h(m) = f(g(m)) + 1 = \max\{f(i) + 1 : i \leq m\}$. Then $(\forall i < m)(\exists (j, k) < h(m))\theta(i, j, k)$ so clearly $(\forall i < m)(\exists j < n)\phi(i, j)$ with $n = h(m)$. This completes the proof. $\square$

4.2. Lemma. *Let M be any model of the basic axioms plus* Σ_0^0 *induction plus* Σ_1^0 *collection. Then there exists a model M′ of* RCA_0^* *such that M is a submodel of M′ and has the same first order part.*

Proof. Let M' be the model with the same first-order part as M and $\mathcal{S}^{M'} = \Delta_1^0 - \mathrm{Def}(M)$ = the set of all $X \subseteq |M|$ such that X is Δ_1^0 definable over M allowing parameters from $|M| \cup \mathcal{S}^M$. Clearly $\mathcal{S}^M \subseteq \mathcal{S}^{M'}$ so we need only verify that M' satisfies Δ_1^0 comprehension and Σ_0^0 induction.

Let θ be any Σ_0^0 formula with parameters from $|M| \cup \mathcal{S}^{M'}$ and no free set variables. We claim that there exist a Σ_1^0 formula Θ_Σ and a Π_1^0 formula Θ_Π with parameters from $|M| \cup \mathcal{S}^M$ only, having the same free variables as θ and equivalent to θ over M'. We define Θ_Σ and Θ_Π by recursion on the number of symbols in θ. If θ is $t_1 = t_2$ or $t_1 < t_2$ put $\Theta_\Sigma = \Theta_\Pi = \theta$. If θ is $t_1 \in X$ put $\Theta_\Sigma = \phi(t_1)$ and $\Theta_\Pi = \psi(t_1)$ where ϕ and ψ are as in the Δ_1^0 definition of the parameter $X \in \Delta_1^0 - \mathrm{Def}(M)$. If $\theta = {\sim}\theta'$ put $\Theta_\Sigma = {\sim}\Theta'_\Pi$ and $\Theta_\Pi = {\sim}\Theta'_\Sigma$. If $\theta = (\forall i < t)\, \theta'$ put $\Theta_\Sigma = \exists n\, (\forall i < t)\, (\exists j < n)\, \theta''$ where $\Theta'_\Sigma = \exists j\, \theta''$. If $\theta = \theta' \wedge \theta''$ put $\Theta_\Sigma = \exists k\, ((\exists i < k)\, \theta'_0 \wedge (\exists j < k)\, \theta''_0)$ where $\Theta'_\Sigma = \exists i\, \theta'_0$ and $\Theta''_\Sigma = \exists j\, \theta''_0$. The proof that Θ_Σ and Θ_Π are equivalent to θ over M' is a straightforward application of Σ_1^0 collection.

From the previous claim it follows easily that for any Σ_1^0 (respectively Π_1^0) formula with parameters from $|M| \cup \mathcal{S}^{M'}$ and no free set variables, there exists an equivalent Σ_1^0 (respectively Π_1^0) formula with parameters from $|M| \cup \mathcal{S}^M$ only. Hence M' satisfies Δ_1^0 comprehension.

Now given $X \in \mathcal{S}^{M'}$ let $\theta(i, j)$ and $\theta'(i, j)$ be Σ_0^0 formulas with parameters from $|M| \cup \mathcal{S}^M$ and no free variables except i and j, such that $X = \{a \in |M| : M$ satisfies $\exists j\, \theta(a, j)\} = \{a \in |M| : M$ satisfies $\forall j\, \theta'(a, j)\}$. Then M satisfies $\forall i\, \exists j\, (\theta(i, j) \vee {\sim}\theta'(i, j))$. Hence by Σ_1^0 collection M satisfies $\forall m\, \exists n\, (\forall i < m)\, (\exists j < n)\, (\theta(i, j) \vee {\sim}\theta'(i, j))$. For any such m and n we have $(\forall i < m)\, (i \in X \leftrightarrow (\exists j < n)\, \theta(i, j))$. By Σ_0^0 induction in M it follows that if X is nonempty, then X has a least element. It is now clear that M' satisfies Σ_0^0 induction. This completes the proof of Lemma 4.2. □

Let L_1 be the language which is just like L_2 except that the set variables are omitted. The *first-order part of a theory* T in L_2 is the restriction of T to L_1.

4.3. Theorem. *The first-order parts of models of* RCA_0^* *are precisely the models for* L_1 *which satisfy the basic axioms plus* Σ_0^0 *induction plus* Σ_1^0 *collection.* (In the terminology of [7] these are just the models of $B\Sigma_1 + \exp$.)

Proof. Immediate from Lemma 4.1 and 4.2. □

4.4. Corollary. *The first-order part of* RCA_0^* *is just the theory in* L_1 *whose axioms are the basic axioms,* Σ_0^0 *induction, and* Σ_1^0 *collection.* (This is the theory $B\Sigma_1 + \exp$ of [7].)

Proof. Immediate from Theorem 4.3 plus Gödel's completeness theorem. □

We now consider the effect of adding weak König's lemma to RCA_0^*. It will turn out that this modification does not affect the first-order part of the theory.

Within RCA_0^* we define Seq_2 to be the set of all (natural numbers which are codes for) finite sequences of elements of the set $\{0, 1\}$. For any $X \subseteq \mathbb{N}$ and $n \in \mathbb{N}$ we define $X[n] \in \mathrm{Seq}_2$ to be the sequence $X[n] = \langle x_0, x_1, \ldots, x_{n-1}\rangle$ where $x_i = 0$ if $i \notin X$, $x_i = 1$ if $i \in X$. A *tree* is a set $T \subseteq \mathrm{Seq}_2$ such that every initial segment of an element of T is an element of T. A *path* through T is a set $X \subseteq N$ such that $X[n] \in T$ for all $n \in N$. *Weak König's lemma* is the assertion that for every infinite tree $T \subseteq \mathrm{Seq}_2$ there exists a path through T. Let WKL_0^* be the theory in L_2 whose axioms are those of RCA_0^* plus weak König's lemma. (Similarly WKL_0 consists of RCA_0 plus weak König's lemma. See [1], [2], [3], [4].)

4.5. Lemma. *Let M be any countable model of* RCA_0^*. *Let $T \in \mathcal{S}^M$ be such that T is satisfied in M to be an infinite subtree of* Seq_2. *Then there exists a countable model M' of* RCA_0^* *such that*:

(i) *M is a submodel of M' with the same first-order part*;

(ii) *T is satisfied in M' to have a path.*

Proof. We use a generalization of a forcing construction due to Jockusch and Soare [8, Theorem 2.4]. Let $\mathcal{T}^M$ be the set of all $T \in \mathcal{S}^M$ such that T is satisfied in M to be an infinite subtree of Seq_2. We say that $\mathcal{D} \subseteq \mathcal{T}^M$ is *dense* if $(\forall T \in \mathcal{T}^M)$ $(\exists T' \in \mathcal{D})$ $(T' \subseteq T)$. We say that $\mathcal{D}$ is *definable* if it is definable over M allowing parameters from $|M| \cup \mathcal{S}^M$. We say that $X \subseteq |M|$ is *M-generic* if for each definable $\mathcal{D} \subseteq \mathcal{T}^M$ there exists $T \in \mathcal{D}$ such that X is a path through T.

Suppose that X is M-generic. Let M' be the model with the same first-order part as M and $\mathcal{S}^{M'} = \mathcal{S}^M \cup \{X\}$. We claim that M' satisfies Σ_0^0 induction and Σ_1^0 collection.

We now prove the claim. Σ_0^0 induction is clear since $X[k] \in \mathrm{Seq}_2^M$ for each $k \in |M|$. To prove Σ_1^0 collection let $\phi(i, j)$ be a Σ_1^0 formula with parameters from $|M| \cup \mathcal{S}^{M'}$ and suppose that M' satisfies $\forall i\, \exists j\, \phi(i, j)$. Write $\phi(i, j)$ in normal form as $\exists k\, \theta(i, j, X[k])$ where $\theta(i, j, \sigma)$ is Σ_0^0 with parameters from $|M| \cup \mathcal{S}^M$ only. Let $\mathcal{E}$ be the set of all $T \in \mathcal{T}^M$ such that M satisfies

$$\exists i\, (\forall \tau \in T)\, (\forall j \leqslant \mathrm{lh}(\tau))\, (\forall k \leqslant \mathrm{lh}(\tau)) \sim \theta(i, j, \tau[k]).$$

Here $\mathrm{lh}(\tau)$ denotes the length of τ and $\tau[k]$ is the unique initial segment of τ of length k. Let $\mathcal{D}$ be the set of all $T \in \mathcal{T}^M$ such that $T \in \mathcal{E} \vee \sim(\exists T' \in \mathcal{E})\, (T' \subseteq T)$. Clearly $\mathcal{D}$ is dense and definable so let $T \in \mathcal{D}$ be such that X is a path through T. Since $\forall i\, \exists j\, \exists k\;\; \theta(i, j, X[k])$ holds, we cannot have $T \in \mathcal{E}$. Hence there is no $T' \in \mathcal{E}$ with $T' \subseteq T$. For each $i \in |M|$ let T_i be the subtree of T consisting of all $\tau \in T$ such that $(\forall j \leqslant \mathrm{lh}(\tau))\, (\forall k \leqslant \mathrm{lh}(\tau)) \sim \theta(i, j, \tau[k])$. Since $T_i \notin \mathcal{E}$ we must have that T_i is satisfied in M to be finite. Thus M satisfies

$$\forall i\, \exists n\, (\forall \tau \in T)\, (\mathrm{lh}(\tau) = n \rightarrow (\exists j < n)\, (\exists k < n)\, \theta(i, j, \tau[k])).$$

By Σ_1^0 collection in M we get

$$\forall m\, \exists n\, (\forall \tau \in T)(\mathrm{lh}(\tau) = n \rightarrow (\forall i < m)\,(\exists j < n)\,(\exists k < n)\, \theta(i, j, \tau[k])).$$

In particular we have

$$\forall m\, \exists n\, (\forall i < m)\,(\exists j < n)\,(\exists k < n)\, \theta(i, j, X[k])$$

so M' satisfies $\forall m\, \exists n\, (\forall i < m)\,(\exists j < n)\, \phi(i, j)$. Thus we have Σ_1^0 collection in M'. This proves our claim.

We shall now complete the proof of Lemma 4.5. Let $T \in \mathcal{T}^M$ be given. Using the countability of M, we can find an M-generic $X \subseteq |M|$ such that X is a path through T. Let M' be as in our claim. By Lemma 4.2 we can find a model M'' of RCA_0^* such that M' is a submodel of M'' and has the same first-order part. Then clearly M'' satisfies the conclusions of Lemma 4.5. This completes the proof. □

4.6. Theorem. *Let M be any countable model of* RCA_0^*. *Then there exists a countable model M' of* WKL_0^* *such that M is a submodel of M' and has the same first-order part.*

Proof. Use Lemma 4.5 repeatedly to get a sequence of models $\langle M_i : i \in \omega \rangle$ such that $M_0 = M$, each M_i is a submodel of M_{i+1} with the same first-order part, each M_i is a model of RCA_0^*, and for each $T \in \mathcal{T}^{M_i}$ there exists $j > i$ such that T is satisfied in M_j to have a path. Put $M' = \bigcup \{M_i : i \in \omega\}$, i.e. M' is the model with the same first-order part as M and $\mathcal{S}^{M'} = \bigcup \{\mathcal{S}^{M_i} : i \in \omega\}$. Then clearly M' is a model of WKL_0^*. This completes the proof. □

A formula is said to be *arithmetical* if it contains no set quantifiers. A formula is said to be Π_1^1 if it is of the form $\forall X\, \phi$ with ϕ arithmetical. A *sentence* is a formula with no free variables.

4.7. Corollary. WKL_0^* *is a conservative extension of* RCA_0^* *with respect to* Π_1^1 *sentences. In other words, any* Π_1^1 *sentence which is provable in* WKL_0^* *is already provable in* RCA_0^*.

Proof. Suppose that the Π_1^1 sentence $\forall X\, \phi$ is not provable in RCA_0^*. By Gödel's completeness theorem let M be a countable model of RCA_0^* plus $\exists X \sim\phi$. By Theorem 4.6, let M' be a model of WKL_0^* such that M is a submodel of M' with the same first-order part. By absoluteness M' satisfies $\exists X \sim\phi$ so by the soundness theorem $\forall X\, \phi$ is not provable in WKL_0^*. □

We now study the relationship between RCA_0^* and EFA. Here EFA is the theory in L_1 consisting of the basic axioms plus Σ_0^0 induction. (The acronym EFA stands for *elementary function arithmetic.* EFA is essentially just the theory $\mathrm{I}\Sigma_0 + \exp$ of [7].)

Let

$$M = (|M|, +^M, \cdot^M, \exp^M, <^M, 0^M, 1^M)$$

be any model of EFA. A *proper initial segment* of M is any set $|I| \subseteq |M|$ such that $\forall a \forall b\, ((a \in |M| \wedge b \in |I| \wedge a <^M b) \rightarrow a \in |I|)$ and $0^M, 1^M \in |I|$ and $\forall a \forall b\, ((a, b \in |I|) \rightarrow (a +^M b,\ a \cdot^M b,\ \exp^M(a, b) \in |I|))$ and $|I| \neq |M|$. We may then consider the model

$$I = (|I|, +^I, \cdot^I, \exp^I, <^I, 0^I, 1^I)$$

where $0^I = 0^M$, $1^T = 1^M$, and $+^I$, $\cdot^I$, $\exp^I$ and $<^I$ are the restrictions to $|I|$ of $+^M$, $\cdot^M$, $\exp^M$ and $<^M$ respectively. By absoluteness I is again a model of EFA. From Lemma 4.1 and Theorem 4.8 below it will follow that I is also a model of Σ_1^0 collection.

A set $X \subseteq |I|$ is said to be *M-coded* if there exists an M-finite set X' such that $X = X' \cap |I|$. We may regard I as a model for L_2 by defining $\mathcal{S}^I$ to be the set of all M-coded subsets of $|I|$.

4.8. Theorem. *Let M be any model of* EFA *and let*

$$I = (|I|, \mathcal{S}^I, +^I, \cdot^I, \exp^I, <^I, 0^I, 1^I)$$

be as above where $|I|$ is any proper initial segment of $|M|$. Then I is a model of WKL_0^*.

Proof. To see that I satisfies weak König's lemma, let $T \in \mathcal{S}^I$ be such that T is satisfied in I to be an infinite tree. Let T' be an M-finite set such that $T = T' \cap |I|$. By Σ_0^0 induction in M let $\tau \in T' \cap \mathrm{Seq}_2^M$ be of maximal length such that $(\forall n \leq \mathrm{lh}(\tau))\ (\tau[n] \in T')$. Clearly $\mathrm{lh}(\tau) > m$ for all $m \in |I|$. Put $X = \{m \in |I| : \tau(m) = 1\}$. Clearly X is an M-coded path through T. (This idea goes back to Scott and Tennenbaum; see [8].)

It remains to show that I satisfies Δ_1^0 comprehension. Clearly I satisfies Σ_0^0 comprehension. We shall now show that Δ_1^0 comprehension follows from Σ_0^0 comprehension plus weak König's lemma. Let $\phi(n)$ and $\psi(n)$ be Σ_1^0 and Π_1^0 respectively such that $\forall n\, (\phi(n) \leftrightarrow \psi(n))$. Let $\phi(n) \equiv \exists j\, \theta_1(n, j)$ and $\psi(n) \equiv \forall j \sim \theta_0(n, j)$ where θ_0 and θ_1 are Σ_0^0. By Σ_0^0 comprehension let T be the set of all $\tau \in \mathrm{Seq}_2$ such that

$$(\forall n < \mathrm{lh}(\tau))\, (\forall j < \mathrm{lh}(\tau))\, (\forall i < 2)(\theta_i(n, j) \rightarrow \tau(n) = i).$$

Clearly T is an infinite tree. By weak König's lemma let X be a (unique) path through T. Then clearly $\forall n\, (n \in X \leftrightarrow \phi(n))$. Thus we have Δ_1^0 comprehension. This completes the proof of Theorem 4.8. $\square$

A *Π_2^0 formula* is a formula of the form $\forall i\, \exists j\, \theta$ where θ is Σ_0^0. A *Π_2^0 sentence* is a Π_2^0 formula with no free variables.

4.9. Corollary. WKL$_0^*$ *is a conservative extension of* EFA *for* Π_2^0 *sentences. In other words, any* Π_2^0 *sentence which is provable in* WKL$_0^*$ *is already provable in* EFA.

Proof. Suppose that we have a Π_2^0 sentence $\forall i\, \exists j\, \theta(i, j)$ which is not provable in EFA. Form a theory consisting of EFA plus $\sim\exists j\, \theta(a, j)$ plus $b_0 = a$, $b_{n+1} = b_n^{b_n}$, $b_n < c$ where a, b_n $(n \in \omega)$, and c are new constant symbols. By Gödel's compactness theorem, let M be a model of this theory. Let $|I|$ be the proper initial segment of $|M|$ consisting of all $b \in |M|$ such that $b <^M b_n$ for some $n \in \omega$. By Theorem 4.8, I is a model of WKL$_0^*$. Also $a^M \in |I|$ so by absoluteness I satisfies $\sim\exists j\, \theta(a, j)$. Thus $\forall i\, \exists j\, \theta(i, j)$ is not provable in WKL$_0^*$. This proves Corollary 4.9. □

Recall that the class of *elementary recursive functions* is the smallest class containing the initial functions and closed under composition and bounded primitive recursion. Equivalently, a recursive function $f(i)$ is elementary if its running time is dominated by some function of the form $F(i) = 2(k, i)$ where $2(0, i) = i$, $2(k+1, i) = 2^{2(k,i)}$, $k \in \omega$.

4.10. Corollary. *Suppose that* WKL$_0^*$ *proves the sentence* $\forall i\, \exists j\, \phi$ *where* ϕ *is* Σ_1^0. *Then there exists an elementary recursive function* $f(i)$ *such that* EFA *proves* $\forall i$ $(\exists j < f(i))\, \phi$.

Proof. An easy variant of the proof of Corollary 4.9. □

Remark. The results about RCA$_0^*$, WKL$_0^*$, and EFA, which we have presented in this section, are analogous to previously known results about RCA$_0$, WKL$_0$ and PRA (= primitive recursive arithmetic). Namely, the first-order part of RCA$_0$ is Σ_1^0 induction (Friedman); WKL$_0$ is a conservative extension of RCA$_0$ with respect to Π_1^1 sentences (Harrington); and WKL$_0$ is a conservative extension of PRA with respect to Π_2^0 sentences (Parsons, Kirby, Paris, Friedman). For model-theoretic proofs of thse results see Simpson [4]. These proofs are originally due to Kirby and Paris [10], Friedman (unpublished), and Harrington (unpublished). See also Parsons [11]. Our proofs of Theorems 4.3, 4.6 and 4.8 are based on the model-theoretic methods of Kirby, Paris, Friedman, and Harrington.

References

[1] H. Friedman, S.G. Simpson, and R.L. Smith, Countable algebra and set existence axioms, Annals Pure Appl. Logic 25 (1983) 141–181; Addendum 27 (1985) 319–320.

[2] S.G. Simpson, Reverse Mathematics, in: A. Nerode and R. Shore, eds., Recursion Theory, Proc. Symp. Pure Math. 42 (Amer. Math. Soc., Providence, RI, 1985) 461–471.

[3] S.G. Simpson, Which set existence axioms are needed to prove the Cauchy/Peano theorem for ordinary differential equations?, J. Symbolic Logic 49 (1984) 361–380.

[4] S.G. Simpson, Subsystems of Second Order Arithmetic, in preparation.
[5] H. Friedman, Provable equivalents of induction I, manuscript, Ohio State University, July 14, 1982, 5 pp.; Postscript July 14, 1982, 1 page.
[6] B.L. van der Waerden, Modern Algebra, Vol. 1, (Ungar Pub. Co., New York, 1953).
[7] J.B. Paris and L.A.S. Kirby, Σ_n-Collection schemas in arithmetic, in: A. MacIntyre et al., eds., Logic Colloquium 77. (North-Holland, Amsterdam, 1978) 199–210.
[8] C.G. Jockusch, Jr. and R.I. Soare, Π_1^0 classes and degrees of theories, Trans. Amer. Math. Soc. 173 (1972), 35–56.
[9] A. Fröhlich and J.C. Shepherdson, Effective procedures in field theory, Trans. Roy. Soc. London 248 (1956) 407–432.
[10] L. Kirby and J.B. Paris, Initial segments of models of Peano's axioms, in: Set Theory and Heirarchy Theory V, Lecture Notes in Math. 619 (Springer, Berlin, 1977) 211–226.
[11] C. Parsons, On a number theoretic choice schema and its relation to induction, in: J. Myhill et al., eds., Intuitionism and Proof Theory (North-Holland, Amsterdam, 1970) 459–473.