Algebraic Number Theory over Weak Fragments of Arithmetic

Takashi Satō*

December 5, 2020

Abstract

第 1 節では文献を引用して 1)RCA_0^* とその周辺，2) 逆数学の先行結果，3) 何が問われているのか，を見る．第 2 節で本研究で得られた結果を述べる．主なものは，1) 一階算術 Elementary Function Arithmetic はイデアル論の基本定理（素イデアル分解）を証明する．2) イデアル論の基本定理と数学的帰納法の同値性について．

1 Backgroud

The following is from "Simpson and Smith, Factorization of Polynomials and Σ_1^0-Induction, Annals of Pure and Applied Logic 31, 1986." Here [1] is "Friedman, Simpson, and Smith, Countable Algebra and Set Existence Axioms, Annals of Pure and Applied Logic 25, 1983".

> **In the present paper, we study the weaker system RCA_0^* consisting of addition, mutiplication, exponentiation, Δ_1^0 comprehension, and Σ_0^0 induction. Thus RCA_0 is equivalent to RCA_0^* plus Σ_1^0 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^*.**

- 2.5. Every countable field has an algebraic closure.
- 2.12. Every countable ordered field has a real closure.
- 2.4. Every polynomial $f(X) \in F$ has an irreducible divisor where F is a countable field.

*harunohirune@gmail.co.jp, twitter: @harunohirune

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

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

- 次のように，RCA_* 上で Σ^0_1 帰納法と同値になる数学の定理があるだろう，と予想した.

In an unpublished abstract [5], Friedman has announced another result of the above type. Namely, according to Friedman, Σ^0_1 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^0_1 induction. However, we suspect that there are many such results waiting to be discovered.

- これまでに出たのは，“Hatzikiriakou, Algebraic Disguises of Σ^0_1 Induction, Archive for Mathematical Logic 29, 1989” と，“Simpson and Rao, unpublished”（後述）のみ.

The reader who is not familiar with the program of “reverse mathematics” nor with the development of countable algebra in subsystems of second order arithmetic should read [2] and [4]. In [3] it was conjectured that the statement “Every torsion-free, finitely generated, abelian group is free” is equivalent, over RCA_0^*, to Σ^0_1 induction. Our first theorem (2.1) establishes this and incorporates an unpublished result of Friedman, (see [4]). Our second theorem (2.6) stregthens the first one by establishing that the Fundamental Structure Theorem for Finitely Generated Abelian Group is also equivalent, over RCA_0^*, to Σ^0_1 induction.

- 本研究では，これに「イデアル論の基本定理」(任意の代数体における素イデアル分解定理) を加えた．より強く，$\Sigma^{k_1}_{k_2}$ 帰納法と同値になる命題を与えた.

The following is from "S. G. Simpson, Open Problems in Reverse Mathematics, 1999." (The same manuscript can be found in "H. Friedman and S. G. Simpson, Issues and Problems in Reverse Mathematics, Contemporary Mathematics Volume 257, 2000.")

5 Replacing RCA_0 by a Weaker Base Theory

In all but section X.4 of my book [32], RCA_0 is taken as the base theory for reverse mathematics. That is to say, reversals are stated as theorems of RCA_0. An important research direction for the future is to replace RCA_0 by weaker base theories. In this way we can hope to substantially broaden the scope of reverse mathematics, by obtaining reversals for many ordinary mathematical theorems which are provable in RCA_0.

A start on this has already been made. In Simpson/Smith [33] we defined RCA_0^* to be the same as RCA_0 except that Σ^0_1 induction is weakened to Σ^0_0 induction, and exponentiation of natural numbers is assumed. Thus RCA_0 is equivalent to RCA_0^* plus Σ^0_1 induction. It turns out that RCA_0^* is conservative over EFA (elementary function arithmetic) for Π^0_2 sentences, just as RCA_0 is conservative over PRA (primitive recursive arithmetic) for Π^0_2 sentences.

One project for the future is to redo all of the known results in reverse mathematics using RCA_0^* as the base theory. The groundwork for this has already been laid, but there are some difficulties. For example, we know that Ramsey's theorem for exponent 3 is equivalent to ACA_0 over RCA_0, but it unclear whether RCA_0 can be replaced by RCA_0^*. Other problems of this nature are listed in my book [32, remark X.4.3].

Another project is to find ordinary mathematical theorems that are equivalent to Σ^0_1 induction over RCA_0^*. Several results of this kind are already known and are mentioned in my book [32, §X.4]. For example, Hatzikiriakou [14] has shown that the well known structure theorem for finitely generated Abelian groups is equivalent to Σ^0_1 induction over RCA_0^*.

A more visionary project would be to replace RCA_0^* by even weaker base theories, dropping exponentiation and Δ^0_1 comprehension. One could even consider base theories that are conservative over the theory of discrete ordered rings. At the present time, almost nothing is known about this.

The following is from "S. G. Simpson, Subsystems of Second Order Arithmetic, second edition, 2009 Appendix, Chapter X. Additional Results".

X.4. Reverse Mathematics for RCA_0

Throughout this book we have used RCA_0 as our base theory for Reverse Mathematics. An important research direction for the future is to weaken the base theory. We can then hope to find mathematical theorems which are equivalent over the weaker base theory to RCA_0, in the sense of Reverse Mathematics. There are a few results in this direction, which we now present.

Definition X.4.1 (RCA_0^* and WKL_0^*). Let $\mathrm{L}_2(\exp)$ be L_2, the language of second order arithmetic, augmented by a binary operation symbol $\exp(m,n) = m^n$ intended to denote exponentiation. We take $\exp(t_1,t_2) = t_1^{t_2}$ as a new kind of numerical term, and for each $k < \omega$ we define the Σ^0_k and Σ^1_k formulas of $\mathrm{L}_2(\exp)$ accordingly. We define RCA_0^* to be the $\mathrm{L}_2(\exp)$-theory consisting of RCA_0 minus Σ^0_1 induction plus Σ^0_0 induction plus the exponentiation axioms: $m^0 = 1$, $m^{n+1} = m^n \cdot m$. We define WKL_0^* to be RCA_0 plus weak König's lemma.

Thus we have

$$\mathsf{RCA}_0 \equiv \mathsf{RCA}_0^* + \Sigma^0_1 \text{ induction},$$

and

$$\mathsf{WKL}_0 \equiv \mathsf{WKL}_0^* + \Sigma^0_1 \text{ induction}.$$

Paralleling the results of §§IX.1–IX.3, we have:

Theorem X.4.2 (conservation theorems). *The first order part of* WKL_0^* *and of* RCA_0^* *is the* $\mathrm{L}_1(\exp)$*-theory consisting of the basic axioms* I.2.4(i) *plus the exponentiation axioms plus* Σ^0_0 *induction plus* Σ^0_1 *bounding.* WKL_0^* *is conservative over* RCA_0^* *for* Π^1_1 *sentences.* WKL_0^* *and* RCA_0^* *have the same consistency strength as* EFA *and are conservative over* EFA *for* Π^0_2 *sentences.*

Proof. See Simpson/Smith [250, §4]. □

Remark X.4.3. An interesting project would be to redo all of the known results in Reverse Mathematics using RCA_0^* instead of RCA_0 as the base theory, replacing WKL_0 by WKL_0^*. The groundwork for this has been laid in Simpson/Smith [250], and much of it would be routine. Note however that bounded Σ^0_1 comprehension is not available in RCA_0^* or in WKL_0^* yet has played a key role in the proofs of several important results, including theorems III.7.2, III.7.6, IV.6.4, IV.7.9, IV.8.2, and V.6.8.

THEOREM X.4.4 (Reverse Mathematics for RCA_0). *The following are pairwise equivalent over* RCA_0^*.

1. Σ^0_1 *induction*.
2. *Bounded* Σ^0_1 *comprehension*.
3. *For every countable field* K, *every polynomial* $f(x) \in K[x]$ *has only finitely many roots in* K.
4. *For every countable field* K, *every polynomial* $f(x) \in K[x]$ *has an irreducible factor.*
5. *For every countable field* K, *every polynomial* $f(x) \in K[x]$ *can be factored into finitely many irreducible polynomials.*
6. *Every finitely generated vector space over* $\mathbb{Q}$ (*or over any countable field*) *has a basis.*
7. *Every finitely generated, torsion-free Abelian group is of the form* $\mathbb{Z}^m$, $m \in \mathbb{N}$.
8. *The structure theorem for finitely generated Abelian groups.*

PROOF. The proof of $1 \leftrightarrow 2$ has been sketched in remark II.3.11. The equivalences $1 \leftrightarrow 2$, $1 \leftrightarrow 3$, $1 \leftrightarrow 4$ and $1 \leftrightarrow 5$ are from Simpson/Smith [250]. The equivalence $1 \leftrightarrow 6$ is due to Friedman (unpublished). Compare theorem III.4.3. The equivalences $1 \leftrightarrow 6$, $1 \leftrightarrow 7$ and $1 \leftrightarrow 8$ are proved in Hatzikiriakou [107, 108]. □

The following is from "S. G. Simpson and J. Rao, Reverse Algebra, in Handbook of Recursive Mathematics Volume 2, Chapter 21, p. 1365, 1998."

Theorem 2.4 *Within* RCA_0^**, one can prove that the following algebraic theorems are equivalent to* Σ^0_1*-Induction, therefore equivalent to* RCA_0*:*

(1) (Friedman; see Hatzikiriakou [3]) *Every finitely generated vector space over a countable field has a basis.*

(2) (Hatzikiriakou [3]) *Every torsion-free, finitely generated abelian group is free.*

(3) (Hatzikiriakou [3]) *The Fundamental Structure Theorem for Finitely Generated Abelian Groups.*

(4) (Simpson-Smith [12]) *For each countable field* F *and every* $f(x) \in F[x]$*,* $f(x)$ *has only finitely many roots in* F*.*

(5) (Simpson-Smith [12]) *For each countable field* F *and every* $f(x) \in F[x]$*,* $f(x)$ *has an irreducible factor.*

(6) (Simpson-Smith [12]) *For each countable field* F*,* $F[x]$ *is a unique factorization domain.*

(7) (Rao-Simpson [9]) *For each countable field* F*,* $F[x]$ *is a principal ideal domain.*

(8) (Rao-Simpson [9]) *Every countable Euclidean domain is a unique factorization domain.*

(9) (Rao-Simpson [9]) *Every countable Euclidean domain is a principal ideal domain.*

(10) Gauss's Theorem (Rao-Simpson [9]) *If* R *is a countable unique factorization domain, so is the polynomial ring* $R[x]$*.*

(11) (Friedman-Simpson-Smith [1], Rao [8]) *The Fundamental Theorem of Galois Theory.*

The following is from "Antonio Montalbán, Open Questions in Reverse Mathematics, The Bulletin of Symbolic Logic Volume 17, Number 3, Sept. 2011, p. 448, §6. Changing the setting, 6.1. Changing the base, 6.1.2. Weakening the base."

Friedman and Simpson [FS00, Sec 10] proposed the study of RCA_* as a base, where, in RCA_* (introduced by Simpson and Smith [SS86]), Σ^0_1-induction is replaced by Σ^0_0-induction and the exponentiation function is assumed. Little work has been done on this. However, for example, Nemoto recently showed that most of the analysis of determinacy statements can be done over RCA_*, and she was able to separate two determinacy statements over RCA_*, both of which are equivalent to WKL_0 over RCA_0.

- 他の記号との整合性から，RCA_0^* より RCA_* と書くのがよいという意見がある．利便性も考え，これに従う．

2 RCA_* でできること

- イデアル分解定理に向けて，適切な，なるべく弱い形式体系で理論を展開させる．なぜ弱い体系か？
  - 定理をより精彩に表現できる．定理の価値を高める．
  - 現代的な抽象代数学に対する，近代的なアルゴリズミックな数学の再評価．
  - 書かれた証明と，それを実際に確かめる手順の乖離が少なくなる．
- 1) 初等算術, 2) （算術化した）数理論理学，3) （算術化した）体論，4) 代数的整数論，の順に見る．

2.1 Arithmetic

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

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

- Simpson and Smith から引用．primitive recursion が bounded primitive recursion に制限されるのが，RCA_0 と RCA_* とのちがいを特徴づける．
- たとえば，ユークリッドの互除法や素因数分解は，その手続きが RCA_* で正当化されるほど具体的で，直ぐに証明できる．弱い一階算術で直接証明することもできる（Cf. Hajek and Pudluk, or Kaye）．

Proposition 2.1 (RCA_*; Bezout's Identity)**.** 自然数 m と n につき，次のような自然数 k と l がある．

$$km + ln = (m, n).$$

ただし (m, n) は m と n の最大公約数．

Proposition 2.2 (RCA_*; Fundamental Theorem of Arithmetic)**.** 2 以上の自然数は，いくつかの素数の積として，順番を除いて一通りに表される．

2.2 Mathematical Logic

- Simpson, Subsystems of Second Order Arithmetic, II.8. は数理論理学を RCA_0 で展開している．精査すると，これらはすべて RCA_* でできるとわかる．
- A を一階述語論理の公理系とする．すべての文 σ について $A \vdash \sigma$ か $A \vdash \neg\sigma$ となるとき，A は完全 (complete) という．
- モデルとは領域と，関数記号と関係記号の解釈に加え，真理条件を満たすような（すべての）文への付値を言う．

Proposition 2.3 (RCA_*; Weak Completeness Theorem)**.** A を無矛盾な一階述語論理の公理系とする．さらに，もし，A が完全であるか，論理的帰結について閉じているなら，A のすべての文を真とするモデルがある．

- ヘンキンのターム・モデルの構成の形式化による．

Proposition 2.4 (RCA_*; Soundness Theorem)**.** 一階述語論理の公理系 A について，A のすべての文を真とするモデルがあるなら，A は矛盾を証明しない．

- それぞれの証明について，各ステップごとに真であることが保存されることを帰納法で言えばよい．
- すべての文に付値を与えるのは大変．少なくとも，A と A の部分論理式のインスタンスには付値が与えられているとき，A の弱いモデルという．

Proposition 2.5 (RCA_*^+; Strong Soundness Theorem)**.** 一階述語論理の公理系 A について，A のすべての文を真とする弱いモデルがあるなら，A は矛盾を証明しない．

- シーケント計算 LK のカット除去定理から出る．カットのない証明には subformula property が成り立つからである．
- LK のカット除去定理は RCA_* に加え，超指数関数の存在を仮定しないと証明できないことが，本研究集会で指摘された．このとき，RCA_*^+ と書こう．

Proposition 2.6 (RCA_*^+; Cut Elimination Theorem)**.** シーケント体系 LK の証明 p について，p と同じ結論を持つカットを含まない証明 p' が存在する．

Proposition 2.7 (RCA_*^+; Consistency of EFA)**.** 一階算術の体系 Elementary Function Arithmetic は無矛盾である．

- EFA は足算，掛算，累乗，Σ_0^0 帰納法より成る．

2.3 Field Theory

- 算術化にあたり，高々可算な体のみを扱う．
- Friedman, Simpson, and Smith を “redo in RCA_*” して次を得た．一部には超指数関数が必要．
- 体 K について，$\mathrm{IRR}(K) = \{f \in K[X] : f \text{ is irreducible}\}$ とする．

Proposition 2.8 (RCA_*; Existence and Structure of Finite Fields)**.** For each prime p and $1 \leq n$, there uniquely exists the p^n-element field, say $\mathrm{GF}(p^n)$. $\mathrm{GF}(p^n)$ is embeddable into $\mathrm{GF}({p'}^{n'})$ if and only if $p = p'$ and $n|n'$. Moreover, there exists an algebraic closure of $\mathrm{GF}(p)$ for each p as a “union” of $\{\mathrm{GF}(p^n) : 1 \leq n\}$.

Proposition 2.9 (RCA_*; Quantifier Elimination)**.** Let AF and ACF be respectively the usual set of field axioms and the usual set of axioms for an algebraically closed field. (i) ACF admits elimination of quantifiers, i.e., for any formula ϕ there exists a quantifier-free formula ϕ^* such that ACF proves $\phi \leftrightarrow \phi^*$. (ii) For any quantifier-free formula ϕ, if ACF proves ϕ then AF proves ϕ.

Theorem 2.10 (RCA_*^+; Existence of Algebraic Closure)**.** Every field has an algebraic closure.

- ただし，有理数体の代数閉包の存在は RCA_* で証明できると思われる．

Proposition 2.11 (RCA_*; Dimension Theorem)**.** Let K be a field. If a K-vector space V has an n-element basis then every subset of V consisting of more than n elements is linearly dependent. Consequently, every basis of V consists of n elements.

Proposition 2.12 (RCA_*^+; Primitive Element Theorem)**.** Let $L = K(\alpha_1, \ldots, \alpha_n)$ and each a_i is algebraic over K. Suppose that $\mathrm{IRR}(K)$ exists and $\alpha_2, \ldots, \alpha_n$ are separable. Then, there exists $\theta \in L$ such that $L = K(\theta)$. The degree of a minimal polynomial of θ over K equals $[L : K]$. Moreover, the image $\Phi(K)$ exists.

Proposition 2.13 (RCA_*^+; Galois Correspondence)**.** Let K be a field, $f \in K[X]$ be a separable polynomial, and L be the least splitting field of f over K. Moreover, assume that $\mathrm{IRR}(K)$ exists. Then, there exists a finite group $G = \mathrm{Gal}(L/K)$ of order $[L : K]$ whose elements are in one-to-one correspondence with the automorphisms of L over K and whose (normal) subgroups are in one-to-one correspondence with the (normal) field extensions of K within L. The usual Galois correspondences hold.

Proposition 2.14 (RCA_*^+; Translation Theorem)**.** Let L_1/K and L_2/K be intermediate finite extensions of M/K. Suppose that $L_1 = K(\theta)$ where θ is separable. Moreover, assume that $\mathrm{IRR}(K)$ exists. Then, $[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2]$ and $\mathrm{Gal}(L_1L_2/L_2) \simeq \mathrm{Gal}(L_1/L_1 \cap L_2)$.

2.4 Algebraic Number Theory

- 素因数分解は，一般の代数体において，素イデアル分解として拡張される．このデデキントの定理がイデアル論の礎となる．
- 代数体の素イデアル分解定理は EFA で表現できる．$\mathbb{Q}$ の代数閉包の存在などにより，RCA_* で証明できる．RCA_* で証明できる Π^0_2 論理式は EFA で証明できるので；

Theorem 2.15. EFA は代数体の素イデアル分解定理を証明する．

- 同様にして，分岐理論がいくらか展開できる．reversal への応用を念頭に，とりあえず円分体についての結果を示した．

Theorem 2.16. EFA は以下を証明する：素数 p は $\mathbb{Q}(\zeta_n)$ において $p|n$ のときに限り分岐する．

- RCA_* で，代数体をどう定義するか？　$\mathbb{Q}$ の有限次拡大体（$\mathbb{Q}$ 上のベクトル空間とみなしたとき有限個の基底を持つもの）と定義するのがよいだろう．このとき，代数体の部分体が代数体であることは，自明ではない．

Theorem 2.17 (基底律)**.** $k \in \mathbb{N}$ とする．以下は RCA_* で Σ^0_k 帰納法（$\mathsf{I}\Sigma^0_k$）と同値である：ある代数体の部分体で，Σ^0_k 論理式で定義されるものは，有限個の基底を持つ（ので，再び代数体となる）．

- 素イデアル分解と数学的帰納法の同値性．代数体のイデアルは有限個の生成元でコードされるので，任意の長さの素イデアル分解表は有限列でコードされます．

Theorem 2.18 (イデアル論の基本定理)**.** $k \in \mathbb{N}$ とする．以下は RCA_* で Σ^0_k 帰納法と同値である：Σ^0_k 論理式で定義される代数体において，任意有限長の素イデアル分解表がある．

- 以上のことから，次の問題を出します．

Question 2.19. イデアル論の基本定理（素イデアル分解定理）または，算術の基本定理（素因数分解定理）の論理的な強さを帰納法で特徴づけられるか？