Prime Ideal Factorization within Weak Fragments of Arithmetic*

Takashi Satō†

December 19, 2020

Abstract

この発表では，以下の結果を報告する．1 節では代数学と逆数学について簡単に見る．2 節では素イデアル分解定理と一階算術について簡単に見て，結果を言う．

Lemma 0.1. RCA_0^* proves that there exists an algebraic closure of $\mathbb{Q}$.

Theorem 0.2 (S.)**.** Over RCA_0^*,

1. every algebraic fields admits the unique prime ideal factorization,
2. a prime p ramifies in a cyclotomic field $\mathbb{Q}(\zeta_n)$ if and only if $p|n$, and,
3. Σ^0_k-induction scheme is equivalent to the assertion that there exists a table of the prime ideal factorization of arbitrary length for every Σ^0_k-definable algebraic field.

Corollary 0.3.

1. Elementary Arithmetic proves the unique prime ideal factorization for algebraic number fields.
2. It also proves that a prime p ramifies in a cyclotomic field $\mathbb{Q}(\zeta_n)$ if and only if $p|n$.
3. Over Elementary Arithmetic plus $\mathsf{B}\Sigma_1$, Σ^0_k-induction scheme $(1 \leq k)$ is equivalent to the following assertion: There exists a table of the prime ideal factorization of arbitrary length for every Σ^0_k-definable algebraic field.

*SLACS 2020 https://sites.google.com/view/slacs2020/home での発表 “Algebraic Number Theory within Weak Fragments of Arithmetic”の続き．

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

1　背景・代数学と逆数学

近現代の代数学．その起りと抽象化．

- 1799 年，ガウス，代数学の基本定理
- ガロアの理論
- クンマー，円分体のイデアル
- デデキント，素イデアル分解定理
- 1897 年，ヒルベルト，数論報告
- ネーター
- 1920 年，高木，類体論
- 1930 年，ヴェルデン，現代代数学
- ブルバキ，数学原論
- グロタンディーク

ヴェルデン，現代代数学，第 1 巻，42 節，有限回の手続きで体を構成すること，より．

In attempting to construct the decomposition field of a polynomial by the methods of Section 35 in a similar manner, we face the problem of factoring a polynomial in a given or already constructed field. There is no universal method by which, for any explicitly known field K, a decomposition into prime factors of the polynomials in $\mathsf{K}[x]$ could be performed in a finite number of steps, and there are reasons for the assumption that such a general method is impossible.[14] On the other hand, we have seen that there are such methods for factorizations into primes for special fields (fields of rationals, fields of the Gaussian integers, of the rational functions in n indeterminates with rational coefficients, of the residue classes modulo p, etc.).

逆数学へ．Simpson/Smith, Factorization of Polynomials and Σ^0_1 Induction, Annals of Pure and Applied Logic, 1986, より．

Theorem 1.1. Over RCA^*_0, Σ^0_1-induction is equivalent to the following assertion: For every countable field F and every polynomial $f(X) \in F[X]$, $f(X)$ has a finite factorization into irreducible polynomials over F.

- RCA^*_0 は，足算，掛算，累乗，順序，Σ^0_0 帰納法，Δ^0_1 集合存在公理より成る．

Friedman/Simpson/Smith, Countable Algebra and Set Existence Axioms, Annals of Pure and Applied Logic, 1983.

- 群・環・体の存在・構造定理の逆数学現象.
- RCA_0 で，算術化された完全性定理を使い，次を証明：任意の可算な体につき，その代数閉包が存在する.
- RCA_0 は，足算，掛算，累乗，順序，Σ^0_1 帰納法，Δ^0_1 集合存在公理より成る.

S., Reverse Mathematics and Isbell's Zig-Zag Theorem, Mathematical Logic Quarterly, 2014.

Theorem 1.2. Over RCA_0, WKL_0 is equivalent to Isbell's Zig-Zag Theorem for countable monoids: $b \in B$ is "dominated" by A if and only if b has a "zig-zag" over A where $A \subset B$ are countable monoids.

- 半群論の逆数学現象.
- あからさまな存在・構造定理でない「普通の」定理.
- 「Π^1_1 文 $\Leftrightarrow$ Σ^0_1 文」は，完全性定理と同じ形．他にも WKL_0 と同値になる例がある.

S. and Yamazaki, Reverse Mathematics and Order Theoretical Fixed Point Theorems, Archive for Mathematical Logic, 2017.

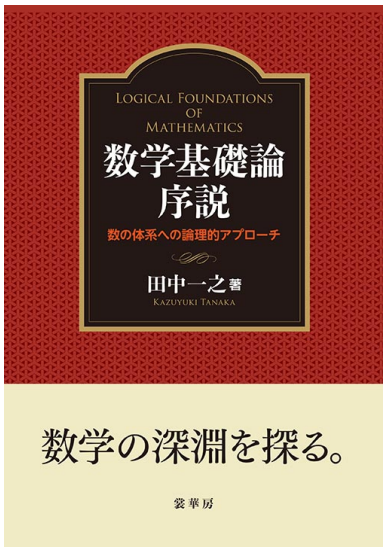
Theorem 1.3. Over RCA_0, ACA_0 is equivalent to each of following theorems:

- Abian-Brown's Least Fixed Point Theorem: If P is a countable and complete poset, then every order-preserving self map on P has a least fixed point.
- Markowsky's Converse of the above: If P is a countable poset such that every order-preserving self map has a least fixed point, then P is complete.
- Davis' Converse of Tarski's Fixed Point Theorem: If L is a countable lattice such that every order-preserving self map has a fixed point, then L is complete.

- 束論の逆数学現象.
- 「普通の」定理.

逆数学の文献.

- S. G. Simpson, Subsystems of Second Order Arithmetic, 1999-2010.



東北大学教授　Ph. D. 田中一之著／ A5 判／ 388 頁／定価 5940 円（本体 5400 円＋税 10 %）／ 2019 年 6 月発行

数学セミナー

2021 年 2 月号　予価本体 1090 円＋税／ 2021 年 1 月 12 日発売予定　特集＝逆数学

2　結果・イデアル分解定理と「逆算術」

イデアル分解定理は，次のように発展した．

- 算術の基本定理：0 と ± 1 以外の整数は有限個の素数の積として一意に書ける．
- デデキントによるイデアル論の基本定理：代数体（$\mathbb{Q}$ の有限次拡大体）の整数環の自明でないイデアルは素イデアルの積として一意に書ける．
- 一意分解の特徴づけ：デデキント環の自明でないイデアルは素イデアルの積として一意に書ける．
- ラスカー＝ネーターの定理：ネーター環の自明でないイデアルは準素イデアルの共通部分として一意に書ける．

Hajek and Pudluk, Metamathematics of First Order Arithmetic, 1993, より．

1.58 Theorem. (1) In $I\Sigma_1$ we may Δ_1 define general power and factorial functions; i.e. total functions x^y and $x!$ such that the formulas $z = x^y$ and $z = x!$ are Δ_1 in $I\Sigma_1$ and $I\Sigma_1$ proves the following:

$$x^0 = 1 \text{ and } x^{S(y)} = x^y * x\,,$$
$$0! = 1 \text{ and } (S(x))! = x! * S(x)\,.$$

(2) $I\Sigma_1$ proves that there are infinitely many primes. In $I\Sigma_1$ we may define an increasing Δ_1 enumeration of all primes.

(3) $I\Sigma_1$ proves the prime factorization theorem.

代数体のイデアル分解定理をなるべく弱い体系で示す.
J. Avigad, Number Theory and Elementary Arithmetic, Philosophia Mathematica, 2003, より.

Grand conjecture. *Every theorem published in the Annals of Mathematics whose statement involves only finitary mathematical objects (i.e., what logicians call an arithmetical statement) can be proved in elementary arithmetic.*

- Elementary Arithmetic（初等算術）は，足算，掛算，累乗，順序，Σ_0^0 帰納法より成る.

Hajek and Pudluk, Metamathematics of First Order Arithmetic, 1993, より.

The most basic theorem about such systems of Bounded Arithmetic is the following one, which is usually referred to as *Parikh's Theorem.*

1.4 Theorem. Let ψ be a Σ_0^f formula and let π be a Π_0^f formula. Suppose that

$$I\Sigma_0^f(f) + \pi \vdash (\forall x)(f(x) \leq f(x+1)),$$
$$I\Sigma_0^f(f) + \pi \vdash (\forall x)(\exists y)\psi(x,y).$$

Then for some term $t(x)$ of $L(f)$

$$I\Sigma_0^f(f) + \pi \vdash (\forall x)(\exists y \leq t(x))\psi(x,y).$$

再び Simpson and Smith より，証明体系の拡大が conservative なこと.

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].)

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.

- ここでの EFA は Elementary Function Arithmetic の略で, Elementary Arithmetic と同じ.

得られた結果を述べる．

Lemma 2.1. RCA_0^* proves that there exists an algebraic closure of $\mathbb{Q}$.

Proof. RCA_0^* でやる．ACF を代数閉体の言語とする．ただし，代数的に閉じていることを表す文は，

$$(\forall x_0, \ldots, x_{n-1})(\exists y)(y^n + x_{n-1}y^{n-1} + \cdots + x_1 y + x_0 = 0)$$

でなく，

$$(\forall x_0, \ldots, x_{n-1})(\exists y_0, \ldots, y_n)(X^n + x_{n-1}X^{n-1} + \cdots + x_1 X + x_0 = (X - y_0)(X - y_1)\cdots(X - y_n))$$

とする．すると，ACF は量化記号消去ができる．つまり，それぞれの文 φ につき，$\mathsf{ACF} \vdash \varphi \leftrightarrow \varphi^*$ となる量化記号がない文 φ^* がある．ところで，素数 p につき，ヴェルデンの構成により，標数が p の代数閉体は存在する．[1] よって，ACF ＋「標数が p」はモデル（領域と付値関数）を持ち，無矛盾である．このことより，ACF は無矛盾である．よって，弱い完全性定理より，ACF はモデルを持つ．$\mathbb{Q}$ の代数閉包は，このモデルから取り出せる． □

RCA_0^* は一般の可算な体 K の代数閉包の存在を証明する，という話がある．このことは Simpson and Smith で問われている．2.5 が「Every countable field has an algebraic closure.」2.12 が「Every countable ordered field has a real closure.」

In the present paper, we study the weaker system $\mathbf{RCA}_0^*$ consisting of addition, mutiplication, exponentiation, Δ_1^0 comprehension, and Σ_0^0 induction. Thus $\mathbf{RCA}_0$ is equivalent to $\mathbf{RCA}_0^*$ plus Σ_1^0 induction. It is known that $\mathbf{RCA}_0^*$ is properly weaker than $\mathbf{RCA}_0$. It turns out that some but not all of the results of [1] which were proved in $\mathbf{RCA}_0$ can be proved in $\mathbf{RCA}_0^*$. For instance, it appears that $\mathbf{RCA}_0^*$ 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 $\mathbf{RCA}_0^*$. Lemma 2.4 of [1] is definitely not provable in $\mathbf{RCA}_0^*$.

[1] ヴェルデンの構成は標数が 0 のときも RCA_0^* でできるかもしれないが，明らかでない．

Theorem 2.2 (S.)**.** Over RCA_0^*,

1. every (Σ_0^0-definable) algebraic fields admits the unique prime ideal factorization,
2. a prime p ramifies in a cyclotomic field $\mathbb{Q}(\zeta_n)$ if and only if $p|n$, and,
3. Σ_k^0-bounded comprehension axiom ($1 \leq k$) is equivalent to the assertion that there exists a table of the prime ideal factorization of arbitrary length for every Σ_k^0-definable algebraic field.

Corollary 2.3. 1. Elementary Arithmetic proves the unique prime ideal factorization for algebraic number fields.

2. It also proves that a prime p ramifies in a cyclotomic field $\mathbb{Q}(\zeta_n)$ if and only if $p|n$.
3. Over Elementary Arithmetic plus $\mathsf{B}\Sigma_1$, Σ_k^0-induction scheme ($1 \leq k$) is equivalent to the following assertion: There exists a table of the prime ideal factorization of arbitrary length for every Σ_k^0-definable algebraic field.

- 1 と 2 は Avigad の Grand Conjecture に「イデアル論の基本定理」と「円分体の分岐理論」のケース・スタディを加える.
- 3 は一階算術の逆数学現象（逆算術？）と見れる.