数理解析研究所講究録
第 1646 巻 2009 年 28-33

$\tilde{\mathbb{Q}}$ の subrings, subfields の決定問題について

鹿児島国際大学国際文化学部　福崎賢治 (Kenji Fukuzaki)
Faculty of Intercultural Studies,
The international University of Kagoshima

このノートでは、言語を ring language $L=\{+,-,\cdot,0,1\}$ として、L-structure R を考える。したがって R は単位元 1 を含み、field も含む。ただし関数体のような場合は、不定元を（0, 1 のように）言語 L に追加する。主に、有理数体の代数的閉包 $\tilde{\mathbb{Q}}$ の subring R （subfields を含む）の decidability, Diophantine decidability について今まで得られた結果についての概略を紹介する。

1　一般的な注意

任意の first order $L-$sentence をとったとき、その R の中での真偽を判定する uniform な algorithm が存在するとき、R は decidable であるという。そうでないとき R は undecidable であるという。

任意の positive exitential $L-$sentence をとったとき、その R の中での真偽を判定する uniform な algorithm が存在するとき、R は Diophantine decidable であるという。そうでないとき R は Diophantine undecidable であるという。

Diophantine decidability は、R が $\tilde{\mathbb{Q}}$ の subring、もしくはその上の関数体等であるとき、次の定義と同等である。

任意の多変数の R 上の多項式をとる。ただし R が recursive でないときは、係数は適当な大きな recursive subring R_0 に制限するものとする。number fields およびその代数的整数環は recursive であるからそのままである。$\mathbb{R}$ に対しては $R_0=\mathbb{R}\cap\tilde{\mathbb{Q}}$、$\mathbb{C}$ に対してはは $R_0=\tilde{\mathbb{Q}}$、$\mathbb{C}(t)$ に対しては $R_0=\tilde{\mathbb{Q}}(t)$ とする。これらも recursive である。一般に F を number field としたとき $F(t)$ は recursive であり、$\tilde{\mathbb{Q}}(t)$ も recursive である。これが関数体等の場合、言語に不定元を constant symbol として入れる理由である。この状況下でその多項式が R に解をもつかどうかを判定する uniform な algorithm が存在するとき、R は Diophantine decidable であるという。そうでないとき R は Diophantine undecidable であるという。つまり、Hilbert 10^{th} Problem over R が positive answer をもつときが Diophantine decidable であり、negarive answer をもつとき Diophantine undecidable である。

decidability と Diophantine decidability の関係として、

Fact 1 R が *L-decidable* ならば R は *L-Diophantine decidable* であるが、逆は成り立たない。

反例として、$C[\![X,Y]\!]$ がある。Diophantine decidable であるが、その full theory は decidable ではない。ただし言語は $\{+,-,\cdot,0,1,X,Y\}$ である。

R とその商体の関係として、

Fact 2 R とその商体 $Q(R)$ の *decidability* は一致しない。

例として、the field of all totally algebraic numbers $K = \mathbb{Q}^{tr}$ とその代数的整数環 O_K があげられる。K は decidable であるが O_K は undecidable である。今のところ逆の例は見つかっていないように思われる。$\alpha \in \tilde{\mathbb{Q}}$ が totally real とは α およびその $\mathbb{Q}$ 上の共役がすべて実数であることである。

R とその商体 $Q(R)$ の Diophantine decidability が一致しない例は、多項式環、関数体、べき級数環、べき級数体を含めても見つかっていないように思われる。というより、あまりまだ分かっていない。

一般的に、L' とその拡大 L の関係として、

Fact 3 R を *L-structure* とする。R が *(Diophantine) decidable in the language* L ならば R は *(Diophantine) decidable in the language* L' であるが、逆は成り立たない。

反例として、$\mathbb{Z}$ があげられる。$\mathbb{Z}$ は $L = \{+,-,\cdot,0,1\}$-structure である。$L' = \{+,-,0,1\}$ とすると、$\mathbb{Z}$ は L'-decidable であるが、L-decidable ではない。

Ax, Kochen, Ershov らは、ring language $\{+,-,\cdot,0,1\}$ を拡大した valued fields の language のもとで、$\mathbb{Q}_p$ は decidable なことを示した。したがって ring language のもとでも $\mathbb{Q}_p$ は decidable である。

2 $\mathbb{Q}$ 上有限次数な環

$\tilde{\mathbb{Q}}$ の subring R の $\mathbb{Q}$ 上の次数とはその商体の拡大次数のことである。$\tilde{\mathbb{Z}}$ を the ring of all algebraic integers とする。

Fact 4 $\mathbb{Q}$ 上有限次数な $\tilde{\mathbb{Q}}$ の *subring* R およびその商体は *undecidable* である。

J. Robinson はすべての number field およびその代数的整数環は undecidable なことを、それらの中で $\mathbb{N}$ が definable であること証明することによって示した。彼女は代数的整数環に対しては uniform に $\mathbb{N}$ が定義できることを証明した。後に Rumely によって number field に対しても uniform に $\mathbb{N}$ が定義できることが示された。(つまりひとつの formula によって共通に $\mathbb{N}$ が定義できる。) したがって The theory of algebraic integer rings of finite degree および the theory of number fields も undecidable である。(つまり共通の theory も)

Diophantine decidability に関しては、J. Denef, L. Lipshitz, T.Pheidas, Shlapentokh, Poonen らによって次の結果が得られている。

Fact 5 *number field* k *が次の条件のいずれかを満たすとき、その代数的整数環* O_k *は Diophantine undecidable である。*

1. k は *totally real* である。(*totally real* な元からなっている。)
2. k は *totally real number field* の *2* 次拡大である。
3. k はただ *1* 組の *conjugate* な *non-real embeddings* をもつ。
4. $E(\mathbb{Q})$ と $E(k)$ が同じ *rank* をもつような $\mathbb{Q}$ 上の *elliptic curve* E がある。

Mordell-Weil theorem によって、E 上の有理点の集合 $E(\mathbb{Q})$ と k-有理点の集合 $E(k)$ は有限生成な abelian group である。4 で rank とは有限生成な abelian group としての rank である。条件 4 はすべての number field に対して成り立つであろうと思われているがまだ証明されていない。

Conjecture 6 任意の *number field* k *に対して、その代数的整数環* O_k *は Diophantine undecidable である。*

number fields に対しては何もわかっていない。むしろ大きな予想として、

Conjecture 7 $\mathbb{Q}$ *は Diophantine undecidable である。*

体でなく、$\mathbb{Q}$ 上有限次数な $\tilde{\mathbb{Q}}$ の subring ではない環、つまり number field k と O_k の中間の環に関してもあまり分かっていない。$\mathbb{Z}$ と $\mathbb{Q}$ の intermediate ring に関しては次の結果が知られている。そのような環は、S をすべての素数の集合 $\mathcal{P}$ の subset としたとき $\mathbb{Z}[S^{-1}]$ の形である。

Fact 8 S *が有限のときは* $\mathbb{Z}[S^{-1}]$ *は Diophantine undecidable である。*

これは J. Robinson の 1949 年の論文から $\mathbb{Z}$ が $\mathbb{Z}[S^{-1}]$ の中で Diophantine definable (つまり positive exitential formula で定義できる) ことからわかる。無限の S に対しては、2003 年 Poonen により、

Fact 9 $\mathbb{Z}[S^{-1}]$ 上の $\mathbb{Z}$ の *Diophantine model* が存在するような自然密度 1 の $\mathcal{P}$ の *ecursive* な *subset* S がある。

S の自然密度とは

$$\lim_{X\to\infty} \frac{\#\{p \in S : p \leq X\}}{\#\{p \in \mathcal{P} : p \leq X\}}$$

のことである。(もし存在すれば)

$\mathbb{Q}$ 以外の number field k と O_k の中間の環に関しては Shlapentokh により、

Fact 10 M を *totally real field* もしくは *totally real field* の 2 次の *totally complex extension* とする。任意の $\varepsilon > 0$ に対して *Dirichret density* が $1 - [M : \mathbb{Q}]^{-1} - \varepsilon$ よりも大きい M の *prime* の集合 W_M があり、M と O_M の中間環 O_{M,W_M} は *Diophantine undecidable* である。

ここで O_{M,W_M} はその divisor が W_M の prime の power の product だけからなる M の元のなす環のことで、W_M の Dirichret density とは、$\mathcal{P}$ を M の prime の集合として、

$$\lim_{Re(s)>1} \frac{\sum_{\mathfrak{p}\in W_M} 1/N\mathfrak{p}^s}{\sum_{\mathfrak{p}\in \mathcal{P}} 1/N\mathfrak{p}^s}$$

のことである。

3 $\mathbb{Q}$ 上無限次数な環

1962 年 J. Robinson は次の定理を証明した。

Theorem 11 *The natural numbers can be defined arithmetically in any totally real algebraic integer ring A such that there is a smallest interval $(0, s)$ with s real or ∞, which contains infinitely many complete conjugate sets of numbers of A.*

In particular such a ring is undecidable.

たとえば $K = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$ (ここで l は 1 より大きい自然数) としたとき O_K には区間 $(0,4)$ にその $\mathbb{Q}$ 上の共役元が全てはいる代数的整数が無限個あり、それより小さい区間 $(0,s)$ には有限個しかないから O_K は undecidable である。($\{2+2\cos(2\pi/l^n) : n \in \mathbb{N}\}$ を考えればよい。)

このようにして多くの $\mathbb{Q}$ 上無限次数な undecidable な環が得られる。$\mathbb{Q}^{tr}$ の代数的整数環 $\mathbb{Z}^{tr}$ も undecidable であり、$\mathbb{Q}(\{\sqrt{n} : n \in \mathbb{N}\})$ の代数的整数環も undecidable である。

残念ながら上の定理から得られる例以外にはundecidableな$\mathbb{Q}$上無限次数な環は今のところ得られていない。円分体のtowerの代数的整数環もdecidableかundecidableかわかっていない。

一方Diophantine undecidabileであるものはほとんど知られていないように思われる。唯一、$\tilde{\mathbb{Z}}$のsubringではないが、ある無限次のtotally real extension of $\mathbb{Q}$の中でFact 10に似た結果が得られている。[6]を参照のこと。

$\mathbb{Q}$上無限次数な$\tilde{\mathbb{Q}}$のsubfieldに関しては何もわかっていない。筆者は最近lを$l \equiv -1 \pmod 4$なる素数でしかも2がその代数的整数環の中でprime elementとなるような素数ならば$\bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$はundecidableであることを証明したが、検討中である。

decidableな$\tilde{\mathbb{Z}}$の$\mathbb{Q}$上無限次数なsubringに関しては、突破口として、

Fact 12 $\tilde{\mathbb{Z}}$は*decidable*である。

まずRumelyがDiophantine decidableであることを示し、後にVan den Driesがfull-decidabilityを示した。

次にPrestel, Schmidにより、

Fact 13 $\tilde{\mathbb{Z}} \cap \mathbb{R}$は*decidable*である。

今Mを素数の空でない有限個の集合とし、$\mathbb{Q}^M$をthe field of totally M-adic algebraic numbers、つまりその$\mathbb{Q}$上の最少多項式がすべての$\mathbb{Q}_p$ $(p \in M)$でlinear factorに分解するようなalgebraic numberのなす体とする。Ershovにより、

Fact 14 $\mathbb{Q}^M$は*decidable*である。

これを用い、Darnièreにより、

Fact 15 $\mathbb{Q}^M \cap \tilde{\mathbb{Z}}$は*decidable*である。

さらにErshovにより、

Fact 16 商体が$\tilde{\mathbb{Q}}$であるような*integrally closed ring*は*decidable*である。

一方体としては、前に述べたようにFried, Haran, Völkleinらにより、

Fact 17 $\mathbb{Q}^{tr}$は*decidable*である。

参考文献

[1] Luck Darnière. Decidability and local-global principles. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pp. 145–167. Providence RI, American Mathematical Society, 2000.

[2] Thanases Pheidas. Extensions of Hilbert's tenth problem. *J. Symbolic Logic*, **59**(2): 372–397, 1994.

[3] Thanases Pheidas and Karim Zahidi. Undecidability of existential theories of rings and fields. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pp. 49–105. Providence RI, American Mathematical Society, 2000.

[4] Bjorn Poonen. Undecidability in number theory. *Notices of American Mathematical Society*, **55**(3): 344–351, 2008.

[5] Alexandra Shlapentokh. *Hilbrt's tenth problem. Diophantine classes and extensions to global fields.* New Mathematical Monograph, vol. 7, Cambridge University Press, Cambridge, 2007.

[6] Alexandra Shlapentokh. On Diophantine Definability and Decidability in some infinite totally real extensions of $\mathbb{Q}$. *Trans. Amer. Math. Soc.*, **356**(8): 3189–3207, 2003.