数理解析研究所講究録 第2119巻 2019年 71-74

On a proof of undecidability of the ring of algebraic integers

Kenji Fukuzaki
International University of Kagoshima

Abstract Let K be an algebraic extension of the rationals and A be the ring of algebraic integers of K. As to the method of proving undecidability of the ring A, it seems that the only one method has been known, which is due to Julia Robinson, especially for infinite algebraic extensions of the rationals. (See [Vi].) We discuss an alternative method for the ring of algebraic integers of cyclotomic towers for some rational primes.

1 Beth's definability theorem

Let $K = K_p$ be the field obtained by adjoining to $\mathbb{Q}$ all p-power roots of unity where p is a rational prime integer, and A its ring of algebraic integers. Videla ([Vi]) proved that $\mathbb{Z}$ is $\mathfrak{L}$-definable in A using a result of J. Robinson ([Ro]) giving a condition for undecidability of algebraic integer rings and a result of D. Rohrlich about points on elliptic curves in cyclotomic towers.

We discuss a method to prove that $\mathbb{N}$ is definable in A, using Beth's definability theorem.

Let P and P' be two new n-placed relation symbols, not in the language $\mathfrak{L}$. Let $\Sigma(P)$ be a set of sentences of the language $\mathfrak{L}\cup\{P\}$, and let $\Sigma(P')$ be the corresponding set of sentences of $\mathfrak{L}\cup\{P'\}$ formed by replacing P everywhere by P'. We say that $\Sigma(P)$ *defines* P *implicitly* iff

$$\Sigma(P)\cup\Sigma(P') \models (\forall x_1 \ldots x_n)[P(x_1 \ldots x_n) \leftrightarrow P'(x_1 \ldots x_n)].$$

Equivalently, if $(\mathfrak{A}, R)$ and $(\mathfrak{A}, R')$ are models of $\Sigma(P)$, then $R = R'$. $\Sigma(P)$ is said to *define* P *explicitly* iff there is a formula $\varphi(x_1 \ldots x_n)$ of $\mathfrak{L}$ such that

$$\Sigma(P) \models (\forall x_1 \ldots x_n)[P(x_1 \ldots x_n) \leftrightarrow \varphi(x_1 \ldots x_n)].$$

Beth' definability theorem states that *if* $\Sigma(P)$ *defines* P *implicitly iff* $\Sigma(P)$ *defines* P *explicitly.*

Let $\Sigma(P) = \mathrm{Th}_{\mathfrak{L}\cup\{P\}}(A, \mathbb{N})$. We assume (R, N) and (R, N') are models of $\Sigma(P)$. We shall prove $N = N'$.

Models of $\mathrm{Th}_{\mathfrak{L}}(\mathbb{Z})$ are called *Peano ring.* It is known that every Peano ring different from $\mathbb{Z}$ has infinite transcendental degree over $\mathbb{Z}$ ([JL]), Since $\mathbb{N}$ is definable in $\mathbb{Z}$ and $\mathbb{Z}$ is interpretable in $\mathbb{N}$, we get the following.

Lemma 1. *In the standard model* $(A, \mathbb{N})$, $\Sigma(P)$ *defines* $\mathbb{N}$ *implicitly.*

Thus we may only consider nonstandard models.

2 Cyclotomic towers

Let $K = K_p = \mathbb{Q}(\{\zeta_{p^n} : n \in \mathbb{N}\})$ where p is a rational prime integer and ζ_{p^n} is a primitive p^n-th root of unity. Let A be its ring of algebraic integers.

It is known that rational primes 2 is primitive in $\mathbb{Z}/p^n$ for every $n > 0$ if 2 is a primitive in $\mathbb{Z}/p$ and $2^{p-1} = 1 + kp$ with $(k, p) = 1$. It follows that 2 remains prime in every subextension $K_n = \mathbb{Q}(\zeta_{p^n})$ where ζ_{p^n} is a primitive p^n-th root of unity. (See [Na], p. 182.) For example, $p = 3, 5, 11, 13, \ldots$ are such primes. Let p be such a prime and consider $K = K_p$. We see that 2 remains prime in A. We shall prove $\mathbb{N}$ is definable in A, from which follows that A is undecidable.

We shall look into $\mathfrak{L} \cup \{P\}$-properties of A, that is, $\Sigma(P)$-sentences which hold in $(A, \mathbb{N})$. We notice that $\mathfrak{L} \cup \{P\}$-properties of A hold in (R, N) which is a nonstandard model of $\Sigma(P) = \mathrm{Th}_{\mathfrak{L} \cup \{P\}}(A, \mathbb{N})$.

Lemma 2. *Let $x \in A$ be a non-zero element such that every non-unit factor of x is divisible by 2. then $x = 2^m u$ for some $m \in \mathbb{N}$ and some unit u of A.*

Since 2 is a prime element of A the above lemma is obviously true. Noting that 2^n is $\mathfrak{L} \cup \{P\}$-definable in A for $n \in P$, we see that this is an $\mathfrak{L} \cup \{P\}$-property of A. (See [Ka], p. 67.)

Lemma 3. *Let $\varphi(x, \bar{y})$ is an $\mathfrak{L} \cup \{P\}$-formula which implies $x \in P$, where $\bar{y}$ is a sequence of free variables of of finite length. Then*

$$(A, \mathbb{N}) \models \forall \bar{y}[\exists x \varphi(x, \bar{y}) \to \exists z(\varphi(z, \bar{y}) \wedge \forall w < z \neg\varphi(w, \bar{y}))].$$

This is the least number principle for $\mathbb{N}$. Thus, we can use the least number principle for S in the case of $\mathfrak{L} \cup \{P\}$-formulas.

3 Toward a proof

We assume (R, N) and (R, N') are models of $\Sigma(P)$. We note that $\mathbb{N} \subset S$ and $\mathbb{N} \subset S$. From now on we suppose $N \neq N'$ by way of contradiction.

We have two exponentiation of base 2 in R, that is, $2^N = \{2^a : a \in N\}$ and $2^{N'} = \{2^\alpha : \alpha \in N'\}$.

Lemma 4. *We have $2^N \neq 2^{N'}$.*

Proof. Suppose $2^N = 2^{N'}$. We may assume that there is an element $\alpha \in N' \setminus N$ by symmetry. By Euclidean division applied for N', there is $\beta \in N'$ with $2^\beta \leq \alpha < 2^{\beta+1}$, where $<$ and $\leq$ are defined by

$$x < y \text{ iff } y - x \neq 0 \wedge \exists z_1, z_2, z_3, z_4(y - x = z_1^2 + \cdots + z_4^2),$$

$$x \leq y \text{ iff } x = y \vee x < y.$$

By assumption there is $b \in N$ with $2^b \leq \alpha < 2^{b+1}$. We see that $2^b < \alpha < 2^{b+1}$ since $\alpha \notin N$. Consider $\mathfrak{L} \cup \{P\}$-formula

$$x \in P \wedge \exists y \notin P(2^x < y < 2^{x+1}).$$

We see that $b \in N$ satisfies the above $\mathfrak{L} \cup \{P\}$-formula taking α for y in (R, S). By the least number principle applied for (R, N), there is the least number $m \in N$ such that $2^m < z < 2^{m+1}$ for some $z \notin N$.

On the other hand, we note that $\alpha - 2^m \in N'$ and $2^N \in N'$, therefore for all $a \in N$, 2^a and $\alpha - 2^m$ are comparable, that is,

$$2^a < \alpha - 2^m \vee 2^a = \alpha - 2^m \vee 2^a > \alpha - 2^m.$$

Further, if $\alpha - 2^m = 2^a$ for some $a \in N$ then it would be the case that $\alpha \in N$. Thus we have

$$2^a < \alpha - 2^m \vee 2^a > \alpha - 2^m$$

for all $a \in N$.

Let $y = \alpha - 2^m$. Then we have $y < 2^m$ since $2^m - y = 2^{m+1} - \alpha$. Consider $\mathfrak{L} \cup \{P\}$-formula

$$x \in P(y < 2^x),$$

where y is a parameter. Again by the least number principle applied for (R, N), there is $d \in N$ with $d \leq m$ such that $y < 2^d$. and $2^{d-1} < y$ follows, a contradiction. □

Now let $2^\alpha \notin N$. Then, by Lemma 2, we have $2^\alpha = 2^n u$ for some $n \in N$ and for some unit $u \neq 1$. We want to use induction or the least number principle for $\mathfrak{L} \cup \{P\}$-formulas. If we adopt induction applied for (R, N'), we must write sufficient $\mathfrak{L} \cup \{P\}$-properties of 2^n to derive a contradiction. . We must note that P expresses N', not N. We must need more $\mathfrak{L} \cup \{P\}$-properties which hold in $(A, \mathbb{N})$. We hope that someone would succeed it.

For cyclotomic towers $K_2 = \mathbb{Q}(\{\zeta_{2^n} : n \in \mathbb{N}\})$, we have the following fact. (see [Na], p. 382.)

Fact 5. *Let $L/\mathbb{Q}$ is finite algebraic extension and M be the Galois closure of L over $\mathbb{Q}$. Let p be a rational prime integer.*

Then p remains prime in L iff the Galois group $G(M/\mathbb{Q})$is cyclic and generated by $F_{m/\mathbb{Q}}(p)$, where $F_{m/\mathbb{Q}}(p)$ is the Frobenius automorphism associated with p.

Thus there is no prime integer which remains prime in $K_2 = \mathbb{Q}(\{\zeta_{2^n} : n \in \mathbb{N}\})$: its subextension $\mathbb{Q}(\zeta_{2^3})$ is not cyclic..

References

[CK] C. C. Chang and H. J. Keisler, Model Theory, Vol. 73 of Studies in Logic and the foundations of Mathematics, North-Holland, Amsterdam, 1973.

[BS] J. L. Bell and A. B. Slomson, Models and Ultraproducts. North-Holland, Amsterdam, American Elsevier, New York, 1974.

[JL] C. U. Jensen and H. Lenzing. Model Theoretic Algebra with Particular Emphasis on Fields, Rings, Modules. Vol. 2 of Algebra , Logic and Applications, Gordon and Breach Science Publishers, New York, 1989.

[Na] W. Narkiewicz. Elementary and Analytic Theory of Numbers Second Edition, Polish Scientific Publishers, Warszawa, 1990.

[Ka] R. Kaye, Models of Peano Arithmetic, Clarendon Press, Oxford, 1991.

[Ro] J. Robinson. On the decision problem for algebraic rings. In *Studies in mathematical analysis and related topics*, pp. 297–304, Stanford Univ. Press, Stanford, Calif., 1962.

[Vi] C. R. Videla, The Undecidability of Cyclotomic Towers, *Proceedings of the AMS*, Vol. 128, No. 12, 3671-3674.

The International University of Kagoshima,8-34-1, Sakanoue,
Kagoshima-shi, 891-0197, Japan
e-mail: fukuzaki@eco.iuk.ac.jp