Rings of totally real integers with $\mathbb{N}$

Kenji Fukuzaki *

Abstract Let A be a ring of totally real integers (not necessarily of finite degree over the rationals). Let $\mathfrak{L}$ be the ring language, and let P be a new 1-placed relation symbol not in the language $\mathfrak{L}$. We consider $(A, \mathbb{N})$, the expansion of A to the language $\mathfrak{L} \cup \{P\}$ with $P^A = \mathbb{N}$. We show that for $x \in A$ and $n \in \mathbb{N}$, x^n is $\mathfrak{L} \cup \{P\}$-definable.

1 Exponentiation by exponents in $\mathbb{N}$

We shall show that for $x \in A$ and $n \in \mathbb{N}$, x^n is $\mathfrak{L} \cup \{P\}$-definable in $(A, \mathbb{N})$, that is, there is a $\mathfrak{L} \cup \{P\}$-formula $\varphi(x, n, y)$ such that, given x, $\Sigma(P)$ implies

- for all $n \in P$, there exists a unique y,
- $\varphi(x, 0, y)$ implies $y = 1$, and
- for all $n \in P$ and for all y, z, $\varphi(x, n, y)$ and $\varphi(x, n+1, z)$ implies $z = yx$.

Then, $\varphi(x, n, y)$ means $y = x^n$ in $(A, \mathbb{N})$. (We write $x \in P$ instead of $P(x)$.)

We begin by introducing the partial order on A which is used in [Ro]. An algebraic number x is totally non-negative ($x \gg 0$) if x and all its real conjugates are non-negative. We write $x \ll y$ to indicate that $y - x$ is totally non-negative. (J. Robinson used the symbol $\ll$ in [Ro], but we use $\ll$.) We write $x \lll y$ if $x \ll y$ and $x \neq y$.

Siegel [Sie] proved that an algebraic number x is the sum of four squares of numbers in the field $\mathbb{Q}(x)$ iff it is totally non-negative. Hence in any ring of totally real integers,

$$x \ll y \Leftrightarrow \exists t, u, v, w, z[t^2(y - x) = u^2 + v^2 + w^2 + z^2 \wedge t \neq 0].$$

We see that $\ll$ is a partial order on A and that $x \ll y$ implies $x + z \ll y + z$, $0 \ll x$ and $0 \ll y$ implies $0 \ll xy$.

We note that, for $s, t \in \mathbb{Z}$, usual order relation $s \leq t$ coincides with $s \ll t$. We also note that $\mathbb{Z}$ is $\mathfrak{L} \cup \{P\}$-definable in $(A, \mathbb{N})$ and for $\alpha \in A$ there is an $n \in \mathbb{N}$ with $-n \ll \alpha \lll n$.

Lemma 1. *Given two totally real integers t and m with $m \gg 0$, there is at most one totally real integer a such that $t \equiv a \pmod{m}$ and $-m \ll 2a \lll m$, that is, such an integer a is unique if it exists.*

Proof. Suppose that there are two such totally real integers a, b. Then there is $v \in \mathbb{Z}^{tr}$ with $a - b = mv$. Let K be the Galois closure of $\mathbb{Q}(a, b, m)$. For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have

$$|m^\sigma v^\sigma| = |a^\sigma - b^\sigma|, \quad |2a^\sigma - 2b^\sigma| < 2m^\sigma.$$

Thus $|v^\sigma| < 1$ for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, so that $v = 0$ and $a = b$. □

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

This is a simple improvement of Lemma 3 of [Ro].

Using the above lemma, we have the following :

Proposition 2 (Gödel's β-function for rings of totally real integers)**.** *Let $n \in \mathbb{N}$ with $x_0, x_1, \ldots, x_{n-1} \in A$. Then, there are $a \in A$ and $k \in \mathbb{N}$ such that*

$$-(i+1)k - 1 \lll 2x_i \ll ((i+1)k+1) \text{ and}$$
$$a \equiv x_i \pmod{((i+1)k+1)}$$

hold for all $i < n$. If $a \equiv y_i \pmod{((i+1)k+1)}$ then $y_i = x_i$, for all i.

Proof. Choose $k \in \mathbb{N}$ so that $-k \lll 2x_i \ll k$ for all $i < n$. Put $m_i = (i+1)k + 1$. Then $m_0, m_1, \ldots, m_{n-1}$ are pairwise coprime. Let

$$M = m_0 m_1 \cdots m_{n-1} = m_0 M_0 = m_1 M_1 = \cdots = m_{n-1} M_{n-1}$$

and let $t_i \in \mathbb{N}$ be such that $M_i t_i \equiv 1 \pmod{m_i}$ for each i. We let $a = x_0 M_0 t_0 + x_1 M_1 t_1 + \cdots + x_{n-1} M_{n-1} t_{n-1}$. Then, $a \equiv x_i \pmod{m_i}$ for each i. For each m_i, $a \bmod m_i$ is unique by the above lemma, hence $a \bmod m_i$ must be x_i. □

We define $\beta(a, k, i)$ to be $a \bmod (i+1)k + 1$.

Gödel's β-function for $\mathbb{N}$ (or models of PA), $\beta(a, k, i)$, is defined to be the remainder of Euclidean division $a \div ((i+1)k+1)$, which equals x_i. It exists for every a, k, i. For rings of totally real integers, it is not the case. Nevertheless, for a given sequence of totally real integers $x_0, x_1, \ldots, x_{n-1}$, if we take $k \in \mathbb{N}$ with $-k \lll 2x_i \ll k$ for all $i < n$ and construct the above a, then $a \bmod m_i$ exists uniquely and equals x_i for each i. Note that such $k \in \mathbb{N}$ always exists.

Thus, for any sequence $x_0, x_1, \ldots, x_{n-1} \in A$ there are $a \in A$ and $k \in \mathbb{N}$ such that $\beta(a, k, i) = x_i$ for $i < n$. Any such sequence can be extended.

Lemma 3. *Given a sequence $x_0, x_1, \ldots, x_n \in A$, let $a \in A$ and $k \in \mathbb{N}$ be such that $\beta(a, k, i) = x_i$ for $i < n$. Then, there are $a' \in A$ and $k' \in \mathbb{N}$ such that $\beta(a, k, i) = \beta(a', k')$ for $i < n$ and $\beta(a', k', n) = x_n$.*

For a proof, see [K, p.60].

Now, we let $\varphi(x, n, y)$ be the following formula:

" *$n \in P$ and there are a, k with $k \in P$ such that*

- $a \equiv 1 \pmod{m_0}$,
- *for every $i < n$,*
  there is b such that $a \equiv b \pmod{m_i}$ and $-m_i \lll 2b \ll m_i$, and
  there is c such that $a \equiv c \pmod{m_{i+1}}$ and $-m_{i+1} \lll 2c \ll m_{i+1}$, and $c = bx$,
- $a \equiv y \pmod{m_n}$ *and $-m_n \lll 2y \ll m_n$* ",

where $m_i = (i+1)k + 1$.

Proposition 4. *For $x \in A$, the formula $\varphi(x, n, y)$ defines function of $\mathbb{N}$ to A and its function satisfies the recursive definition of x^n in $(A, \mathbb{N})$.*

Proof. We need to show both existence and uniqueness of y such that $\varphi(x, n, y)$ holds and the defined function y satisfies the recursive definition of x^n. This follows by induction on $n \in \mathbb{N}$, using the above proposition and lemma. □

Thus, x^n is definable in $(A, \mathbb{N})$. The properties of exponentiation are easily proved by induction on $n \in \mathbb{N}$. If $x \in \mathbb{N}$, $x^n \in \mathbb{N}$ follows by induction. It is known that even in models of PA (not $\mathrm{Th}(\mathbb{N})$), exponentiation is definable. See [K, p. 68].

References

[K] 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.

[Sie] C. Siegel. Darstellung total positive Zahlen durch Quadrate, *Mathematishe Zeitschrift*, Vol. 10, pp. 246–275, 1921.