M. Yasumoto
Nagoya Math. J.
Vol. 70 (1978), 167-172

A NOTE ON SOME ORDERED RING

MASAHIRO YASUMOTO

An ordered ring with the least positive element 1 is a "$\boldsymbol{Z}$-ring" if for each natural number n,

$$\forall x \exists y \exists m(x = ny + m) \qquad 0 \leqq m < n .$$

An element $x \neq 0$ of a $\boldsymbol{Z}$-ring is "infinitely divisible" if for infinitely many natural numbers n,

$$\exists y \ (x = ny) .$$

For example, $\boldsymbol{Z}$ (the set of integers) is a $\boldsymbol{Z}$-ring with no infinitely divisible element. Another example of $\boldsymbol{Z}$-rings is $R = \{f(X) \in \boldsymbol{Q}[X] \mid f(0) \in \boldsymbol{Z}\}$ where $\boldsymbol{Q}$ is the set of rationals and X is placed greater than all rationals. Then R has infinitely divisible elements, X, X^2, etc. In this paper we prove

THEOREM. *There exists a $\boldsymbol{Z}$-ring A $(\neq \boldsymbol{Z})$ which has no infinitely divisible element.*

Remark 1. The ring A which we construct has the following additional properties.

1) $\forall x \forall a > 0 \ \exists y \exists b \ (x = ay + b \ \& \ 0 \leqq b < a)$.

2) A is a unique factorization domain, i.e. every element can be uniquely factorized to a finite product of prime elements.

The existence of such $\boldsymbol{Z}$-ring was suggested by R. Kurata. (see Remark 2)

We introduce some notations. (refer to [1]). Let $\boldsymbol{N}$ be the set of natural numbers. We say that $F \subset P(\boldsymbol{N})$ (the power set of $\boldsymbol{N}$) is "a nonprincipal ultrafilter" if

1) $a \in F$ & $b \in F$ imply $a \cap b \in F$.

2) $a \in F$ & $a \subset b$ imply $b \in F$.

3) $a \notin F$ implies $\boldsymbol{N} - a \in F$.

Received May 26, 1977.

https://doi.org/10.1017/S0027763000021851 Published online by Cambridge University Press

4) If a is finite then $a \notin F$.

We introduce an equivalence relation by F into $Z^N = Z \times Z \times \cdots$ as follows.

$$(n_0, n_1, n_2, \cdots)_{\tilde{F}}(m_0, m_1, m_2, \cdots)$$

if and only if

$$\{i \in N \mid n_i = m_i\} \in F .$$

Since F is an ultrafilter, $\tilde{F}$ is the equivalence relation. We say that $Z^N/\tilde{F}$ is the ultrapower of Z and denote it by Z^*. Let $(n_i)^*$ be the equivalence class of (n_i). We can well define

$$(n_i)^* + (m_i)^* = (n_i + m_i)^*$$
$$(n_i)^* \cdot (m_i)^* = (n_i \cdot m_i)^*$$
$$(n_i)^* \leqq (m_i)^* \qquad \text{if } \{i \in N \mid n_i \leqq m_i\} \in F .$$

We may assume $Z \subset Z^*$ by identifying n with $(n, n, n, \cdots)^*$.

By Los's theorem [1] Z^* is the elementary extension of Z, in other words, for any first-order formula $\phi(v_1, v_2, \cdots, v_k)$ of the language of the ordered ring and for any integers $n_1, n_2, \cdots, n_k$, $\phi(n_1, n_2, \cdots, n_k)$ holds in Z^*, if and only if it holds in Z. For example, "the axioms of the ordered ring" and "$\forall x \forall a > 0\ \exists y \exists b\ (x = ay + b),\ 0 \leqq b < a$" are first-order formulae. So Z^* is a Z-ring. But "there is no infinitely divisible element" can not be a first-order formula. In fact, Z^* has infinitely divisible elements, $(2, 2^2, 2^3, \cdots)^*$, $(1!, 2!, 3!, 4!, \cdots)^*$, etc.

In the following we construct a subring A of Z^* which satisfies the theorem.

Proof of the theorem. Let p_n be the n-th prime number,

$$A_{n,m} = \left\{kp_n^{m!} + \sum_{i=1}^{m-1} p_n^{i!} + [\log p_n] \,\middle|\, k = 0, \pm 1, \pm 2, \cdots\right\}$$

where "[ ]" denotes the integer part.

Obviously, $m_1 \leqq m_2$ implies $A_{n,m_1} \supset A_{n,m_2}$. Since $p_1^{n!}, p_2^{n!}, \cdots, p_n^{n!}$ are mutually prime, $B_n = \bigcap_{i=1}^n A_{i,n}$ is not empty. Pick $0 \leqq c_n \in B_n$ and define $c = (c_1, c_2, \cdots, c_n, \cdots)$.

Let $A' = \{f(c^*) \in Z^* \mid f(X) \in Z[X]\}$ and

$$A = \{z \in Z^* \mid \exists n \in Z\ (n \neq 0\ \&\ nz \in A')\} .$$

We prove that A satisfies the theorem.

By the definition of A and by the fact that Z^* is a Z-ring, it is easily checked that A is a Z-ring. By the definition of c, c^* is infinitely large in Z^* i.e. for each $n \in Z$ $(n < c^*)$ in Z^*. So $A \neq Z$.

For each $x \in A'$, we define $f_x(X) \in Z[X]$ to be $f_x(c^*) = x$. We write $x|y$ if $\exists z$ $(y = zx)$. We prove that there is no infinitely divisible element in A.

LEMMA 1. *For each* $x \in A$, $\{n \in Z | p_n | x$ *in* $Z^*\}$ *is finite.*

Proof. We may assume $x \in A'$.

By the definition of c,

$$\begin{aligned} c^* &\equiv [\log p_n] && (\mathrm{mod}\ p_n) \\ (c^*)^k &\equiv [\log p_n]^k && (\mathrm{mod}\ p_n) \\ x &\equiv f_x([\log p_n]) && (\mathrm{mod}\ p_n)\,. \end{aligned}$$

Since $f_x(X) \in Z[X]$,

$$\lim_{n\to\infty} \frac{f_x([\log p_n])}{p_n} = 0\,.$$

Therefore, for all but finitely many n,

$$|f_x([\log p_n])| < p_n\,.$$

Since $\{n \in Z | f_x([\log p_n]) = 0\}$ is finite, for all but finitely many n,

$$x \not\equiv 0 \qquad (\mathrm{mod}\ p_n)\,.$$

The result follows.

LEMMA 2. *For each* $x \in A$ *and each* $n \in N$,

$$\{m \in Z | p_n^{m!} | x \text{ in } Z^*\} \qquad \text{is finite}\,.$$

Proof. Similar to the proof of Lemma 1. We may assume $x \in A'$.

By the definition of c,

$$\begin{aligned} c^* &\equiv \sum_{i=1}^{m-1} p_n^{i!} + [\log p_n] && (\mathrm{mod}\ p_n^{m!}) \\ (c^*)^k &\equiv \left(\sum_{i=1}^{m-1} p_n^{i!} + [\log p_n]\right)^k && (\mathrm{mod}\ p_n^{m!}) \\ x &\equiv f_x\left(\sum_{i=1}^{m-1} p_n^{i!} + [\log p_n]\right) && (\mathrm{mod}\ p_n^{m!})\,. \end{aligned}$$

https://doi.org/10.1017/S0027763000021851 Published online by Cambridge University Press

Since $f_x(X) \in Z[X]$,

$$\left|\lim_{m\to\infty} \frac{f_x\left(\sum_{i=1}^{m-1} p_n^{i!} + [\log p_n]\right)}{p_n^{m!}}\right| \leqq \lim_{m\to\infty} \frac{Kp_n^{M\cdot(m-1)!}}{p_n^{m!}} = 0$$

where K and M are some constant numbers depending only on $f_x(X)$.

Therefore for all but finitely many m,

$$\left|f_x\left(\sum_{i=1}^{m-1} p_n^{i!} + [\log p_n]\right)\right| < p_n^{m!} .$$

Since $\{m \in Z \mid f_x(\sum_{i=1}^{m-1} p_n^{i!} + [\log p_n]) = 0\}$ is finite, for all but finitely many m,

$$x = f_x\left(\sum_{i=1}^{m-1} p_n^{i!} + [\log p_n]\right) \qquad (\bmod p_n^{m!})$$

and

$$0 < \left|f_x\left(\sum_{i=1}^{m-1} p_n^{i!} + [\log p_n]\right)\right| < p_n^{m!} .$$

This proves Lemma 2.

By lemma 1 and lemma 2, every $x \in A$ is not infinitely divisible in Z^*, and therefore so is in A. So our theorem is proved.

Remark. Our original motivation is to construct a model which resembles the set of natural numbers, but is not the same. The positive part of A above constructed resembles the set of natural numbers in the following sence. (It is easily checked.)

1) The positive part of A satisfies mathematical induction for any formula $\phi(x)$ of the language $L = \langle +, =, < \rangle$.

2) The positive part of A satisfies mathematical induction of the product form. Namely, for any formula $\phi(x)$ of the language $L = \langle +, =, \cdot, < \rangle$, if $\phi(1)$, $\phi(p)$ for any prime p, and

$$\forall x < a(x \mid a \to \phi(x)) \to \phi(a) , \qquad \text{then } \forall x \phi(x) .$$

On the other hand, the theorem of Lagrange does not hold. For example, c^* can not be a sum of squares.

Further results about A above constructed.

In the following, we prove that A cannot be an Euclidean ring (Lemma 3), but admits Euclidean algorithm (Lemma 4).

Let a and b be elements of A. We define $a \ll b$ iff $b - a > n$ for any $n \in \boldsymbol{Z}$.

LEMMA 3. *A cannot be an Euclidean ring.*

Proof. If not, there exist a well-ordered set W and a map ρ from A onto W such that

(*) $\forall x \forall a \exists y \exists b \;\; x = ay + b$ and $\rho(b) < \rho(a)$.

Let $B = \{\rho(x) \mid x \in A - \boldsymbol{Z}\}$. Then there is an element $a_0 \in A - \boldsymbol{Z}$ such that $\rho(a_0)$ is the least element of B. We may assume that $a_0 > 0$. We take an x_0 such that $0 \ll x_0 \ll a_0$.

By (*), there exist y and b such that

$$x_0 = a_0 y + b \quad \text{and} \quad \rho(b) < \rho(a_0) .$$

Then by the definition of a_0, $b \in \boldsymbol{Z}$.

Since 1 is the least positive element, $y \geqq 1$. So $x_0 - b \geqq a_0$. This is contrary to $x_0 \ll a_0$.

Let a be an element of A, then there exist $f(X) \in \boldsymbol{Z}[X]$ and $n \in \boldsymbol{Z}$ such that $a = f(c^*)/n$. We can well define $\deg(a) = \deg(f(X))$.

We notice that $a < b$ implies $\deg(a) \leqq \deg(b)$.

LEMMA 4. *A admits Euclidean algorithm.*

Proof. Let a and b be elements of A and assume $a > b > 0$.

We prove by induction on $\deg(a)$.

(1) If $\deg(a) = 0$, then $a, b \in Z$. This case is obvious.

(2a) Let $\deg(a) = n$ and $\deg(b) < n$.

There exist y and d such that

$$a = by + d \quad \text{and} \quad 0 \leqq d < b .$$

Then $\deg(d) \leqq \deg(b) < n$. By the induction hypothesis, Euclidean algorithm for b and d exists.

(2b) Let $\deg(a) = \deg(b) = n$.

We can write

$$a = \frac{1}{m}(a_0 c^{*n} + \cdots + a_n)$$

$$b = \frac{1}{m}(b_0 c^{*n} + \cdots + b_n)$$

where $m, a_0, \cdots, a_n, b_0, \cdots, b_n$ are elements of $\boldsymbol{Z}$ and $0 < b_0 \leqq a_0$.

Since $a_0, b_0 \in \boldsymbol{Z}$, there is a system of equations

$$\begin{aligned} a_0 &= q_1 b_0 + r_1 \\ b_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_k &= q_{k+2} r_{k+1} \end{aligned} \qquad \begin{pmatrix} q_1, q_2, \cdots, q_{k+2}, r_1, r_2, \cdots, r_{k+1} \in \boldsymbol{Z} \\ b_0 > r_1 > r_2 > \cdots > r_{k+1} > 0 \end{pmatrix}$$

Then

$$\begin{aligned} a &= q_1 b + R_1 \\ b &= q_2 R_1 + R_2 \\ &\vdots \\ R_k &= q_{k+2} R_{k+1} + R_{k+2} \end{aligned} \qquad \left(\begin{array}{l} \text{If } 1 \leqq i \leqq k+1, \\ R_i = \dfrac{1}{m}(r_i c^{*n} + \cdots). \\ \deg (R_{k+2}) < n. \end{array} \right)$$

So case (2b) is reduced to (2a).

References

[1] Bell, J. L. and Slomson, A. B.: Models and Ultraproducts. Amsterdam, North-Holland Publishing Company, 1969.

[2] Chang, C. C. and Keisler, J.: Model Theory, North-Holland.

Nagoya University

https://doi.org/10.1017/S0027763000021851 Published online by Cambridge University Press