DEMONSTRATIO MATHEMATICA
Vol. V No 1 1973

Roman Kiełpiński, Daniel Simson

DECOMPOSABILITY OF ELEMENTS IN THE RING OF STRUCTURAL NUMBERS

If $X = \{x_t\}_{t\in T}$ is an arbitrary non-empty set, we define a ring $S\langle X\rangle$ as the factor ring $Z_2[X]/(X^2)$ where $Z_2[X]$ is the polynomial ring over the field $Z_2 = \{0,1\}$ and (X^2) is the ideal in $Z_2[X]$ generated by all elements x^2 where $x\in X$. In [3], it is shown that the ring $S\langle X\rangle$ is isomorphic to the ring of structural numbers $S\{X\}$ defined in [1]. Throughout this paper we shall identify the ring $S\langle X\rangle$ and $S\{X\}$, and elements of $S\langle X\rangle$ will be called structural numbers.

It follows from [3] that any structural number s can be uniquely expressed in the form

$$(1)\qquad s = e + \sum e_{t_1,\dots,t_n}\left\langle x_{t_1}x_{t_2}\dots x_{t_n}\right\rangle$$

where the sum is taken over all finite subsets $\{t_1,\dots,t_n\}$ of T, $\left\langle x_{t_1}x_{t_2}\dots x_{t_n}\right\rangle$ is the coset represented by the polynomial $x_{t_1}x_{t_2}\dots x_{t_n}$, e and $e_{t_1,\dots,t_n}$ are elements of Z_2 and only a finite number of them are unequal to zero. Hence the Abelian group $S\langle X\rangle$ has the following direct sum decomposition

$$S\langle X\rangle = S_0 \oplus S_1 \oplus \dots \oplus S_n \oplus \dots$$

such that $S_iS_j \subseteq S_{i+j}$, where S_n denotes the Abelian subgroup of $S\langle X\rangle$ consisting of all homogenous structural numbers of degree n (see [3]); it means that any structural number s can be uniquely expressed in the form

(2) $$s = s_0 + s_1 + \dots + s_n$$

where $s_i \in S_i$. Finally, by [3] Theorem 3.3, every non-invertible structural number can be expressed as a product of irreducible structural numbers.

The aim of this paper is to study conditions which reflect the decomposability of a given structural number. In particular, we obtain some criteria of irreducibility. We describe an algorithm allowing one to decide in a finite number of steps whether a given homogenous structural can be expressed as a product of homogenous numbers of degree one. Using this algorithm one can find such expression if it exists of course.

Throughout this paper we use the notations and terminology from [3].

We start with the following general result.

P r o p o s i t i o n 1. Let R and S be arbitrary rings with identity elements and let $f:R \longrightarrow S$ be a ring homomorphism ($f(1) = 1$). Moreover, suppose that any non-zero-divisor in R is invertible and any zero-divisor d in R is nilpotent, i.e. $d^i = 0$ for some $i \geqslant 1$. Then an element p in R is irreducible if $f(p)$ is irreducible in S.

P r o o f. Suppose $p = rt$, $r,t \in R$. The $f(p) = f(r)f(t)$ and by our assumptions either $f(r)$ or $f(t)$ is invertible. Assume, for example, $f(t)$ is invertible. Then, by the assumptions, t is a non-zero-divisor. Hence t is invertible and the proposition is proved.

For any $x \in X$ we define a ring homomorphism

(3) $$p_x : S\langle X\rangle \longrightarrow S\langle X\rangle$$

by formula $p_x(s) = s + d_x(s)\langle x\rangle$, where d_x is the derivation from [3] Theorem 2.2. Then in view of Proposition 1 we obtain.

C o r o l l a r y 2. A structural number s is irreducible if $p_x(s)$ is irreducible for some $x \in X$.

E x a m p l e 1. If $x_1,\ldots,x_n$ are distinct elements of X then the structural number

$$s = \langle x_1x_2\rangle + \langle x_3x_4\rangle + \ldots + \langle x_{n-1}x_n\rangle$$

is irreducible for $n \geqslant 4$. In fact, since $\langle x_1x_2\rangle + \langle x_3x_4\rangle$ is irreducible of course, then so does s by induction using the previous Corollary.

R e m a r k 3. Fix an element x of X. Then any structural number s can be uniquely expressed in the form

$$s = p_x(s) + \langle x\rangle d_x(s). \tag{4}$$

By Corollary 2, if $p_x(s)$ is irreducible then so does s. Now suppose that $p_x(s) = v'v''$, where $d_x(v') = d_x(v'') = 0$. If there exist u' and u'' such that $d_x(s) = v'u'' + v''u'$ and $d_x(u') = d_x(u'') = 0$, then

$$s = (v' + \langle x\rangle u')(v'' + \langle x\rangle u'').$$

Following [1] Definition 2-4, we call a decomposition

$$s = t_1t_2\cdot\ldots\cdot t_n$$

canonical if any element t_i has the form

$$t_i = t_{i1} + t_{i2} + \ldots + t_{in}, \quad t_{ij} \in S_j, \tag{5}$$

with $t_{i1} \neq 0$. A divisor of s of the type (5) will be called a canonical divisor.

For the next Proposition we shall need the following.

L e m m a 4. If $0 \neq t \in S_1$, then $\mathrm{Ann}(t) = (t)$ where $\mathrm{Ann}(t)$ denotes the annihilator of t (see [2]).

P r o o f. Immediately follows from [2] Theorem 17.

P r o p o s i t i o n 5. Suppose that $s = s's''$ where $s = s_1 + \ldots + s_q$, $s' = s'_1 + \ldots + s'_q$, $s'_1 \neq 0$, $s'' = s''_p + \ldots + s''_q$, $s''_p \neq 0$. If $s_1 = \ldots = s_{p+n} = 0$ for some $n \geqslant 1$, then there exist elements $d_i \in S_{p+i-2}$, $i = 1,2,\ldots,n$, such that

$$(6)\quad \begin{cases} s''_p = s'_1 d_1 \\ s''_{p+1} = s'_2 d_1 + s'_1 d_2 \\ \dots\dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots \\ s''_{p+n-1} = s'_n d_1 + s'_{n-1} d_2 + \dots + s'_1 d_n \end{cases}$$

$$s_{p+n+1} = s'_1(s''_{p+n} + s'_{n+1}d_1 + \dots + s'_3 d_{n-1} + s'_2 d_n).$$

P r o o f. We shall prove the Proposition by induction on n. If $n = 1$ then the equality $s = s's''$ yields

$$s'_1 s''_p = s_{p+1} = 0$$

$$s_{p+2} = s'_1 s''_{p+1} + s'_2 s''_p .$$

Then, in virtue of the previous Lemma, we have

$$s''_p \in \mathrm{Ann}(s'_1) = (s'_1),$$

or equivalently, there exists an element $t = t_0 + t_1 + \dots + t_l$, $t_i \in S_i$, $l \geqslant p-1$, such that $s''_p = s'_1 t$. Hence $s''_p = s'_1 t_{p-1}$. Then, setting $d_1 = t_{p-1}$ we get

$$s_{p+2} = s'_1(s''_{p+1} + s'_2 d_1),$$

which proves the Proposition for $n = 1$.

Suppose that it has been proved for n. We shall prove that it is also true for n+1. Since $s_{p+n+1} = 0$ then as in the first part of the proof we find an element $d_{n+1} \in S_{p+n-1}$ such that

$$(7)\quad s''_{p+n} + s'_{n+1}d_1 + \dots + s'_2 d_n = s'_1 d_{n+1} .$$

Further, from the equality $s = s's''$ we derive

$$s_{p+n+2} = s'_1 s''_{p+n+1} + s'_2 s''_{p+n} + \dots + s'_{n+2} s''_p .$$

Then, in view of (6) we have

$$s_{p+n+2} = s'_1 s''_{p+n+1} +$$

$$s'_2(s'_{n+1}d_1 + s'_n d_2 + \dots + s'_3 d_{n-1} + s'_2 d_n + s'_1 d_{n+1}) +$$

$$s'_3(s'_n d_1 + s'_{n-1} d_2 + \dots + s'_2 d_{n-1} + s'_1 d_n) +$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$s'_{n+1}(s'_2 d_1 + s'_1 d_2) +$$

$$s'_{n+2} s'_1 d_1$$

$$= s'_1(s''_{p+n+1} + s'_{n+2} d_1 + \dots + s'_4 d_{n-1} + s'_3 d_n + s'_2 d_{n+1}) +$$

$$(8) \quad \begin{cases} s'_2(s'_{n+1} d_1 + s'_n d_2 + \dots + s'_3 d_{n-1} + s'_2 d_n) + \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ s'_{n+1} s'_2 d_1 . \end{cases}$$

It is easy to check by induction that the sum (8) is zero. Then, together with (6) and (7), this shows that the Proposition holds for $n+1$. The proof is completed.

C o r o l l a r y 6. Let $s = s_n + \dots + s_q$, $s_i \in S_i$, be a structural number with $s_n \neq 0$. Then

(a) if s_n admits no canonical divisors, the so does s,

(b) if $n \leqslant 4$ and s_n is irreducible, then so does s.

P r o o f. (a) immediately follows from Proposition 5. To prove (b), assume that $s = s' \cdot s''$ where $s'_0 = s''_0 = 0$. If $s'_1 = s''_1 = 0$, then $s_1 = s_2 = s_3 = 0$ and $s_4 = s'_2 s''_2$, so we obtain a contradiction. Consequently, the statement (b) follows from Proposition 5.

Now we consider the following question: "When does a given homogenous structural number admit a canonical decomposition?" For this purpose we need the following two results

L e m m a 7. Let $t_1,\dots,t_n$ be a non-zero elements of S_1. Then $t \in S_1 \cap (t_1,\dots,t_n)$ if and only if $t = e_1t_1 + \dots$ $\dots + e_nt_n$ for some $e_i \in Z_2$.

P r o o f. Easy.

L e m m a 8. Suppose that $s = t_1t_2\cdot\ldots\cdot t_n = t_1't_2'\cdot\ldots$ $\ldots\cdot t_m \neq 0$ where $t_i, t_i' \in S_1$. Then $n=m$ and $(t_1,\dots,t_n) =$ $= (t_1',\dots,t_n')$.

P r o o f. See [2] Corollary 18.

A basic tool for our considerations are the following two propositions:

P r o p o s i t i o n 9. Let x be a fixed element of X and let

$$s = p_x(s) + \langle x\rangle d_x(s)$$

be a homogenous structural number of degree n (i.e., $s \in S_n$). Then

(a) when $p_x(s) \neq 0$ admits no canonical decompositions, then so does s,

(b) when $p_x(s) = 0$ $n \geqslant 3$ and $d_x(s) \neq 0$ admits no canonical decompositions, then so does s.

P r o o f. Assume that s admits a canonical decomposition. Then there exist $e_1,\dots,e_n \in Z_2$ and $u_1,\dots,u_n \in S_1$ with $d_x(u_i) = 0$ for $i=1,\dots,n$, such that

$$\begin{aligned} s &= (u_1 + e_1\langle x\rangle)(u_2 + e_2\langle x\rangle)\ \dots\ (u_n + e_n\langle x\rangle) \\ &= u_1u_2\ \dots\ u_n + \left(\sum_{i=1}^{n} e_iu_1\ \dots\ \hat{u}_i\ \dots\ u_n\right)\langle x\rangle \end{aligned}$$

where $\hat{u}_i$ means delete u_i. Hence we get

$$p_x(s) = u_1u_2\ \dots\ u_n$$

$$d_x(s) = \sum_{i=1}^{n} e_iu_1\ \dots\ \hat{u}_i\ \dots\ u_n \tag{9}$$

and therefore the statement (a) of the Proposition follows. Now suppose that $p_x(s) = 0$ and $d_x(s) \neq 0$. Then $e_i u_1 \dots \dots \hat{u}_i \dots u_n \neq 0$ for some i. Without loss of generality we may assume $i=1$. If follows that the elements $u_2, \dots, u_n$ are linearly independent over the field Z_2. Thus, in virtue of [2] Theorem 17, we have

$$u_1 \in \mathrm{Ann}(u_2 u_3 \dots u_n) = (u_2, u_3, \dots, u_n).$$

By Lemma 7, u_1 has the form

$$u_1 = k_2 u_2 + \dots + k_n u_n, \quad k_i \in Z_2 .$$

Hence $u_1 \dots \hat{u}_i \dots u_n = k_i u_2 \dots u_n$ and therefore

$$d_x(s) = \left(\sum_{i=1}^{n} e_i k_i \right) u_2 u_3 \dots u_n \quad \text{with} \quad k_1 = 1,$$

which proves the second statement of the Proposition.

P r o p o s i t i o n 10. Let x be a fixed element of X and let

$$s = p_x(s) + \langle x \rangle d_x(s)$$

be a non-zero homogenous structural number of degree n. Suppose that

$$0 \neq p_x(s) = u_1 u_2 \dots u_n, \quad u_i \in S_1, \quad d_x(u_i) = 0.$$

Then s admits a canonical decomposition if and only if the equality (9) holds for some $e_1, \dots, e_n \in Z_2$. Moreover, if $e_1, \dots, e_n \in Z_2$ are such that (9) holds then we have a composition

$$s = (u_1 + e_1 \langle x \rangle)(u_2 + e_2 \langle x \rangle) \dots (u_n + e_n \langle x \rangle).$$

P r o o f. The "only if" part and the last statement of the Proposition are obvious. To prove the "if" part suppose that s has the following canonical decomposition

$$s = (u_1' + e_1'\langle x\rangle)(u_2' + e_2'\langle x\rangle) \ldots (u_n' + e_n'\langle x\rangle)$$

where $e_i' \in Z_2$, $u_i' \in S_1$ and $d_x(u_i') = 0$ for $i = 1,\ldots,n$. Then we have

$$p_x(s) = u_1u_2 \ldots u_n = u_1'u_2' \ldots u_n'$$

$$d_x(s) = \sum_{i=1}^{n} e_i'u_1' \ldots \hat{u}_i' \ldots u_n'.$$

By Lemmas 7 and 8, there exist elements $e_{ij} \in Z_2$, $i,j = 1,2,\ldots,n$, such that

$$u_i' = \sum_{j=1}^{n} e_{ij}u_j, \quad i=1,2,\ldots n.$$

Using this equality it is not difficult to check that

$$d_x(s) = \sum_{i=1}^{n} e_iu_1 \ldots \hat{u}_i \ldots u_n$$

for some $e_i \in Z_2$, which completes the proof.

Now we describe an algorithm allowing one to decide in a finite number of steps whether a given homogenous structural number admits a canonical decomposition.

Let $s \in S_n$, $n \geqslant 1$, be a fixed homogenous structural number of degree n and let $x_1,x_2,\ldots,x_m$ be all such elements of X that $d_{x_i}(s) \neq 0$.

Clearly $n \leqslant m$. We inductively define a sequence of structural numbers

$$a_1(s),\ a_2(s),\ldots,a_{m-n}(s),\ b_1(s),\ b_2(s),\ldots,b_{m-n}(s)$$

setting $a_1(s) = p_{x_m}(s)$, $b_1(s) = d_{x_m}(s)$, $a_{i+1}(s) = p_{x_{m-i}}(a_i)$, $b_{i+1}(s) = d_{x_{m-i}}(a_i)$. Then we have

$$s = a_1(s) + \langle x_m \rangle b_1(s)$$
$$a_1(s) = a_2(s) + \langle x_{m-1} \rangle b_2(s)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_{m-n-1}(s) = a_{m-n}(s) + \langle x_{n+1} \rangle b_{m-n}(s)$$
$$a_{m-n}(s) = e\langle x_1 x_2 \ldots x_n \rangle$$

where e is either 0 or 1. Observe also that

$$a_i(s),\ b_i(s) \in S\langle x_1, x_2, \ldots, x_{m-i} \rangle \subseteq S\langle X \rangle$$

and that the degree of any $b_i(s)$ is less then the degree of s.

First suppose $e \neq 0$ and consider the following equation

$$b_{m-n}(s) = \sum_{i=1}^{n} Y_i \langle x_1 \rangle \ldots \langle \hat{x}_i \rangle \ldots \langle x_n \rangle.$$

If this equation has no solution in Z_2 then it follows from Proposition 10 that $a_{m-n-1}(s)$ admits no canonical decompositions. Hence, applying Proposition 9a we infer that $a_{m-n-2}(s), \ldots, a_1(s)$ and s admit no canonical decompositions. If the equation has a solution $Y_1 = e_1, \ldots, Y_n = e_n \in Z_2$, then we have

$$a_{m-n-1}(s) = t_1 t_2 \ldots t_n$$

where $t_i = \langle x_i \rangle + e_i \langle x_{n+1} \rangle$, by Proposition 10, and we consider a new equation

$$b_{m-n-1}(s) = \sum_{i=1}^{n} Z_i t_1 \ldots \hat{t}_i \ldots t_n .$$

Continuing in this manner we either prove that s admits no canonical decompositions or we find a canonical decomposition of s.

Next suppose $e = 0$. Let $q \leqslant m-n$ be such that $b_q(s) \neq 0$ and $b_j(s) = 0$ for all $j > q$. If $b_q(s)$ admits no canonical decompositions then, by Proposition 9 (b), so does $a_{q-1}(s) = \langle x_{m-q+1}\rangle b_q(s)$. Then by Proposition 9 (a), $a_{q-2}(s), \dots, a_1(s)$ and s admit no canonical decompositions. Finally, if $b_q(s)$ admits a canonical decomposition, then so does $a_{q-1}(s)$ of course and we may apply the procedure from the case $e \neq 0$.

Observe that in the case $e = 0$ we reduce the canonical decomposability of the structural number s to the canonical decomposability of an structural number $b_q(s)$ with the degree less then the degree of s. If the degree of s is 2 then $b_q(s) \in S_1$ and therefore s trivially admits a canonical decomposition.

Consequently, to find a canonical decomposition of a given homogenous structural number it is sufficient to solve a finite number of systems of linear equations over the field Z_2.

E x a m p l e 2. Choose $x_1, \dots, x_n \in X$ and fix elements $e_{ij} \in Z_2$ for all $1 \leqslant i < j \leqslant n$. Consider the following structural number

$$s(x_1, \dots, x_n) = \sum_{i<j} e_{ij}\langle x_i x_j\rangle.$$

It is clear that

$$a_i = a_i(s(x_1, \dots, x_n)) = s(x_1, \dots, x_{n-1})$$

$$b_i = b_i(s(x_1, \dots, x_n)) = \sum_{k=1}^{n-1} e_{k(n-i+1)}\langle x_k\rangle$$

Now assume that $e_{ij} = 1$ for all $i < j \leqslant 4$. Then we have

$$a_{n-3} = (\langle x_1\rangle + \langle x_3\rangle)(\langle x_2\rangle + \langle x_3\rangle)$$

$$b_{n-3} = \langle x_1\rangle + \langle x_2\rangle + \langle x_3\rangle$$

$$a_{n-4} = a_{n-3} + b_{n-3}\langle x_4\rangle.$$

Since the equation $Y_1(\langle x_1\rangle + \langle x_3\rangle) + Y_2(\langle x_2\rangle + \langle x_3\rangle) = b_{n-3}$ has no solution in Z_2 of course, then a_{n-4} admits no canonical decompositions and hence so does $s(x_1,\dots,x_n)$ for any elements e_{ij}, $4 \leqslant i < j \leqslant n$.

Example 3. We find a canonical decomposition of the following structural number

$$s = \langle x_1x_2x_3\rangle + \langle x_1x_3x_4\rangle + \langle x_2x_3x_4\rangle + \langle x_2x_3x_5\rangle + \langle x_3x_4x_5\rangle .$$

Observe that $a_1 = \langle x_1x_2x_3\rangle + \langle x_1x_3x_4\rangle + \langle x_2x_3x_4\rangle$, $a_2 = \langle x_1x_2x_3\rangle$, $b_1 = \langle x_2x_3\rangle + \langle x_3x_4\rangle$, $b_2 = \langle x_1x_3\rangle + \langle x_2x_3\rangle$. Since the equation

$$Y_1\langle x_2x_3\rangle + Y_2\langle x_1x_3\rangle + Y_3\langle x_1x_2\rangle = b_2$$

holds for $Y_1 = Y_2 = 1$, $Y_3 = 0$, then

$$a_1 = (\langle x_1\rangle + \langle x_4\rangle)(\langle x_2\rangle + \langle x_4\rangle)\langle x_3\rangle .$$

Subsequently, we consider the following equation

$$b_1 = Z_1(\langle x_2\rangle + \langle x_4\rangle)\langle x_3\rangle + Z_2(\langle x_1\rangle + \langle x_4\rangle)\langle x_3\rangle +$$
$$+ Z_3(\langle x_1\rangle + \langle x_4\rangle)(\langle x_2\rangle + \langle x_4\rangle) .$$

Since this equation holds for $Z_1 = 1$, $Z_2 = Z_3 = 0$, then we obtain the following canonical decomposition of s

$$s = (\langle x_1\rangle + \langle x_4\rangle + \langle x_5\rangle)(\langle x_2\rangle + \langle x_4\rangle)\langle x_3\rangle .$$

REFERENCES

[1] S. Bellert, H. Woźniacki: Analiza i synteza układów elektrycznych metodą liczb strukturalnych, Warszawa 1968.

[2] R. Kiełpiński, D. Simson: On the lattice of ideals in the ring of structural numbers. Demonstratio Math. 5(1973)45-55.

[3] D. Simson: Some remarks on the ring of structural numbers, Demonstratio Math. 4 (1972) 215-222.

INSTITUTE OF MATHEMATICS, NICHOLAS COPERNICUS UNIVERSITY OF TORUŃ

Received September 5th, 1972.

Addresses of the Authors: Roman Kiełpiński, ul. Rusa 17/25, 87-100 Toruń
and Daniel Simson, ul. Chrobrego 11/20, 87-100 Toruń.