DEMONSTRATIO MATHEMATICA
Vol. V No 1 1973

Roman Kiełpiński, Daniel Simson

ON THE LATTICE OF IDEALS IN THE RING OF STRUCTURAL NUMBERS

Throughout this paper $S\langle X\rangle$ denotes the ring of structural numbers on a set X. By [5] it may be represented as the residue class ring of the polynomial ring $Z_2[X]$ modulo the ideal generated by squares of all elements of X. In the sequel we use the notations and terminology from [5].

The aim of this paper is to show the following equality

$$I = \mathrm{Ann}(\mathrm{Ann}\ I)$$

for any finitely generated ideal I in $S\langle X\rangle$. Here Ann T denotes the annihilator in $S\langle X\rangle$ of a subset T od $S\langle X\rangle$.

Moreover we show that the annihilator of the ideal generated by linearly independent elements $t_1,\dots,t_m$ of S_1 is equal to the ideal generated by the product $t_1,\dots,t_m$.

1. At first we assume that X is a finite set, e.g. $X = \{x_1,\dots,x_n\}$. By [5] Lemma 1.2 it follows that the elements $\langle x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}\rangle$, where ε_i are equal 0 or 1, form a standart basis of $S\langle X\rangle$ over Z_2. These elements are called monomials. The degree of the monomial $\langle x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}\rangle$ is $\varepsilon_1+\dots+\varepsilon_n$. As in [5] $S_m = S_m\langle X\rangle$ denotes the vector subspace over Z_2 in $S\langle X\rangle$ generated by all monomials of degree m. Observe that $\dim S_m = \binom{n}{m}$ for $0\leqslant m\leqslant n$, $S_m=0$ for $m>n$, and $\dim S\langle X\rangle = 2^n$.

The element $\langle x_1^o \dots x_n^o \rangle$ is the unity of $S\langle X\rangle$ and henceforth will be also denoted by 1.

By [5] any element s of $S\langle X\rangle$ has a unique expression

$$s = s_o + s_1 + \dots + s_n$$

where $s_i \in S_i$. If $s_o = s_1 = \dots = s_{m-1} = 0$, $s_m \neq 0$, then the number m is denoted by $\partial(s)$. The function ∂ is defined only for non-zero elements of $S\langle X\rangle$. It is clear that if $ss' \neq 0$ then $\partial(ss') \geqslant \partial(s) + \partial(s')$.

L e m m a 1. If s is a non-zero element of $S\langle X\rangle$ and $\partial(s) < n$, then there exists an element $x \in X$ such that $\langle x\rangle s \neq 0$.

P r o o f. Suppose that $\langle x_i\rangle s = 0$ for $i = 1,\dots,n$. Then $s = \langle x_i\rangle d_{x_i}(s)$. Hence we successively obtain

$$\begin{aligned} s &= \langle x_1\rangle d_{x_1}'(s) \\ &= \langle x_1 x_2\rangle d_{x_1} d_{x_2}(s) \\ &\dots\dots\dots\dots \\ &= \langle x_1 x_2 \dots x_n\rangle d_{x_1} d_{x_2} \dots d_{x_n}(s) \end{aligned}$$

and therefore $\partial(s) \geqslant n$, a contradiction.

C o r o l l a r y 2. For any non-zero element s of $S\langle X\rangle$ there exists an element $s' \in$ of $S\langle X\rangle$ such that $ss' = \langle x_1 \dots x_n\rangle$.

P r o o f. In view of the previous lemma, the corollary follows from the fact that the only one non-zero element in S_n is $\langle x_1 \dots x_n\rangle$.

Similarly we obtain

C o r o l l a r y 3. If I is a non-zero ideal in $S\langle X\rangle$, then the element $\langle x_1 \dots x_n\rangle$ belongs to I.

We define a function $\Phi : S\langle X\rangle \longrightarrow Z_2$ in the following way. If $s = \sum e_{(\varepsilon_1 \dots \varepsilon_n)} \langle x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}\rangle$, then we put

$$\Phi(s) = \sum e_{(\varepsilon_1 \dots \varepsilon_n)}.$$

L e m m a 4. (a) Φ is a Z_2 - linear function,
(b) If I is an ideal in $S\langle X\rangle$ and $\Phi(s) = 0$ for all elements of I, then $I = 0$.

P r o o f (a) is obvious. (b) follows from Corollary 3 because $\Phi(\langle x_1 \dots x_n\rangle) = 1$.

Let V be a subspace (over Z_2) of S X . We put

$$V' = \{ s \in S\langle X\rangle : \Phi(sv) = 0 \text{ for any } v \in V\}.$$

By Lemma 4 (a) the set V' is a subspace of $S\langle X\rangle$. Observe that, if $V \subseteq W$ then $W' \subset V'$.

In the sequel we need the following facts from linear algebra.

P r o p o s i t i o n 5. Let V be a finite dimensional vector space over a field K and let V_1, V_2 be two subspaces of V. Then the following statements hold:

(a) $\dim V = \dim V_1 + \dim V/V_1$.

(b) The set $V^* = \mathrm{Hom}(V,K)$ of all K-linear maps from V to K is a vector space over K and

$$\dim V^* = \dim V.$$

(c) $\dim V_1 + \dim V_2 = \dim (V_1 + V_2) + \dim (V_1 \cap V_2)$.

(d) If $V_1 \subset V_2$ and $\dim V_1 = \dim V_2$, then $V_1 = V_2$.

For proofs of the above facts see for instance [1].

Now we prove the fundamental results of this paper.

T h e o r e m 6. Let V and W be subspaces of $S\langle X\rangle$. Then

(a) $\dim V + \dim V' = 2^n$.

(b) $V = (V')'$.

(c) $V' \cap W' = (V + W)'$.

(d) $V' + W' = (V \cap W)'$.

P r o o f. (a) By Proposition 5 (a) and the fact that $\dim S\langle X\rangle = 2^n$, it is sufficient to prove that $\dim V = \dim S\langle X\rangle / V'$.

For any element $v \in V$ we define a linear map

$$f_v : S\langle X\rangle/V' \longrightarrow Z_2$$

by the formula

$$f_v(s + V') = \Phi(v\,s),$$

where $s + V' \in S\langle X\rangle/V'$. Thus we may define a map

$$f : V \longrightarrow (S\langle X\rangle/V')^*$$

by the formula $f(v) = f_v$ for any $v \in V$. If $v_1, v_2 \in V$ and $s \in S\langle X\rangle$ then we obtain

$$\begin{aligned}
\left[f(v_1 + v_2)\right](s + V') &= f_{v_1+v_2}(s + V') \\
&= \Phi((v_1 + v_2)s) \\
&= \Phi(v_1 s) + \Phi(v_2 s) \\
&= f_{v_1}(s + V') + f_{v_2}(s + V') \\
&= (f_{v_1} + f_{v_2})(s + V') \\
&= \left[f(v_1) + f(v_2)\right](s + V').
\end{aligned}$$

This shows that f is a Z_2-linear map. Observe that f is a monomorphism. In fact, if $v \in \operatorname{Ker} f$ and I is the principal ideal in $S\langle X\rangle$ generated by v, then $\Phi(I) = 0$ and therefore $I = 0$ by Lemma 4 (b). Hence $v = 0$ and f is a monomorphism.

Then by Proposition 5 (b) we have

$$\dim V \leqslant \dim (S\langle X\rangle/V')^* = \dim (S\langle X\rangle/V').$$

To prove the opposite inequality, for any $s \in S\langle X\rangle$ we consider the linear map

$$g_s : V \longrightarrow Z_2$$

defined by $g_s(v) = \Phi(sv)$ for $v \in V$. Similarly as in the case of the maps f_v we check that

$$g_{s_1+s_2} = g_{s_1} + g_{s_2}$$

for any s_1, s_2 in $S\langle X\rangle$. Hence we may define a linear map

$$g : S\langle X\rangle \longrightarrow V^*$$

by the formula $g(s) = g_s$ for $s \in S\langle X\rangle$. It is clear that the kernel of g is equal to the subspace V'. Hence, by Proposition 5 (b) we obtain

$$\dim (S\langle X\rangle/V') = \dim \operatorname{Im} g \leqslant \dim V^* = \dim V$$

which completes the proof of the statement (a).

(b) It is clear that $V \subset (V')'$. By the statement (a) we have

$$\begin{aligned} \dim (V')' &= 2^n - \dim V' \\ &= 2^n - (2^n - \dim V) \\ &= \dim V. \end{aligned}$$

Hence $V = (V')'$ by Proposition 5 (d).

We omit the simple proof of the statement (c).

(d) Since $V \cap W \subset V, W$ then $V', W' \subset (V \cap W)'$ and therefore $V' + W' \subset (V \cap W)'$. Since

$$\begin{aligned} \dim (V \cap W)' &= 2^n - \dim (V \cap W) \\ &= 2^n - [\dim V + \dim W - \dim (V + W)] \\ &= (2^n - \dim V) + (2^n - \dim W) - (2^n - \dim (V + W)) \\ &= \dim V' + \dim W' - \dim (V + W)' \\ &= \dim V' + \dim W' - \dim (V' \cap W') \\ &= \dim (V' + W') \end{aligned}$$

then $V' + W' = (V \cap W)'$ by Proposition 5 (d).
This completes the proof of the theorem.

Let T be a non-empty subset of $S\langle X\rangle$. Then $\operatorname{Ann} T$ (or $\operatorname{Ann}_X T$, if it is necessary to mark the set X) denotes the set

$$\{s \in S\langle X\rangle : st = 0 \quad \text{for all} \quad t \in T\}$$

and it is called the annihilator of T. It is clear that $\operatorname{Ann} T$ is an ideal of $S\langle X\rangle$. Moreover

$$\operatorname{Ann} T = \operatorname{Ann}(T),$$

where (T) denotes the ideal generated by T in $S\langle X\rangle$. For a finite set $\{t_1,\dots,t_n\}$ we write $(t_1,\dots,t_n)$ instead of $(\{t_1,\dots,t_n\})$.

L e m m a 7. If I is an ideal, then $\operatorname{Ann} I = I'$.

P r o o f. If $s \in \operatorname{Ann} I$, then of course $sI = 0$ and $\Phi(sI) = 0$. Hence $s \in I'$. Conversely, if $s \in I'$, then $\Phi(sI) = 0$. Since $s \cdot I$ is an ideal in $S\langle X\rangle$, we have $s \cdot I = 0$ by Lemma 4 (b). Hence $s \in \operatorname{Ann} I$, and the lemma is proved.

As a simple consequence of the above lemma and Theorem 6 we obtain the following.

T h e o r e m 8. Let I and J be ideals of $S\langle X\rangle$. Then

(a) $\dim I + \dim \operatorname{Ann} I = 2^n$

(b) $I = \operatorname{Ann}(\operatorname{Ann} I)$

(c) $\operatorname{Ann} I \cap \operatorname{Ann} J = \operatorname{Ann}(I + J)$

(d) $\operatorname{Ann} I + \operatorname{Ann} J = \operatorname{Ann}(I \cap J)$.

R e m a r k. The above theorem shows that $S\langle X\rangle$ (X - finite) is a Frobenius algebra (see [4], § 61).

2. In this section we extend a part of the previous results to the general case. Henceforth we drop the assumption that the set X is finite.

If Y is a subset of X then $S\langle Y\rangle$ may be considered as a subring of $S\langle X\rangle$. It is obvious that for any finite sub set T of $S\langle X\rangle$ there exists a finite subset Y of X such that $T \subset S\langle Y\rangle$. Hence we obtain.

L e m m a 9. The ring $S\langle X\rangle$ is the directed union of all subrings $S\langle Y\rangle$, where Y is a finite subset of X.

L e m m a 10. Let X be a finite set and $X=Y\cup\{x_1,\dots,x_k\}$, $x_i\notin Y$ $(i=1,2,\dots,k)$. If I is an ideal in $S\langle Y\rangle$ then

$$\dim I\, S\langle X\rangle = 2^k\cdot\dim I\,.$$

P r o o f. It is sufficient to prove the lemma for $k=1$. In such a case, if $s_1,\dots,s_d$ are elements of a basis of I, then it is easy to see that the elements

$$s_1,\dots,s_d,s_1\langle x_1\rangle,\dots,s_d\langle x_1\rangle$$

form a basis of $I\,S\langle X\rangle$, and the lemma is proved.

P r o p o s i t i o n 11. Let I be an ideal in $S\langle X\rangle$ generated by a finite set of elements $s_1,\dots,s_d$. Let Y be a finite subset of X such that $s_1,\dots,s_d$ belong to $S\langle Y\rangle$ and let J denotes the ideal generated by $s_1,\dots,s_d$ in $S\langle Y\rangle$. Then

$$\mathrm{Ann}_X\, I = (\mathrm{Ann}_Y\, J)\; S\langle X\rangle.$$

P r o o f. At first we prove the proposition assuming that X is a finite set.
If $X=Y\cup\{x_1,\dots,x_k\}$, $x_i\notin Y$, and Y has n elements, then

$$\begin{aligned}\dim\,(\mathrm{Ann}_Y\, J)\; S\langle X\rangle &= 2^k\dim\mathrm{Ann}_Y\, J\\ &= 2^k(2^n-\dim J)\\ &= 2^{n+k}-\dim I\\ &= \dim\mathrm{Ann}_X\, I,\end{aligned}$$

where the first and third equalities follow from Lemma 10 and two remaining equalities follow from Theorem 8 (a). Hence the statement follows by Proposition 5 (d) since $(\mathrm{Ann}_Y\, J)\; S\langle X\rangle \subset \mathrm{Ann}_X\, I$.

In the general case we have

$$\mathrm{Ann}_X\, I = \bigcup \mathrm{Ann}_Z\{s_1,\ldots,s_d\}$$
$$= \bigcup (\mathrm{Ann}_Y\, J)\, S\langle Z\rangle$$
$$= (\mathrm{Ann}_Y\, J)(\bigcup S\langle Z\rangle)$$
$$= (\mathrm{Ann}_Y\, J)\, S\langle X\rangle,$$

where all sums run over all finite subsets Z of X such that $Y\subset Z$. Hence the proof is completed.

T h e o r e m 2. If I and J are finitely generated ideals in $S\langle X\rangle$, then the following statements hold:

(a) $\mathrm{Ann}\, I$ is finitely generated ideal,

(b) $I = \mathrm{Ann}(\mathrm{Ann}\, I)$,

(c) $\mathrm{Ann}\, I \cap \mathrm{Ann}\, J = \mathrm{Ann}(I + J)$,

(d) $\mathrm{Ann}\, I + \mathrm{Ann}\, J = \mathrm{Ann}(I \cap J)$.

P r o o f. (a) follows immediately from Proposition 11. (b) If $s \in \mathrm{Ann}(\mathrm{Ann}\, I)$, $s_1,\ldots,s_d$ are generators of I, and Y is a finite subset of X such that $s,s_1,\ldots,s_d \in S\langle Y\rangle$, then $s \in \mathrm{Ann}_Y(\mathrm{Ann}_Y\{s_1,\ldots,s_d\})$. By Theorem 8 (b) the last ideal coincides with the ideal J generated by $s_1,\ldots,s_d$ in $S\langle Y\rangle$. Since $J\subset I$, we have proved that $\mathrm{Ann}(\mathrm{Ann}\, I)\subset I$. The opposite inclusion is obvious. (c) is easy and may be omitted. (d) follows simply from (b) and (c) as is shown below

$$\mathrm{Ann}(I\cap J) = \mathrm{Ann}\left[\mathrm{Ann}(\mathrm{Ann}\, I) \cap \mathrm{Ann}(\mathrm{Ann}\, J)\right]$$
$$= \mathrm{Ann}\left[\mathrm{Ann}(\mathrm{Ann}\, I + \mathrm{Ann}\, J)\right]$$
$$= \mathrm{Ann}\, I + \mathrm{Ann}\, J.$$

R e m a r k. Observe that by the above facts it is easy to show that the ring of structural numbers is a coherent ring (see [2] and [3]).

3. In the final section of this paper we compute the annihilator of the ideal generated by finite number of linearly

independent elements of S_1. Suppose that $t_1,\dots,t_m$ are such elements of S_1. If $t_1' = t_1 + \sum_{i=2}^{m} e_i \cdot t_i$, $e_i \in Z_2$, then it is clear that $t_1', t_2, \dots, t_m$ are linearly independent elements too and

$$t_1 \dots t_n = t_1' t_2 \dots t_m .$$

By repeating this argument we obtain.

L e m m a 13. If elements $t_1,\dots,t_m \in S_1$ are linearly independent and elements $t_1',\dots,t_m' \in S_1$ span the same vector subspace as $t_1,\dots,t_m$ then

$$t_1 \dots t_m = t_1' \dots t_m'.$$

C o r o l l a r y 14. Elements $t_1,\dots,t_m \in S_1$ are linearly independent if and only if $t_1 \dots t_m \neq 0$.

P r o o f. If $t_1,\dots,t_m$ are linearly dependent elements, then it is clear that $t_1 \dots t_m = 0$. Assume that $t_1,\dots,t_m$ are linearly independent. Let $Y = \{y_1,\dots,y_n\}$ be a finite subset of X such that $t_1,\dots,t_m \in S\langle Y\rangle$. Let $t_{m+1},\dots,t_n$ be such elements of $S_1\langle Y\rangle$ that the elements $t_1,\dots,t_n$ form a basis of the vector subspace $S_1\langle Y\rangle$. Since the elements $\langle y_1\rangle,\dots,\langle y_n\rangle$ also form a basis of $S_1\langle Y\rangle$, by Lemma 13

$$t_1 \dots t_n = \langle y_1\rangle \dots \langle y_n\rangle \neq 0.$$

Hence, in particular, we obtain that $t_1 \dots t_m \neq 0$.

C o r o l l a r y 15. If $t_1,\dots,t_m$ are linearly independent elements of $S_1\langle X\rangle$, then the Z_2 - subalgebra A of $S\langle X\rangle$ generated by $t_1,\dots,t_m$ is isomorphic to the ring of structural numbers $S\langle Y\rangle$ for any finite set Y with m elements.

P r o o f. Let $Y = \{y_1,\dots,y_m\}$. Consider the homomorphism

$$f: Z_2[y_1,\dots,y_m] \longrightarrow S\langle X\rangle$$

defined by $f(y_i) = t_i$, $i = 1,\dots,m$. Since $t_i^2 = 0$ the ideal generated by squares y_i^2 is contained in Ker f. Hence f induces an epimorphism

$$\bar{f}: S\langle Y\rangle \longrightarrow A.$$

Since $\bar{f}(\langle y_1 \dots y_m\rangle) = t_1 \dots t_m \neq 0$, we have Ker $f = 0$ by Corollary 3. Hence $\bar{f}$ is an isomorphism and the lemma is proved.

L e m m a 16. Let $X = \{x_w\}_{w\in W}$ and $\{t_w\}_{w\in W}$ be a basis of $S_1\langle X\rangle$ Then there exists the unique automorphism $f: S\langle X\rangle \longrightarrow S\langle X\rangle$ such that $f(\langle x_w\rangle) = t_w$ for $w \in W$.

P r o o f. Similarly as in the proof of Corollary 15 we prove that there exists an endomorphism f of $S\langle X\rangle$ such that $f(\langle x_w\rangle) = t_w$ for all $w \in W$. Since the set $\{t_w\}_{w\in W}$ is a basis of $S\langle X\rangle$, all elements $\langle x_w\rangle$, $w \in W$, belong to Im f. Hence f is an epimorphism. By Corollary 15 it is easy to prove that f is a monomorphism. Hence f is an automorphism.

T h e o r e m 17. If $t_1,\dots,t_m$ are linearly independent elements of $S_1\langle X\rangle$, then

(a) $\mathrm{Ann}(t_1,\dots,t_m) = (t_1 \dots t_m)$,

(b) $\mathrm{Ann}(t_1 \dots t_m) = (t_1,\dots,t_m)$.

P r o o f. (a) By Lemma 16 we may suppose that elements $t_1,\dots,t_m$ belong to X. The inclusion $(t_1 \dots t_m) \subset \mathrm{Ann}(t_1,\dots,t_m)$ is obvious. If $t_1 s = t_2 s = \dots = t_m s = 0$, then as in the proof of Lemma 1 we obtain that $s = t_1 \dots t_m d_{t_1} \dots d_{t_m}(s) \in (t_1 \dots t_m)$. Hence the statement (a) is proved. (b) follows from (a) and Theorem 12 (b).

C o r o l l a r y 18. Suppose that

$$t_1 \dots t_m = t_1' \dots t_n' \neq 0,$$

where $t_i, t_j' \in S_1$. Then $m=n$ and $(t_1,\dots,t_m) = (t_1',\dots,t_n')$.

P r o o f. The corollary follows immediately from Corollary 14 and Theorem 17 (b).

REFERENCES

[1] G. B i r k h o f f, S. M a c L a n e: A survey of modern algebra. New York 1954.

[2] N. B o u r b a k i: Algebre commutative. Chap. 1-2. Act. Sci. Ind. 1290, Paris 1961.

[3] S.U. C h a s e: Direct product of modules. Trans. Amer. Math.Soc. 97 (1960) 457-473.

[4] Ch. W. C u r t i s, I. R e i n e r: Representation theory of finite groups and associative algebras. New York 1962.

[5] D. S i m s o n: 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.