FUNCTIONALLY COMPLETE SEMIRINGS

V. I. Varankina, E. M. Vechtomov

Vyatka State University of Humanities (Russia, Kirov)

mathematic@vshu.kirov.ru

The research was performed within the state task of the RF Ministry of Education and Science, the project 1.1375.2014/K.

Abstract. The article is devoted to describing of the structure of functionally complete semirings and their basic properties.

Keywords: semiring, polynomial function, functional completeness, finite field.

A *semiring* is an algebraic structure $\langle S, +, \cdot \rangle$ with binary operations of addition + and multiplication $\cdot$ such that the following axioms are satisfied: addition is associative and commutative, multiplication is associative and distributive over addition from both sides.

If a semiring S has an additive identity 0, besides it is a multiplicative zero, then S is called a *semiring with zero*.

A set S^S of all functions $S \to S$ is a semiring with respect to pointwise addition and multiplication of functions: $(f+g)(a)=f(a)+g(a)$ and $(fg)(a)=f(a)g(a)$ for all $f, g \in S^S$, $a \in S$. We identify every element $a \in S$ with the corresponding constant function. We regard the variable x that takes values in S as the identity map $y=x$.

By $S^*[x]$ denote the subsemiring generated by all constants $a \in S$ and the function x, i.e., by the set $S \cup \{x\}$. Note that for a ring S we have obtained the new ring $S^*[x]$.

A *monomial* in a semiring $S^*[x]$ is a product of an element from S and several copies of variable x with an arbitrary order of the multipliers. All these multipliers are considered as elements from the semiring S^S. Every function $f \in S^*[x]$ is a sum of several monomials and may be a constant term $a_0 \in S$. For a

commutative semiring S every function f from the semiring $S^*[x]$ has the following representation:

$$f=f(x)=a_0+a_1x+n_1x+a_2x^2+n_2x^2+\ldots+a_mx^m+n_mx^m,$$

where $m\in\mathbf{N}$, $a_i\in S\cup\{0\}$ and $n_i\in\mathbf{N}_0$ for each $i=0, 1, \ldots, m$. Note that if S does not have 0 then the coefficients can not equal 0 simultaneously. If S is a commutative semiring with 1, then $f=a_0+a_1x+a_2x^2+\ldots+a_mx^m$.

Similarly, by $S^*[x_1, \ldots, x_n]$ denote the subsemiring in a ring S^{S^n} of all functions $S^n\to S$ that is generated by the set $S\cup\{x_1, \ldots, x_n\}$. Here, each element $a\in S$ is identified with the constant $S^n\to\{a\}$; and independent variables $x_1, \ldots, x_n$ are considered as i-th projections. It means that $x_i(a_1, \ldots, a_n)=a_i$ for every $a_1, \ldots, a_n\in S$, where $i=1,\ldots, n$.

A function from a semiring $S^*[x_1,\ldots, x_n]$ is called a *polynomial function* of n variables $x_1,\ldots, x_n$.

A semiring S is called *functionally complete* if $S^S=S^*[x]$.

We write a polynomial function $f\in S^*[x]$ as $f(x)=a_0+g(x)$, where $a_0\in S$ and the polynomial function $g(x)\in S^*[x]$ does not have a constant term. If f does not have a constant term, then $f(x)=g(x)$.

Theorem 1. *A functionally complete semiring is a finite ring*.

Proof. Let S be an arbitrary functionally complete semiring. Let us split the proof into 3 steps and prove consistently the following:

(I) S is finite.

(II) S is a semiring with 0.

(III) S is a ring.

The statement (I) is obvious. Indeed, if a semiring S is infinite then $|S|^{|S|}=2^{|S|}$. But this power of the set is more than $|S|=|S^*[x]|$.

(II) We will prove existence of 0 in S in several stages.

1) Let $J=\{a\in S: a+a=a\}$ be the set of all additive idempotents in the finite semiring S. It is well-known that there exists at least one idempotent in a finite semigroup. Hence, J is not empty. It is clear that J is an ideal of the semiring S. It

is not difficult to verify that on an additive idempotent semiring J there exists the order $\leq$ such that $a \leq b \Leftrightarrow \exists c \in S\ a+c=b$ $(\forall a, b \in J)$. This order coincides with the natural order: $a \leq b \Leftrightarrow a+b=b$. Note that J is an upper lattice with respect to the order. It is easy to see that a polynomial function $g(x) \in S^*[x]$ without a constant term takes additive idempotents to additive idempotents, i.e., $g(J) \subseteq J$. Besides, the function g is isotonic on J, i.e., $a \leq b \Rightarrow g(a) \leq g(b)$ for all $a, b \in J$.

2) *The ideal J consists of a single element* θ. Assume to the contrary that $|J| \geq 2$. Then in the finite upper lattice J there exist elements $a < b$. Now let us take a polynomial function $f \in S^*[x]$ satisfying $f(a)=b$ and $f(b)=a$. We have

$$a_0+g(a)=b,\ a_0+g(b)=a,\ g(a) \leq b,\ g(b) \leq a,\ g(a) < g(b).$$

It follows that $a_1=g(a) < a < b$ in J. Note that if a summand a_0 is absent, then we get the contradiction: $b=g(a) < g(b)=a$. Arguing in the same way for the pair $a_1 < a$, we get an element $a_2 < a_1$ in J. As a result we build an infinite set in the finite set J. This is impossible. Therefore, $J=\{\theta\}$, having

$$\theta+\theta=\theta,\ \theta s=\theta=s\theta \text{ for any } s \in S.$$

3) For an arbitrary polynomial function $g \in S^*[x]$ without a constant term we have $g(\theta+s)=\theta+g(s)$ for any $s \in S$. This follows from the properties of the element 0 which were indicated in the item 2), the property $g(\theta)=\theta$, and the identity $(\theta+s)^n=\theta+s^n$ being true for all $n \in \mathbf{N}$.

4) Finally, let us prove that the element θ is an additive identity, i. e., $\theta+s=s$ for every $s \in S$. Let us take $s \neq \theta$ and consider the element $t=\theta+s$.

At first, let $t=\theta$, i.e., $\theta+s=\theta$. Let us choose $f \in S^*[x]$ such that $f(\theta)=s$. We get $s=a_0+g(\theta)=a_0+\theta$. Hence $\theta=\theta+s=a_0+\theta+\theta=a_0+\theta=s$. Contradiction. If we write f without a_0, then we have $s=\theta$ too.

Now, let $t \neq \theta$. In this case there exists a function $f \in S^*[x]$ satisfying $f(\theta)=\theta$ and $f(s)=f(t)=s$. From 3) we get

$$s=f(t)=a_0+g(\theta+s)=a_0+\theta+g(s)=\theta+a_0+g(s)=\theta+f(s)=\theta+s.$$

If a_0 is absent, then we have $s=\theta+g(s)=\theta+s$ too.

From 2) and 4) we can conclude that S is a semiring with zero $0=\theta$.

(III) Let us show that S is a ring. If a is a nonzero element from S then we take a function $f \in S^S$ such that $f(0)=a$ and $f(a)=0$. We have $f(x)=a_0+g(x)$, $a_0=f(0)=a$, and $a+g(a)=0$. This means that the element a has the additive inverse.

Theorem 1 and a corresponding result from [1] imply the following:

Theorem 2. *A semiring S is functionally complete if and only if S is either an one-element semiring or a two-element ring with zero multiplication, or isomorphic to the complete matrix ring $M_n(\mathbf{F}_q)$ over a finite field $\mathbf{F}_q$.*

References

1. Werner H. Einführung in die allegemeine Algebra. – Mannheim, Wien, Zürich: Bibliographisches Institut, 1978.