Collect. Math. **46**, 1–2 (1995), 83–95

On the Rank of Semimodules over Semirings

U. Hebisch

Inst. f. Math., TU Bergakademie Freiberg, D-09599 Freiberg, Germany

H. J. Weinert

Inst. f. Math., TU Clausthal, D-38678 Clausthal, Germany

Dedicated, with great respect and gratitude, to the memory of Paul Dubreil

Abstract

In this paper we investigate conditions on a semiring S such that there are semimodules over S with bases of different length. This includes and generalizes corresponding results on rings, in particular one due to P. Dubreil.

§ 1. Introduction

It is a basic fact for many areas of mathematics that for every not necessarily commutative field K each K-module is free and has a unique rank. However, considering free R-modules $({}_RM, +)$ over an arbitrary ring R with identity, the number of elements in a basis of $({}_RM, +)$ may be unique or not, depending on further properties of R. The first results concerning this question are due to J. Dieudonné, P. Dubreil, and C. J. Everett (cf. [3] – [6]), and we also refer to the comprehensive paper [2] by P. M. Cohn and to further references given there.

In this paper we investigate the same problem for semirings and free semimodules over semirings (cf. § 2), which have become more and more important in different branches of theoretical computer science (cf. [7]). Because of the lack of tools available for rings, we mostly have to use other methods in our context.

Moreover, since each free S-semimodule over a ring S is a free S-module, all our statements contain corresponding ring-theoretical results. In some cases, also the latter are new (cf. Thms. 4.5, 4.7, 4.8 and Remark 5.2). In particular, in Thm. 5.3 we generalize a criterion for the uniqueness of the rank of free R-modules given by J. Dieudonné and P. Dubreil to free S-semimodules.

§ 2. Semimodules over semirings

Let $S = (S, +, \cdot)$ be a semiring, which means in general that $(S, +)$ and $(S, \cdot)$ are arbitrary semigroups, connected by the usual distributive laws $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$ for all $a, b, c \in S$. Here we only consider semirings for which $(S, +)$ is commutative and has a neutral element 0, called the *zero* of $(S, +, \cdot)$. Moreover, we also assume that 0 is (multiplicatively) *absorbing,* defined by $0a = a0 = 0$ for all $a \in S$, and that $(S, \cdot)$ has a neutral element 1, called the *identity* of $(S, +, \cdot)$.

DEFINITION 2.1. Let $H = (H, +)$ be a commutative semigroup with a neutral element o and $S = (S, +, \cdot)$ be a semiring as described above. Then $({}_SH, +)$ is called a (*left*) *S-semimodule* iff $ah \in H$ is defined for all $(a, h) \in S \times H$ such that $a(g+h) = ag+ah$, $(a+b)h = ah+bh$, and $(a \cdot b)h = a(bh)$ holds for all $a, b \in S$ and $g, h \in H$. We further assume that $({}_SH, +)$ is *unitary* and 0-*true*, defined by $1h = h$ and $0h = o$ for all $h \in H$, where the latter implies $ao = o$ for all $a \in S$.

For each semiring S and $m, n \in \mathbb{N} = \{1, 2, \ldots\}$ we denote by $M_{m,n}(S)$ the set of all $m \times n$-matrices and by $\mathrm{Mat}(S) = \bigcup_{m,n\in\mathbb{N}} M_{m,n}(S)$ the set of all finite matrices over S. With the usual operations, $(\mathrm{Mat}(S), +, \cdot)$ is a partial (2,2)-algebra, satisfying both associative and the usual distributive laws whenever one side is defined.

DEFINITION 2.2. a) A matrix $A \in M_{m,n}(S)$ is called *right invertible* in $\mathrm{Mat}(S)$ iff there exists $X \in M_{n,m}(S)$ satisfying $AX = E_m$, where E_m denotes the identity matrix in $M_{m,m}(S)$. Dually, A is called *left invertible* iff $YA = E_n$ holds for some $Y \in M_{n,m}(S)$. Clearly, if $A \in M_{m,n}(S)$ is (right and left) *invertible,* then $AB = E_m$ and $BA = E_n$ holds for a unique matrix $B \in \mathrm{Mat}(S)$, called the *inverse* of A.

b) A matrix $A \in M_{m,n}(S)$ is called (multiplicatively) *right cancellable* in $\mathrm{Mat}(S)$ iff

$$(y_1, \ldots, y_m)A = (z_1, \ldots, z_m)A \implies (y_1, \ldots, y_m) = (z_1, \ldots, z_m)$$

holds for all $(y_1, \ldots, y_m)$, $(z_1, \ldots, z_m) \in M_{1,m}(S)$, which is clearly equivalent with $YA = ZA \Longrightarrow Y = Z$ for all $Y, Z \in M_{r,m}(S)$ and each $r \in \mathbb{N}$.

It is obvious that a left invertible matrix $A \in \mathrm{Mat}(S)$ is left cancellable in $\mathrm{Mat}(S)$, and that A is left invertible and right cancellable iff A is invertible in $\mathrm{Mat}(S)$.

DEFINITION 2.3. Let $({}_SH,+)$ be a (in the following always unitary and 0-true) S-semimodule and $\emptyset \neq U \subseteq H$. An element $h \in H$ is called a *linear combination* of U iff it is a formal infinite sum of suitable elements $a_u u$, i. e. $h = \sum^o_{u\in U} a_u u$ for $a_u \in S$ such that $a_u = 0$ for almost all $u \in U$. We call U *weakly linearly independent* iff $o = \sum^o_{u\in U} a_u u$ implies $a_u = 0$ for all $u \in U$, and *strongly linearly independent* iff $\sum^o_{u\in U} a_u u = \sum^o_{u\in U} b_u u$ implies $a_u = b_u$ for all $u \in U$. Further, U is said to be a *generating set* of $({}_SH,+)$ iff $H = \{\sum^o_{u\in U} a_u u \mid a_u \in S\}$ holds, and a *basis* of $({}_SH,+)$ iff U is a strongly linearly independent generating set.

An S-semimodule $({}_SH,+)$ which has a basis U will be called a *free S-semimodule* in the following. (For a characterization of this concept by universal properties, even in a more general setting, we refer to [8], § 3.) If $({}_SH,+)$ has a basis U and $|U|$ is the cardinal number of U, then $({}_SH,+)$ is said to be a *free S-semimodule of rank $|U|$*. Note that a free S-semimodule $({}_SH,+)$ is cancellative or an S-module iff $(S,+,\cdot)$ is additively cancellative or a ring, respectively, and that all our concepts and statements apply directly to the latter case.

Clearly, each semiring $(S,+,\cdot)$ may be considered as an S-semimodule $({}_SS,+)$ with $U = \{1\}$ as a basis, where ah is defined by the multiplication in S. Moreover, for each set I, the direct sum of $|I|$ copies of $({}_SS,+)$ is a free S-semimodule of rank $|I|$.

Proposition 2.4

Let $({}_SH,+)$ be a free S-semimodule with a basis $U = \{u_1,\dots,u_n\}$. To each subset $\{v_1,\dots,v_m\} \subseteq H$ corresponds a matrix $A \in M_{m,n}(S)$ according to $(v_1,\dots,v_m)^T = A(u_1,\dots,u_n)^T$. Then we have

a) $\{v_1,\dots,v_m\}$ is a generating set of $({}_SH,+)$ iff A is left invertible in $\mathrm{Mat}(S)$,

b) $\{v_1,\dots,v_m\}$ is strongly linearly independent iff A is right cancellable in $\mathrm{Mat}(S)$,

c) $\{v_1,\dots,v_m\}$ is a basis of $({}_SH,+)$ iff A is invertible in $\mathrm{Mat}(S)$.

Proof. Obviously, $\{v_1,\dots,v_m\}$ is a generating set iff in $\mathrm{Mat}(S)$ the equation

$$(x_1,\dots,x_m)A = (c_1,\dots,c_n) \tag{2.1}$$

has at least one solution $(x_1,\dots,x_m)$ for each $(c_1,\dots,c_n) \in M_{1,n}(S)$, which in turn holds iff there exists a matrix $X \in M_{n,m}(S)$ satisfying $XA = E_n$. For b), $\{v_1,\dots,v_m\}$ is strongly linearly independent iff (2.1) has at most one solution $(x_1,\dots,x_m)$ for each $(c_1,\dots,c_n) \in M_{1,n}(S)$, i. e. iff A is right cancellable in $\mathrm{Mat}(S)$. From a) and b) one obtains c), since each left invertible and right cancellable matrix $A \in \mathrm{Mat}(S)$ is invertible and conversely. □

§ 3. Semirings with the property R(m,n)

DEFINITION 3.1. A semiring S is said to have the property $R(m,n)$ (or to be an (m,n)-*semiring*) for $m,n \in \mathbb{N}$ iff there exists a left S-semimodule $({}_SH,+)$ which has a basis $U=\{u_1,\dots,u_n\}$ and a basis $V=\{v_1,\dots,v_m\}$.

Theorem 3.2

A semiring S satisfies $R(m,n)$ for some $m \neq n$ iff one of the following statements holds:

a) There are matrices $A \in M_{m,n}(S)$ and $B \in M_{n,m}(S)$ such that $AB = E_m$ and $BA = E_n$, in other words, there are elements $a_{i,k}$ and $b_{k,i}$ in S satisfying the equations

$$(3.1)\quad \sum_{k=1}^{n} a_{i,k}b_{k,j} = \delta_{i,j}\ \ (i,j=1,\dots,m), \quad \sum_{i=1}^{m} b_{k,i}a_{i,\ell} = \delta_{k,\ell}\ \ (k,\ell=1,\dots,n).$$

Henceforth we call such a subset $\{a_{i,k}, b_{k,i}\}$ an (m,n)-system of S.

b) The class $\mathfrak{F}_n(S)$ of all free left S-semimodules of rank n coincides with the class $\mathfrak{F}_m(S)$ of all free left S-semimodules of rank m.

c) The statement b) formulated for right S-semimodules instead of left ones.

Proof. From Prop. 2.4 we obtain $R(m,n) \iff$ a), and also a) $\implies$ b), since each basis $\{u_1,\dots,u_n\}$ provides a basis $\{v_1,\dots,v_m\}$ by $(v_1,\dots,v_m)^T = A(u_1,\dots,u_n)^T$. Finally, b) $\implies R(m,n)$ is clear and the left-right-symmetry of a) implies c). □

Corollary 3.3

Let S be a semiring. Then the rank of each free (left or right) S-semimodule is uniquely determined iff each invertible matrix $A \in \mathrm{Mat}(S)$ is a square one. Moreover, if S has this property, the same holds for each subsemiring of S.

Proposition 3.4

Let S be a semiring satisfying $R(m,n)$ for at least one pair $m \neq n$. Then there is a smallest number m_0 such that $R(m_0,k)$ holds for S and for at least one $k > m_0$, and among those k again a smallest one, say n_0. Moreover, all non-trivial pairs $(m',n') \in \mathbb{N}\times\mathbb{N}$ such that S satisfies $R(m',n')$ are given by

$$(3.2)\quad m', n' \geq m_0 \text{ and } m' \equiv n' \text{ modulo } n_0 - m_0.$$

Proof. The relation σ on $\mathbb{N}$ defined by $m' \,\sigma\, n'$ iff $R(m', n')$ holds for S is reflexive, symmetric and by Thm. 3.2 b) transitive, and $R(m', n')$ implies $R(m' + k, n' + k)$ for each $k \in \mathbb{N}$. So σ is a congruence on $(\mathbb{N}, +)$, which yields (3.2) by well known facts. □

In order to obtain semirings satisfying $R(m, n)$ for any pair $m \neq n$ (and in particular those which are not rings), we start with the polynomial semiring $\Gamma[x_{i,k}, y_{k,i}]$ in the $2mn$ non-commutative indeterminates $x_{i,k}$ and $y_{k,i}$ $(i = 1, \ldots, m; k = 1, \ldots, n)$ over a semiring Γ. Denoting by U the free monoid with e as identity over the set $\{x_{i,k}, y_{k,i}\}$, we may describe $\Gamma[x_{i,k}, y_{k,i}]$ as the free Γ-semimodule with the basis U, established with the multiplication

$$(3.3) \quad (\textstyle\sum_{u\in U}^{o} \alpha_u u)(\sum_{v\in U}^{o} \beta_v v) = \sum_{w\in U}^{o}(\sum_{uv=w} \alpha_u \beta_v) w.$$

As usual, we identify each $\alpha \in \Gamma$ with $\alpha e \in \Gamma[x_{i,k}, y_{k,i}]$ such that Γ is a subsemiring of $\Gamma[x_{i,k}, y_{k,i}]$. Let $\eta_{m,n}$ be the congruence on $\Gamma[x_{i,k}, y_{k,i}]$ generated by the pairs

$$(3.4) \quad (\textstyle\sum_{k=1}^{n} x_{i,k} y_{k,j}, \delta_{i,j}),\ (\sum_{i=1}^{m} y_{k,i} x_{i,\ell}, \delta_{k,\ell})$$

according to (3.1). Then the congruence class semiring $T_{m,n} = \Gamma[x_{i,k}, y_{k,i}]/\eta_{m,n}$, consisting of the classes $[f]_{\eta_{m,n}}$ for $f \in \Gamma[x_{i,k}, y_{k,i}]$, is a (m, n)-semiring according to the next theorem. We shall prove it in two steps in the following sections and note that the elegant proof of corresponding statements for rings in [2], § 5 is not applicable to semirings since it depends essentially on the use of differences.

Theorem 3.5

For each semiring Γ and $m \neq n$ let $T_{m,n} = \Gamma[x_{i,k}, y_{k,i}]/\eta_{m,n}$ be the congruence class semiring introduced above. Then $\alpha \equiv \beta\ (\eta_{m,n})$ implies $\alpha = \beta$ for all $\alpha, \beta \in \Gamma$. Hence Γ may be considered as a subsemiring of $T_{m,n}$, which is then generated by Γ and the (m, n)-system consisting of the classes $[x_{i,k}]_{\eta_{m,n}}$ and $[y_{k,i}]_{\eta_{m,n}}$. Moreover, these classes are pairwise distinct and different from the elements of Γ.

Using these results which will be proved later we obtain:

Theorem 3.6

Let S be a semiring which is generated by a subsemiring Γ and an (m, n)-system $\{a_{i,k}, b_{k,i}\}$ such that $\alpha a_{i,k} = a_{i,k}\alpha$ and $\alpha b_{k,i} = b_{k,i}\alpha$ hold for all $\alpha \in \Gamma$ and all elements of $\{a_{i,k}, b_{k,i}\}$. Then there exists a unique homomorphism φ from $(T_{m,n}, +, \cdot) = (\Gamma[x_{i,k}, y_{k,i}]/\eta_{m,n}, +, \cdot)$ onto $(S, +, \cdot)$ which satisfies

$$(3.5) \quad \varphi([x_{i,k}]_{\eta_{m,n}}) = a_{i,k},\ \varphi([y_{k,i}]_{\eta_{m,n}}) = b_{k,i}, \text{ and } \varphi(\alpha) = \alpha \text{ for all } \alpha \in \Gamma.$$

Proof. There is a unique homomorphism ψ of $\Gamma[x_{i,k}, y_{k,i}]$ onto S satisfying $\psi(x_{i,k}) = a_{i,k}, \psi(y_{k,i}) = b_{k,i}$, and $\psi(\alpha) = \alpha$. Due to (3.1), the congruence λ on $\Gamma[x_{i,k}, y_{k,i}]$ corresponding to ψ contains all pairs (3.4), which yields $\eta_{m,n} \subseteq \lambda$. This implies our assertion by well known facts on universal algebras, cf. e. g. [1], Cor. II.3.8. □

DEFINITION 3.7. a) With respect to Thm. 3.6 we call the congruence class semiring $T_{m,n} = \Gamma[x_{i,k}, y_{k,i}]/\eta_{m,n}$ of $\Gamma[x_{i,k}, y_{k,i}]$ the *free (m,n)-semiring over Γ*.

b) Let $\mathbb{N}_0$ be the semiring of non-negative integers and $\mathbb{Z}$ the ring of integers, and denote by $\eta_{m,n}$ and $\varrho_{m,n}$ the congruences on $\mathbb{N}_0[x_{i,k}, y_{k,i}]$ and $\mathbb{Z}[x_{i,k}, y_{k,i}]$ generated by (3.4). Then we call $\mathbb{N}_0[x_{i,k}, y_{k,i}]/\eta_{m,n}$ the *universal (m,n)-semiring* and $\mathbb{Z}[x_{i,k}, y_{k,i}]/\varrho_{m,n}$ the *universal (m,n)-ring.* This is justified by the following statements, which are proved as above.

Theorem 3.8

a) Let S be a semiring with the property $R(m,n)$ for some $m \neq n$ and $\{a_{i,k}, b_{k,i}\} \subseteq S$ an (m,n)-system. Then there is a unique semiring homomorphism φ of $(\mathbb{N}_0[x_{i,k}, y_{k,i}]/\eta_{m,n}, +, \cdot)$ into $(S, +, \cdot)$ which satisfies

$$\varphi([x_{i,k}]_{\eta_{m,n}}) = a_{i,k},\ \varphi([y_{k,i}]_{\eta_{m,n}}) = b_{k,i}, \text{ and } \varphi(1) = 1. \tag{3.6}$$

b) The corresponding statement holds for each ring S with the property $R(m,n)$ for some $m \neq n$ and the ring $\mathbb{Z}[x_{i,k}, y_{k,i}]/\varrho_{m,n}$.

Remark 3.9. Applying Thm. 3.8 a) to $\mathbb{Z}[x_{i,k}, y_{k,i}]/\varrho_{m,n}$ as a semiring S with the (m,n)-system $\{a_{i,k}, b_{k,i}\} = \{[x_{i,k}]_{\varrho_{m,n}}, [y_{k,i}]_{\varrho_{m,n}}\}$, we obtain a homomorphism φ of $\mathbb{N}_0[x_{i,k}, y_{k,i}]/\eta_{m,n}$ into $\mathbb{Z}[x_{i,k}, y_{k,i}]/\varrho_{m,n}$ determined by (3.6). *However, we do not know so far whether this homomorphism is injective, which is the case iff $\mathbb{N}_0[x_{i,k}, y_{k,i}]/\eta_{m,n}$ is additively cancellative.* We prove this replacing $\mathbb{N}_0$ by an additively cancellative semiring Γ for later use: Such a semiring Γ is embeddable into a smallest ring, consisting of all $\alpha - \beta$ for $\alpha, \beta \in \Gamma$, called the *difference ring $D(\Gamma)$* of Γ. Clearly, $R = D(\Gamma)[x_{i,k}, y_{k,i}]$ is the difference ring of $T = \Gamma[x_{i,k}, y_{k,i}]$. Let $\eta_{m,n}$ and $\varrho_{m,n}$ be the congruences on T and R generated by (3.4). Then, obviously, $T/\eta_{m,n}$ can be embedded into $R/\varrho_{m,n}$ iff the trivial inclusion $\eta_{m,n} \subseteq \varrho_{m,n} \cap (T \times T)$ holds with equality. From a result on difference rings of semirings (cf. [7], Satz II.7.1) it follows that this is the case iff $T/\eta_{m,n}$ is additively cancellative. (To illustrate the other case, e. g. the congruences η on $\mathbb{N}_0$ and ϱ on $\mathbb{Z}$ generated by $(2,4) \in \mathbb{N}_0 \times \mathbb{N}_0$ satisfy $\eta \subset \varrho_n(\mathbb{N}_0 \times \mathbb{N}_0)$.) In fact, the above homomorphism φ is injective for $m = 1 < n$ due to Thm. 4.4, but we could not decide this question for $1 < m < n$ (cf. § 5).

§ 4. The case m = 1

From Thm. 3.2 a) we obtain that a semiring S has the property $R(1,n)$ for some $n \geq 2$ iff S contains an $(1,n)$-system $\{a_1,\ldots,a_n,b_1,\ldots,b_n\}$ defined by

(4.1) $\quad a_1b_1+\ldots+a_nb_n=1 \quad$ and $\quad b_ja_i=\delta_{j,i}$.

At first we investigate, for each $n \geq 2$, the free $(1,n)$-semiring $\Gamma[x_i,y_i]/\eta_{1,n}$ over an arbitrary semiring Γ. Let $(\mathfrak{H},\cdot)$ be the semigroup generated by $x_1,\ldots,x_n,y_1,\ldots,y_n$, an absorbing element O and an identity e, subjected to the defining equations

(4.2) $\quad y_ix_i=e, \;\; y_jx_i=O$ for $i \neq j \;\; (i,j=1,\ldots,n)$.

Obviously, each element $u \in U=\mathfrak{H}\setminus\{O\}$ has a unique presentation $u=P(x)Q(y)$, where $P(x)$ is an element of the free monoid generated by $\{x_1,\ldots,x_n\}$ with e as identity, and $Q(y)$ an element of the free monoid over $\{y_1,\ldots,y_n\}$. Let $\Gamma(\mathfrak{H})=(\Gamma(\mathfrak{H}),+,\cdot)$ be the *contracted semigroup semiring of* $\mathfrak{H}$ *over* Γ, which may be described as the free Γ-semimodule $({}_\Gamma H,+)$ with the basis $U=\mathfrak{H}\setminus\{O\}$ and with the multiplication (3.3), where the absorbing element O of $(\mathfrak{H},\cdot)$ is identified with the zero $o=\sum_{u\in U}^{o} 0u$ of $({}_\Gamma H,+)$. We further identify each $\alpha \in \Gamma$ with $\alpha e \in \Gamma(\mathfrak{H})$. Then $(\Gamma,+,\cdot)$ is a subsemiring of $(\Gamma(\mathfrak{H}),+,\cdot)$ with the common identity $1=1e=e$ and $\alpha u=u\alpha$ for all $\alpha \in \Gamma$ and $u \in U$, the latter as a consequence of (3.3). (For this concept and more general ones concerning semialgebras over semirings we refer to [8], and [7], V.2. and V.3.) Now the following statement is obvious:

Lemma 4.1

Let $\Gamma(\mathfrak{H})$ be the contracted semigroup semiring of $\mathfrak{H}$ over Γ. Then the free $(1,n)$-semiring $\Gamma[x_i,y_i]/\eta_{1,n}$ over Γ can be identified with the congruence class semiring $\Gamma(\mathfrak{H})/\eta_n$, where η_n is the smallest congruence on $\Gamma(\mathfrak{H})$ satisfying

(4.3) $\quad x_1y_1+\ldots+x_ny_n \equiv e$.

In the following, $f \equiv g$ always refers to the congruence η_n in $\Gamma(\mathfrak{H})$. Further, for each *monomial element* $\alpha u=\alpha P(x)Q(y) \in \Gamma(\mathfrak{H})$, the number $\ell_x(\alpha u)=\ell_x(P(x))$ of elements x_i occurring in $P(x)$ is called the *x-degree* of αu and $\ell_y(\alpha u)=\ell_y(Q(y))$ its *y-degree*, and $d(\alpha u)=\ell_x(\alpha u)-\ell_y(\alpha u)$ the *degree difference* of αu. In particular, each $f \in \Gamma(\mathfrak{H})$ can be *decomposed with respect to degree differences* according to $f=\sum_{u\in U}^{o}\alpha_u u=\sum_{\delta\in\mathbb{Z}}^{o} f^{(\delta)}$, where each $f^{(\delta)}$ is the formal infinite sum of all $\alpha_u u$ satisfying $d(\alpha_u u)=\delta$.

Lemma 4.2

For all $f,g \in \Gamma(\mathfrak{H})$ decomposed as described above, $f \equiv g$ is equivalent to $f^{(\delta)} \equiv g^{(\delta)}$ for all $\delta \in \mathbb{Z}$.

Proof. Since η_n is generated by (4.3), $f \equiv g$ holds iff there exists a sequence $f = f_0, f_1, \ldots, f_r = g$ in $\Gamma(\mathfrak{H})$ such that for each $\varrho \in \{0, \ldots, r-1\}$ one either has

(4.4) $\quad f_\varrho = s_\varrho t_\varrho + h_\varrho$ and $f_{\varrho+1} = s_\varrho(\sum_{i=1}^n x_i y_i)t_\varrho + h_\varrho$

or $f_\varrho = s_\varrho(\sum_{i=1}^n x_i y_i)t_\varrho + h_\varrho$ and $f_{\varrho+1} = s_\varrho t_\varrho + h_\varrho$ with elements $s_\varrho, t_\varrho, h_\varrho \in \Gamma(\mathfrak{H})$. Due to (4.2), all monomials occurring in $s_\varrho t_\varrho$ and in $s_\varrho(\sum_{i=1}^n x_i y_i)t_\varrho$ have the same degree difference, which yields $f^{(\delta)} \equiv g^{(\delta)}$ for each $\delta \in \mathbb{Z}$ by decomposing all f_ϱ. □

Proposition 4.3

For all $\alpha, \beta \in \Gamma$, from $\alpha \equiv \beta$ in $\Gamma(\mathfrak{H})$ it follows $\alpha = \beta$. Hence Γ may be considered as a subsemiring of $\Gamma(\mathfrak{H})/\eta_n = \Gamma[x_i, y_i]/\eta_{1,n} = T_{1,n}$. Moreover, this semiring satisfies also the other statements of Thm. 3.5 for the case $m = 1$.

Proof. For $\alpha \equiv \beta$ there is a sequence $\alpha = f_0, f_1, \ldots, f_r = \beta$ in $\Gamma(\mathfrak{H})$ as described in the proof above. Adding more steps if necessary, we may further assume that s_ϱ and t_ϱ are monomials for each ϱ, say $s_\varrho = \gamma_\varrho P_\varrho(x)Q'_\varrho(y)$ and $t_\varrho = P'_\varrho(x)Q_\varrho(y)$. However, from (4.2) we get $Q'_\varrho(y)(\sum_{i=1}^n x_i y_i)P'_\varrho(x) = Q'_\varrho(y)P'_\varrho(x)$ iff $Q'_\varrho(y) \neq e$ or $P'_\varrho(x) \neq e$, which yields $f_\varrho = f_{\varrho+1}$. Canceling those superfluous steps, we may replace (4.4) and its converse by

(4.5) $\quad \{f_\varrho, f_{\varrho+1}\} = \{\gamma_\varrho P_\varrho(x)Q_\varrho(y) + h_\varrho,\ \gamma_\varrho P_\varrho(x)(\sum_{i=1}^n x_i y_i)Q_\varrho(y) + h_\varrho\}.$

By Lemma 4.2, $d(\alpha) = 0$ implies $d(\alpha_u u) = \ell_x(\alpha_u u) - \ell_y(\alpha_u u) = 0$ for each monomial $\alpha_u u$ occurring in any f_ϱ, and we denote by $k-1$ the maximal x-degree $\ell_x(\alpha_u u)$ for all these monomials. Now we are ready to prove

(4.6) $\quad y_1^k f_\varrho x_1^k = \alpha$ for each $\varrho \in \{0, \ldots, r\}$,

which implies $\alpha = y_1^k f_\varrho x_1^k = y_1^k \beta x_1^k = \beta$. Since (4.6) clearly holds for $\varrho = 0$, we go on by induction and compare $\alpha = y_1^k f_\varrho x_1^k$ with $y_1^k f_{\varrho+1} x_1^k$ using (4.5). By the choice of k, (4.2) implies $y_1^k \gamma_\varrho P_\varrho(x)Q_\varrho(y)x_1^k = \gamma_\varrho \sigma_\varrho = y_1^k \gamma_\varrho P_\varrho(x)(\sum_{i=1}^n x_i y_i)Q_\varrho(y)x_1^k$ and $y_1^k h_\varrho x_1^k = \tau_\varrho$ for some $\sigma_\varrho, \tau_\varrho \in \Gamma$. So we get from (4.5) that $\alpha = y_1^k f_\varrho x_1^k$ and $y_1^k f_{\varrho+1} x_1^k$ equal $\gamma_\varrho \sigma_\varrho + \tau_\varrho$. Thus we have proved the first assertion of Prop. 4.3. This, Lemma 4.2 and (4.2) yield the statements concerning the classes $[x_i]$ and $[y_i]$ in Thm. 3.5 for the case $m = 1$. □

Theorem 4.4

Let $T_{1,n} = \Gamma[x_i, y_i]/\eta_{1,n} = \Gamma(\mathfrak{H})/\eta_n$ be the free $(1,n)$-semiring over a semiring Γ. Then $T_{1,n}$ is additively cancellative iff the same holds for Γ. If this is the case, by Remark 3.9 there exists an injective homomorphism φ of $T_{1,n}$ into the free $(1,n)$-ring $D(\Gamma)[x_i, y_i]/\varrho_{1,n}$ over the difference ring $D(\Gamma)$ of Γ satisfying $\varphi([x_i]_{\eta_{1,n}}) = [x_i]_{\varrho_{1,n}}, \varphi([y_i]_{\eta_{1,n}}) = [y_i]_{\varrho_{1,n}}$ and $\varphi(\alpha) = \alpha$ for each $\alpha \in \Gamma$.

Proof. Since Γ is a subsemiring of $T_{1,n}$ by Prop. 4.3, it is enough to show that $T_{1,n}$ is additively cancellative if Γ is assumed to be so. We go by contradiction and disprove

(4.7) $\quad h + f \equiv h + g$ and $f \not\equiv g$ for some $h, f, g \in \Gamma(\mathfrak{H})$.

We denote by M the set of all monomials $\xi_u u \neq 0$ occurring in h, f or g. According to Lemma 4.2 we may assume that all these monomials have the same degree difference, say δ. We further use that $y_i f x_j \equiv y_i g x_j$ for all $i, j \in \{1, \ldots, n\}$ implies $f \equiv g$ as a consequence of (4.3). Hence there is at least one pair (i_k, j_k) such that $y_{i_k} f x_{j_k} \not\equiv y_{i_k} g x_{j_k}$ holds, which implies $y_{i_k} h x_{j_k} \not\equiv 0$ by (4.7). We apply this k times where k is the maximum of the degrees $\ell_x(\xi_u u)$ and $\ell_y(\xi_u u)$ for all $\xi_u u \in M$. Then there are $i_k, i_{k-1}, \ldots, i_1$ such that

(4.8) $\quad Q(y)(h + f)P(x) \equiv Q(y)(h + g)P(x)$ and $Q(y) f P(x) \not\equiv Q(y) g P(x)$

holds for $Q(y) = y_{i_1} \ldots y_{i_k}$ and $P(x) = x_{j_k} \ldots x_{j_1}$. Since all $\xi_u u \in M$ have the same degree difference δ, one easily checks that each $Q(y)\xi_u u P(x) \neq 0$ equals either $\xi_u x_{j_\delta} \ldots x_{j_1}$ for $\delta > 0$ or ξ_u for $\delta = 0$ or $\xi_u y_{i_1} \ldots y_{i_{|\delta|}}$ for $\delta < 0$. Hence (4.8) reads as

$$\alpha x_{j_\delta} \ldots x_{j_1} + \beta x_{j_\delta} \ldots x_{j_1} \equiv \alpha x_{j_\delta} \ldots x_{j_1} + \gamma x_{j_\delta} \ldots x_{j_1} \text{ and } \beta x_{j_\delta} \ldots x_{j_1} \not\equiv \gamma x_{j_\delta} \ldots x_{j_1}$$

for $\delta > 0$, which yields $\alpha + \beta \equiv \alpha + \gamma$ and $\beta \not\equiv \gamma$ for some $\alpha, \beta, \gamma \in \Gamma$ by multiplication with $y_{j_1} \ldots y_{j_\delta}$ from the left. The same follows for $\delta \leq 0$. By Prop. 4.3, this yields $\alpha + \beta = \alpha + \gamma$ and $\beta \neq \gamma$, contradicting that $(\Gamma, +)$ was assumed to be cancellative. □

With similar considerations one can prove:

Theorem 4.5

Let $T_{1,n} = \Gamma[x_i, y_i]/\eta_{1,n}$ be the free $(1,n)$-semiring over a semiring Γ. Then each congruence κ on $T_{1,n}$ is either the identical congruence $\iota_{T_{1,n}}$ or satisfies $\kappa \cap (\Gamma \times \Gamma) \neq \iota_\Gamma$. Hence each $(1,n)$-semiring S generated by Γ and an $(1,n)$-system $\{a_i, b_i\}$ such that $\alpha a_i = a_i \alpha$ and $\alpha b_i = b_i \alpha$ hold for all $i \in \{1, \ldots, n\}$ and $\alpha \in \Gamma$ is isomorphic to $T_{1,n}$ and thus also a free $(1,n)$-semiring.

We close this section dealing with further and somewhat curious properties of semirings (and rings) satisfying $R(1,n)$.

Lemma 4.6

Let S be a semiring containing an $(1,n)$-system $\{a_i, b_i\}$. Then $\{b_1, \ldots, b_n\}$ is a basis of S considered as a (left) S-semimodule $({}_S S, +)$, and one has the following three unique presentations for each $s \in S$:

(4.9) $s = \sum_{j=1}^{n} s_j b_j$ *for* $s_j = sa_j$,

(4.10) $s = \sum_{i=1}^{n} a_i t_i$ *for* $t_i = b_i s$,

(4.11) $s = \sum_{i,j=1}^{n} a_i s_{i,j} b_j$ *for* $s_{i,j} = b_i s a_j$.

Proof. From $s1 = sa_1b_1 + \ldots + sa_nb_n$ *we obtain (4.9), where the* s_j *are uniquely determined since* $s = \sum_{j=1}^{n} r_j b_j$ *implies* $sa_j = r_j$. *Hence* $\{b_1, \ldots, b_n\}$ *is a basis of* $({}_S S, +)$. *Dually it follows (4.10) and that* $\{a_1, \ldots, a_n\}$ *is a basis for the right* S*-semimodule* $(S_S, +)$. *Both together imply (4.11).* □

Theorem 4.7

Let S *be a semiring containing an* $(1, n)$*-system. Then* S *is isomorphic to the semiring* $M_{n,n}(S)$ *of all* $n \times n$*-matrices over* S.

Proof. One easily checks that $\varphi : S \to M_{n,n}(S)$ defined by $\varphi(s) = (s_{i,j})$ for the $s_{i,j} \in S$ determined in (4.11) is such an isomorphism. □

From $S \cong M_{n,n}(S) \supset \{sE_n \mid s \in S\} = S_1 \cong S$ it follows that each $(1, n)$-semiring S contains an infinite chain $S \supset S_1 \supset S_2 \ldots$ of subsemirings isomorphic to S, all with the same identity 1. In particular, an $(1, n)$-system $\{a_i, b_i\}$ of S yields an $(1, n)$-system $\{c_i, d_i\}$ of S_1 by $c_i = \sum_{\nu=1}^{n} a_\nu a_i b_\nu$ and $d_i = \sum_{\mu=1}^{n} a_\mu b_i b_\mu$. As a contrast we note, that there are also various infinite chains $S \supset S_1' \supset S_2' \ldots$ of subsemirings isomorphic to S with different identities as e. g. $1, a_1b_1, a_1a_2b_2b_1, \ldots$ This follows since $s \mapsto a_i s b_i$ defines an injective endomorphism of S for each $i = 1, \ldots, n$. Note also that an $(1, n)$-semiring S satisfies $R(1, k)$ for $k = n + (n-1), n + 2(n-1), \ldots$ In particular, an $(1, 2)$-system generates $(1, k)$-systems for each $k \geq 3$, e. g. $\{a_1, a_2a_1, a_2a_2, b_1, b_1b_2, b_2b_2\}$ for $k = 3$ and $\{a_1a_1, a_1a_2, a_2a_1, a_2a_2, b_1b_1, b_2b_1, b_1b_2, b_2b_2\}$ for $k = 4$. By lack of space we can only announce the following

Theorem 4.8

Let S *be an* $(1, n)$*-semiring which is generated by an* $(1, n)$*-system* $\{a_i, b_i\}$, $(\mathfrak{G}(S), \cdot)$ *the group of all invertible elements* t *of* S *and* $\mathfrak{E}(S)$ *the set of all injective endomorphisms* τ *of* $(S, +, \cdot)$ *satisfying* $\tau(1) = 1$. *Then there is a bijection* $t \mapsto \tau$ *of* $\mathfrak{G}(S)$ *onto* $\mathfrak{E}(S)$ *according to*

(4.12) $a_i \mapsto \tau(a_i) = ta_i = c_i,\ b_i \mapsto \tau(b_i) = b_i t^{-1} = d_i\ (i = 1, \ldots, n)$ *and*

(4.13) $t = c_1b_1 + \ldots + c_nb_n,\ t^{-1} = a_1d_1 + \ldots + a_nd_n$,

which yields also a bijection of $\mathfrak{G}(S)$ *onto the set of all* $(1, n)$*-systems* $\{c_i, d_i\}$ *contained in* S. *Moreover,* $(\mathfrak{E}(S), \cdot)$ *is a group isomorphic to* $(\mathfrak{G}(S), \cdot)$, *and the semigroup* $(S, \cdot)$ *contains isomorphic copies of each symmetric group* $\mathfrak{S}_k, k \in \mathbb{N}$, *and hence of each finite group.*

§ 5. The case m > 1

As a contrast to the situation with $(1,n)$-semirings (cf. Thm. 4.5), for $1 < m < n$ the free (m,n)-semiring $T_{m,n} = \Gamma[x_{i,k}, y_{i,k}]/\eta_{m,n}$ over Γ has congruences $\kappa \neq \iota_{T_{m,n}}$ satisfying $\kappa \cap (\Gamma \times \Gamma) = \iota_\Gamma$, and there are also (m,n)-semirings S generated by Γ and an (m,n)-system which are not free. To show this as well as Thm. 3.5, we use the free $(1,p)$-semiring $T_{1,p}$ over Γ for $p = n - m + 1$, which is generated by its subsemiring Γ and an $(1,p)$-system $\{a_i, b_i\}$ according to Thm. 4.5. There is a unique homomorphism ψ_1 of the polynomial semiring $\Gamma[x_{i,k}, y_{k,i}]$ onto $T_{1,p}$ which satisfies $\psi_1(\alpha) = \alpha$ for all $\alpha \in \Gamma$ and maps the indeterminates $x_{i,k}, y_{k,i}$ in such a way that the matrices $X = (x_{i,k})$ and $Y = (y_{k,i})$ are mapped according to

$$(5.1)\quad X \mapsto A = \begin{pmatrix} a_1 & \dots & a_p & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & & 0 \\ \vdots & & \vdots & & \ddots & \\ 0 & \dots & 0 & 0 & & 1 \end{pmatrix} \qquad Y \mapsto B = \begin{pmatrix} b_1 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ b_p & 0 & \dots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}.$$

From $AB = E_n$ and $BA = E_m$ it follows that $\eta_{m,n} \subseteq \lambda_1$ holds for the congruence λ_1 on $\Gamma[x_{i,k}, y_{k,i}]$ corresponding to ψ_1. As in the proof of Thm. 3.6, we obtain a unique homomorphism φ_1 of $T_{m,n} = \Gamma[x_{i,k}, y_{k,i}]/\eta_{m,n}$ onto $T_{1,p}$ which satisfies $\varphi_1([\alpha]_{\eta_{m,n}}) = \alpha$ for each $\alpha \in \Gamma$ and maps the classes $[x_{i,k}]_{\eta_{m,n}}$ and $[y_{k,i}]_{\eta_{m,n}}$ onto the elements $0, 1, a_1, \dots, a_p, b_1, \dots, b_p \in T_{1,p}$ according to (5.1).

Proposition 5.1

Let $T_{m,n} = \Gamma[x_{i,k}, y_{k,i}]/\eta_{m,n}$ be the free (m,n)-semiring over Γ. Then $\alpha \equiv \beta\ (\eta_{m,n})$ in $\Gamma[x_{i,k}, y_{k,i}]$ implies $\alpha = \beta$ for all $\alpha, \beta \in \Gamma$. Hence Γ may be considered as a subsemiring of $T_{m,n}$. Moreover, this semiring satisfies also the other statements of Thm. 3.5, and is obviously not commutative.

Proof. The first assertion follows immediately from $\psi_1(\alpha) \neq \psi_1(\beta)$ for all $\alpha \neq \beta$ of Γ. Moreover, due to (5.1) and to the validity of Thm. 3.5 for $m = 1$, the classes $[x_{1,1}]_{\eta_{m,n}}, \dots, [x_{1,p}]_{\eta_{m,n}}, [y_{1,1}]_{\eta_{m,n}}, \dots, [y_{p,1}]_{\eta_{m,n}}$ are pairwise distinct and different from all other classes $[x_{i,k}]_{\eta_{m,n}}$ and $[y_{k,i}]_{\eta_{m,n}}$ and all elements of Γ. However, the matrix A in (5.1) can be changed in such a way, that any p elements of any line are used for the entries $a_1, \dots, a_p$, and the matrix B can be chosen correspondingly such that $AB = E_n$ and $BA = E_m$ are satisfied. In this way we obtain homomorphisms ψ_ν of $\Gamma[x_{i,k}, y_{k,i}]$ onto $T_{1,p}$, and the resulting homomorphisms φ_ν of $T_{m,n}$ onto $T_{1,p}$ imply that all classes $[x_{i,k}]_{\eta_{m,n}}$ and $[y_{k,i}]_{\eta_{m,n}}$ are pairwise distinct and different from all elements of Γ. □

Remark 5.2. *The congruences κ_ν on the free (m,n)-semiring $T_{m,n}$ which correspond to the homomorphisms φ_ν of $T_{m,n}$ onto $T_{1,p}$ considered in the above proof are maximal with respect to the property $\kappa_\nu \cap (\Gamma \times \Gamma) = \iota_\Gamma$* (in fact there are $m! \binom{n}{p}$ homomorphisms of this kind). Moreover, *there are also various other congruences on $T_{m,n}$,* since also each $(m-q, n-q)$-system $\{a_{i,k}, b_{k,i}\}$ for $1 \leq q < m$ can be used to obtain matrices satisfying $AB = E_n$ and $BA = E_m$ as in (5.1). Finally, according to (5.1), *the $(1,p)$-system $\{a_i, b_i\}$ of $T_{1,p}$ yields various (m,n)-systems in $T_{1,p}$ consisting of $\{a_i, b_i\}$ and suitable elements equal to* 0 *and* 1.

We have the conjecture that, according to Thm. 4.4, also *each free (m,n)-semiring $T_{m,n} = \Gamma[x_{i,k}, y_{k,i}]/\eta_{m,n}$ is additively cancellative iff Γ has this property.* However, we can only prove that $T_{m,n}$ is additively cancellative if we assume that the classes $[x_{i,k}]_{\eta_{m,n}}$ and $[y_{k,i}]_{\eta_{m,n}}$ are multiplicatively left (or right) cancellable in $T_{m,n}$.

Finally, we generalize one of the early results by J. Dieudonné and P. Dubreil (cf. [3] and [4]) on rings and fields, both commutative or not, to semirings and semifields. We recall that a semiring K with an absorbing zero 0 is called a *semifield* iff $(K \setminus \{0\}, \cdot)$ is a group, and we use the following statements: Each semifield K has no zero divisors, and K is either zero sum free, i. e. $s + t = 0$ implies $s = t = 0$ for all $s, t \in K$, or a field (cf. [7], § I.5, also for a more general concept of a semifield).

Theorem 5.3

Let S be a semiring which is embeddable into any semifield K. Then each free S-semimodule $({}_S H, +)$ has a unique rank.

Proof. By Cor. 3.3, it is enough to show the assertion for each free K-semimodule $({}_K H, +)$. We go by contradiction and assume that K satisfies $R(m,n)$ for some $m < n$. Then K contains an (m,n)-system $\{a_{i,k}, b_{k,i}\}$. This is impossible for $m = 1$, since each $(1,n)$-system contains zero divisors. But for $1 < m < n$, the semifield K is not zero sum free by (3.1), and hence a field. Since each K-module $({}_K H, +)$ over a field has a unique rank, K can also not contain such an (m,n)-system. □

References

1. P. M. Cohn, *Universal Algebra*, Harper & Row, New York 1965.
2. P. M. Cohn, Some remarks on the invariant basis property, *Topology* **5** (1966), 215 – 228.
3. J. Dieudonné, Sur le nombre de dimensions d'un module, *Comptes Rendus Acad. Sci. Paris* **215** (1942), 563 – 565.
4. P. Dubreil, Sur le problemes d'immersion et la théorie des modules, *Comptes Rendus Acad. Sci. Paris* **216** (1943), 625 – 627.
5. P. Dubreil, L'indépendance linéaire dans un module sur un anneau non nécessairement commutatif, *Bull. Sci. Math.* (2) **67** (1943), 84 – 100.
6. C. J. Everett, Vector spaces over rings, *Bull. Amer. Math. Soc.* **48** (1942), 312 – 316.
7. U. Hebisch and H. J. Weinert, *Halbringe - Algebraische Theorie und Anwendungen in der Informatik*, Teubner, Stuttgart 1993.
8. H. J. Weinert, Generalized semialgebras over semirings, *Lecture Notes Math.* **1320** (1988), 380 – 416.