Linear Algebra and its Applications 443 (2014) 139–152

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Bases in semimodules over commutative semirings

Yi-Jia Tan [1]

Department of Mathematics, Fuzhou University, Fuzhou, 350108, China

ARTICLE INFO

Article history:
Received 6 July 2013
Accepted 18 November 2013
Available online 5 December 2013
Submitted by R. Brualdi

MSC:
15A03
16Y60

Keywords:
Semiring
Semimodule
Free semimodule
Basis
Free basis
Cardinality

ABSTRACT

In this paper, the bases of a semimodule over a commutative semiring R are investigated. Some properties and characterizations of the bases are discussed and some equivalent conditions for a basis to be a free basis in a finitely generated free semimodule over R are given. The different possible cardinalities for a basis in a finitely generated free semimodule over R are considered and some equivalent descriptions are obtained for a commutative semiring R satisfying the property that any two bases for a finitely generated free R-semimodule have the same cardinality. Partial results obtained in the paper develop and generalize the corresponding results for commutative join-semirings and for commutative zerosumfree semirings.

1. Introduction

The study of semimodules over semirings has a long history. In 1966, Yusuf [25] introduced the concept of inverse semimodule over a semiring and obtained some analogues to theorems in module theory for inverse semimodules (note that an inverse semimodule M is a semimodule in which the monoid $(M,+)$ is an inverse semigroup). Since then, a number of works on semimodule theory were published (see e.g. [2–4,10,11,18,23,24,26]). In 1999, Golan described semirings and semimodules over semirings in his work [12] comprehensively. Semimodules over semirings appear in many areas of mathematics and are useful in the area of theoretical computer science as well as in the cryptography (see e.g. [13]). In 2007, Di Nola et al. [7] used the notions of semiring and semimodule

E-mail address: yjtan62@126.com.

[1] Supported by the Natural Science Foundation of Fujian Province (2012J01008), China.

0024-3795/$ – see front matter
http://dx.doi.org/10.1016/j.laa.2013.11.024

to introduce the notion of semilinear space in the MV-algebraic setting and obtained some similar results as those of classical linear algebras. But some facts known about bases in linear spaces have not yet been proved in semimodules, one of them is whether each basis has the same cardinality. This question has a positive answer in max-plus algebra (see [6]). In [27], Zhao and Wang investigated the cardinality of a basis in semilinear spaces of n-dimensional vectors over join-semirings and give an answer to the above question in this case. And in [16], Shu and Wang discussed the cardinality of a basis in semilinear space of n-dimensional vectors over a zerosumfree semiring and gave some necessary and sufficient conditions that each basis has the same cardinality. Recently, Shu and Wang [17] investigated the standard orthogonal vectors in semilinear spaces of n-dimensional vectors over commutative zerosumfree semirings.

In the present work, we will investigate the bases for semimodules over a commutative semiring in general. In Section 3, we discuss some basic properties and characterizations of the bases and give some equivalent conditions for a basis to be a free basis in a finitely generated free semimodule over a commutative semiring R. In Section 4, we consider different possible cardinalities for a basis in a finitely generated free semimodule over R and obtain some equivalent descriptions for a commutative semiring R satisfying the property that any two bases for a finitely generated free R-semimodule have the same cardinality. Partial results obtained in this work develop and generalize the corresponding results for commutative join-semirings in [27] and for commutative zerosumfree semirings in [16].

2. Definitions and preliminaries

In this section, we will give some definitions and preliminary lemmas. For convenience, we use $\mathbb{N}$ to denote the set of all positive integers and use $\underline{n}$ to denote the set $\{1, 2, \ldots, n\}$ for $n \in \mathbb{N}$. Also, we use $|S|$ to denote the cardinality for any set S.

Definition 2.1. (See [12].) A *semiring* is an algebraic system $(R, +, \cdot)$ in which $(R, +)$ is an Abelian monoid with identity element 0 and $(R, \cdot)$ is another monoid with identity element 1, connected by ring-like distributivity. Also, $0r = r0 = 0$ for all r in R and $0 \neq 1$. The elements 0 and 1 are called the *zero element* and the *identity element* of R, respectively.

A semiring R is called *commutative* if $ab = ba$ for all a, b in R; R is called a *zerosumfree semiring* (see [12,16]) or an *antiring* (see [8,9,19–22]) if $a + b = 0$ implies that $a = b = 0$ for all a, b in R. A semiring R is called a *join-semiring* (see [27]) if R is a partially ordered set such that (i) 0 is the least element; (ii) 1 is the greatest element; and (iii) $a + b = a \vee b$ of a and b in R (i.e., $a + b$ is the least upper bound of a and b in R). It is clear that any join-semiring is zerosumfree.

Semirings are quite abundant, for example, every ring with identity is a semiring which is not zerosumfree; every Boolean algebra, the fuzzy algebra $\mathbb{F} = ([0, 1], \vee, \wedge)$, every bounded distributive lattice are commutative semirings (in fact, all of them are commutative join-semirings). Also, the set $\mathbb{Z}^0$ of nonnegative integers with the usual operations of addition and multiplication of integers is a commutative semiring which is zerosumfree. The same is true for the set $\mathbb{Q}^0$ of all nonnegative rational numbers and for the set $\mathbb{R}^0$ of all nonnegative real numbers. In addition, the max-plus algebra $(\mathbb{R} \cup \{-\infty\}, \max, +)$ and the min-plus algebra $(\mathbb{R} \cup \{+\infty\}, \min, +)$ are commutative semirings which are zerosumfree (see [5,28]).

A nonempty subset I of a semiring R is called a *left ideal* (resp. *right ideal*) of R if $a + b, ra \in I$ (resp. $a + b, ar \in I$) for any $a, b \in I$ and $r \in R$; I is called an *ideal* of R if it is a left ideal and right ideal of R. An ideal (resp. left ideal, right ideal) I of R is called *a maximal ideal* (resp. *maximal left ideal, maximal right ideal*) if $I \neq R$ and $I \subseteq J \subseteq R$ implies $J = I$ or $J = R$ for any ideal (resp. left ideal, right ideal) J of R. For any ideals I and J of R, we define $I + J = \{a + b \mid a \in I,\ b \in J\}$. It is easy to verify that $I + J$ is the minimum ideal of R which contains I and J.

Let R be a semiring. An element a in R is called *invertible* if there exists $b \in R$ such that $ab = ba = 1$. The element b is called an *inverse* of a in R. It is easy to verify that the inverse of a in R is unique. The inverse of a in R is denoted by a^{-1}. Let $U(R)$ denote the set of all invertible elements in R. An element a in R is called *additively invertible* if there exists $b \in R$ such that $a + b = 0$. The element b is called an *additive inverse* of a in R. If a has an additive inverse then such an inverse is unique. The additive inverse of a in R is denoted by $-a$. We use $V(R)$ to denote the set of all additive invertible elements in R. It is clear that $U(R)$ is a subgroup of the monoid $(R, \cdot)$ and $V(R)$ is an ideal of the semiring R.

Definition 2.2. (See [12].) Let R be a semiring. A *left R-semimodule* is a commutative monoid $(M, +)$ with additive identity θ for which we have a function $R \times M \to M$, denoted by $(\lambda, \alpha) \mapsto \lambda\alpha$ and called *scalar multiplication*, which satisfies the following conditions for all λ, μ in R and α, β in M:

(1) $(\lambda\mu)\alpha = \lambda(\mu\alpha)$;
(2) $\lambda(\alpha + \beta) = \lambda\alpha + \lambda\beta$;
(3) $(\lambda + \mu)\alpha = \lambda\alpha + \mu\alpha$;
(4) $1\alpha = \alpha$;
(5) $\lambda\theta = \theta = 0\alpha$.

Right R-semimodules are defined analogously. In this paper, R-semimodules will always mean left R-semimodules. R-semimodules were studied in [14,16,26,27] under the name *R-semilinear spaces*.

Example 2.1. Let R be a semiring and $R^n = \{(a_1, a_2, \ldots, a_n)^T \mid a_i \in R, i \in \underline{n}\}$, where $(a_1, a_2, \ldots, a_n)^T$ is the transpose of $(a_1, a_2, \ldots, a_n)$ and $n \geqslant 1$. Define

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)^T$$

and

$$\lambda x = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n)^T$$

for $x = (x_1, x_2, \ldots, x_n)^T$, $y = (y_1, y_2, \ldots, y_n)^T \in R^n$ and $\lambda \in R$. Then R^n is an R-semimodule. In particular, $R^1 = R$ is an R-semimodule.

Remark 2.1. If a semiring R is a ring then any R-semimodule is an R-module. In particular, if R is a field then any R-semimodule is a linear space over R.

A nonempty subset N of an R-semimodule M is called a *subsemimodule* of M if N is closed under addition and scalar multiplication. It is clear that if $\{N_i \mid i \in \Omega\}$ is a family of subsemimodules of M then $\bigcap_{i\in\Omega} N_i$ is a subsemimodule of M and if N_1 and N_2 are subsemimodules of M then $N_1 + N_2 = \{a + b \mid a \in N_1,\ b \in N_2\}$ is a subsemimodule of M.

Let S be a nonempty subset of an R-semimodule M. Then the intersection of all subsemimodules of M containing S is a subsemimodule of M, called the *subsemimodule generated by S* and denoted by RS. It is easy to verify that

$$RS = \left\{ \sum_{i=1}^{k} \lambda_i\alpha_i \;\middle|\; \lambda_i \in R,\ \alpha_i \in S,\ i \in \underline{k},\ k \in \mathbb{N} \right\}.$$

The expression $\sum_{i=1}^{k} \lambda_i\alpha_i$ is called a *linear combination* of the elements $\alpha_1, \alpha_2, \ldots, \alpha_k$. If $S = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$, then

$$RS = \left\{ \sum_{i=1}^{m} \lambda_i\alpha_i \;\middle|\; \lambda_i \in R,\ \alpha_i \in S,\ i \in \underline{m} \right\}.$$

Especially, if $S = \{\alpha\}$, then we denote RS by $R\alpha$, i.e.,

$$R\alpha = \{\lambda\alpha \mid \lambda \in R\}.$$

If $RS = M$, then S is called a *generating set* for M. An R-semimodule having a finite generating set is called *finitely generated*. The *rank* of an R-semimodule M, denoted by $r(M)$, is the smallest n for which there exists a generating set for M having cardinality n. It is clear that the rank $r(M)$ exists for any finitely generated R-semimodule M.

Definition 2.3. Let M be an R-semimodule. A nonempty subset S of M is called *linearly independent* if $\alpha \notin R(S\backslash\{\alpha\})$ for any α in S. If S is not linearly independent then it is called *linearly dependent*. The set S is called *free* if each element in M can be expressed as a linear combination of elements in S in at most one way. It is clear that any free set is linearly independent.

Example 2.2. Consider the Boolean lattice $\mathbb{B}_2 = \{0, \sigma_1, \sigma_2, 1\}$, where σ_1 and σ_2 are the atoms of $\mathbb{B}_2$, and 0 and 1 are the least element and the greatest element of $\mathbb{B}_2$, respectively. It is easy to see that $(\mathbb{B}_2, +, \cdot)$ is a commutative semiring with the zero element 0 and the identity element 1, where $+ = \vee$ and $\cdot = \wedge$. In the $\mathbb{B}_2$-semimodule $\mathbb{B}_2^3$, the sets $\{\alpha_2, \alpha_4\}$ and $\{\alpha_1, \alpha_3, \alpha_5\}$ are linearly independent and the set $\{e_1, e_2\}$ is free, but the set $\{\alpha_1, \alpha_2\}$ is linearly dependent, where

$$\alpha_1 = (\sigma_1, \sigma_1, \sigma_1)^T, \qquad \alpha_2 = (\sigma_1, 1, \sigma_1)^T, \qquad \alpha_3 = (0, \sigma_1, \sigma_1)^T, \qquad \alpha_4 = (0, 1, \sigma_1)^T,$$
$$\alpha_5 = (0, \sigma_2, 0)^T, \qquad e_1 = (1, 0, 0)^T, \qquad e_2 = (0, 1, 0)^T.$$

Definition 2.4. Let M be an R-semimodule. A linearly independent generating set for M is called a *basis* for M and a free generating set for M is called a *free basis* for M. An R-semimodule having a free basis is called a *free R-semimodule*.

Remark 2.2. Any finitely generated R-semimodule has at least a basis and any free basis is a basis.

Example 2.3. The R-semimodule R^n in Example 2.1 is a finitely generated free R-semimodule and the set $E = \{e_1, e_2, \dots, e_n\}$ is a free basis for R^n, where $e_1 = (1, 0, \dots, 0)^T$, $e_2 = (0, 1, \dots, 0)^T, \dots, e_n = (0, 0, \dots, 1)^T$. It can be seen that $r(R^n) = n$.

Example 2.4. Consider the $\mathbb{B}_2$-semimodule $\mathbb{B}_2^3$ in Example 2.2.

Let $M = \{\theta, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\} \subseteq \mathbb{B}_2^3$, where

$$\theta = (0, 0, 0)^T, \qquad \alpha_1 = (\sigma_1, \sigma_1, \sigma_1)^T, \qquad \alpha_2 = (\sigma_1, 1, \sigma_1)^T,$$
$$\alpha_3 = (0, \sigma_1, \sigma_1)^T, \qquad \alpha_4 = (0, 1, \sigma_1)^T, \qquad \alpha_5 = (0, \sigma_2, 0)^T.$$

Then M is a finitely generated $\mathbb{B}_2$-semimodule and the all bases for M are $T_1 = \{\alpha_1, \alpha_4\}$, $T_2 = \{\alpha_2, \alpha_3\}$, $T_3 = \{\alpha_2, \alpha_4\}$ and $T_4 = \{\alpha_1, \alpha_3, \alpha_5\}$, and $r(M) = 2$. It is easy to verify that each basis for M is not free and M is not a free $\mathbb{B}_2$-semimodule.

Remark 2.3. Example 2.4 shows that two different bases in an R-semimodule may have different cardinality.

Let R be a semiring. We denote by $M_{m\times n}(R)$ the set of all $m \times n$ matrices over R. Especially, we put $M_n(R) = M_{n\times n}(R)$. For $A \in M_{m\times n}(R)$, we denote by a_{ij} or A_{ij} the (i, j)-entry of A.

For any $A, B \in M_{m\times n}(R)$ and $C \in M_{n\times l}(R)$, we define:

$$A + B = (a_{ij} + b_{ij})_{m\times n}; \qquad AC = \left(\sum_{k=1}^{n} a_{ik}c_{kj}\right)_{m\times l}.$$

It is easy to verify that $(M_n(R), +, \cdot)$ is a semiring and the identity element in the semiring $M_n(R)$ is the identity matrix I_n.

For any given $A \in M_{m\times n}(R)$, the *factor rank* of A, denoted by $\rho_s(A)$, is the least positive integer k such that $A = BC$ for some $B \in M_{m\times k}(R)$ and $C \in M_{k\times n}(R)$. A matrix $A \in M_n(R)$ is said to be *invertible* in $M_n(R)$ if $AB = BA = I_n$ for some $B \in M_n(R)$. The matrix B is called an *inverse* of A in

$M_n(R)$. Obviously, if A is invertible in $M_n(R)$ then its inverse is unique. The inverse of A is denoted by A^{-1}.

The following lemmas are used.

Lemma 2.1. *Let R be a commutative semiring. Then for any $a, b \in V(R)$ and $r \in R$, we have $(-a)r = -ar$ and $(-a)(-b) = ab$.*

Proof. First, it is easy to see that $-a \in V(R)$ and $-(-a) = a$ for any $a \in V(R)$. For any $a, b \in V(R)$ and $r \in R$, we have $(-a)r + ar = ((-a) + a)r = 0 \cdot r = 0$ and so $(-a)r = -ar$ and $(-a)(-b) = -a(-b) = -(-ab) = ab$. $\square$

Lemma 2.2. *(See [15].) Let R be a commutative semiring and $A, B \in M_n(R)$. If $AB = I_n$, then $BA = I_n$.* $\square$

Lemma 2.3. *Let R be a commutative semiring satisfying $1 \notin V(R)$ and $1 = u + v$ implies $u \in U(R)$ or $v \in U(R)$ for all $u, v \in R$ and let $A \in M_n(R)$. If $a_{ii} \in U(R)$ for all $i \in \underline{n}$ and $a_{ij} \in V(R)$ for all $i, j \in \underline{n}$ with $i \neq j$, then A is invertible in $M_n(R)$.*

Proof. We shall prove the lemma by induction on n. It is clear if $n = 1$, and we may assume it holds for $n - 1$ $(n - 1 \geqslant 1)$. Suppose that $A = (a_{ij}) \in M_n(R)$ satisfying $a_{ii} \in U(R)$ for all $i \in \underline{n}$ and $a_{ij} \in V(R)$ for all $i, j \in \underline{n}$ with $i \neq j$. Let $P = I_n + \sum_{i=2}^{n}(-a_{i1})a_{11}^{-1}E_{i1}$ and $Q = I_n + \sum_{j=2}^{n}(-a_{1j})a_{11}^{-1}E_{1j}$, where E_{ij} denotes the $n \times n$ matrix all of whose entries are 0 excepts its (i, j)-entry, which is 1. Then P and Q are invertible in $M_n(R)$ since $P(I_n + \sum_{i=2}^{n} a_{i1}a_{11}^{-1}E_{i1}) = (I_n + \sum_{i=2}^{n} a_{i1}a_{11}^{-1}E_{i1})P = I_n$ and $Q(I_n + \sum_{j=2}^{n} a_{1j}a_{11}^{-1}E_{1j}) = (I_n + \sum_{j=2}^{n} a_{1j}a_{11}^{-1}E_{1j})Q = I_n$. Also, we have

$$
\begin{aligned}
PAQ &= \left(I_n + \sum_{i=2}^{n}(-a_{i1})a_{11}^{-1}E_{i1}\right)\left(\sum_{s,t=1}^{n} a_{st}E_{st}\right)\left(I_n + \sum_{j=2}^{n}(-a_{1j})a_{11}^{-1}E_{1j}\right) \\
&= \left(\sum_{s,t=1}^{n} a_{st}E_{st} + \sum_{i=2}^{n}\sum_{t=1}^{n}(-a_{i1})a_{11}^{-1}a_{1t}E_{it}\right)\left(I_n + \sum_{j=2}^{n}(-a_{1j})a_{11}^{-1}E_{1j}\right) \\
&= \sum_{s,t=1}^{n} a_{st}E_{st} + \sum_{i=2}^{n}\sum_{t=1}^{n}(-a_{i1})a_{11}^{-1}a_{1t}E_{it} \\
&\quad + \sum_{s=1}^{n}\sum_{j=2}^{n} a_{s1}(-a_{1j})a_{11}^{-1}E_{sj} + \sum_{i=2}^{n}\sum_{j=2}^{n}(-a_{i1})(-a_{1j})a_{11}^{-1}E_{ij} \\
&= \sum_{i,j=1}^{n} a_{ij}E_{ij} + \sum_{i=2}^{n}\sum_{j=1}^{n}\left(-a_{i1}a_{11}^{-1}a_{1j}\right)E_{ij} \\
&\quad + \sum_{i=1}^{n}\sum_{j=2}^{n}\left(-a_{i1}a_{1j}a_{11}^{-1}\right)E_{ij} + \sum_{i=2}^{n}\sum_{j=2}^{n}\left(a_{i1}a_{1j}a_{11}^{-1}\right)E_{ij} \quad \text{(by Lemma 2.1)} \\
&= \sum_{i,j=1}^{n} a_{ij}E_{ij} + \sum_{i=2}^{n}(-a_{i1})E_{i1} + \sum_{j=2}^{n}(-a_{1j})E_{1j} + \sum_{i=2}^{n}\sum_{j=2}^{n}\left(-a_{i1}a_{1j}a_{11}^{-1}\right)E_{ij} \\
&= a_{11}E_{11} + \sum_{i=2}^{n}\sum_{j=2}^{n}\left(a_{ij} + \left(-a_{i1}a_{1j}a_{11}^{-1}\right)\right)E_{ij}
\end{aligned}
$$

$$= \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} + (-a_{21}a_{12}a_{11}^{-1}) & \cdots & a_{2n} + (-a_{21}a_{1n}a_{11}^{-1}) \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a_{n2} + (-a_{n1}a_{12}a_{11}^{-1}) & \cdots & a_{nn} + (-a_{n1}a_{1n}a_{11}^{-1}) \end{pmatrix}.$$

Put $A_1 = \begin{pmatrix} a_{22}+(-a_{21}a_{12}a_{11}^{-1}) & \cdots & a_{2n}+(-a_{21}a_{1n}a_{11}^{-1}) \\ \cdots & \cdots & \cdots \\ a_{n2}+(-a_{n1}a_{12}a_{11}^{-1}) & \cdots & a_{nn}+(-a_{n1}a_{1n}a_{11}^{-1}) \end{pmatrix}$. For any $i, j \in \{2, 3, \ldots, n\}$, if $i \neq j$, then $a_{ij} + (-a_{i1}a_{1j}a_{11}^{-1}) \in V(R)$ (because $V(R)$ is an ideal of R); if $i = j$, let $a_{ii} + (-a_{i1}a_{1i}a_{11}^{-1}) = r_i$. Then $a_{ii} = a_{i1}a_{1i}a_{11}^{-1} + r_i$ and so $1 = a_{ii}^{-1}a_{i1}a_{1i}a_{11}^{-1} + a_{ii}^{-1}r_i$. This implies that $a_{ii}^{-1}a_{i1}a_{1i}a_{11}^{-1} \in U(R)$ or $a_{ii}^{-1}r_i \in U(R)$. If $a_{ii}^{-1}a_{i1}a_{1i}a_{11}^{-1} \in U(R)$ then $a_{i1} \in U(R)$. Since $a_{i1} \in V(R)$, we have $a_{i1} + (-a_{i1}) = 0$ and so $1 + a_{i1}^{-1}(-a_{i1}) = 0$. This means that $1 \in V(R)$, which is a contradiction. Therefore $a_{ii}^{-1}r_i \in U(R)$ and so $r_i \in U(R)$. By the induction hypothesis, A_1 is invertible in $M_{n-1}(R)$, and so the matrix $\begin{pmatrix} a_{11} & 0 \\ 0 & A_1 \end{pmatrix}$ is invertible in $M_n(R)$ (because a_{11} is invertible). Then $A = P^{-1}\begin{pmatrix} a_{11} & 0 \\ 0 & A_1 \end{pmatrix}Q^{-1}$ is invertible. □

Notation 2.1. A ring R is called *quasilocal* if it has a unique maximal left ideal I. A generating set S for an R-module M is called an *i-basis* for M (see [1]) if for $\alpha_1, \alpha_2, \ldots, \alpha_m$ in S and $\lambda_1, \lambda_2, \ldots, \lambda_m$ in R, $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_m\alpha_m = \theta$ implies each λ_i is a nonunit. It is easy to see that S is an i-basis for M if and only if S is a basis for M. A ring R satisfies the invariant i-basis number property (IiBN) (see [1]) if for each R-module M with an i-basis, any two i-bases for M have the same cardinality.

Lemma 2.4. *Let R be a commutative ring. If R has a unique maximal ideal, then for each R-module M with a basis, any two bases for M have the same cardinality.*

Proof. If R has a unique maximal ideal, then R is quasilocal (note that left ideal and ideal are coincident in a commutative ring). Since a ring is quasilocal if and only if it satisfies IiBN (see Theorem 3.4 in [1]), the ring R satisfies IiBN, i.e., for each R-module M with an i-basis, any two i-bases for M have the same cardinality. Since i-basis and basis are coincident in any R-module, we have that for each R-module M with a basis, any two bases for M have the same cardinality. □

3. Some basic properties and characterizations of bases

In this section, we will discuss some basic properties and characterizations of bases in a semimodule over a commutative semiring R and give some equivalent conditions for a basis to be a free basis in a finitely generated free R-semimodule. Partial results generalize the corresponding results for commutative zerosumfree semirings in [16].

Theorem 3.1. *Let M be an R-semimodule. If M has an infinite basis then every basis for M is infinite.*

Proof. Let S be an infinite basis for M. If M has a finite basis T then each element in T can be expressed as a linear combination of elements in S. For each $\beta \in T$, choose a representation $\beta = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n$, where $\alpha_i \in S$, $\lambda_i \in R$ $(1 \leqslant i \leqslant n)$. Put $\beta(S) = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $T' = \bigcup_{\beta \in T} \beta(S)$. Then $T' \subseteq S$ and T' is finite and so $S \backslash T' \neq \phi$. Clearly, each element in T can be expressed as a linear combination of elements in T'. Since any element in S can be expressed as a linear combination of elements in T, any element in S can be expressed as a linear combination of elements in T'. Then there exists $\alpha \in S \backslash T' \subseteq S$ such that $\alpha \in RT' \subseteq R(S \backslash \{\alpha\})$. This contradicts the definition of S. Therefore every basis for M is infinite. □

Remark 3.1. Theorem 3.1 shows that if an R-semimodule M has a finite basis then any basis for M is finite. Since any finitely generated R-semimodule has at least a finite basis, every basis for a finitely generated R-semimodule is finite.

In the following M is supposed to be a finitely generated R-semimodule.

Let $T=\{\beta_1,\beta_2,\dots,\beta_n\}$ be a generating set for M and $S=\{\alpha_1,\alpha_2,\dots,\alpha_m\}\subseteq M$. Then each element in S is a linear combination of the elements in T, say

$$\begin{cases}\alpha_1=a_{11}\beta_1+a_{21}\beta_2+\cdots+a_{n1}\beta_n,\\ \alpha_2=a_{12}\beta_1+a_{22}\beta_2+\cdots+a_{n2}\beta_n,\\ \quad\cdots\\ \alpha_m=a_{1m}\beta_1+a_{2m}\beta_2+\cdots+a_{nm}\beta_n\end{cases}$$

or

$$(\alpha_1,\alpha_2,\dots,\alpha_m)=(\beta_1,\beta_2,\dots,\beta_n)A,$$

where $A=(a_{ij})\in M_{n\times m}(R)$. If S and T are bases for M, then the matrix A is called a *transition matrix* from the basis T to the basis S.

Remark 3.2. In an R-semimodule, the transition matrix from a basis to another basis need not be unique. For example, consider the bases $T_3=\{\alpha_2,\alpha_4\}$ and $T_4=\{\alpha_1,\alpha_3,\alpha_5\}$ for the $\mathbb{B}_2$-semimodule M in Example 2.4. It is easy to verify that the matrices $A_1=\begin{pmatrix}1&0\\1&1\\1&1\end{pmatrix}$ and $A_2=\begin{pmatrix}\sigma_1&\sigma_2\\\sigma_1&\sigma_1\\\sigma_2&\sigma_2\end{pmatrix}$ are both transition matrices from the basis T_4 to the basis T_3.

Theorem 3.2. *Let M be an R-semimodule with $r(M)=r$ and $S=\{\alpha_1,\alpha_2,\dots,\alpha_m\}$ and $T=\{\beta_1,\beta_2,\dots,\beta_n\}$ be bases for M. Then*

(1) *$\rho_s(A)\geqslant r$ for any transition matrix A from T to S;*
(2) *there exists a transition matrix A from T to S such that $\rho_s(A)=r$.*

Proof. (1) Let $A\in M_{n\times m}(R)$ be any transition matrix A from T to S and $\rho_s(A)=k$. Then $A=BC$ for some $B\in M_{n\times k}(R)$ and $C\in M_{k\times m}(R)$. Let $\gamma_l=\sum_{j=1}^n b_{jl}\beta_j$ for all $l\in\underline{k}$ and $\Gamma=\{\gamma_1,\gamma_2,\dots,\gamma_k\}$. Then $\Gamma\subseteq M$ and $\alpha_i=\sum_{j=1}^n a_{ji}\beta_j=\sum_{j=1}^n(\sum_{l=1}^k b_{jl}c_{li})\beta_j=\sum_{l=1}^k c_{li}(\sum_{j=1}^n b_{jl}\beta_j)=\sum_{l=1}^k c_{li}\gamma_l$ for all $i\in\underline{n}$. Thus $M=RS=R\Gamma$, i.e., Γ is a generating set for M. Then $r=r(M)\leqslant k=\rho_s(A)$. This proves (1).

(2) Since $r(M)=r$, M has a basis Γ with $|\Gamma|=r$. Let $\Gamma=\{\gamma_1,\gamma_2,\dots,\gamma_r\}$ and let $B\in M_{n\times r}(R)$ be a transition matrix from T to Γ and $C\in M_{r\times m}(R)$ a transition matrix from Γ to S, i.e.,

$$(\gamma_1,\gamma_2,\dots,\gamma_r)=(\beta_1,\beta_2,\dots,\beta_n)B$$

and

$$(\alpha_1,\alpha_2,\dots,\alpha_m)=(\gamma_1,\gamma_2,\dots,\gamma_r)C.$$

Then

$$(\alpha_1,\alpha_2,\dots,\alpha_m)=(\beta_1,\beta_2,\dots,\beta_n)BC.$$

Put $A=BC$, we have that A is a transition matrix from T to S and $\rho_s(A)\leqslant r$. Since $\rho_s(A)\geqslant r$ (by (1)), we have $\rho_s(A)=r$. This proves (2). $\square$

Theorem 3.3. *Let M be a finitely generated free R-semimodule. Then for any basis S and any free basis T for M, we have $|T|\leqslant|S|$.*

Proof. By Remark 3.1, S and T are finite. Let $S=\{\alpha_1,\alpha_2,\dots,\alpha_m\}$ and $T=\{\beta_1,\beta_2,\dots,\beta_n\}$, and let

$$(\alpha_1,\alpha_2,\dots,\alpha_m)=(\beta_1,\beta_2,\dots,\beta_n)A$$

and

$$(\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1, \alpha_2, \ldots, \alpha_m)B,$$

where $A \in M_{n\times m}(R)$ and $B \in M_{m\times n}(R)$. Then

$$(\beta_1, \beta_2, \ldots, \beta_n) = (\beta_1, \beta_2, \ldots, \beta_n)AB.$$

Since T is a free basis for M, we have $AB = I_n$. In the following we prove $m \geqslant n$.

Suppose that $m < n$. Let $A_1 = (A, O_1)$ and $B_1 = \binom{B}{O_2}$, where $O_1 \in M_{n\times(n-m)}(R)$ and $O_2 \in M_{(n-m)\times n}(R)$ are zero matrices. Then $A_1, B_1 \in M_n(R)$ and $A_1B_1 = AB = I_n$. By Lemma 2.2, we have $B_1A_1 = I_n$. On the other hand, $B_1A_1 = \binom{B}{O_2}(A, O_1) = \begin{pmatrix} BA & O \\ O & O \end{pmatrix} \neq I_n$ (because $m < n$). This is a contradiction. Therefore $m \geqslant n$, i.e., $|S| \geqslant |T|$. The proof is completed. □

In the following we give some equivalent conditions for a basis to be a free basis in a finitely generated free R-semimodule.

Theorem 3.4. *Let M be a free R-semimodule with $r(M) = r$ and T a free basis for M. Then for any basis S for M, the following statements are equivalent.*

(1) *S is a free basis for M.*
(2) $|S| = r$.
(3) *The transition matrix from T to S is unique and invertible.*

Proof. Since T is a free basis for M, we have $|T| = r(M) = r$ (by Theorem 3.3 and the definition of $r(M)$). Let $T = \{\beta_1, \beta_2, \ldots, \beta_r\}$.

(1) $\Longrightarrow$ (2). It follows from Theorem 3.3 and the definition of $r(M)$.

(2) $\Longrightarrow$ (3). Suppose that $|S| = r$. Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ and A be a transition matrix from T to S and B a transition matrix from S to T, i.e., $(\alpha_1, \alpha_2, \ldots, \alpha_r) = (\beta_1, \beta_2, \ldots, \beta_r)A$ and $(\beta_1, \beta_2, \ldots, \beta_r) = (\alpha_1, \alpha_2, \ldots, \alpha_r)B$. Then $(\beta_1, \beta_2, \ldots, \beta_r) = (\beta_1, \beta_2, \ldots, \beta_r)AB$. This implies that $AB = I_r$ (because T is a free basis for M). By Lemma 2.2, we have $BA = I_r$ and so A is invertible in $M_r(R)$. If A_1 and A_2 are transition matrices from T to S then $(\alpha_1, \alpha_2, \ldots, \alpha_r) = (\beta_1, \beta_2, \ldots, \beta_r)A_1$ and $(\alpha_1, \alpha_2, \ldots, \alpha_r) = (\beta_1, \beta_2, \ldots, \beta_r)A_2$, and so $(\beta_1, \beta_2, \ldots, \beta_r)A_1 = (\beta_1, \beta_2, \ldots, \beta_r)A_2$. Since T is free, $A_1 = A_2$.

(3) $\Longrightarrow$ (1). If the transition matrix A from T to S is invertible, then $|S| = |T| = r$ and $A \in M_r(R)$ and $BA = I_r$ for some $B \in M_r(R)$. Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$. Then $(\alpha_1, \alpha_2, \ldots, \alpha_r) = (\beta_1, \beta_2, \ldots, \beta_r)A$.

For any $\beta \in M$, if $\beta = \sum_{i=1}^r \lambda_i\alpha_i = \sum_{i=1}^r \mu_i\alpha_i$ for some $\lambda_i, \mu_i \in R$, i.e.,

$$\beta = (\alpha_1, \alpha_2, \ldots, \alpha_r)\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_r \end{pmatrix} = (\alpha_1, \alpha_2, \ldots, \alpha_r)\begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_r \end{pmatrix},$$

then

$$(\beta_1, \beta_2, \ldots, \beta_r)A\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_r \end{pmatrix} = (\beta_1, \beta_2, \ldots, \beta_r)A\begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_r \end{pmatrix}.$$

Since $T = \{\beta_1, \beta_2, \ldots, \beta_r\}$ is a free basis for M, we have

$$A\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_r \end{pmatrix} = A\begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_r \end{pmatrix}.$$

This implies

$$BA\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_r\end{pmatrix}=BA\begin{pmatrix}\mu_1\\ \mu_2\\ \vdots\\ \mu_r\end{pmatrix}.$$

But $BA=I_r$, we have

$$\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_r\end{pmatrix}=\begin{pmatrix}\mu_1\\ \mu_2\\ \vdots\\ \mu_r\end{pmatrix},$$

i.e., $\lambda_i=\mu_i$ for all $i\in\underline{r}$. Then S is a free basis for M. $\square$

By Theorem 3.4, we have

Corollary 3.1. *For any finitely generated free R-semimodule M, the following statements are equivalent.*

(1) *All bases for M have the same cardinality.*
(2) *Each basis for M is a free basis.* $\square$

Since R^n is a finitely generated free R-semimodule, by Corollary 3.1, we have

Corollary 3.2. *In the R-semimodule R^n, all bases have the same cardinality if and only if each basis is a free basis.* $\square$

Remark 3.3. Since any zerosumfree semiring is a semiring, Corollary 3.2 generalizes Theorem 3.2 in [16].

4. The cardinalities of bases in a finitely generated free semimodule

In this section, we consider the different possible cardinalities for a basis for a given finitely generated free R-semimodule and characterize the commutative semirings R satisfying the property that any two bases for a finitely generated free R-semimodule have the same cardinality. Partial results in this section generalize the corresponding results for commutative join-semirings in [27].

Lemma 4.1. *If the R-semimodule R has a basis with q elements, then R has a basis with r elements for any $r\in\underline{q}$.*

Proof. Let $U=\{u_1,u_2,\dots,u_q\}$ is a basis for the R-semimodule R. Then $1=\lambda_1u_1+\lambda_2u_2+\cdots+\lambda_qu_q$ for some $\lambda_1,\lambda_2,\dots,\lambda_q\in R$. For any $r\in\underline{q}$, let $v=\lambda_ru_r+\cdots+\lambda_qu_q$. If $r=1$ then $\{v\}=\{1\}$ is a basis for R. If $1<r\leqslant q$, then $1=\lambda_1u_1+\cdots+\lambda_{r-1}u_{r-1}+v$ and so $\{u_1,\dots,u_{r-1},v\}$ is a generating set for R. In the following we prove $\{u_1,\dots,u_{r-1},v\}$ is a basis for R.

It is clear that each u_i, $(1\leqslant i\leqslant r-1)$, cannot be expressed as a linear combination of the elements $u_1,\dots,u_{i-1},u_{i+1},\dots,u_{r-1},v$. If v can be expressed as a linear combination of the elements $u_1,\dots,u_{r-1}$ then $v=k_1u_1+\cdots+k_{r-1}u_{r-1}$ for some $k_1,\dots,k_{r-1}\in R$, and so $1=\lambda_1u_1+\cdots+\lambda_{r-1}u_{r-1}+v=(\lambda_1+k_1)u_1+\cdots+(\lambda_{r-1}+k_{r-1})u_{r-1}$. This means that $\{u_1,\dots,u_{r-1}\}$ is a generating set for R, which contradicts the definition of U. Then v cannot be expressed as a linear combination of the elements $u_1,\dots,u_{r-1}$. Therefore, $\{u_1,\dots,u_{r-1},v\}$ is a basis for R. $\square$

Notation 4.1. For any finitely generated R-semimodule M, let

$$\mu(M)=\{m\in\mathbb{N}\mid \text{there exists a basis } T \text{ for } M \text{ such that } |T|=m\}.$$

Notation 4.2. For any commutative semiring R, let $\kappa(R)=\max\{t\in\mathbb{N}\mid$ the R-semimodule R has a basis with t elements$\}$.

Example 4.1. Consider the commutative semiring $(\mathbb{B}_2,+,\cdot)$ in Example 2.2, where $\mathbb{B}_2=\{0,\sigma_1,\sigma_2,1\}$ is a Boolean lattice, and $+=\vee$ and $\cdot=\wedge$. It is easy to verify that the set $\{\sigma_1,\sigma_2\}$ is a basis of the maximum length for the $\mathbb{B}_2$-semimodule $\mathbb{B}_2$ and so $\kappa(\mathbb{B}_2)=2$.

Example 4.2. Consider the integral ring $(\mathbb{Z},+,\cdot)$, it is a commutative semiring. For every positive integer t with $t\geqslant 2$, let $p_1,p_2,\ldots,p_t$ be t different prime numbers in $\mathbb{Z}$ and let $u_i=\prod_{1\leqslant j\leqslant t,\, j\neq i}p_j$ for $i\in\underline{t}$ and $U=\{u_1,u_2,\ldots,u_t\}$. Then, U is a basis for the $\mathbb{Z}$-semimodule $\mathbb{Z}$. By the arbitrariness of t, we have $\kappa(\mathbb{Z})=+\infty$.

Theorem 4.1. *Let M be a free R-semimodule with $r(M)=n$.*

(1) *If the R-semimodule R has a basis with q elements, then $\{n,n+1,\ldots,qn\}\subseteq\mu(M)$.*
(2) *If $\kappa(R)=+\infty$, then $\mu(M)=\{n,n+1,\ldots\}$.*

Proof. (1) Let $F=\{f_1,f_2,\ldots,f_n\}$ be a free basis for M. Then $M=\sum_{1\leqslant i\leqslant n}Rf_i$. For any $m\in\{n,n+1,\ldots,qn\}$, we choose $m_1,m_2,\ldots,m_n\in\underline{q}$ such that $m=\sum_{1\leqslant i\leqslant n}m_i$. By Lemma 4.1, R has a basis U_i with m_i elements for each $i\in\underline{n}$. Let $U_i=\{u_{i1},u_{i2},\ldots,u_{im_i}\}$ and $S_i=\{u_{i1}f_i,u_{i2}f_i,\ldots,u_{im_i}f_i\}$ for each $i\in\underline{n}$, and let $S=\bigcup_{1\leqslant i\leqslant n}S_i$. In the following we prove the set S is a basis for M.

For any $\alpha\in M$, we have $\alpha=\sum_{1\leqslant i\leqslant n}\alpha_i$ for some $\alpha_i\in Rf_i$ $(1\leqslant i\leqslant n)$ (because $M=\sum_{1\leqslant i\leqslant n}Rf_i$). For each $i\in\underline{n}$, we have $\alpha_i=r_if_i$ for some $r_i\in R$. Since $U_i=\{u_{i1},u_{i2},\ldots,u_{im_i}\}$ is a basis for R, $r_i=\sum_{1\leqslant j\leqslant m_i}\lambda_{ij}u_{ij}$ for some $\lambda_{i1},\lambda_{i2},\ldots,\lambda_{im_i}\in R$, and so $\alpha_i=r_if_i=\sum_{1\leqslant j\leqslant m_i}\lambda_{ij}(u_{ij}f_i)$, i.e., α_i is a linear combination of the elements in S_i for each $i\in\underline{n}$. Therefore, α is a linear combination of the elements in S. This means that S is a generating set for M. If S is not a basis for M, then there exists $\beta\in S=\bigcup_{1\leqslant i\leqslant n}S_i$ such that β is a linear combination of the elements in $S\backslash\{\beta\}$. Since $\beta\in\bigcup_{1\leqslant i\leqslant n}S_i$, we can assume $\beta=u_{ij}f_i$ for some $i\in\underline{n}$ and some $j\in\underline{m_i}$. Then

$$\begin{aligned}
u_{ij}f_i&=\sum_{1\leqslant s\leqslant n,\, s\neq i}\left(\sum_{1\leqslant t\leqslant m_s}k_{st}u_{st}f_s\right)+\sum_{1\leqslant t\leqslant m_i,\, t\neq j}k_{it}u_{it}f_i\\
&=\sum_{1\leqslant s\leqslant n,\, s\neq i}\left(\sum_{1\leqslant t\leqslant m_s}k_{st}u_{st}\right)f_s+\left(\sum_{1\leqslant t\leqslant m_i,\, t\neq j}k_{it}u_{it}\right)f_i,
\end{aligned}$$

where $k_{s1},\ldots,k_{sm_s}$ $(1\leqslant s\leqslant n,\ s\neq i)$, $k_{i1},\ldots,k_{i,j-1},k_{i,j+1},\ldots,k_{im_i}\in R$. Since $\{f_1,f_2,\ldots,f_n\}$ is a free basis for M, we have $u_{ij}=\sum_{1\leqslant t\leqslant m_i,\, t\neq j}k_{it}u_{it}$. This contradicts the definition of U_i. Then, $S=\bigcup_{1\leqslant i\leqslant n}S_i$ is a basis for M. Furthermore, we can prove $S_i\cap S_j=\phi$ for all $i,j\in\underline{n}$ with $i\neq j$. Therefore, $|S|=\sum_{1\leqslant i\leqslant n}|S_i|=\sum_{1\leqslant i\leqslant n}m_i=m$, i.e., $m\in\mu(M)$. Then $\{n,n+1,\ldots,qn\}\subseteq\mu(M)$.

(2) For any $m\geqslant n$, there exists $q\in\mathbb{N}$ such that $qn\geqslant m$. Since $\kappa(R)=+\infty$, R has a basis U with q elements (by Lemma 4.1). By (1), we have $\{n,n+1,\ldots,qn\}\subseteq\mu(M)$ and so $m\in\mu(M)$. Then $\mu(M)=\{n,n+1,\ldots\}$. $\square$

Since R^n is a free R-semimodule with $r(R^n)=n$, by Theorem 4.1(2), we have

Corollary 4.1. *If $\kappa(R)=+\infty$, then $\mu(R^n)=\{n,n+1,\ldots\}$.* $\square$

In [27], Zhao and Wang introduced the concept of irredundant decomposition of elements in a join-semiring: Let R be a join-semiring and $r\in R$. A subset $\{u_1,u_2,\ldots,u_t\}$ of R is called a *decomposition* of r if $r = \sum_{1 \leqslant i \leqslant t} u_i$. Furthermore, if $r \neq \sum_{1 \leqslant j \leqslant t, j \neq i} u_j$ for any $i \in \underline{t}$, then the decomposition U is called *irredundant*.

Remark 4.1. In a commutative join-semiring R, a subset $U = \{u_1, u_2, \dots, u_t\} \subseteq R$ is an irredundant decomposition of the identity 1 if and only if it is a basis of the R-semimodule R. In fact, if U is an irredundant decomposition of 1, then $1 = \sum_{1 \leqslant i \leqslant t} u_i$ and so $r = \sum_{1 \leqslant i \leqslant t} ru_i$ for any $r \in R$. This means that U is a generating set for the R-semimodule R. If U is not a basis for the R-semimodule R, then there exists $i_0 \in \underline{t}$ such that $u_{i_0} = \sum_{i \in \underline{t},\, i \neq i_0} k_i u_i$, where $k_i \in R$, and so $1 = \sum_{i \in \underline{t}} u_i = \sum_{i \in \underline{t},\, i \neq i_0} (1 + k_i) u_i = \sum_{i \in \underline{t},\, i \neq i_0} u_i$ (note that $1 + a = 1$ for any a in a join-semiring), which contradicts the definition of U. Thus, U is a basis for R. Conversely, let U be a basis for the R-semimodule R. Then $1 = \sum_{1 \leqslant i \leqslant t} \lambda_i u_i$, where $\lambda_i \in R$. Thus $1 = \sum_{1 \leqslant i \leqslant t} \lambda_i u_i \leqslant \sum_{1 \leqslant i \leqslant t} u_i \leqslant 1$ (because 1 is the greatest element of the join-semiring R). Then $1 = \sum_{1 \leqslant i \leqslant t} u_i$. If $1 = \sum_{i \in \underline{t},\, i \neq i_0} u_i$ for some $i_0 \in \underline{t}$ then $u_{i_0} = \sum_{i \in \underline{t},\, i \neq i_0} u_{i_0} u_i$, i.e., u_{i_0} is a linear combination of the elements in $U \backslash \{u_0\}$, which contradicts the definition of U. Then U is an irredundant decomposition of 1. $\square$

Remark 4.2. Since any commutative join-semiring is a commutative semiring, by Remark 4.1, Corollary 4.1 generalizes Theorem 3.2 in [27].

Theorem 4.2. *Let R be a commutative zerosumfree semiring and M a free R-semimodule with $r(M) = n$. If $\kappa(R) = q$ then $\mu(M) = \{n, n+1, \dots, qn\}$.*

To prove Theorem 4.2, we need a lemma.

Lemma 4.2. *Let $\kappa(R) = q$ and U a finite generating set for the R-semimodule R with $|U| \geqslant q$. Then there exists $V \subseteq U$ such that V is a generating set for R and $|V| = q$.*

Proof. We will prove the statement by induction on $|U| - q$. It is clear if $|U| - q = 0$ since in this case $|U| = q$. Assume it holds for $|U| - q = k$ $(k \geqslant 0)$. Then for $|U| - q = k + 1$, we have $|U| = q + k + 1$. Since $\kappa(R) = q$, there exists $u \in U$ such that u is a linear combination of the elements in $U \backslash \{u\}$. Then $U \backslash \{u\}$ is a generating set for R and $|U \backslash \{u\}| - q = k$. By the induction hypothesis, there exists $V \subseteq U \backslash \{u\}$ such that V is a generating set for R with $|V| = q$. The proof is completed. $\square$

Proof of Theorem 4.2. Let $F = \{f_1, f_2, \dots, f_n\}$ be a free basis for M and $\kappa(R) = q$. For any positive integer $m \geqslant qn + 1$, if $S = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ is a generating set for M, then

$$\alpha_j = \sum_{1 \leqslant i \leqslant n} a_{ij} f_i$$

for any $j \in \underline{m}$, where $a_{ij} \in R$, and for every $i \in \underline{n}$,

$$f_i = \sum_{1 \leqslant j \leqslant m} \lambda_j \alpha_j$$

for some $\lambda_1, \lambda_2, \dots, \lambda_m \in R$. Thus

$$f_i = \sum_{1 \leqslant j \leqslant m} \lambda_j \left(\sum_{1 \leqslant h \leqslant n} a_{hj} f_h \right) = \left(\sum_{1 \leqslant j \leqslant m} \lambda_j a_{ij} \right) f_i + \sum_{\substack{1 \leqslant h \leqslant n \\ h \neq i}} \left(\sum_{1 \leqslant j \leqslant m} \lambda_j a_{hj} \right) f_h.$$

This implies that

$$1 = \lambda_1 a_{i1} + \lambda_2 a_{i2} + \cdots + \lambda_m a_{im}$$

and

$$0 = \lambda_1 a_{h1} + \lambda_2 a_{h2} + \cdots + \lambda_m a_{hm}$$

for all $h \in \underline{n}$ with $h \neq i$ (because F is a free basis for M).

By the equality $1 = \lambda_1 a_{i1} + \lambda_2 a_{i2} + \cdots + \lambda_m a_{im}$, we have $r = r\lambda_1 a_{i1} + r\lambda_2 a_{i2} + \cdots + r\lambda_m a_{im}$ for all $r \in R$. Then the set $\{\lambda_j a_{ij} \mid j \in \underline{m}\}$ is a generating set for R. Since $\kappa(R) = q$, there exists a subset V of the set $\{\lambda_j a_{ij} \mid j \in \underline{m}\}$ such that V is a generating for R and $|V| = q$ (by Lemma 4.2). Let $V = \{\lambda_{i_k} a_{ii_k} \mid k \in \underline{q}\}$, where $i_1, i_2, \ldots, i_q \in \underline{m}$. Then

$$1 = \mu_1 \lambda_{i_1} a_{ii_1} + \mu_2 \lambda_{i_2} a_{ii_2} + \cdots + \mu_q \lambda_{i_q} a_{ii_q},$$

for some $\mu_1, \mu_2, \ldots, \mu_q \in R$.

By the equality $0 = \lambda_1 a_{h1} + \lambda_2 a_{h2} + \cdots + \lambda_m a_{hm}$, we have $\lambda_j a_{hj} = 0$ for all $j \in \underline{m}$ and all $h \in \underline{n}$ with $h \neq i$ (because R is zerosumfree). Then $\lambda_{i_k} a_{hi_k} = 0$ for all $k \in \underline{q}$ and all $h \in \underline{n}$ with $h \neq i$ and so $\mu_k \lambda_{i_k} a_{hi_k} = 0$ for all $k \in \underline{q}$ and all $h \in \underline{n}$ with $h \neq i$. Thus

$$0 = \mu_1 \lambda_{i_1} a_{hi_1} + \mu_2 \lambda_{i_2} a_{hi_2} + \cdots + \mu_q \lambda_{i_q} a_{hi_q}$$

for all $h \in \underline{n}$ with $h \neq i$.

Therefore, we have

$$\begin{aligned}
\sum_{1 \leqslant k \leqslant q} \mu_k \lambda_{i_k} \alpha_{i_k} &= \sum_{1 \leqslant k \leqslant q} \mu_k \lambda_{i_k} \left(\sum_{1 \leqslant h \leqslant n} a_{hi_k} f_h \right) \\
&= \left(\sum_{1 \leqslant k \leqslant q} \mu_k \lambda_{i_k} a_{ii_k} \right) f_i + \sum_{\substack{1 \leqslant h \leqslant n \\ h \neq i}} \left(\sum_{1 \leqslant k \leqslant q} \mu_k \lambda_{i_k} a_{hi_k} \right) f_h \\
&= f_i,
\end{aligned}$$

i.e., f_i can be expressed as a linear combination of the elements $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_q}$. Let $S' = \bigcup_{1 \leqslant i \leqslant n} \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_q}\}$. Then each element in F can be expressed as a linear combination of the elements in S' and so S' is a generating set for M since every element in M can be expressed as a linear combination of the elements in F. Since $|S'| \leqslant qn < |S|$, there exists an α in $S \backslash S'$ which can be expressed as a linear combination of the elements in S'. Certainly, α can be expressed as a linear combination of the elements in $S \backslash \{\alpha\}$ (because $S' \subseteq S \backslash \{\alpha\}$), i.e., $S = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is linearly dependent. This means that the cardinality of any basis for M is less than or equal to qn. By Theorems 3.3 and 4.1(1), we have $\mu(M) = \{n, n+1, \ldots, qn\}$. $\square$

Since R^n is a free R-semimodule and $r(R^n) = n$, by Theorems 4.2, we have

Corollary 4.2. *If R is a commutative zerosumfree semiring and $\kappa(R) = q$, then $\mu(R^n) = \{n, n+1, \ldots, qn\}$.*

Remark 4.3. Since any commutative join-semiring is a commutative zerosumfree semiring, Corollary 4.2 generalizes Theorem 3.1 in [27].

Remark 4.4. Whether Theorem 4.2 holds for an arbitrary commutative semiring R is not known.

Finally, we give some equivalent descriptions for the commutative semirings R satisfying the property that any two bases for a finitely generated free R-semimodule have the same cardinality.

Theorem 4.3. *For any commutative semiring R, the following statements are equivalent.*

(1) $\kappa(R) = 1$.
(2) *For any $u, v \in R$, $1 = u + v$ implies that either $u \in U(R)$ or $v \in U(R)$.*
(3) *Any two bases for a finitely generated free R-semimodule M have the same cardinality.*

Proof. (1) $\Longrightarrow$ (2). Let $\kappa(R) = 1$. For any $u, v \in R$, if $1 = u + v$ then $r = ru + rv$ for any $r \in R$. This means that $\{u, v\}$ is a generating set for the R-semimodule R. Since $\kappa(R) = 1$, we have that $\{u, v\}$ is linearly dependent in the semimodule R and so $v = \lambda u$ for some $\lambda \in R$ or $u = \gamma v$ for some $\gamma \in R$. If $v = \lambda u$, then $1 = u + v = u(1 + \lambda)$ and so $u \in U(R)$. Similarly, if $u = \gamma v$ then $v \in U(R)$.

(2) $\Longrightarrow$ (3). Suppose that for any $u, v \in R$, $1 = u + v$ implies either $u \in U(R)$ or $v \in U(R)$. In the following we show that any two bases for M have the same cardinality. There are two cases to be considered:

Case 1. The identity element 1 of R is not additively invertible, i.e., $1 \notin V(R)$. In this case, $u \notin V(R)$ for all $u \in U(R)$, i.e., $U(R) \cap V(R) = \phi$. Let $r(M) = n$ and $F = \{f_1, f_2, \dots, f_n\}$ be a free basis for M, and let $S = \{\alpha_1, \alpha_2, \dots, \alpha_m\}$ be a generating set for M with $m > n$. In the following we prove the set S is linearly dependent.

Let $(\alpha_1, \alpha_2, \dots, \alpha_m) = (f_1, f_2, \dots, f_n)A$ and $(f_1, f_2, \dots, f_n) = (\alpha_1, \alpha_2, \dots, \alpha_m)B$ with $A \in M_{n\times m}(R)$ and $B \in M_{m\times n}(R)$. Then $(f_1, f_2, \dots, f_n) = (f_1, f_2, \dots, f_n)AB$ and so $AB = I_n$ (because $F = \{f_1, f_2, \dots, f_n\}$ is free). Thus

$$a_{i1}b_{1i} + a_{i2}b_{2i} + \dots + a_{im}b_{mi} = 1$$

for all $i \in \underline{n}$ and

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{im}b_{mj} = 0$$

for all $i, j \in \underline{n}$ with $i \neq j$.

For any $i \in \underline{n}$, by the equality $a_{i1}b_{1i} + a_{i2}b_{2i} + \dots + a_{im}b_{mi} = 1$, we have that there exists $\theta(i) \in \underline{m}$ such that $a_{i\theta(i)}b_{\theta(i)i} \in U(R)$ (because $1 = u + v$ implies either $u \in U(R)$ or $v \in U(R)$ for any $u, v \in R$) and so $a_{i\theta(i)} \in U(R)$ and $b_{\theta(i)i} \in U(R)$.

By the equality $a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{im}b_{mj} = 0$, we have that $a_{ik}b_{kj} \in V(R)$ for all $i, j \in \underline{n}$ and $k \in \underline{m}$ with $i \neq j$, i.e., there exists $r_{ijk} \in R$ such that $a_{ik}b_{kj} + r_{ijk} = 0$. Since $b_{\theta(j)j} \in U(R)$, we have $a_{i\theta(j)} + r_{ij\theta(j)}b^{-1}_{\theta(j)j} = 0$, i.e., $a_{i\theta(j)} \in V(R)$ for all $i, j \in \underline{n}$ with $i \neq j$. Therefore $\theta(i) \neq \theta(j)$ for all $i \neq j$ (because $a_{i\theta(i)} \in U(R)$ and $a_{i\theta(j)} \in V(R)$ and $U(R) \cap V(R) = \phi$). That is, θ is an injective mapping from $\underline{n}$ to $\underline{m}$.

Put $D = (d_{ij}) \in M_n(R)$ such that $d_{ij} = a_{i\theta(j)}$. Then D is an $n \times n$ submatrix of A and $(\alpha_{\theta(1)}, \alpha_{\theta(2)}, \dots, \alpha_{\theta(n)}) = (f_1, f_2, \dots, f_n)D$. Since $d_{ii} = a_{i\theta(i)} \in U(R)$ and $d_{ij} = a_{i\theta(j)} \in V(R)$ for all $i, j \in \underline{n}$ with $i \neq j$, we have that D is invertible (by Lemma 2.3). Then $(f_1, f_2, \dots, f_n) = (\alpha_{\theta(1)}, \alpha_{\theta(2)}, \dots, \alpha_{\theta(n)})D^{-1}$, and so each f_i is a linear combination of $\alpha_{\theta(1)}, \alpha_{\theta(2)}, \dots, \alpha_{\theta(n)}$. This means that $\{\alpha_{\theta(1)}, \alpha_{\theta(2)}, \dots, \alpha_{\theta(n)}\}$ is a generating set for M. Since $m > n$, there exists an $\alpha_{i_0} \in S/\{\alpha_{\theta(1)}, \alpha_{\theta(2)}, \dots, \alpha_{\theta(n)}\}$ such that α_{i_0} is a linear combination of $\alpha_{\theta(1)}, \alpha_{\theta(2)}, \dots, \alpha_{\theta(n)}$. Certainly, α_{i_0} is a linear combination of the elements in $S/\{\alpha_{i_0}\}$. Then the set S is linearly dependent. This implies that the cardinality of any basis for M is less than or equal to n. On the other hand, by Theorem 3.3, the cardinality of any basis for M is greater than or equal to n, and so any two bases for M have the same cardinality n.

Case 2. The identity element 1 of R is additively invertible, i.e., $1 \in V(R)$. In this case, R is a commutative ring and M is an R-module. Suppose that R has more than one maximal ideal; say I and J are two distinct maximal ideals of R. Then $I + J = R$ and so $1 = u + v$ for some $u \in I$ and some $v \in J$. If $u \in U(R)$ then $I = R$, which is a contradiction; similarly, if $v \in U(R)$ then $J = R$, which is a contradiction. Therefore, R has at most a maximal ideal. On the other hand, by Zorn's Lemma, R has at least a maximal ideal. Then R has a unique maximal ideal. By Lemma 2.4, any two bases for M have the same cardinality.

(3) $\Longrightarrow$ (1). Suppose that any two bases for M has the same cardinality, say, n. Then $r(M) = n$ and $\mu(M) = \{n\}$. Let $\kappa(R) = q$. Then $\{n, n+1, \dots, qn\} \subseteq \mu(M)$ (by Theorem 4.1(1)) and so $q = 1$. This completes the proof. □

Since R^n is a free R-semimodule and $r(R^n) = n$, by Theorem 4.3, we have

Corollary 4.3. *For any commutative semiring R, the cardinality of each basis for R^n is n if and only if $\kappa(R) = 1$.* □

Remark 4.5. The semirings R satisfying the property $\kappa(R) = 1$ are quite abundant, for example, every field F, the fuzzy algebra $\mathbb{F} = ([0, 1], \vee, \wedge)$, the nonnegative integer semiring $(\mathbb{Z}^0, +, \cdot)$, the nonnegative rational number semiring $(\mathbb{Q}^0, +, \cdot)$, the nonnegative real number $(\mathbb{R}^0, +, \cdot)$, the max-plus algebra $(\mathbb{R} \cup \{-\infty\}, \max, +)$ and the min-plus algebra $(\mathbb{R} \cup \{+\infty\}, \min, +)$ are this type of semirings. By Corollary 4.3, the cardinality of each basis for R^n is n if R is in this type of semirings.

5. Conclusions

This paper discussed some properties and characterizations of the bases for a semimodule over a commutative semiring R and gave some equivalent conditions for a basis to be a free basis in a finitely generated free semimodule over R. Also, this paper considered the different possible cardinalities for a basis in a finitely generated free semimodule and obtained some equivalent descriptions for a commutative semiring R satisfying the property that any two bases for a finitely generated free R-semimodule have the same cardinality. Partial results obtained in the paper develop and generalize the corresponding results for commutative join-semirings in [27] and for commutative zerosumfree semirings in [16].

Acknowledgements

The author would like to thank the referees for a number of constructive comments and valuable suggestions.

References

[1] D.D. Anderson, J. Robeson, Bases for modules, Expo. Math. 22 (2004) 283–296.
[2] S.K. Bhambri, Extensions of semimodules and injective semimodules, Southeast Asian Bull. Math. 34 (2010) 25–41.
[3] W. Briec, C. Horvath, On the separation of convex sets in some idempotent semimodules, Linear Algebra Appl. 435 (2011) 1542–1548.
[4] G. Cohen, S. Gaubert, J.P. Quadrat, Duality and separation theorems in idempotent semimodules, Linear Algebra Appl. 379 (2004) 395–422.
[5] R.A. Cuninghame-Green, Minimax Algebra, Lecture Notes in Econom. and Math. Systems, vol. 166, Springer-Verlag, Berlin, 1979.
[6] R.A. Cuninghame-Green, P. Butkovič, Bases in max algebra, Linear Algebra Appl. 389 (2004) 107–120.
[7] A. Di Nola, A. Lettieri, I. Perfilieva, V. Novak, Algebraic analysis of fuzzy systems, Fuzzy Sets and Systems 158 (2007) 1–22.
[8] D. Dolžan, P. Oblak, Invertible and nilpotent matrices over antirings, Linear Algebra Appl. 430 (2009) 271–278.
[9] D. Dolžan, P. Oblak, Idempotent matrices over antirings, Linear Algebra Appl. 431 (2009) 823–832.
[10] R. Ebrahimi Atani, S. Ebrahimi Atani, On subsemimodules of semimodules, Bul. Acad. Ştiinţe Repub. Mold., Mat. 63 (2) (2010) 20–30.
[11] R. Ebrahimi Atani, Prime subsemimodules of semimodules, Int. J. Algebra 4 (26) (2010) 1299–1306.
[12] J.S. Golan, Semirings and Their Applications, Kluwer Academic Publishers, 1999.
[13] G. Maze, C. Monico, J. Rosenthal, Public key cryptography based on semigroup actions, Adv. Math. Commun. 1 (2007) 489–507.
[14] I. Perfilieva, Semi-linear spaces, in: H. Noguchi, H. Ishii, et al. (Eds.), Proceedings of Seventh Czech–Japanese Seminar on Data Analysis and Decision Making under Uncertainty, Hyogo, Japan, 2004, pp. 127–130.
[15] C. Reutenauer, H. Straubing, Inversion of matrices over a commutative semiring, J. Algebra 88 (1984) 350–360.
[16] Q.Y. Shu, X.P. Wang, Bases in semilinear spaces over zorosumfree semirings, Linear Algebra Appl. 435 (2011) 2681–2692.
[17] Q.Y. Shu, X.P. Wang, Standard orthogonal vectors in semilinear spaces and their applications, Linear Algebra Appl. 437 (2012) 2733–2754.
[18] M. Takahashi, Structures of semimodules, Kobe J. Math. 4 (1987) 79–101.
[19] Y.J. Tan, On invertible matrices over antirings, Linear Algebra Appl. 423 (2007) 428–444.
[20] Y.J. Tan, On nilpotent matrices over antirings, Linear Algebra Appl. 429 (2008) 1243–1253.
[21] Y.J. Tan, On nilpotency of matrices over antirings, Linear Algebra Appl. 433 (2010) 1541–1554.
[22] E.M. Vechtomov, Two general structure theorems on submodules, in: Abelian Groups and Modules, vol. 15, Tomsk State University, Tomsk, 2000, pp. 17–23 (in Russian).
[23] H.X. Wang, A note on endomorphism semirings of semimodules, Kobe J. Math. 5 (1988) 155–160.
[24] H.X. Wang, M. Takahashi, On epimorphisms of semimodules, Kobe J. Math. 6 (1989) 297–298.
[25] S.M. Yusuf, Inverse semimodules, J. Natur. Sci. Math. 6 (1966) 111–117.
[26] S. Zhao, X.P. Wang, Invertible matrices and semilinear spaces over commutative semirings, Inform. Sci. 180 (2010) 5115–5124.
[27] S. Zhao, X.P. Wang, Bases in semilinear spaces over join-semirings, Fuzzy Sets and Systems 182 (2011) 93–100.
[28] U. Zimmermann, Linear and Combinatorial Optimization in Ordered Algebraic Structures, Ann. Discrete Math., vol. 10, North-Holland, 1981.