Secondary representation of semimodules over a commutative semiring

Reza Ebrahimi Atani and Shahabaddin Ebrahimi Atani

Abstract

In this paper, we analyze some results on the theory secondary representation of semimodules over a commutative semiring with non-zero identity analogues to the theory secondary representation of modules over a commutative ring with non-zero identity.

1. Introduction

Semimodules constitute a fairly natural generalization of modules, with broad applications in the mathematical foundations of computer science [4]. The main part of this paper is devoted to stating and proving analogues to several well-known results in the theory of modules.

For the sake of completeness, we state some definitions and notations used throughout. By a *commutative semiring* we mean an algebraic system $R = (R, +, \cdot)$ such that $(R, +)$ and $(R, \cdot)$ are commutative semigroups, connected by $a(b + c) = ab + ac$ for all $a, b, c \in R$, and there exists $0 \in R$ such that $r + 0 = r$ and $r0 = 0r = 0$ for all $r \in R$. Throughout this paper let R be a commutative semiring. A (*left*) *semimodule* M *over a semiring* R is a commutative additive semigroup which has a zero element, together a mapping from $R \times M$ into M (sending (r, m) to rm) such that $(r+s)m = rm + sm$, $r(m + p) = rm + rp$, $r(sm) = (rs)m$ and $0m = r0_M = 0_M$ for all $m, p \in M$ and $r, s \in R$.

Let M be a semimodule over the semiring R, and let N be a subset of M. We say that N is a *subsemimodule* of M, or an R-*subsemimodule* of M, percisely when N is itself an R-semimodule with respect to the operations

2000 Mathematics Subject Classification: 16Y60

Keywords: Semiring, k-subsemimodule, Q_M-subsemimodule, commutative semiring.

for M (so $0_M \in N$). It is easy to see that if $r \in R$, then

$$rM = \{rm : m \in M\}$$

is a subsemimodule of M. The semiring R is considered to be also a semimodule over itself. In this case, the subsemimodules of R are called *ideals* of R. A *subtractive subsemimodule* (= *k-subsemimodule*) N is a subsemimodule of M such that if $x, x + y \in N$, then $y \in N$ (so $\{0_M\}$ is a k-subsemimodule of M). If M is a semimodule over a semiring R, then M is *Artinian* if any non-empty set of k-subsemimodules of M has minimal member with respect to the set inclusion. This definition is equivalent to the descending chain condition on k-subsemimodules of M. A *prime ideal* of R is a proper ideal P of R in which $x \in P$ or $y \in P$ whenever $xy \in P$.

A subsemimodule N of a semimodule M over a semiring R is called a *partitioning subsemimodule* (=Q_M*-subsemimodule*) if there exists a non-empty subset Q_M of M such that

(1) $RQ_M \subseteq Q_M$;

(2) $M = \cup\{q + N : q \in Q_M\}$;

(3) If $q_1, q_2 \in Q_M$ then $(q_1 + N) \cap (q_2 + N) \neq \emptyset$ if and only if $q_1 = q_2$.

It is easy to see (cf. [5]) that if $M = Q_M$, then $\{0\}$ is a Q_M-subsemimodule of M.

Remark 1.1. Let M be a semimodule over a semiring R, and let N be a Q_M-subsemimodule of M. We put $M/N = \{q + N : q \in Q_M\}$. Then M/N forms a commutative additive semigroup which has zero element under the binary operation $\oplus$ defined as follows: $(q_1 + N) \oplus (q_2 + N) = q_3 + N$ where $q_3 \in Q_M$ is the unique element such that $q_1 + q_2 + N \subseteq q_3 + N$. Note that by the definition of Q_M-subsemimodule, there exists a unique $q_0 \in Q_M$ such that $0_M + N \subseteq q_0 + N$. Then $q_0 + N$ is a zero element of M/N.

Now let $r \in R$ and suppose that $q_1 + N, q_2 + N \in M/N$ are such that $q_1 + N = q_2 + N$ in M/N. Then $q_1 = q_2$, we must have $rq_1 + N = rq_2 + N$. Hence we can unambiguously define a mapping from $R \times M/N$ into M/N (sending $(r, q_1 + N)$ to $rq_1 + N$) and it is routine to check that this turns the commutative semigroup M/N into an R-semimodule. We call this R-semimodule the *residue class semimodule* or *factor semimodule* of M modulo N [4].

We need the following theorem proved in [5, Lemma 2.4, Proposition 2.5, Theorem 2.6, Theorem 2.7 and Theorem 2.10].

Theorem 1.2. *Assume that N is a Q_M-subsemimodule of a seminodule M over a semiring R and let T, L be k-subsemimodules of M containing N. Then the following hold:*

(i) *If $q_0 + N$ is a zero in M/N, then $q_0 + N = N$.*

(ii) *N is a k-subsemimodule of M.*

(iii) *$L/N = \{q + N : q \in Q_M \cap L\}$ is a k-subsemimodule of M/N.*

(iv) *If H is a k-subsemimodule of M/N, then $H = K/N$ for some k-subsemimodule K of M.*

(v) *$T/N = L/N$ if and only if $T = L$.* □

2. Secondary semimodules

We begin with the key lemma of this paper.

Lemma 2.1. *Let M be a semimodule over a semiring R, N an Q_M-subsemimodule of M and q_0 the unique element Q_M such that $q_0 + N$ is the zero in M/N. Then the following hold:*

(i) *$q_0 \in N$ and if $q \in N \cap Q_M$, then $q \in N$.*

(ii) *If $q_1, q_2 \in Q_M$ and $a, b \in N$ with $q_1 + a = q_2 + b$, then $q_1 = q_2$.*

(iii) *If for each $n \in N$, there exists $n' \in N$ such that $n + n' = 0$, then $N = a + N = \{a + n : n \in N\}$ for every $a \in N$.*

Proof. (i) Since by Theorem 1.2, $q_0 + N = N$ is a k-subsemimodule of M, we must have $q_0 \in N$. Moreover, since $q + q_0 \in (q + N) \cap (q_0 + N)$, we get $q = q_0 \in N$.

(ii) Since $q_1 + a \in (q_1 + N) \cap (q_2 + N)$, we must have $q_1 = q_2$.

(iii) It is suffices to show that $N \subseteq a + N$. Let $n \in N$. Since N is a Q_M subsemimodule, there is an element $q \in Q_M$ and $n' \in N$ such that $n = q + n'$, so $q \in N$ since every Q_M-submodule is a k-subsemimodule. By assumption, $a + a' = 0$ for some $a' \in N$. Hence $n = a + a' + q + n' \in a + N$, and the proof is complete. □

Assume that R is a semiring and let N be an R-subsemimodule of a semimodule M. Then N is a *relatively divisible subsemimodule* (or an *RD-subsemimodule*) if $rN = N \cap rM$ for all $r \in R$. Since $rN \subseteq N \cap rM$, we see that N is an *RD*-subsemimodule of M if and only if for all $x \in M$ and $r \in R$, $rx \in N$ implies $rx = ry$ for some $y \in N$. Hence, N is an

RD-subsemimodule of M if and only if $a \in N$ and the equation $rx = a$ has a solution in M, then it is solvable in N too.

Lemma 2.2. *Let R be a semiring, and let P, N be subsemimodules of the R-semimodule M such that $P \subseteq N \subseteq M$. Then:*

(i) *If P is an RD-subsemimodule of N and N is an RD-subsemimodule of M, then P is an RD-subsemimodule of M.*

(ii) *If P is an RD-subsemimodule of M, then P is an RD-subsemimodule of N.*

Proof. The proof is straightforward. □

Proposition 2.3. *Let R be a semiring, M an R-semimodule, P a Q_M-subsemimodule of M and N a k-subsemimodule of M such that $P \subseteq N \subseteq M$. Then:*

(i) *If N is an RD-subsemimodule of M, then N/P is an RD-subsemimodule of M/P.*

(ii) *If P is an RD-subsemimodule of M and N/P is an RD-subsemimodule of M/P, then N is an RD-subsemimodule of M.*

Proof. (i) Let $rx = q_1 + P$ be an equation over N/P that admits a solution in M/P, say, $r(q_2 + P) = q_1 + P$ where $q_2 \in Q_M$ and $q_1 \in Q_M \cap N$, so $rq_2 = q_1$. By the purity of N in M the equation $rx = q_1$ has a solution $x = a$ in N. Then $a = q_3 + b$ for some $q_3 \in Q_M \cap N$ and $b \in P$ (since N is a k-subsemimodul), so $rq_3 + rb = q_1$. Hence $rq_3 = q_1$ by Lemma 2.1. Thus $r(q_3 + P) = q_1 + P$. Hence $x = q_3 + P$ is a solution of our original equation.

(ii) Let $rx = a$ be an equation over N which has a solution $x = c$ in M. There are elements $q_1 \in N \cap Q_M$, $q_2 \in Q_M$ and $e, f \in P$ such that $a = q_1 + e$ and $c = q_2 + f$, so $rq_2 + rf = q_1 + e$. Hence $rq_2 = q_1$. Therefore, we must have $r(q_2 + P) = q_1 + P$. By purity of N/P in M/P there exist $q_3 + P \in N/P$ such that $r(q_3 + P) = q_1 + P$, where $q_3 \in N \cap Q_M$, so $rq_3 = q_1$. Since $r(q_3 + f) = rq_2 + rf = q_1 + e$, we get $x = q_3 + f$ is a solution of our original equation. □

Proposition 2.4. *Let M be a semimodule over a semiring R, N an Q_M-subsemimodule of M and $r \in R$. Let q_0 be the unique element of Q_M such that $q_0 + N$ is the zero in M/N. Then:*

(i) *$rM + N$ is an $(rQ)_M$-subsemimodule of M. In particular,*

$$(rM + N)/N = \{rq + N : rq \in rQ_M \cap (rM + N)\}$$

is a k-subsemimodule of M/N.

(*ii*) $r(M/N) = (rM + N)/N$. *In particular,* $N/N = \{q_0 + N\}$.

Proof. (*i*) Clearly, $R(rQ) \subseteq rQ$ and $\bigcup\{rq + N : q \in Q_M\} \subseteq rM + N$. For the reverse inclusion, assume that $rm + n \in rM + N$ where $m \in M$ and $n \in N$. There are elements $q \in Q$ and $n_1 \in N$ such that $m = q + n_1$ since N is a Q_M-subsimimodule of M, so $rm + n = rq + rn_1 + n \in rq + N$. Hence $rM + N = \cup\{rq + N : q \in Q\}$. It is easy to see that if $rq_1, rq_2 \in rQ$, then $(rq_1 + N) \cap (rq_2 + N) \neq \emptyset$ if and only if $rq_1 = rq_2$. It follows from Theorem 1.2 that $rM + N$ is a k-subsemimodule of M containing N. Then $(rM + N)/N$ is a k-subsemimodule of M/N by Theorem 1.2.

(*ii*) Since the inclusion $(rM + N)/N \subseteq r(M/N)$ is trivial, we will prove the reverse inclusion. Let $r(q + N) = rq + N \in r(M/N)$. Since $rq \in (rM + N) \cap rQ$, we must have $r(q + N) \in (rM + N)/N$ by (*i*), and we have equality. Finally, $N/N = \{q + N : q \in N \cap Q_M\} = \{q_0 + N\}$ by Lemma 2.1. □

Let R be a semiring with identity. An R-semimodule M is said to be *secondary* if $M \neq 0$ and if, for each $r \in R$, the endomorphism $\varphi_{r,M}$ (i.e., multiplication by r in M) is either surjective or nilpotent. Equivalently, M is secondary if and only if either $rM = M$ or $r^n M = 0$ for some n for every $r \in R$. It is easy to see that the nilradical of M is a prime ideal P, and M is said to be P-secondary [7].

Proposition 2.5. *Let N be a proper Q_M-subsemimodule of a P-secondary semimodule M over a semiring R. Then M/N is a P-secondary R-semimodule.*

Proof. Assume that q_0 is the unique element Q_M such that $q_0 + N$ is the zero in M/N and let $r \in R$. If $r \in P$, then $r(M/N) = (rM + N)/N = (M + N)/N = M/N$ by Proposition 2.4. If $r \notin P$, then there is a positive integer s such that $r^s(M/N) = (r^s M + N)/N = N/N = \{q_0 + N\}$, as required. □

Theorem 2.6. *Assume that R is a semiring and let N be a non-zero proper RD-subsemimodule (resp. pure subsemimodule) of an R-semimodule M. If N is a Q_M-subsemimodule of M, then M is P-secondary if and only if N and M/N are secondary.*

Proof. If M is secondary, then M/N is secondary by Proposition 2.7. To see that N is secondary, assume that $a \in R$. If $a \in P$, then $a^n N \subseteq a^n M = 0$ for some n. So suppose that $a \notin P$. Then $aN = N \cap aM = N \cap M = N$ since N is an RD-submodule. Conversely, assume that both N and M/N are secondary and let q_0 be the unique element Q_M such that $q_0 + N$ is the zero in M/N. Let $r \in R$. If $r \in P$, then $r^m(M/N) = (r^mM + N)/N = N/N = \{q_0 + N\}$ by Proposition 2.6 and $r^mN = 0$ for some m. Hence $r^mM \subseteq N$ by Proposition 2.4 and Theorem 1.2, and $0 = r^mN = r^mM \cap N = r^mM$. If $r \notin P$, then $rM + N = M$, $rN = N$ and $N = rN = N \cap rM$, so we must have $rM = M$. Thus M is secondary. □

Let R be a semiring. An element $a \in R$ is said to be *regular* if there exists $b \in R$ such that $a = a^2b$, and R is said to be regular if each of its elements is regular.

Theorem 2.7. *Assume that R is a regular semiring and let N be a non-zero proper Q_M-subsemimodule of an R-semimodule M. Then M is secondary if and only if N and M/N are secondary.*

Proof. By Theorem 2.6, it suffices to show that every subsemimodule of M is a RD-subsemimodule of M. Let N be a subsemimodule of M. It is enough to show that if $n \in N$ and the equation $rx = n$ (where $r \in R$) has a solution in M, say m, then it is solvable in N. By assumption, there is an element $s \in R$ such that $r = r^2s$. Hence $r(sn) = r^2sm = rm = n$. Therefore, the equation $rx = n$ has a solution $x = sn$ in N. □

Lemma 2.8. *Let R be a semiring. Then finite sum of P-secondary semimodules is P-secondary.*

Proof. Let $M = M_1 + \ldots + M_k$, where for each i, M_i is P-secondary. Let $a \in R$. If $a \in P$, then there is a positive integer n such that $a^nM_i = 0$ for every i. Hence $a^nM = 0$. Similarly, if $a \notin P$, then $aM = M$. Thus M is P-secondary. □

Let M be a semimodule over a semiring R. A *secondary representation* of M is an expression of M as a sum of secondary submodules, say $M = N_1 + \ldots + N_k$. The representation is said to be *minimal* if (1) the prime ideals $\text{nilrad}(N_i) = P_i$ are distinct and (2) none of the summand N_i is redundant. By Lemma 2.8, any secondary representation of M can be refined to a minimal one. If M has a secondary representation, we shall say that M is *representable* [7].

Definition 2.9. Let R be a semiring. An R-semimodule M is *sum-irreducible* if $M \neq 0$ and the sum of any two proper subsemimodules of M is always a proper subsemimodule. An R-semimodule M is *strongly subtractive* if every subsemimodule of M is a k-subsemimodule and for each $m \in M$ there exists $m' \in M$ such that $m + m' = 0$ [2].

Theorem 2.10 *Every strongly subtractive Artinian semimodule M over a semiring R has a secondary representation.*

Proof. First, we show that if M is sum-irreducible, then M is secondary. Suppose M is not secondary. Then there is an element $r \in R$ such that $rM \neq M$ and $r^n M \neq 0$ for all positive integers n. By assumption, there exists a positive integer k such that $r^k M = r^{k+1} M = \dots$ Set $M_1 = \mathrm{Ker}\varphi_{r^k,M}$ and $M_2 = r^k M$. Then M_1 and M_2 are proper subsemimodules of M. Let $x \in M$. Then $r^k x = r^{2k} y$ for some $y \in M$. We can write $y + y' = 0$ for some $y' \in M$. Hence $r^k y + r^k y' = 0$, $r^{2k} y + r^{2k} y' = 0$ and $x = (x + r^k y') + r^k y$, where $x + r^k y' \in M_1$ and $r^k y \in M_2$. Hence $M = M_1 + M_2$, and therefore M is not sum-irreducible.

Next, suppose that M is not representable. Then the set of non-zero subsemimodules of M which are not representable has a minimal element N. Certainly N is not secondary and $N \neq 0$. Hence N is the sum of two strictly smaller subsemimodules N_1 and N_2. By the minimality of N, each N_1, N_2 is representable, and therefore so also is N, which is a contradiction. □

References

[1] **P. J. Allen**: *A fundamental theorem of homomorphisms for simirings*, Proc. Amer. Math. Soc. **21** (1969), 412 – 416.

[2] **H. M. Al-Thani**: *The Jacobson radical of type* (3, 1), Inter. J. Modern Math. **2** (2007), 27 – 33.

[3] **S. Ebrahimi Atani**: *The ideal theory in quotients of commutative semirings*, Glasnik Matematički **42** (2007), 301 – 308.

[4] **R. Ebrahimi Atani, S. Ebrahimi Atani and S. Mirzakuchaki**: *Public key cryptography using semigroup actions and semirings*, J. Discrete Math. Sci. Cryptography, to appear.

[5] **R. Ebrahimi Atani and S. Ebrahimi Atani**: *Prime subsemimodules of semimodules*, submitted.

[6] **R. Ebrahimi Atani and S. Ebrahimi Atani**: *Ideal theory in commutative semirings*, Buletinul Acad. Sci. Republ. Moldova, ser. Math. **2(57)** (2008), $14-23$.

[7] **I. G. Macdonald**: *Secondary representation of modules over a commutative ring*, Sympos. Math., **XI** (1973), $23-43$.

Received May 28, 2008

Department of Mathematics
University of Guilan
P.O.Box 1914, Rasht,
Iran
E-mail: ebrahimi@guilan.ac.ir