ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT

Journal of Algebra 271 (2004) 846–854

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

On finite congruence-simple semirings

Chris Monico

Department of Mathematics and Statistics, Texas Tech University, Lubbock, TX 79409-1042, USA

Received 6 May 2002

Communicated by Michel Broué

Abstract

In this paper, we describe finite, additively commutative, congruence simple semirings. The main result is that the only such semirings are those of order 2, zero-multiplication rings of prime order, matrix rings over finite fields, ones with trivial addition, and those that are additively idempotent.

Keywords: Semirings; Congruence simple; Congruence free

1. Introduction to semirings

The notion of semirings seems to have first appeared in the literature in a 1934 paper by Vandiver [4]. Though the concept of a semiring might seem a bit strange and unmotivated, additively commutative semirings arise naturally as the endomorphisms of commutative semigroups. Furthermore, every such semiring is isomorphic to a sub-semiring of such endomorphisms [2]. For a more thorough introduction to semirings and a large collection of references, the reader is referred to [2].

Definition 1. A *semiring* is a nonempty set S together with two associative operations, $+$ and $\cdot$, such that for all $a, b, c \in S$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

A semiring is called *additively* (*multiplicatively*) *commutative* if $(S, +)$ $((S, \cdot))$ is commutative. If both $(S, +)$ and $(S, \cdot)$ are commutative, S is simply called *commutative*.

The classification of finitely generated c-simple (see Definition 4) commutative semirings has only recently been given in [1]. In this paper, we progress toward a classification

E-mail address: monico.1@nd.edu.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2003.09.034

of the class of finite c-simple semirings which are only additively commutative. The main result will be given in Theorem 12.

Definition 2. An element α of a semiring is called *additively* (*multiplicatively*) *absorbing* if $\alpha + x = x + \alpha = \alpha$ ($\alpha \cdot x = x \cdot \alpha = \alpha$) for all $x \in S$. An element ∞ of a semiring is called an *infinity* if it is both additively and multiplicatively absorbing.

Note that an additive identity in a semiring need not be multiplicatively absorbing. If, however, a semiring has a multiplicatively absorbing additive identity, we call it a *zero*, and denote it by 0. A semiring S with additive identity o is called *zero-sum free* if for all $a, b \in S$, $a + b = o$ implies $a = b = o$.

Definition 3. Let S be a semiring and $\mathcal{B} \subseteq S$ a subset. Then $\mathcal{B}$ is called a *bi-ideal* of S if for all $b \in \mathcal{B}$ and $s \in S$, $b + s, s + b, bs, sb \in \mathcal{B}$.

Definition 4. A *congruence relation* on a semiring S is an equivalence relation $\sim$ that also satisfies

$$x_1 \sim x_2 \quad \Rightarrow \quad \begin{cases} c + x_1 \sim c + x_2, \\ x_1 + c \sim x_2 + c, \\ cx_1 \sim cx_2, \\ x_1 c \sim x_2 c, \end{cases}$$

for all $x_1, x_2, c \in S$. A semiring S that admits no congruence relations other than the trivial ones, id_S and $S \times S$, is said to be *congruence-simple*, or *c-simple*.

Note that the trivial semiring of order 1 and every semiring of order 2 are congruence-simple. Also note that if $\mathcal{B} \subseteq S$ is a bi-ideal then $\mathrm{id}_S \cup (\mathcal{B} \times \mathcal{B})$ is a congruence relation. Thus, if $\mathcal{B} \subseteq S$ is a bi-ideal and S is c-simple, then $|\mathcal{B}| = 1$ or $\mathcal{B} = S$.

The following theorem, due to Bashir, Hurt, Jančařék, and Kepka in [1, Theorem 14.1], classifies finite c-simple commutative semirings.

Theorem 5. *Let S be a commutative, congruence-simple, finite semiring. Then one of the following holds*:

(1) *S is isomorphic to one of the five semirings $T_1, \ldots, T_5$ of order* 2 *defined in* Table 1;
(2) *S is a finite field*;
(3) *S is a zero-multiplication ring of prime order*;
(4) *S is isomorphic to $V(G)$* (*defined below*), *for some finite abelian group G.*

For a multiplicative abelian group G, set $V(G) = G \cup \{\infty\}$. Extend the multiplication of G to $V(G)$ by the rule $x\infty = \infty x = \infty$ for all $x \in V(G)$. Define an addition on $V(G)$ by the rules $x + x = x$, $x + y = \infty$ for all $x, y \in V(G)$ with $x \neq y$.

We first note that a complete classification up to isomorphism of finite, additively commutative, c-simple semirings is probably not possible. To see this, note that $V(G)$ is c-simple for any finite group G. Furthermore, if G_1 and G_2 are two non-isomorphic

Table 1
Commutative semirings of order two

$(T_1,+)$	0	1	$\cdot$	0	1	$(T_2,+)$	0	1	$\cdot$	0	1
0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	1	0	0	1	0	1

$(T_3,+)$	0	1	$\cdot$	0	1	$(T_4,+)$	0	1	$\cdot$	0	1
0	0	0	0	0	0	0	0	0	0	1	1
1	0	1	1	0	0	1	0	1	1	1	1

$(T_5,+)$	0	1	$\cdot$	0	1	$(T_6,+)$	0	1	$\cdot$	0	1
0	0	0	0	0	1	0	0	0	0	0	0
1	0	1	1	1	1	1	0	1	1	0	1

$(T_7,+)$	0	1	$\cdot$	0	1	$(T_8,+)$	0	1	$\cdot$	0	1
0	0	1	0	0	0	0	0	1	0	0	0
1	1	0	1	0	0	1	1	0	1	0	1

groups, then $V(G_1)$ and $V(G_2)$ are non-isomorphic semirings. Thus a classification of finite, additively commutative, c-simple semirings up to isomorphism would require a classification of finite groups.

2. Basic results

The goal of this section is to derive some basic structure information for finite, additively commutative, c-simple semirings.

Lemma 6. *Let S be a finite, additively commutative, c-simple semiring. If the multiplication table of S has two identical rows* (*columns*), *then one of the following holds*:

(1) *there exists $c \in S$ such that $xy = c$ for all $x, y \in S$*;
(2) $|S| = 2$.

Proof. Observe that the relation $\sim$ defined by

$$x \sim y \quad \text{if} \quad xz = yz \quad \text{for all } z \in S$$

is a congruence relation. By assumption, there exist $r_1 \neq r_2$ such that $r_1 z = r_2 z$ for all $z \in S$ so $\sim = S \times S$. Thus

$$xz = yz \quad \text{for all } x, y, z \in S. \tag{1}$$

Suppose that $(S, \cdot)$ is not left-cancellative. Then there exist $a, b, c, d \in S$ such that $da = db = c$ and $a \neq b$. But $xa = ya$, $xb = yb$ for all $x, y \in S$. Hence $da = ya$, $db = yb$ and so $ya = yb = c$ for all $y \in S$. Consider now the congruence relation $\approx$ defined by

$$x \approx y \quad \text{if} \quad zx = zy \quad \text{for all } z \in S.$$

Since $a \neq b$ and $a \approx b$, it follows that $\approx = S \times S$, whence $zx = zy$ for all $x, y, z \in S$. Then for all $x, y \in S$ we have $xy = xa = da = c$.

Suppose now that $(S, \cdot)$ is left-cancellative. Fix $x \in S$ and let $z = x^2$. Then $xz = zx$. But $yz = xz$ and $yx = zx$ for all $y \in S$, so $yz = yx$. By left-cancellation, $x^2 = z = x$, so S is multiplicatively idempotent. Furthermore, for all $w \in S$ $w + w = w^2 + w^2 = (w + w)w = w^2 = w$, so S is additively idempotent. We will now show, by contradiction, that $|S| \leqslant 2$.

Suppose $|S| = n > 2$. For each nonempty subset $A \subseteq S$ let

$$\sigma_A = \sum_{x \in A} x$$

and $\sigma = \sigma_S$. Suppose that $A \subset S$ with $|A| = n - 1$. Consider the relation $\sim = \mathrm{id}_S \cup \{(\sigma_A, \sigma), (\sigma, \sigma_A)\}$. Clearly, $\sim$ is an equivalence relation. Since $(S, \cdot)$ is idempotent, Eq. (1) implies that for each $c \in S$,

$$c\sigma_A = \sigma_A\sigma_A = \sigma_A \quad \text{and} \quad c\sigma = \sigma\sigma = \sigma.$$

Thus, $c\sigma_A \sim c\sigma$. Similarly,

$$\sigma_A c = c^2 = c \quad \text{and} \quad \sigma c = c^2 = c$$

so that $\sigma_A c \sim \sigma c$. Since $(S, +)$ is idempotent, $\sigma + c = \sigma$ and

$$\sigma_A + c = \begin{cases} \sigma_A, & \text{if } c \in A, \\ \sigma, & \text{otherwise.} \end{cases}$$

Thus $\sim$ is a congruence relation. Since $|S| > 2$, it must be the case that $\sim = \mathrm{id}_S$, so $\sigma_A = \sigma$ for all proper $A \subset S$ with $|A| = n - 1$.

By induction, we will now show that $\sigma_A = \sigma$ for any nonempty subset $A \subseteq S$. Suppose this is known to hold for all A with $|A| = k \geqslant 2$. Let $A \subset S$ with $|A| = k - 1$ and again consider the relation

$$\sim = \mathrm{id}_S \cup \bigl\{(\sigma_A, \sigma), (\sigma, \sigma_A)\bigr\}.$$

As above, $\sim$ is a multiplicative equivalence relation. Furthermore,

$$\sigma_A + c = \begin{cases} \sigma_A, & \text{if } c \in A, \\ \sigma_{A \cup \{c\}}, & \text{otherwise.} \end{cases}$$

But $c \notin A$ implies $|A \cup \{c\}| = k$, so $\sigma_{A \cup \{c\}} = \sigma$ by the inductive assumption. Thus $\sim$ is again a congruence relation. Since $\sim \neq S \times S$, it follows that $\sim = \mathrm{id}_S$, so $\sigma_A = \sigma$.

In particular, this shows that for each $w \in S$, $w = \sigma_{\{w\}} = \sigma$, a contradiction. Thus $|S| = 2$.

It only remains to see that the same statement holds if “rows” is replaced by “columns.” If S has two identical columns, consider the reciprocal semiring $(S', +, \otimes)$ defined by $(S', +) = (S, +)$ and $x \otimes y = yx$. This semiring is c-simple and has two identical rows so the above argument applies. $\square$

Lemma 7. *Let S be a finite, additively commutative, c-simple semiring. Then one of the following holds*:

- $(S, +)$ *is a group, hence* $(S, +, \cdot)$ *is a ring*;
- S *has an additively absorbing element* α.

Proof. Consider the relation $\sim$ defined by

$$x \sim y \quad \text{if} \quad x + t = y + t \quad \text{for some } t \in S.$$

It is easy to see that $\sim$ is a congruence relation. If $\sim = \mathrm{id}_S$, then $(S, +)$ is cancellative, hence a group. It follows easily that $(S, +, \cdot)$ is a ring. On the other hand, suppose $\sim = S \times S$. Then for all $x, y \in S$ there exists $t_{x,y} \in S$ such that $x + t_{x,y} = y + t_{x,y}$. Set

$$\sigma = \sum_{x \in S} x \quad \text{and} \quad \alpha = \sigma + \sigma.$$

For $x, y \in S$ there exists $\sigma' \in S$ such that $\sigma = t_{x,y} + \sigma'$. Then

$$x + \sigma = x + t_{x,y} + \sigma' = y + t_{x,y} + \sigma' = y + \sigma.$$

In particular, $x + \sigma = \sigma + \sigma$ for all $x \in S$. Thus, for all $x \in S$,

$$x + \alpha = x + \sigma + \sigma = (\sigma + \sigma) + \sigma = \sigma + \sigma = \alpha. \qquad \square$$

Theorem 8. *Let S be a finite, additively commutative, c-simple semiring. Then one of the following holds*:

- $(S, +, \cdot)$ *is a ring*;
- S *has an infinity*;
- S *is additively idempotent.*

Proof. With respect to Lemma 7, one may assume that there is an additively absorbing element $\alpha \in S$. Consider the relation T defined by

$$x \, T \, y \quad \text{if} \quad 2x = 2y.$$

Then T is a congruence relation, whence $T = \mathrm{id}_S$ or $T = S \times S$.

Case I: Suppose $T = S \times S$. Then for all $x \in S$, $x + x = \alpha + \alpha = \alpha$. Thus, $x\alpha = x(\alpha + \alpha) = x\alpha + x\alpha = \alpha$. Similarly, $\alpha x = \alpha$ so α is an infinity.

Case II: Suppose $T = \mathrm{id}_S$. Consider the congruence relation $\sim$ defined by $x \sim y$ if there exist $u, v \in S \cup \{o\}$ and $i \geqslant 0$ such that

$$2^i x = y + u, \qquad 2^i y = x + v.$$

Then $2(2x) = (x) + 3x$ and $2(x) = (2x) + o$, so $x \sim 2x$ for all $x \in S$. If $\sim = \mathrm{id}_S$, then $x = 2x$ for all $x \in S$, whence $(S, +)$ is idempotent. Suppose now that $\sim = S \times S$ and let $x \in S$. Then $x\alpha \sim \alpha$, so there exists $v \in S \cup \{o\}$ and $i \geqslant 0$ such that $2^i x\alpha = \alpha + v = \alpha$. Then

$$x\alpha = x(2^i \alpha) = 2^i x\alpha = \alpha,$$

so $x\alpha = \alpha$. Similarly, $\alpha x = \alpha$ so α is an infinity. □

Corollary 9. *If S is a finite, additively commutative, c-simple semiring with zero then one of the following holds*:

- $S \cong \mathrm{Mat}_n(\mathbb{F}_q)$ *for some $n \geqslant 1$ and some finite field $\mathbb{F}_q$*;
- *S is a zero-multiplication ring ($S^2 = \{0\}$) of prime order*;
- *S is additively idempotent.*

3. The ∞ case

In this section, we show that a finite, additively commutative, c-simple semiring with ∞ is either additively idempotent, has trivial addition, or has order 2.

Lemma 10. *Let S be a finite, additively commutative, c-simple semiring with ∞ and $|S| > 2$. Then one of the following holds*:

(1) *S is additively idempotent*;
(2) *$S + S = \{\infty\}$ and $(S, \cdot)$ is a congruence-free semigroup.*

Proof. Consider the congruence relation defined by

$$x \; T \; y \quad \text{if} \quad 2x = 2y.$$

Case I: $T = \mathrm{id}_S$. Then $2x = 2y$ iff $x = y$. Set $x \sim y$ if there exists $i \geqslant 0$ and $u, v \in S \cup \{o\}$ such that

$$2^i x = y + u, \qquad 2^i y = x + v.$$

Then $\sim$ is a congruence relation and $x \sim 2x$ for all $x \in S$. But $x \nsim \infty$ for $x \neq \infty$, so $\sim \neq S \times S$. Thus, $\sim = \mathrm{id}_S$, and so S is additively idempotent.

Case II: $T = S \times S$. Then $x + x = \infty$ for all $x \in S$. For $\emptyset \neq A \subseteq S$, let

$$\sigma_A = \sum_{x \in A} x.$$

Let $N = |S|$ and suppose that $|A| = N - 1$. Then for every $c \in S$, $\sigma_A + c = \infty$, since $c \in A$, $c = \infty$, or $\sigma_A = \infty$. Furthermore,

$$c\sigma_A = \sum_{x \in A} cx = \begin{cases} \infty, & \text{if } cx_1 = cx_2 \text{ for some distinct } x_1, x_2 \in A, \\ \sigma_A, & \text{otherwise.} \end{cases}$$

Similarly, $\sigma_A c = \infty$ or $\sigma_A c = \sigma_A$. Thus, $\mathcal{B} = \{\sigma_A \mid A \subset S \text{ with } |A| = N - 1\}$ is a bi-ideal. Furthermore, $\infty \in A$ implies $\sigma_A = \infty$. Thus, $|\mathcal{B}| \leqslant 2$ and so $\mathcal{B} = S \Rightarrow |S| = 2$, a contradiction. Thus $\mathcal{B} = \{\infty\}$, so $\sigma_A = \infty$ for all $A \subset S$ with $|A| = N - 1$.

By induction, we will show that $\sigma_A = \infty$ for all $A \subset S$ with $|A| = 2$. Assume $\sigma_A = \infty$ for all $A \subset S$ with $|A| = k + 1 > 2$.

Suppose now that $A \subset S$ with $|A| = k \geqslant 2$. Then for $c \in S$,

$$\sigma_A + c = \begin{cases} \infty, & \text{if } c \in A, \\ \sigma_{A \cup \{c\}}, & \text{otherwise.} \end{cases}$$

By assumption, if $c \notin A$ then $\sigma_{A \cup \{c\}} = \infty$, so $\sigma_A + c = \infty$ for all $c \in S$. Also

$$c\sigma_A = \sum_{x \in A} cx = \begin{cases} \infty, & \text{if } cx_1 = cx_2 \text{ for some distinct } x_1, x_2 \in A, \\ \sigma_B, & \text{for some } |B| = k \text{ otherwise.} \end{cases}$$

The same is easily seen to hold for $\sigma_A c$. Observe that $\sigma_X = \infty$ for some $X \subset S$ with $|X| = k$, so

$$\mathcal{B} = \left\{\sigma_A \;\middle|\; A \subset S \text{ with } |A| = k\right\}$$

is a bi-ideal of S.

Case (i): $\mathcal{B} = \{\infty\}$. Then $\sigma_A = \infty$ for all $A \subset S$ with $|A| = k$, so we may apply the induction and conclude that $\sigma_A = \infty$ for all $A \subset S$ with $|A| = 2$. Thus, $x + y = \infty$ for all $x, y \in S$.

Case (ii): $\mathcal{B} = S$. We will show directly that $x + y = \infty$ for all $x, y \in S$. By assumption this holds for $x = y$, so suppose $x \neq y$. Then there exist $A_1, A_2 \subset S$ with $|A_1| = |A_2| = k$ and $\sigma_{A_1} = x$, $\sigma_{A_2} = y$,

$$A_1 \cap A_2 \neq \emptyset \quad \Rightarrow \quad x + y = \sigma_{A_1} + \sigma_{A_2} = \infty,$$
$$A_1 \cap A_2 = \emptyset \quad \Rightarrow \quad x + y = \sigma_{A_1} + \sigma_{A_2} = \sigma_{A_1 \cup A_2}.$$

But $|A_1 \cup A_2| > k$. In particular, either $|A_1 \cup A_2| = k + 1$ or there exist $\emptyset \neq B_1, B_2 \subset S$ with $|B_1| = k + 1$, $B_1 \cap B_2 = \emptyset$ and $B_1 \cup B_2 = A_1 \cup A_2$. By assumption, $\sigma_{B_1} = \infty$ and we have

$$x + y = \sigma_{A_1 \cup A_2} = \sigma_{B_1 \cup B_2} = \sigma_{B_1} + \sigma_{B_2} = \infty + \sigma_{B_2} = \infty.$$

Thus $x + y = \infty$ for all $x, y \in S$. Finally, note that since $S + S = \{\infty\}$, any nontrivial congruence relation on $(S, \cdot)$ is also a nontrivial congruence relation on $(S, +, \cdot)$, whence $(S, \cdot)$ is a congruence-free semigroup. □

The following is [3, Theorem 3.7.1].

Theorem 11. *Let $I = \{1, 2, \ldots, m\}$, $\Lambda = \{1, 2, \ldots, n\}$, and $P = (p_{ij})$ be an $n \times m$ matrix of 1's and 0's such that no row or column is identically zero, no two rows are identical, and no two columns are identical. Let $S = (I \times \Lambda) \cup \{\infty\}$ and define a binary relation on S by*

$$(i, \lambda) \cdot (j, \mu) = \begin{cases} (i, \mu) & \text{if } p_{\lambda j} = 1, \\ \infty & \text{otherwise}, \end{cases} \qquad (i, \lambda) \cdot \infty = \infty \cdot (i, \lambda) = \infty \cdot \infty = \infty.$$

Then S is a congruence-free semigroup of order $mn + 1$. Conversely, every finite congruence-free semigroup with an absorbing element is isomorphic to one of this kind.

4. Main theorem

Theorem 12. *Let S be a finite, additively commutative, congruence-simple semiring. Then one of the following holds*:

(1) $|S| \leqslant 2$;
(2) $S \cong \mathrm{Mat}_n(\mathbb{F}_q)$ *for some finite field* $\mathbb{F}_q$ *and some* $n \geqslant 1$;
(3) *S is a zero multiplication ring of prime order*;
(4) *S is additively idempotent*;
(5) *$(S, \cdot)$ is a semigroup as in Theorem 11 with absorbing element $\infty \in S$ and $S + S = \{\infty\}$.*

Proof. Apply Theorems 8 and 11, Lemma 10, and Corollary 9. Also notice that if $(S, \cdot)$ is a semigroup as in Theorem 11, and we define $S + S = \{\infty\}$, then $(S, +, \cdot)$ is necessarily congruence-free. □

Observe the similarity between this theorem and Theorem 5. Recall that for a finite group G, $V(G)$ is a finite, additively commutative, c-simple semiring and is additively idempotent. So the semirings $V(G)$ do fall into the fourth case of Theorem 12. Note also that for $n > 1$, the matrix semiring $\mathrm{Mat}_n(V(G))$ is not c-simple. To see this, consider a matrix with all but one entry equal to infinity, and apply Lemma 6. In view of this,

Table 2
A c-simple semiring of order 3

+	a	1	b
a	a	1	b
1	1	1	b
b	b	b	b

·	a	1	b
a	a	a	b
1	a	1	b
b	a	b	b

it might be tempting to conjecture that the additively idempotent semirings are precisely those of the form $V(G)$. However, the semiring in Table 2 provides a counter-example to that conjecture. This semiring is additively idempotent yet has order 3 and is not of the form $V(G)$. At present, we have no strongly supported conjecture for a meaningful description of the semirings in the fourth case of Theorem 12, though we do believe that some good description might be possible.

Acknowledgments

The author thanks the anonymous referee for his/her careful reading and valuable input which greatly increased the quality of this work. This research was supported by a fellowship from the Center for Applied Mathematics at the University of Notre Dame, and in part by NSF grant DMS-00-72383.

References

[1] R. El Bashir, J. Hurt, A. Jančařék, T. Kepka, Simple commutative semirings, J. Algebra 236 (2001) 277–306, doi:10.1006/jabr.2000.8483.
[2] U. Hebisch, H.J. Weinert, Semirings and semifields, in: Handbook of Algebra, Vol. 1, Elsevier, Amsterdam, 1996.
[3] J. Howie, Fundamentals of Semigroup Theory, Oxford Univ. Press, Oxford, 1995.
[4] H.S. Vandiver, Note on a simple type of algebra in which the cancellation law of addition does not hold, Bull. Amer. Math. Soc. 40 (1934) 916–920.