Acta Sci. Math. 46 (1983), 17—27

Simple semimodules over commutative semirings

J. JEŽEK and T. KEPKA

The problem of describing all simple medial groupoids (and so all minimal varieties of medial groupoids) is still open, although simple groupoids and minimal varieties are described in various special subclasses (see e.g. [2], [3], [4], [5]; in a yet unpublished paper the authors described all finite simple medial groupoids and all simple commutative medial groupoids). It turns out that for the solution of this problem it is advantageous to have a description of all simple commutative semigroups with two commuting endomorphisms at hand. Now, commutative semigroups with a family of commuting endomorphisms are actually nothing else than semimodules over commutative semirings. For this reason the authors became interested in simple semimodules over commutative semirings. Moreover, the problem of simple semimodules deserves a special attention, and this is why the present paper came to life.

Section 1 contains the basic definitions. In Section 2 we prove that the class of simple semimodules over a commutative semiring can be divided into three subclasses:

(1) two-element semimodules with zero addition;

(2) simple cancellative semimodules;

(3) simple idempotent semimodules.

In Section 3 we describe the two-element semimodules with zero addition and in Section 4 the simple cancellative semimodules (at least in the case when the commutative semiring is finitely generated or, more generally, finitely c-generated). We do not know all simple idempotent semimodules. However, in Section 5 we characterize all simple idempotent semimodules with a zero element o such that $\{o\}$ is a subsemimodule; in particular, all finite simple idempotent semimodules are found. Further, we repeat from [6] the description of simple idempotent semimodules over a commutative semiring with at most two generators. Finally, in Section 6 we give a formula for the number of isomorphism classes of m-element semimodules over the free commutative semiring with n generators (n, m are finite).

Received June 24, 1981.

1. Preliminaries

By a commutative semiring we mean an algebra $R=R(+, \cdot)$ with two binary operations such that $R(+)$ and $R(\cdot)$ are commutative semigroups and $x(y+z)=xy+xz$ for all $x, y, z\in R$. Throughout this paper let R be a commutative semiring.

By a (left $R-$) semimodule we mean an algebra $M=M(+, rx)$ with one binary operation $+$ and a family of unary operations $x\mapsto rx$ $(r\in R)$ such that $M(+)$ is a commutative semigroup and

$$r(x+y)=rx+ry, \quad (r+s)x=rx+sx, \quad rs\cdot x=r\cdot sx$$

for all $x, y\in M$ and $r, s\in R$.

A semimodule M is said to be

— trivial if $\mathrm{Card}\,(M)=1$,

— idempotent if it satisfies the identity $x+x=x$ (i.e., if $M(+)$ is a semilattice; in this case we write $x\leqq y$ iff $x=x+y$),

— a semimodule with zero addition if it satisfies the identity $x+y=u+v$,

— cancellative if $x+y=x+z$ implies $y=z$,

— a module if $M(+)$ is a group,

— simple if id_M and $M\times M$ are the only congruences 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.

By a bi-ideal of a semimodule M we mean a non-empty subset I of M such that $M+I\subseteqq I$ and $RI\subseteqq I$. The equivalence $(I\times I)\cup\mathrm{id}_M$ is then a congruence of M and we denote by M/I the corresponding factor semimodule. If M is simple, then every bi-ideal of M is either at most one-element or equal M.

An element a of a semimodule M is said to be the neutral element (the zero element, resp.) of M if $x+a=x$ ($x+a=a$, resp.) for all $x\in M$. The neutral element is usually denoted by 0 and the zero element by o.

For some results on semimodules with a neutral element over a commutative semiring with a neutral and a unit element see, e.g., [1].

For a semimodule M, put $\mathrm{Ann}\,(M)=\{r\in R; rx=ry \text{ for all } x, y\in M\}$. If $\mathrm{Ann}\,(M)$ is non-empty, then this set is evidently an ideal of R and there exists an element $e\in M$ such that $e=e+e=re=sx$ for all $r\in R$, $s\in\mathrm{Ann}\,(M)$ and $x\in M$; the set $\{e\}$ is a subsemimodule of M.

1.1. Lemma. *Let M be a simple semimodule with $\mathrm{Ann}\,(M)\neq\emptyset$. Then the element e with $sx=e$ for all $s\in\mathrm{Ann}\,(M)$ is either a neutral or a zero element of M.*

Proof. The set $\{e+x; x\in M\}$ is a bi-ideal of M containing e, so that it equals either $\{e\}$ or M. In the first case evidently e is a zero element. If $\{e+x; x\in M\}=M$ then it is easy to verify that e is a neutral element.

A subsemiring S of R is said to be a closed subsemiring if $b\in S$ whenever $a+b\in S$ for some $a\in S$. Let K be a non-empty subset of R. We shall say that R is c-generated by K if R is the only closed subsemiring of R containing K.

For every non-empty set X there exists the free commutative semiring over X; its elements are the formal sums of elements of the free commutative (multiplicatively denoted) semigroup over X. If R is a free semiring over a set X of cardinality $k\geqq 1$, then the variety of R-semimodules is equivalent to the variety of algebras $A(+, f_1, \ldots, \ldots, f_k)$ such that $A(+)$ is a commutative semigroup and $f_1, \ldots, f_k$ are pairwise commuting endomorphisms of $A(+)$.

Let f be a homomorphism of a semiring S onto a semiring R. Then for any R-semimodule M we can define an S-semimodule structure on M by $sx=f(s)\cdot x$ (for all $s\in S$ and $x\in M$). This correspondence provides an equivalence between the variety of R-semimodules and some subvariety of the variety of S-semimodules. Since every semiring is a homomorphic image of some free semiring, it follows that in order to describe all simple semimodules over arbitrary (commutative) semirings it would suffice to describe all simple semimodules over free (commutative) semirings.

2. The fundamental classification theorem

2.1. Theorem. *Let M be a non-trivial simple semimodule over R. Then exactly one of the following conditions holds:*

(1) *M is a two-element semimodule with zero addition;*

(2) *M is cancellative;*

(3) *M is idempotent.*

Proof. If Card $(M)=2$, then everything is clear. Now we shall assume that Card $(M)\geqq 3$. The rest of the proof will be divided into several lemmas.

2.2. Lemma. *M is not a semimodule with zero addition.*

Proof. Suppose, on the contrary, that there exists an element o such that $x+y=o$ for all $x, y\in M$. We have $ro=r(o+o)=ro+ro=o$ for all $r\in R$. If $r\in R$, then Ker (L_r), where $L_r(x)=rx$ for all $x\in M$, is a congruence of M; since M is simple, it follows that either L_r is injective or $rx=o$ for all $x\in M$. From this it follows that $((M\setminus\{o\})\times(M\setminus\{o\}))\cup \mathrm{id}_M$ is a congruence of M; since M is simple, Card $(M)\leqq 2$, a contradiction.

A semimodule M is said to be unipotent if $x+x=y+y$ for all $x, y\in M$.

2.3. Lemma. *Suppose that M is unipotent; put $o=x+x$ for all $x\in M$. Then either M is cancellative or $x+o=o$ for all $x\in M$.*

Proof. Put $f(x)=x+x+x$ for all $x\in M$. Then f is an endomorphism of M and we have either $\mathrm{Ker}(f)=M\times M$ or $\mathrm{Ker}(f)=\mathrm{id}_M$. If $\mathrm{Ker}(f)=M\times M$ then $x+o=f(x)=f(o)=o$ for all $x\in M$. Let $\mathrm{Ker}(f)=\mathrm{id}_M$ and $a+c=b+c$ for some $x, b, c\in M$. Then $f(a)=a+o=a+c+c=b+c+c=b+o=f(b)$ and so $a=b$.

2.4. Lemma. *Suppose that M is unipotent. Then M is cancellative.*

Proof. Suppose, on the contrary, that M is not cancellative. Put $o=x+x$ for all $x\in M$. By 2.3, $x+o=o$ for all $x\in M$.

Suppose that $a=b+c\neq o$ for some $a, b, c\in M$. Put $M^*=M\cup\{0\}$ and $I=\{x+a;\ x\in M^*\}\cup\{x+ra;\ x\in M^*, r\in R\}$, where $0+a=a$. Then I is a bi-ideal of M containing $\{a, o\}$ and so $I=M$. In particular, $b\in I$ and $c\in I$. We shall consider only the case when $b=x+ra$ and $c=y+sa$ for some $x, y\in M^*$ and $r, s\in R$. (The remaining three cases are similar.) Then $a=b+c=z+ra+sa$ where $z=x+y\in M^*$ and therefore $a=z+r(z+ra+sa)+s(z+ra+sa)=z+rz+sz+r^2a+s^2a+rsa+sra=$ $=z+rz+sz+r^2a+s^2a+o=o$, a contradiction.

We have proved that M is a semimodule with zero addition. However, this is in contradiction with 2.2.

2.5. Lemma. *Suppose that M is not unipotent. Then M is either idempotent or cancellative.*

Proof. Put $g(x)=x+x$ for all $x\in M$. Then g is an endomorphism of M; since M is simple and not unipotent, g is injective. From this it follows that M can be embedded into a simple semimodule M' in which the mapping $x\mapsto x+x$ is an automorphism; since subsemimodules of idempotent semimodules are idempotent and subsemimodules of cancellative semimodules are cancellative, it is enough to proceed under the assumption that g is an automorphism of M. Put $M^*=M\cup\{0\}$ and define a binary relation H on M by $(x, y)\in H$ iff $x=u+g^i(y)$ and $y=v+g^j(x)$ for some $u, v\in M^*$ and some integers $i, j\leqq 0$ (if $j<i$ then $x=u+g^i(y)=u+g^{i-1}(y)+g^{i-1}(y)=$ $=z_1+g^{i-1}(y)=\ldots=z_{i-j}+g^j(y)$; similarly if $i<j$, and thus we can assume that $i=j$). Obviously, H is an equivalence. Let $x, y, z\in M$, $u, v\in M^*$, $k\leqq 0$, $x=u+g^k(y)$, $y=v+g^k(x)$. Then $z=g^{-k}g^k(z)=w+g^k(z)$ for some $w\in M^*$ and we have $x+z=$ $=u+w+g^k(y+z)$ and $y+z=v+w+g^k(x+z)$. Moreover, $rx=rx+g^k(ry)$ and $ry=rv+g^k(rx)$. We have shown that H is a congruence of M.

If $H=\mathrm{id}_M$ then M is idempotent, since $g(x)=x+g^0(x)$ and $x=0+g^{-1}(g(x))$ imply $(x, g(x))\in H$ for all $x\in M$.

Let $H\neq\mathrm{id}_M$, so that $H=M\times M$. Let $a+c=b+c$ for some $a, b, c\in M$. Put $N=\{x\in M;\ a+x=b+x\}$. If $x\in N$, then $g(a+g^{-1}(x))=a+a+x=a+b+x=$ $=b+b+x=g(b+g^{-1}(x))$, so that $a+g^{-1}(x)=b+g^{-1}(x)$ and consequently

$g^{-1}(x)\in N$. Now, let $y\in M$. We have $c\in N$, $(c, y)\in H$ and so $y=z+g^k(c)$ for some $z\in M^*$ and $k\geqq 0$. But $g^k(c)\in N$ and so $a+y=a+g^k(c)+z=b+g^k(c)+z=b+y$, i.e., $y\in N$. We have proved $N=M$. In particular, $g(a)=a+a=a+b=b+b=g(b)$, $a=b$, and M is cancellative.

3. Two-element semimodules with zero addition

Denote by $\mathrm{IND}_1(R)$ the set of all subsets I of R with the following properties:
(1) $R+R\subseteq I$;
(2) $RI\subseteq I$;
(3) if $r, s\in R\setminus I$ then $rs\in R\setminus I$.
For every $I\in\mathrm{IND}_1(R)$ define a semimodule $Z_{R,I}$ as follows: $Z_{R,I}=\{0, 1\}$; $x+y=0$; if $r\in I$ then $rx=0$; if $r\in R\setminus I$ then $rx=x$.

3.1. Theorem. *The semimodules $Z_{R,I}$ with $I\in\mathrm{IND}_1(R)$ are pairwise non-isomorphic two-element semimodules with zero addition; every two-element semimodule with zero addition is isomorphic to one of them.*

Proof. Easy.

3.2. Proposition. *Let R be a free commutative semiring over a set K of cardinality $\alpha\geqq 1$. Then* $\mathrm{Card}\,(\mathrm{IND}_1(R))=2^\alpha$.

Proof. It is easy to verify that the mapping $I\mapsto I\cap K$ is a one-to-one mapping of $\mathrm{IND}_1(R)$ onto the set of all subsets of K.

It follows that if R is a commutative semiring which can be generated by a set of cardinality $\alpha\geqq 1$ then $1\leqq\mathrm{Card}\,(\mathrm{IND}_1(R))\leqq 2^\alpha$. If R contains a neutral element then $\mathrm{Card}\,(\mathrm{IND}_1(R))=1$.

4. Simple cancellative semimodules

4.1. Lemma. *Let M be a cancellative semimodule. Then there exists a unique (up to isomorphism over M) module N such that M is a subsemimodule of N and $N=\{a-b;\ a, b\in M\}$. Moreover, if M is simple then N is also simple.*

Proof. Define a binary relation H on $M\times M$ by $((a, b), (c, d))\in H$ iff $a+d=b+c$. Then H is a congruence of the semimodule $M\times M$. Put $N=(M\times M)/H$ and denote by g the corresponding natural homomorphism. We have $g(a, a)=g(b, b)=0$ for all $a, b\in M$ and 0 is a neutral element of N. Moreover, $g(a, b)+g(b, a)=0$ and we see that N is a module. The mapping $a\mapsto g(a+a, a)$ is an injec-

tive homomorphism of M into N and we can identify any element $a\in M$ with the element $g(a+a, a)$ of N. The rest is easy.

4.2. Lemma. *Let M be a module. Then M is simple iff $\{0\}$ and M are the only submodules of M.*

Proof. Easy.

4.3. Lemma. *Let M be a simple cancellative semimodule having a neutral element 0. Then M is a module.*

Proof. Denote by N the set of all $a\in M$ such that $a+b=0$ for some $b\in M$. Then N is a subsemimodule of M and the relation H on M, defined by $(x, y)\in H$ iff $x+N=y+N$, is a congruence of $M(+)$; let us prove that it is a congruence of the semimodule M. For this, it is enough to show that if $x+N=y+N$, $r\in R$ and $a\in N$, then $rx+a\in ry+N$. We have $x+a=y+b$ and $ra+c=0$ for some $b, c\in N$; we have $rx+a=rx+ra+c+a=r(x+a)+c+a=r(y+b)+c+a=ry+rb+c+a\in ry+N$. It follows that H is a congruence of the semimodule M. Since M is simple, either $H=M\times M$ or $H=\mathrm{id}_M$. If $H=M+M$, then $N=M$, M is a module and we are through. Let $H=\mathrm{id}_M$, so that $N=\{0\}$. Put $K=((M\setminus\{0\})\times(M\setminus\{0\}))\cup\mathrm{id}_M$. Let us prove that K is a congruence of M. Evidently, K is a congruence of $M(+)$. Let $x, y\in M\setminus\{0\}$ and $r\in R$. Since M is simple, the kernel of the endomorphism $x\mapsto rx$ equals either $M\times M$ or id_M; since $r0=0$, it follows that either $rz=0$ for all $z\in M$ or $x\mapsto rx$ is injective; from this it follows that $(rx, ry)\in K$. Since M is simple, it follows that $K=\mathrm{id}_M$ and M contains just two elements; thus M is a module.

4.4. Theorem (The description of simple modules).

(1) *Let f be a homomorphism of the semiring R into a field F such that $F=\{a-b+c\cdot 1;\ a, b\in f(R)\cup\{0\},\ c\in Z\}$ where Z denotes the set of integers. Then F is a simple R-module (if we put $rx=f(r)x$).*

(2) *Every non-trivial simple R-module can be constructed in the way described in* (1).

(3) *Let f and g be homomorphisms of R into fields F and G, resp., such that $F=\{a-b+c\cdot 1;\ a, b\in f(R)\cup\{0\},\ c\in Z\}$ and $G=\{a-b+c\cdot 1;\ a, b\in g(R)\cup\{0\},\ c\in Z\}$. Then the R-semimodules, F, G are isomorphic iff there is a field isomorphism h of F onto G such that $h(f(r))=g(r)$ for all $r\in R$.*

Proof. (1) Evidently, every submodule of the R-module F is an ideal of the field F and we can use 4.2.

(2) Let M be a non-trivial simple R-module. Denote by F the set of endomorphisms of M and define two binary operations on F by $(\varphi+\psi)(x)=\varphi(x)+\psi(x)$ and $(\varphi\psi)(x)=\varphi(\psi(x))$. Evidently, F is a skew field. For every $r\in R$ denote by $f(r)$ the endomorphism $x\mapsto rx$, so that f is a homomorphism of R into F. Let us fix an

element $u \in M \setminus \{0\}$. For every $x \in F$ put $g(x) = x(u)$. It follows from 4.2 that g is an isomorphism of the R-module F onto the R-module M. Put $S = \{a - b + c \cdot 1;\ a, b \in f(R) \cup \{0\},\ c \in Z\}$. Then S is a submodule of F and $g(S) \neq \{0\}$. Consequently $g(S) = M$ and $S = F$. Now it is clear that F is commutative.

(3) Let k be a semimodule isomorphism of F onto G. Put $h(x) = k(x)(k(1))^{-1}$ for all $x \in F$. Then h is a field isomorphism with the desired property.

4.5. Theorem. *Let M be a non-trivial simple cancellative semimodule. Then there exist a field F and a homomorphism f of R into F such that $F = \{a - b + c \cdot 1;\ a, b \in f(R) \cup \{0\},\ c \in Z\}$, where Z denotes the set of integers, M is a subsemimodule of the R-module F and $F = \{a - b;\ a, b \in M\}$. Moreover, $M = F$ if $0 \in M$.*

Proof. Apply 4.1, 4.3 and 4.4.

4.6. Example. Denote by Q the field of rational numbers. Put $R_1 = \{x \in Q;\ x > 0\}$ and $R_2 = \{x \in Q;\ x \geqq 1\}$. Then R_1 and R_2 are commutative semirings. R_1 is a simple cancellative R_1-semimodule, $Q = \{a - b;\ a, b \in R_1\}$; R_2 is a cancellative R_2-semimodule, $Q = \{a - b;\ a, b \in R_2\}$, and R_2 is not simple.

4.7. Theorem. *Let R be finitely generated (or, more generally, finitely c-generated). Then every simple cancellative semimodule is a finite module of prime power order.*

Proof. Let f and F be as in 4.5. Since R is finitely c-generated, F is a finitely generated ring. However, then F is finite. Then evidently $0 \in M$ and $M = F$ by 4.5.

For every prime power p^n (i.e. every prime number p and every positive integer n) denote by $\mathrm{GF}(p^n)$ the finite field with p^n elements. For every prime power p^n and every positive integer m let $S(p, n, m)$ denote the set of ordered m-tuples $(a_1, \ldots, a_m)$ of elements of $\mathrm{GF}(p^n)$ such that $GF(p^n)$ is generated as a ring by the set $\{a_1, \ldots, a_m, 1\}$ (observe that this set is always non-empty). Define an equivalence $\sim$ on $S(p, n, m)$ by $(a_1, \ldots, a_m) \sim (b_1, \ldots, b_m)$ iff $b_1 = f(a_1), \ldots, b_m = f(a_m)$ for some automorphism f of $\mathrm{GF}(p^n)$.

4.8. Lemma. $\mathrm{Card}\,(S(p, n, m)/\sim) = (1/n) \sum_{k|n} \mu(n/k) p^{mk}$, *$\mu$ being the Möbius function.*

Proof. Well known and easy.

4.9. Proposition. *Let R be a free commutative semiring freely generated by a finite set of cardinality $m \geqq 1$. Let p^n be a prime power. Then the number of isomorphism classes of simple modules of order p^n equals $(1/n) \sum_{k|n} \mu(n/k) p^{mk}$.*

Proof. It follows from 4.4 and 4.8.

5. Simple idempotent semimodules

Denote by $\mathrm{IND}_2(R)$ the set of all subsets I of R with the following properties:

(1) $R+I\subseteq I$;

(2) $RI\subseteq I$;

(3) if $r, s\in R\setminus I$ then $r+s\in R\setminus I$;

(4) if $r, s\in R\setminus I$ then $rs\in R\setminus I$.

For every $I\in\mathrm{IND}_2(R)$ define a semimodule $X_{R,I}$ as follows: $X_{R,I}=\{0, 1\}$; $0+0=0+1=1+0=0$; $1+1=1$; if $r\in I$ then $rx=0$; if $r\in R\setminus I$ then $rx=x$.

Denote by $\mathrm{IND}_3(R)$ the set of all non-empty subsets I of R with the following properties:

(1) $I+I\subseteq I$;

(2) $RI\subseteq I$;

(3) if $r, s\in R$ and $s\notin I$ then $r+s\notin I$;

(4) if $r, s\in R\setminus I$ then $rs\in R\setminus I$.

For every $I\in\mathrm{IND}_3(R)$ define a semimodule $Y_{R,I}$ as follows: $Y_{R,I}=\{0, 1\}$; $0+0=0+1=1+0=0$; $1+1=1$; if $r\in I$ then $rx=1$; if $r\in R\setminus I$ then $rx=x$.

5.1. Theorem. *The semimodules $X_{R,I}$ with $I\in\mathrm{IND}_2(R)$ and the semimodules $Y_{R,I}$ with $I\in\mathrm{IND}_3(R)$ are pairwise non-isomorphic two-element idempotent semimodules; every two-element idempotent semimodule is isomorphic to one of them.*

Proof. Straightforward.

5.2. Proposition. *Let R be a free commutative semiring over a set K of cardinality $\alpha\geqq 1$. Then* $\mathrm{Card}\,(\mathrm{IND}_2(R))=2^\alpha$ *and* $\mathrm{Card}\,(\mathrm{IND}_3(R))=2^\alpha-1$.

Proof. Easy.

5.3. Theorem. *Let M be an idempotent semimodule with a zero element o such that $\{o\}$ is a subsemimodule of M; let* $\mathrm{Card}\,(M)\geqq 3$. *Then M is simple iff the following three conditions are satisfied:*

(1) *$a+b=0$ for all pairs $a, b\in M$ such that $a\neq b$;*

(2) *for every $r\in R$, the mapping $x\mapsto rx$ is either constant (with value o) or a permutation of M;*

(3) *if $x, y\in M\setminus\{o\}$ then $y=rx$ for some $r\in R$.*

Proof. First, let M be simple. For every $a\in M$ denote by K_a the set of all $x\in M$ such that $x\leqq ra$ (i.e. $x=x+ra$) for some $r\in R$. Evidently, K_a is a bi-ideal of M containing o, and so either $K_a=\{o\}$ or $K_a=M$. Put $L=\{a\in M;\ K_a=\{o\}\}$. Evidently, L is a bi-ideal of M, and so either $L=M$ or L contains at most one element.

If $L=M$ then M is a semimodule with zero multiplication; since M is simple, Card $(M)\leqq 2$, a contradiction. Hence Card $(L)\leqq 1$. Then evidently $L\subseteq\{o\}$ and so we have proved that if $a\in M\setminus\{o\}$ and $x\in M$ then $x\leqq ra$ for some $r\in R$.

Let $a, b, c\in M$ be such that $a+b\neq o$ and $b+c\neq o$. Then $b\neq o$ and, as we have just proved, there are elements $r, s\in R$ with $b\leqq r(a+b)$ and $b\leqq s(b+c)$. We have $b\leqq ra+rb\leqq rb\leqq rsb+rsc$ and $b\leqq sb+sc\leqq sb\leqq sra+srb$. Consequently, $b\leqq rs(a+b+c)$ and so $a+b+c\neq o$.

Define a relation H on M by $(x, y)\in H$ iff either $x=y$ or $x+y\neq 0$. Using the assertion proved above, it is easy to check that H is a congruence of M. Hence either $H=\mathrm{id}_M$ or $H=M\times M$. We get $H=\mathrm{id}_M$, and (1) is proved.

Let $r\in R$. The mapping $x\mapsto rx$ is an endomorphism of M, so that its kernel equals either id_M or $M\times M$. Hence the mapping $x\mapsto rx$ is either constant (with value o, since $ro=o$) or injective; if it is injective, then it is a permutation of M, since rM is evidently a bi-ideal of M. We have proved (2) and the assertion (3) is similar.

Now, let the conditions (1), (2), (3) be satisfied. Consider a congruence $H\neq\mathrm{id}_M$ of M. Put $L=\{x\in M\setminus\{o\};\ (x, o)\in H\}$. There is a pair $(a, b)\in H$ with $a\neq b$. We have $a+b=o$ and $(a, o)\in H$, $(b, o)\in H$. Hence L is non-empty. It follows from (3) that $L=M\setminus\{o\}$, so that $H=M\times M$.

5.4. Theorem. *Let M be a finite simple idempotent semimodule containing at least three elements. Then M contains a zero element o and $\{o\}$ is a subsemimodule of M (so that M is as in 5.3).*

Proof. Since M is a finite semilattice, it contains a zero element o. Suppose that Ann $(M)\neq\emptyset$ and the element e with $sx=e$ for all $s\in\mathrm{Ann}\,(M)$ is a neutral element of M. Then evidently $M\setminus\{e\}$ is a bi-ideal of M, so that it contains at most one element, contradicting Card $(M)\geqq 3$.

Hence e is either a zero element or Ann (M) is empty; in both these cases evidently $\{o\}$ is a subsemimodule.

In the rest of this section let R be the free commutative semiring over a set $\{f, g\}$ of cardinality 2. We shall give a list of all simple idempotent R-semimodules in this case. Denote by Z the set of integers and by E the set of real numbers. For every positive integer n denote by $Z_n(+)$ the cyclic group of integers modulo n, and ι_n the natural homomorphism of $Z(+)$ onto $Z_n(+)$. For every pair r, s of integers such that $(r, s)\neq(0, 0)$ denote by GCD(r, s) the greatest common divisor of r, s. The promised list is the following (denote here by $\wedge$ the binary semimodule operation):

(1) the semimodule U_1 with $U_1=\{0, 1\}$, $0\wedge 1=0$, $f(x)=x$, $g(x)=1$;

(2) the semimodule U_2 with $U_2=\{0, 1\}$, $0\wedge 1=0$, $f(x)=1$, $g(x)=x$;

(3) the semimodule U_3 with $U_3=\{0, 1\}$, $0\wedge 1=0$, $f(x)=g(x)=0$;

(4) the semimodule U_4 with $U_4=\{0, 1\}$, $0\wedge 1=0$, $f(x)=g(x)=1$;

(5) for any positive integer n, the semimodule A_n with $A_n=\{0, 1, \ldots, n\}$, $x\wedge y=x$ if $x=y$, $x\wedge y=0$ if $x\neq y$, $f(0)=0, f(1)=2, f(2)=3, \ldots, f(n-1)=n\, f(n)=1$, $g(x)=0$;

(6) for any positive integer n, the semimodule B_n with $B_n=\{0, 1, \ldots, n\}$, $x\wedge y=x$ if $x=y$, $x\wedge y=0$ if $x\neq y$, $f(x)=0$, $g(0)=0$, $g(1)=2$, $\ldots$, $g(n-1)=n$, $g(n)=1$;

(7) for every quadruple $z=(p, q, r, s)$ of integers such that $p, q, r\geqq 1$, $0\leqq s<r$ and $\mathrm{GCD}(r, s)=1$, the semimodule C_z with $C_z=\{0\}\cup\{Z_{rp}\times Z_{rq})/K_z$ where K_z is the subgroup $\{(\iota_{rp}(0), \iota_{rq}(0)), (\iota_{rp}(p), \iota_{rq}(-sq)), (\iota_{rp}(2p), \iota_{rq}(-2sq)), \ldots, (\iota_{rp}((r-1)p, \iota_{rq}(-(r-1)sq))\}$, $x\wedge y=x$ if $x=y$, $x\wedge y=0$ if $x\neq y$, $f(0)=g(0)=0$, $f(H)=H+(\iota_{rp}(1), \iota_{rq}(0))$ and $g(H)=H+(\iota_{rp}(0), \iota_{rq}(1))$ for all $H\in(Z_{rp}\times Z_{rq})/K_z$;

(8) for every pair $z=(n, m)$ of positive integers, the semimodule D_z with $D_z=\{0\}\cup(Z\times Z)/K_z$ where K_z is the subgroup of $Z(+)\times Z(+)$ generated by (n, m), $x\wedge y=x$ if $x=y$, $x\wedge y=0$ if $x\neq y$, $f(0)=g(0)=0$, $f(H)=H+(1, 0)$ and $g(H)=H+(0, 1)$ for all $H\in(Z\times Z)/K_z$;

(9) for every pair r, s of integers such that $\mathrm{GCD}(r, s)=1$ and either $r<0<s$ or $s<0<r$, the semimodule $E_{r,s}$ with $E_{r,s}=Z$, $x\wedge y=\mathrm{Min}(x, y)$, $f(x)=x+r$, $g(x)=x+s$;

(10) for every $u\in\{-1, 1\}$ and every irrational number q such that either $u<0<q$ or $q<0<u$, the semimodule $F_{u,q}$ with $F_{u,q}=E$, $x\wedge y=\mathrm{Min}(x, y)$, $f(x)=x+u$, $g(x)=x+q$;

(11) for every u, q as in (10), every subsemimodule of $F_{u,q}$.

As it is proved in [6], these R-semimodules, together with the trivial R-semimodule, are simple idempotent R-semimodules and every simple idempotent R-semimodule is isomorphic to one of them; the semimodules in (1)—(11) are pairwise non-isomorphic, with the following exception: if M_1 is a subsemimodule of F_{u_1,q_1} and M_2 is a subsemimodule of F_{u_2,q_2}, then $M_1\cong M_2$ iff $u_1=u_2$, $q_1=q_2$ and $M_2=M_1+a$ for some real number a.

6. The number of isomorphism classes of finite simple semimodules

Let R be the free commutative semiring over a set of finite cardinality $n\geqq 1$. For $m\geqq 1$, let $N(n, m)$ denote the number of isomorphism classes of simple R-semimodules having m elements.

Denote by $\alpha(n, k)$ the number of equivalences defined on an n-element set and having exactly k blocks. Denote by $\lambda(n, m)$ the number of isomorphism classes of m-element algebras $A(f_1, \ldots f_n)$ with unary operations f_i such that each f_i is a permutation of A, $f_i f_j=f_j f_i$ for all i, j and $f_i(x)\neq f_j(x)$ for all $i, j\in\{1, \ldots, n\}$, $i\neq j$, $x\in A$, and such that $A(f_1, \ldots, f_n)$ contains no proper subalgebra.

The following theorem can be derived from the above results.

6.1. Theorem. (1) $N(n, 1)=1$ *for every* $n\geqq 1$.

(2) $N(n, 2)=2^{n+2}-1$ *for every* $n\geqq 1$.

(3) $N(n, 3)=2\cdot 3^n-2^n$ *for every* $n\geqq 1$.

$$(4)\quad N(n, m)=\sum_{\substack{1\leqq k\leqq n\\ k+1\leqq m}}\alpha(n, k)\,\lambda(k, m-1)+\sum_{\substack{2\leqq t\leqq n\\ t\leqq m}}t\alpha(n, t)\,\lambda(t-1, m-1)$$

for every $n\geqq 1$ *and* $m\geqq 6$ *such that* m *is not a prime power.*

$$(5)\quad N(n, p^m)=\sum_{\substack{1\leqq k\leqq n\\ k+1\leqq p^m}}\alpha(n, k)\,\lambda(k, p^m-1)+\sum_{\substack{2\leqq t\leqq n\\ t\leqq p^m}}t\alpha(n, t)\,\lambda(t-1, p^m-1)+$$
$$+(1/m)\sum_{k|m}\mu(m/k)\,p^{nk}$$

for every prime number $p\geqq 2$ *and all integers* $n, m\geqq 1$ *such that* $p^m\geqq 3$.

The values $\lambda(1, m)$ and $\lambda(2, m)$ can be computed as follows:

$$\lambda(1, m)=1 \quad \text{for every } m\geqq 1;$$
$$\lambda(2, m)=-1+\sum_{\substack{1\leqq k\leqq m\\ k|m}}\varphi(k)\varepsilon(m/k) \quad \text{for every } m\geqq 1,$$

where φ denotes Euler's function and $\varepsilon(n)$ is the number of all $i\in\{1, \ldots, m\}$ such that i divides n.

As it follows from the results and remarks of this paper, every simple semimodule over a commutative semiring with at most two generators is of cardinality $\leqq 2^{\aleph_0}$. We shall end this paper with the following open problem.

Problem. Let R be a finitely generated (or countable) commutative semiring and let M be a simple R-semimodule. Is it true that Card $(M)\leqq 2^{\aleph_0}$?

References

[1] B. Csákány, Primitive classes of algebras which are equivalent to classes of semi-modules and modules (Russian), *Acta Sci. Math.*, **24** (1963), 157—164.

[2] B. Csákány, Varieties of affine modules, *Acta Sci. Math.*, **37** (1975), 3—10.

[3] B. Csákány and L. Megyesi, Varieties of idempotent medial quasigroups, *Acta Sci. Math.*, **37** (1975), 17—23.

[4] J. Ježek and T. Kepka, Atoms in the lattice of varieties of distributive groupoids in: *Lattice Theory* (Proc. Conf. Szeged 1974), Colloq. Math. Soc. J. Bolyai, vol. 14, North-Holland (Amsterdam, 1976); 185—194.

[5] J. Ježek and T. Kepka, Varieties of abelian quasigroups, *Czechoslovak Math. J.*, **27** (1977), 473—503.

[6] J. Ježek, Simple semilattices with two commuting automorphisms, *Algebra Universalis*, to appear.

MAT.—FIZ. FAK., UNIVERSITÁ KARLOVA
SOKOLOVSKÁ 83
18600 PRAHA 8, CZECHOSLOVAKIA