Acta Universitatis Carolinae. Mathematica et Physica

Vítězslav Kala; Tomáš Kepka; Petr Němec

Norms on semirings. I.

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 51 (2010), No. 1, 29--48

Persistent URL: `http://dml.cz/dmlcz/143644`

Norms on Semirings I.

VÍTĚZSLAV KALA, TOMÁŠ KEPKA and PETR NĚMEC

Praha

Received November 4, 2009, revised December 16, 2009

Various norms defined on semirings and rings are studied.

The study of semirings is interesting not only because of the structural properties, but also because of certain cryptological applications. Recently, it was shown by Monico and Maze in [3] and [4] that there are close connections between public key cryptography based on the Discrete Logarithm Problem and finite congruence- and/or ideal-simple semirings and finite semimodules over such semirings. It is known (see e.g. [1] and [2]) that (except for some non-important trivial cases) there are three basic classes of simple semirings, namely additively cancellative, additively idempotent and additively nil of index 2. It seems that possible connections of additively cancellative simple semirings with discrete logarithms and perhaps also with cryptography based on primes can be investigated using norms and seminorms on semirings.

The present note summarizes a few auxiliary results on semiring-valued norms defined on (semi)rings. All the material collected here is fairly basic, elementary, and of folklore character, and therefore we are not going to attribute any of the results to any particular source.

Throughout the paper, let $Q = Q(+, \cdot, \leq)$ be a non-trivial (i.e., having at least two elements) linearly ordered commutative and associative semiring. That is, $a + b =$

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Republic

Department of Mathematics, PřF UJEP, České mládeže 8, 400 96 Ústí nad Labem, Czech Republic

Partly supported by the institutional grant MSM00210839, by the Grant Agency of the Czech Republic, grant GAČR # 201/09/0296 and by the grant agency of Charles University, grant # 8648/2008.

2000 Mathematics Subject Classification. 16Y60

Key words and phrases. semiring, parasemifield, semifield, norm

E-mail address: kala@karlin.mff.cuni.cz, kepka@karlin.mff.cuni.cz, nemec@tf.czu.cz

$= b + a, ab = ba, a + (b + c) = (a + b) + c, a(bc) = (ab)c, a(b + c) = ab + ac$ for all $a, b, c \in Q$, $\leq$ is a linear (or total) ordering on Q and $a \leq b$ implies $a + c \leq b + c$ and $ac \leq bc$. We shall denote by $0_Q \in Q$ ($0_Q \notin Q$, resp.) the fact that 0_Q is the neutral element in $Q(+)$ ($Q(+)$ has no neutral element, resp.). Instead of 0_Q we shall also use only the symbol 0. Similarly, $1_Q \in Q$ ($1_Q \notin Q$, resp.) means that 1_Q is the neutral element of $Q(\cdot)$ ($Q(\cdot)$ has no neutral element, resp.) and we shall often write 1 instead of 1_Q.

1. Positive and negative cones

We denote by Q_{ps} and Q_{ng} the positive and negative cones of the ordered semiring. That is, $Q_{ps} = \{a | x \leq a + x \text{ for every } x \in Q\}$ and $Q_{ng} = \{a | a + x \leq x \text{ for every } x \in Q\}$.

1.1 Lemma. (i) *Either $Q_{ps} = \emptyset$ ($Q_{ng} = \emptyset$, resp.) or Q_{ps} (Q_{ng}, resp.) is a subsemigroup of $Q(+)$.*

(ii) *$Q_{ng} \leq Q_{ps}$. Moreover, if $a \leq b$ and $a \in Q_{ps}$ ($b \in Q_{ng}$, resp.) then $b \in Q_{ps}$ ($a \in Q_{ng}$, resp.).*

(iii) *If $0_Q \notin Q$ then $Q_{ps} \cap Q_{ng} = \emptyset$.*

(iv) *If $0_Q \in Q$ then $Q_{ps} = \{a | 0 \leq a\}, Q_{ng} = \{a | a \leq 0\}, Q_{ps} \cap Q_{ng} = \{0\}$ and $Q_{ps} \cup Q_{ng} = Q$.*

Proof. (i) We have $x \leq a + x \leq a + b + x$ for all $a, b \in Q_{ps}, x \in Q$. The other case is symmetric.

(ii) We have $b \leq a + b \leq a$ for all $a \in Q_{ps}, b \in Q_{ng}$. Thus $b \leq a$.

(iii) and (iv). If $e \in Q_{ps} \cap Q_{ng}$ then $e + x \leq x \leq e + x$ and $e + x = x$ for every $x \in Q$. Thus $e = 0_Q$ and we see that $Q_{ps} \cap Q_{ng} = \{0\}$ provided that $Q_{ps} \cap Q_{ng} \neq \emptyset$.

Now, assume that $0 \in Q$. If $a \in Q_{ps}$ then $0 \leq a + 0 = a$. Conversely, if $0 \leq a$ then $x = x + 0 \leq x + a$ for every $x \in Q$ and hence $a \in Q_{ps}$. Thus $Q_{ps} = \{a | 0 \leq a\}$ and, symmetrically, $Q_{ng} = \{a | a \leq 0\}$. Using the linearity of the order $\leq$, the equality $Q_{ps} \cup Q_{ng} = Q$ easily follows. □

1.2 Lemma. *Let $a \in Q$ and put $M_a = \{x | x \leq a + x\}$ and $N_a = \{y | a + y \leq y\}$. Then*

(i) *Either $M_a = \emptyset$ ($N_a = \emptyset$, resp.) or M_a (N_a, resp.) is an ideal of $Q(+)$.*

(ii) *$M_a \cup N_a = Q$.*

(iii) *$M_a \cap N_a = \{z | z + a = a\}$.*

(iv) *If $M_a \neq \emptyset \neq N_a$ then $M_a + N_a \subseteq M_a \cap N_a$.*

(v) *Either $M_a \neq \emptyset$ or $N_a \neq \emptyset$.*

(vi) *$M_a = \emptyset$ ($N_a = \emptyset$, resp.) if and only if $a + x < x$ ($x < a + x$, resp.) for every $x \in Q$.*

(vii) *$M_a = Q$ ($N_a = Q$, resp.) if and only if $a \in Q_{ps}$ ($a \in Q_{ng}$, resp.).*

(viii) *If $0_Q \notin Q$ then $M_a \cap N_a \neq Q$ and either $M_a \neq Q$ or $N_a \neq Q$.*

Proof. (i) We have $x \le a + x$ and $x + u \le a + x + u$ for all $x \in M_a$ and $u \in Q$. Thus $x + u \in M_a$. The other case is symmetric.

(ii) $M_a \cup N_a = Q$ follows from the linearity of the order $\le$.

(iii) Clear from the definition of the sets M_a, N_a.

(iv) Use (i).

(v) Use (ii).

(vi) and (vii). Easy to see.

(viii) The element a is not neutral in Q, and so $M_a \cap N_a \neq Q$ by (iii). The rest is clear.

□

In the remaining part of this section (except for 1.12) we shall assume that $0_Q \in Q$.

1.3 Lemma. *Assume that $Q \cdot 0 = \{w\}$. Then:*

(i) *$Q \cdot w = \{w\}$ and $2w = w$.*

(ii) *The set $\{x|w + x = x\}$ is a bi-ideal of the semiring Q.*

(iii) *If Q is bi-ideal-simple then either $w = 0$ or w is a bi-absorbing element of the semiring Q.*

(iv) *If $1_Q \in Q$ then $w = 0$.*

Proof. (i) We have $xw = xw0 = w$ for every $x \in Q$ and $w + w = 0w + 0w = = (0 + 0)w = 0w = w$.

(ii) If $w + x = x$ then $w + x + y = x + y$ and $w + xy = wy + xy = (w + x)y = xy$ for every $y \in Q$.

(iii) Use (ii).

(iv) We have $w = 0 \cdot 1 = 0$.

□

1.4 Lemma. *If $a \in Q_{ps}$ ($a \in Q_{ng}$, resp.) is such that $0a \le 0$ ($0 \le 0a$, resp.), then $0a + 0x = 0x$ for every $x \in Q$. Moreover, if $1_Q \in Q$ then $0a = 0$.*

Proof. We have $x \le a + x$, and so $0x \le 0a + 0x$. But $0a \le 0$ implies $0a + 0x \le 0x$, and hence $0a + 0x = 0x$. Now, setting $x = 1_Q$, we get $0a = 0a + 0 = 0$.The other case is symmetric. □

1.5 Lemma. *Just one of the following cases takes place:*

(1) *$0 \cdot 0 = 0$ and $0b \le 0 \le 0a$ for all $a \in Q_{ps}$ and $b \in Q_{ng}$ (i.e., $0a \in Q_{ps}$ and $0b \in Q_{ng}$);*

(2) *$0 < 0a$ for every $a \in Q_{ps}$;*

(3) *$0b < 0$ for every $b \in Q_{ng}$.*

Moreover, if $1_Q \in Q$ then (1) is true.

Proof. First, assume that neither (2) nor (3) is true. Then $0a_1 \le 0 \le 0b_1$ for some $a_1 \in Q_{ps}, b_1 \in Q_{ng}$. But $0 \le a_1, b_1 \le 0$, and hence $0 \cdot 0 \le 0a_1 \le 0 \le 0b_1 \le 0 \cdot 0$ and $0 \cdot 0 = 0$. Moreover, $0 \le a$ implies $0 = 0 \cdot 0 \le 0a$ and, similarly, $b \le 0$ implies

$0b \leq 0$. Further, suppose that (2) and (3) hold simultaneously. Then $0 < 0 \cdot 0 < 0$, a contradiction. Finally, if $1_Q \in Q$ then $0 = 0 \cdot 1$ and either $1 \in Q_{ps}$ or $1 \in Q_{ng}$. Thus (1) is true. □

1.6 Lemma. *Let $a, b \in Q$ be such that $a + b = 0$. Then $a \in Q_{ps}$ if and only if $b \in Q_{ng}$. In particular, if $Q_{ps} = Q$ ($Q_{ng} = Q$, resp.) then $\widetilde{Q} = \{u|0 \in Q + u\} = \{0\}$.*

Proof. If $a \in Q_{ps}$ or $b \in Q_{ng}$ then $b \leq a + b = 0 \leq a$, hence $b \in Q_{ng}$ and $a \in Q_{ps}$. □

1.7 Lemma. *Assume that $Q \cdot 0 = \{0\}$. Then $Q_{ps} \cdot Q_{ng} = \{0\}$.*

Proof. If $0 \leq a$ and $b \leq 0$ then $0 = 0b \leq ab \leq a0 = 0$, and hence $ab = 0$. □

1.8 Lemma. *Assume that $Q \cdot 0 = \{0\}$. Then:*

(i) *The set $\widetilde{Q} = \{u|0 \in Q + u\}$ is an ideal of the semiring Q.*

(ii) *$Q \cdot \widetilde{Q} = \{0\}$.*

(iii) *$a, b \in \widetilde{Q}$ whenever $a + b \in \widetilde{Q}$.*

(iv) *Either $\widetilde{Q} = \{0\}$ or $\widetilde{Q}$ is a (non-trivial) zero-multiplication subring of the semiring Q.*

(v) $\mathrm{Ann(Q)} = \{\mathrm{u|Qu} = 0\}$ *is an ideal of the semiring Q and $\widetilde{Q} \subseteq \mathrm{Ann(Q)}$.*

Proof. (i) We have $0 \in \widetilde{Q}$ and, if $u + v = 0$ then $ux + vx = 0$, so that $ux \in \widetilde{Q}$. If $u_1 + v_1 = 0 = u_2 + v_2$ then $(u_1 + u_2) + (v_1 + v_2) = 0$, and so $u_1 + u_2 \in \widetilde{Q}$. Consequently, $\widetilde{Q}$ is an ideal of the semiring.

(ii) First, $(\widetilde{Q} \cap Q_{ps})Q_{ng} = 0 = (\widetilde{Q} \cap Q_{ng})Q_{ps}$ follows from 1.7. Moreover, if $a \in \widetilde{Q} \cap Q_{ps}$ and $a + b = 0$, then $b \in Q_{ng}$ by 1.6 and we have $bc = 0$ for every $c \in Q_{ps}$. Consequently, $0 = 0c = ac + bc = ac$. We have proved that $(\widetilde{Q} \cap Q_{ps})Q_{ps} = 0$, and hence $(\widetilde{Q} \cap Q_{ps})Q = 0$, since $Q = Q_{ps} \cup Q_{ng}$ by 1.1(iv). Symmetrically, $(\widetilde{Q} \cap Q_{ng})Q = 0$ and, together, $\widetilde{Q}Q = 0$.

(iii), (iv) and (v). Easy. □

1.9 Lemma. *Assume that $Q \cdot 0 = \{0\}$. Let $a, b \in Q$ be such that $a + b \in$* Ann(Q). *Then:*

(i) *$xa, xb \in \widetilde{Q}$ for every $x \in Q$.*

(ii) *$yxa = 0 = yxb$ for all $x, y \in Q$.*

(iii) *$b \in$* Ann(Q) *if and only if $a \in$* Ann(Q).

Proof. (i) We have $xa + xb = 0$.

(ii) By (i) and 1.8(v), $xa \in$ Ann(Q), and so $yxa = 0$.

(iii) If $a \in$ Ann(Q) then $0 = xa + xb = xb$. □

1.10 Lemma. *Assume that $Q \cdot 0 = \{0\}$ and that at least one of the following two conditions is satisfied.*

(1) $\widetilde{Q} = \{0\}$*;*

(2) *For every $x \in Q$ there exist $m \geq 1$ and $u_1, \dots, u_m, v_1, \dots, v_m \in Q$ such that $x = u_1 v_1 + \cdots + u_m v_m$.*

Then:

(i) $a, b \in \mathrm{Ann(Q)}$ *whenever $a, b \in Q$ are such that $a + b \in \mathrm{Ann(Q)}$.*

(ii) *Either* $\mathrm{Ann(Q)} = \mathrm{Q}$ *(and then $\widetilde{Q} = 0$) or $Q \backslash \mathrm{Ann(Q)}$ is an ideal of $Q(+)$.*

Proof. (i) Combine 1.9(i), (ii), (iii).

(ii) If $\mathrm{Ann(Q)} = \mathrm{Q}$ and (2) is true, then $Q = 0$. The rest is clear from (i).

□

1.11 Remark. Assume that $Q \cdot 0 = \{0\}$. Now, define a relation ρ on Q by $(u, v) \in \rho$ if and only if $u = v + a$ for some $a \in \widetilde{Q}$. Since $\widetilde{Q}(+)$ is a subgroup of $Q(+)$, we see that ρ is an equivalence. Clearly, it is stable with respect to the addition. Moreover, if $u = v + a$ then $uz = vz$ for every $z \in Q$ (by 1.8(ii)). In particular, ρ is a congruence of the semiring Q.

Clearly, $\rho = id_Q$ if and only if $\widetilde{Q} = \{0\}$ and $\rho = Q \times Q$ if and only if $\widetilde{Q} = Q$ ($\widetilde{Q}$ is a zero-multiplication ring in the latter case).

1.12 Remark. The operations of the semiring $Q(+, \cdot)$ and the dual order $\leq^{-1}$ are compatible as well and $\overline{Q}(+, \cdot, \leq^{-1})$ is again a linearly ordered semiring. We have $\overline{Q}_{ps} = Q_{ng}$ and $\overline{Q}_{ng} = Q_{ps}$.

2. Additively cancellatice semirings

This section is an immediate continuation of the preceding one.

2.1 Lemma. *The following conditions are equivalent:*

(i) *The semiring Q is additively cancellative. (i.e., $a + c = b + c$ implies $a = b$).*

(ii) *The order $\leq$ is additively cancellative (i.e., $a + c \leq b + c$ implies $a \leq b$).*

Proof. (i) implies (ii). If $a + c \leq b + c$ and $b \leq a$, then $b + c \leq a + c$, and hence $a + c = b + c$. Since Q is additively cancellative, we get $a = b$, and so $a \leq b$. If $b \nleq a$ then $a < b$, since the order $\leq$ is linear. Thus $a \leq b$ anyway.

(ii) implies (i). If $a + c = b + c$ then $a + c \leq b + c$ and $a \leq b$. Similarly, $b \leq a$, and therefore $a = b$.

□

In the rest of this section, we will assume that the equivalent conditions of 2.1 are satisfied.

2.2 Lemma. *The following conditions are equivalent for $a \in Q$:*

(i) *$a \leq 2a$ ($2a \leq a$, resp.).*

(ii) *$u \le a + u$ ($a + u \le u$, resp.) for at least one $u \in Q$.*
(iii) *$a \in Q_{ps}$ ($a \in Q_{ng}$, resp.).*

Proof. (i) implies (ii) and (iii) implies (i) trivially.

(ii) implies (iii). We have $u + x \le u + a + x$, and hence $x \le a + x$ for every $x \in Q$. The other case is symmetric.

□

2.3 Lemma. (i) *Either $Q_{ps} = \emptyset$ ($Q_{ng} = \emptyset$, resp.) or Q_{ps} (Q_{ng}, resp.) is an ideal of the semiring Q.*
(ii) *$Q_{ps}Q_{ng} \subseteq Q_{ps} \cap Q_{ng} \subseteq \{0_Q\}$.*
(iii) *$Q_{ps} \cup Q_{ng} = Q$.*

Proof. (i) Assume that $Q_{ps} \neq \emptyset$, the other case being symmetric. By 1.1(i), Q_{ps} is a subsemigroup of $Q(+)$. Furthemore, if $a \in Q_{ps}$ and $x \in Q$, then $ax \le 2ax$ and $ax \in Q_{ps}$ by 2.2. Thus Q_{ps} is an ideal of Q.

(ii) Since both Q_{ps} and Q_{ng} are ideals of Q (when non-empty), we get $Q_{ps}Q_{ng} \subseteq$ $\subseteq Q_{ps} \cap Q_{ng}$. By 1.1(iii), (iv), we have $Q_{ps} \cap Q_{ng} \subseteq \{0_Q\}$.

(iii) For every $a \in Q$, either $a \le 2a$ and $a \in Q_{ps}$ by 2.2 or $2a \le a$ and $a \in Q_{ng}$ again by 2.2.

□

2.4 Lemma. *Assume that $0_Q \notin Q$. Then just one of the following two cases takes place:*
(1) *$Q_{ps} = Q$ and $b < a + b$ for all $a, b \in Q$.*
(2) *$Q_{ng} = Q$ and $a + b < b$ for all $a, b \in Q$.*

Proof. By 2.3(iii), we have $Q = Q_{ps} \cup Q_{ng}$. Now, assume that $Q_{ps} \neq \emptyset$, the other case being symmetric. Since $0 \notin Q$, the equality $Q_{ng} = \emptyset$ follows from 2.3(ii). Consequently, $Q_{ps} = Q$ and $b \le a + b$ for all $a, b \in Q$. If $b = a + b$ then $a \in Q_{ng}$ by 2.2(ii), a contradiction. Thus $b < a + b$. □

In the remaining part of this section (except for 2.14, 2.15, and 2.16), we will assume that $0_Q \in Q$.

2.5 Lemma. (i) $Q \cdot 0 = 0$.
(ii) *If $a \in Q_{ps}$ and $b \in Q_{ng}$ are such that $a + b \in Q_{ps}$ ($a + b \in Q_{ng}$, resp.), then $b \in$ Ann(Q) ($a \in$ Ann(Q), resp.).*
(iii) *Either $Q_{ps} \subseteq$ Ann(Q) or $Q_{ng} \subseteq$ Ann(Q).*
(iv) $\widetilde{Q} \subseteq$ Ann(Q).

Proof. (i) We have $Q \cdot 0 = (Q_{ps} \cup Q_{ng}) \cdot 0 = Q_{ps} \cdot 0 \cup Q_{ng} \cdot 0 \subseteq Q_{ps}Q_{ng} \subseteq \{0\}$ by 2.3.

(ii) We have $0 = (a + b)c = ac + bc = bc$ for every $c \in Q_{ng}$ by 2.3. Then $bQ_{ng} = 0$, and hence $bQ = 0$ follows from 2.3 again. Thus $b \in$ Ann(Q). The other case is symmetric.

(iii) Assume that $Q_{ng} \nsubseteq \mathrm{Ann(Q)}$, the other case being symmetric. If $b \in$ $\in Q_{ng} \backslash \mathrm{Ann(Q)}$ then $b + Q_{ps} \subseteq Q_{ng}$ by (ii). Using (ii) again, we get $Q_{ps} \subseteq \mathrm{Ann(Q)}$.

(iv) Combine (i) and 1.8(v).

□

2.6 Lemma. *Let $a, b \in Q_{ps}$ ($a, b \in Q_{ng}$, resp.) be such that $a + b \in \mathrm{Ann(Q)}$. Then $a, b \in \mathrm{Ann(Q)}$.*

Proof. Assume $a, b \in Q_{ps}$, the other case being symmetric. We have $xa + xb = 0$ for every $x \in Q$. By 2.3(iv), we get $xa, xb \in Q_{ps}$ and it follows from 1.6 that $xa, xb \in$ $\in Q_{ng}$, too. Thus $xa, xb \in Q_{ps} \cap Q_{ng} = \{0\}$, $xa = 0 = xb$ and, finally, $a, b \in$ $\in \mathrm{Ann(Q)}$. □

2.7 Lemma. *Either* $\mathrm{Ann(Q)} = \mathrm{Q}$ *or the set* $Q \backslash \mathrm{Ann(Q)}$ *is an ideal of* $Q(+)$.

Proof. Immediate from 2.6. □

Now (except for 2.14, 2.15, 2.16), assume that $Q_{ng} \subseteq \mathrm{Ann(Q)}$, the other case being symmetric (see 2.5(iii) and 1.12). Then we have $Q_{ng} \cup \widetilde{Q} \subseteq \mathrm{Ann(Q)}$ and we put $K = Q \backslash \mathrm{Ann(Q)}$.

2.8 Lemma. (i) $K = Q_{ps} \backslash \mathrm{Ann(Q)} \subseteq \mathrm{Q_{ps}} \backslash \{0\}$.

(ii) *$Q = K \cup \mathrm{Ann(Q)}$ and $K \cap \mathrm{Ann(Q)} = \emptyset$.*

(iii) *Either $K = \emptyset$ (and then $\mathrm{Ann(Q)} = \mathrm{Q}$) or K is an ideal of $Q(+)$.*

Proof. (i) Clearly, $Q_{ps} \backslash \mathrm{Ann(Q)} \subseteq \mathrm{K}$. On the other hand, if $a \in K$ then $a \notin Q_{ng}$, and so $a \in Q_{ps}$. Thus $K = Q_{ps} \backslash \mathrm{Ann(Q)}$. The inclusion $K \subseteq Q_{ps} \backslash \{0\}$ is clear.

(ii) Obvious.

(iii) See 2.7.

□

Define a relation $\sigma (= \sigma_Q)$ on Q by $(a, b) \in \sigma$ if and only if $ax = bx$ for all $x \in Q$.

2.9 Lemma. (i) *σ is a congruence of the semiring Q and $\rho \subseteq \sigma$ (see 1.11).*

(ii) $\mathrm{Ann(Q)}$ *is a block of σ.*

(iii) *$\sigma = Q \times Q$ if and only if* $\mathrm{Ann(Q)} = \mathrm{Q}$.

(iv) *If $a, b, c \in Q$ are such that $(a + c, b + c) \in \sigma$, then $(a, b) \in \sigma$.*

(v) *If $a, b, c, d \in Q$ are such that $(a, b) \in \sigma, (c, d) \in \sigma$ and $a \leq c$, then either $b \leq d$ or $(a, c) \in \sigma$ and $(b, d) \in \sigma$.*

Proof. (i) Easy to check directly.

(ii) Clearly, $\mathrm{Ann(Q)} = \{\mathrm{a} | (\mathrm{a}, 0) \in \sigma\}$.

(iii) This follows immediately from (ii).

(iv) We have $ax + cx = bx + cx$ for every $x \in Q$. Since $Q(+)$ is cancellative, we get $ax = bx$.

(v) If $b \nleq d$ then $d < b$ and $cx = dx \leq bx = ax$ for every $x \in Q$. But $a \leq c$ implies $ax \leq cx$, and so $ax = cx$ and $(a, c) \in \sigma$. Then $(b, d) \in \sigma$. □

2.10 Remark. Let Ann(Q) $\neq$ Q (i.e., $ab \neq 0$ for some $a, b \in Q$). Then $\sigma \neq$ $\neq Q \times Q$ by 2.9(iii) and $P = Q/\sigma$ is a non-trivial semiring. According to 2.9(iv), P is additively cancellative. Moreover, it follows from 2.9(v) that the order $\leq$ induces an order (we denote it again $\leq$) on the factorsemiring P. Thus P becomes a linearly ordered semiring.

(i) If $a \in Q_{ps}$ then $0_Q \leq a$, and hence $0_P = 0_Q/\sigma \leq a/\sigma$ and $a/\sigma \in P_{ps}$. If $a \in Q \backslash Q_{ps}$ then $a \in$ Ann(Q) (see 2.8), $a/\sigma = 0_P$ and $a/\sigma \in P_{ps}$. It follows that $P_{ps} = P$.

(ii) Clearly, $a/\sigma \in$ Ann(P) if and only if $axy = 0$ for all $x, y \in Q$. In particular, if the condition 1.10(2) is satisfied, then Ann(P) $= \{0_P\}$.

(iii) Clearly, $(a/\sigma, b/\sigma) \in \sigma_P$ if and only if $axy = bxy$ for all $x, y \in Q$. Again, if 1.10(2) is true, then $\sigma_P = id_P$.

(iv) We have $P_{ps} = P$ by (i) and it follows that $\widetilde{P} = \{0_P\}$ (use 1.6 or 2.7).

Define a relation $\sigma_m (= \sigma_{Q,m})$, $m \geq 1$, on Q by $(a, b) \in \sigma_m$ if and only if $ax_1 \cdots x_m =$ $= bx_1 \cdots x_m$ for all $x_1, \ldots, x_m \in Q$.

2.11 Lemma. (i) *σ_m is a congruence of the semiring Q.*

(ii) *If $a, b, c \in Q$ are such that $(a + c, b + c) \in \sigma_m$, then $(a, b) \in \sigma_m$.*

(iii) *If $a, b, c, d \in Q$ are such that $(a, b) \in \sigma_m, (c, d) \in \sigma_m$ and $a \leq c$, then either $b \leq d$ or $(a, c) \in \sigma_m$ and $(b, d) \in \sigma_m$.*

Proof. Similar to that of 2.9. □

Clearly, $\sigma = \sigma_1 \subseteq \sigma_2 \subseteq \sigma_3 \subseteq \ldots$ and we put $(\overline{\sigma}_Q =)\overline{\sigma} = \bigcup \sigma_m, m \geq 1$.

2.12 Lemma. (i) *$\overline{\sigma}$ is a congruence of the semiring Q.*

(ii) *$\overline{\sigma} = Q \times Q$ if and only if for every $a \in Q$ there exists a positive integer n such that $ax_1 \cdots x_n = 0$ for all $x_1, \ldots, x_n \in Q$,*

(iii) *If $a, b, c \in Q$ are such that $(a + c, b + c) \in \overline{\sigma}$, then $(a, b) \in \overline{\sigma}$.*

(iv) *If $a, b, c, d \in Q$ are such that $(a, b) \in \overline{\sigma}, (c, d) \in \overline{\sigma}$ and $a \leq c$, then either $b \leq d$ or $(a, c) \in \overline{\sigma}$ and $(b, d) \in \overline{\sigma}$.*

Proof. An easy consequence of 2.11. □

2.13 Remark. Assume that $\overline{\sigma} \neq Q \times Q$ (see 2.12(ii)) and put $\overline{P} = Q/\overline{\sigma}$. Then $\overline{P}$ is a non-trivial additively cancellative semiring that is linearly ordered (see 2.12(iii), (iv)). Moreover, $\overline{P}_{ps} = \overline{P}$ and $\overline{P}_{ng} = \{0_{\overline{P}}\}$ (see 2.10(i)). Consequently, $\widetilde{\overline{P}} = \{0_{\overline{P}}\}$.

2.14 Remark. Assume that either $0_Q \notin Q$ or $0_Q \in Q$ and $\widetilde{Q} = \{0\}$ (see 1.6 and 2.10(iv)). Now, define a relation $\leq_0$ on Q by $a \leq_0 b$ if and only if $b = a + u$ for some $u \in Q \cup \{0\}$. It is easy to check that $\leq_0$ is an ordering that is compatible with the addition and multiplication.

(i) The ordering $\leq_0$ is contained in the ordering $\leq$ if and only if $Q_{ps} = Q$.

(ii) The ordering $\leq_0$ is contained in the ordering $\leq^{-1}$ if and only if $Q_{ng} = Q$.

(iii) The following conditions are equivalent:

(iii1) The ordering $\le$ is contained in the ordering $\le_0$.
(iii2) The orderings $\le$ and $\le_0$ coincide.
(iii3) The semiring Q is semisubtractive and $Q_{ps} = Q$.
(iv) The following conditions are equivalent:
(iv1) The ordering $\le^{-1}$ is contained in the ordering $\le_0$.
(iv2) The orderings $\le^{-1}$ and $\le_0$ coincide.
(iv3) The semiring Q is semisubtractive and $Q_{ng} = Q$.

2.15 Lemma. *Assume that $1_Q \in Q$. Then $Q_{ps} = Q$ ($Q_{ng} = Q$, resp.) if and only if $1_Q \le 2_Q$ ($2_Q \le 1_Q$, resp.).*

Proof. If $1_Q \le 2_Q$ then $a \le 2a = a + a$, and so $a + x \le a + a + x$ for all $a, x \in Q$. Using 2.1, we get $x \le a + x$. □

2.16 Corollary. If $1_Q \in Q$ then either $Q_{ps} = Q$ or $Q_{ng} = Q$.

3. Difference rings

In this section, let Q be additively cancellative. We denote by R the difference ring of Q. That is, $R = \{u - v | u, v \in Q\}$, R is a commutative and associative ring (possibly without unit element).

3.1 Lemma. *Let $u_1, u_2, v_1, v_2, z_1, z_2, w_1, w_2 \in Q$ be such that $u_1 - v_1 = u_2 - v_2$, $z_1 - w_1 = z_2 - w_2$ and $u_1 + w_1 \le z_1 + v_1$. Then $u_2 + w_2 \le z_2 + v_2$.*

Proof. We have $u_1 + v_2 = u_2 + v_1, z_1 + w_2 = z_2 + w_1, u_2 + v_1 + w_1 + w_2 = u_1 + v_2 + w_1 + w_2 \le z_1 + v_1 + v_2 + w_2 = z_2 + w_1 + v_1 + v_2$. Consequently, $u_2 + w_2 \le z_2 + v_2$ by 2.1. □

In view of 3.1, define a relation $\le_R$ on R by $u - v \le_R z - w$ if and only if $u + w \le z + v$.

3.2 Lemma. *The relation $\le_R$ is a linear ordering that is compatible with the addition of the ring R.*

Proof. First, $u - v \le_R u - v$, since $u + v \le u + v$. Thus $\le_R$ is reflexive. If $u - v \le_R z - w \le_R u - v$ then $u + w \le z + v \le u + w, u + w = z + v$ and $u - v = z - w$. Thus the relation $\le_R$ is antisymmetric. Finally, if $u - v \le_R z - w \le_R r - s$ then $u + w \le z + v, z + s \le r + w, u + w + s \le z + v + s \le r + w + v$, and hence $u + s \le r + v$ and $u - v \le_R r - s$. That is, the relation $\le_R$ is transitive and we have checked that $\le_R$ is an ordering on R. Moreover, if $u, v, r, s \in Q$ then either $u + s \le r + v$ and $u - v \le_R r - s$ or $r + v \le u + s$ and $r - s \le_R u - v$. Thus the ordering $\le_R$ is linear.

It remains to show the compatibility. If $u - v \le_R z - w$ then $u + w \le z + v, u + w + r + s \le z + w + r + s$, and therefore $u - v + r - s = (u + r) - (v + s) \le_R (z + r) - (w + s) = z - w + r - s$.

□

3.3 Lemma. *The following conditions are equivalent for $a, b \in Q$:*

(i) $a \leq b$.

(ii) $a \leq_R b$.

(iii) $0 \leq_R b - a$.

(iv) $a - b \leq_R 0$.

Proof. The conditions (ii), (iii), and (iv) are equivalent due to 3.2. If $a \leq b$ then $2a \leq a + b, 2a + b \leq a + 2b$ and $a = 2a + b - (a + b) \leq_R (2b + a) - (a + b) = b$. Conversely, if $2a - a = a \leq_R b = 2b - b$ then $2a + b \leq 2b + a, a + b \leq 2b$ and, finally, $a \leq b$. □

3.4 Lemma. *If $\alpha, \beta \in R$ and $\alpha \leq_R \beta$ then $a\alpha \leq_R a\beta$ for every $a \in Q$.*

Proof. We have $\alpha = u - v, \beta = z - w, u + w \leq z + v$. Then $au + aw \leq az + av$, and so $a\alpha = au - av \leq_R az - aw = a\beta$. □

3.5 Lemma. (i) $R_{ps} = \{\alpha \in R | 0_R \leq_R \alpha\} = \{u - v | v \leq u\}$.

(ii) $R_{ng} = \{\alpha \in R | \alpha \leq_R 0_R\} = \{u - v | u \leq v\}$.

(iii) $R_{ps} \cap Q = Q_{ps}$ *and* $R_{ng} \cap Q = Q_{ng}$.

Proof. (i) Clearly, $0_R \leq_R u - v$ if and only if $v \leq u$.

(ii) Symmetric to (i).

(iii) If $a \in Q$ then $a - a = 0_R \leq_R a$ if and only if $a \leq 2a$. Using 2.2, we get $R_{ps} \cap Q = Q_{ps}$. The other case is symmetric.

□

3.6 Lemma. *The following conditions are equivalent:*

(i) *R_{ps} is a subsemiring of the ring R.*

(ii) *If $\alpha \leq_R \beta$ then $\alpha\gamma \leq_R \beta\gamma$ for every $\gamma \in R_{ps}$ (i.e., R, together with $\leq_R$, is a linearly ordered ring in the usual sense).*

(iii) *If $\alpha \leq_R \beta$ then $\beta\gamma \leq_R \alpha\gamma$ for every $\gamma \in R_{ng}$.*

(iv) *If $u, v, z, w \in Q$ are such that $u < v$ and $w < z$, then $vw + uz \leq vz + uw$.*

Proof. (i) implies (ii). We have $\beta - \alpha \in R_{ps}$ and $\gamma \in R_{ps}$. Then $\beta\gamma - \alpha\gamma \in R_{ps}$, and so $\alpha\gamma \leq_R \beta\gamma$.

(ii) is equivalent to (iii). Easy to see.

(iii) implies (iv). We have $v - u \in R_{ps}, z - w \in R_{ps}$, and so $vz - vw - uz + uw = (v - u)(z - w) \in R_{ps}$. Then $vw + uz \leq vz + uw$.

(iv) implies (i). Let $\alpha = v - u$ and $\beta = z - w$ be in R_{ps}, $u \leq v, w \leq z$. Then $0 \leq_R vz - vw - uz + uw = (v - u)(z - w) = \alpha\beta$. Thus $\alpha\beta \in R_{ps}$.

□

3.7 Lemma. (i) $a - b \in \mathrm{Ann(R)}$ *if and only if* $(a, b) \in \sigma_Q$ (see 2.9).

(ii) $\mathrm{Ann(R)} = \{0_\mathrm{R}\}$ *if and only if* $\sigma_Q = id_Q$.

Proof. It is easy. □

3.8 Lemma. *The following conditions are equivalent:*

(i) $\alpha\beta \neq 0_R$ *for all* $\alpha, \beta \in R\backslash\{0_R\}$.

(ii) $uz + vw \neq vz + uw$ *whenever* $u, v, w, z \in Q$ *are such that* $u < v$ *and* $w < z$.

Proof. It is easy. □

3.9 Lemma. (i) $1_R \in R$ *if and only if there are* $a, b \in Q$ *such that* $au = bu + u$ *for every* $u \in Q$ *(then* $1_R = a - b$*).*

(ii) *If* $1_Q \in Q$ *then* $1_Q = 1_R$.

Proof. It is easy. □

3.10 Remark. Let Q be a non-trivial additively cancellative semiring such that either $0_Q \notin Q$ or $0_Q \in Q$ and $\widetilde{Q} = \{0_Q\}$ (see 2.14). Assume further that Q is semisubtractive and put $\leq = \leq_0$. Then $\leq$ is a linear ordering that is compatible with the semiring operations of Q. Clearly, $Q_{ps} = Q$.

Now, we check that the condition 3.6(iv) is satisfied. Indeed, if $v = u + a$ and $z = w + b$, then $c = vw + uz = uw + aw + uw + ub = 2uw + aw + ub, d = vz + uw = = uw + ub + aw + ab + uw = 2uw + aw + ub + ab = c + ab$, and hence $c \leq d$.

It follows from 3.6 that R together with $\leq_R$ is a linearly ordered ring. Clearly, $R_{ps} = Q \cup \{0_R\}$.

(i) If $\alpha \in R, \alpha = u - v$, then either $v \leq u$ and $\alpha \in Q \cup \{0\}$ or $u < v, v = u + a, a \in Q$, and $\alpha = -a$. Thus $R = Q \cup (-Q) \cup \{0\}$.

(ii) $\mathrm{Ann(R)} = \mathrm{Ann(Q)} \cup (-\mathrm{Ann(Q)}) \cup \{0\}$.

(iii) If $0_Q \notin Q$ then $\alpha\beta \neq 0$ for all $\alpha, \beta \in R\backslash\{0\}$ (use 3.8). Consequently, the multiplicative semigroup $Q(\cdot)$ is cancellative. (In fact, if $ab = ac, a, b, c \in \in Q, b \leq c, c = b + u, u \in Q \cup \{0\}$, then $ab = ab + au, au = 0, u = 0$ and $b = c$.)

(iv) Assume that $0_Q \in Q$. If $a, b \in Q$ are such that $ab = 0$ and $a \leq b$, then $b = a + u$, $a^2 + au = 0$ and $a^2 = 0 = au$, since $\widetilde{Q} = \{0\}$.

(v) Assume that $0_Q \in Q$. Then $\alpha\beta \neq 0$ for all $\alpha, \beta \in R\backslash\{0\}$ if and only if $a^2 \neq 0$ for every $a \in Q\backslash\{0\}$ (combine (iv) and 3.8).

(vi) $1_R \in R$ if and only if $1_Q \in Q$; then $1_R = 1_Q$.

Indeed, if $1_Q \in Q$ then $1_R = 1_Q$. Conversely, if $a \in Q$ is such that $-a = 1_R$ (see (i)), then $a = -a^2 \in \widetilde{Q}, a = 0_Q$ and $Q = \{0\}$, a contradiction.

3.11 Remark. Assume that $Q = Q_{ps}$ and that the equivalent conditions of 3.6 are satisfied. The difference ring R, together with $\leq_R$, is a linearly ordered ring (in the normal sense). Consequently, R_{ps} is a semisubtractive semiring that is linearly ordered by $\leq_R$. Of course, Q is a subsemiring of R_{ps} and $\leq_R \restriction Q = \leq$. Moreover, $0 \in R_{ps}, \widetilde{R_{ps}} = \{0\}$ and either $0 \notin Q$ or $0 \in Q$ and $\widetilde{Q} = \{0\}$.

3.12 Remark. Let S, together with $\leq_S$, be a non-trivial ordered ring (in the usual sense). Then $Q = S_{ps}$, together with $\leq = \leq_S \restriction Q$, is a linearly ordered semiring that is additively cancellative and that satisfies the equivalent conditions of 3.6. Moreover, Q is semisubtractive, $Q_{ps} = Q$ and $\widetilde{Q} = \{0\}$.

3.13 Remark. Let Q be a non-trivial semiring. Combining 3.11 and 3.12, we see that the following two conditions are equivalent:

(1) Q is additively cancellative and can be linearly ordered in such a way that $Q_{ps} = Q$ and 3.6(iv) is true.

(2) There exists a linearly ordered ring S such that Q is a subsemiring of S_{ps}.

3.14 Example. Put $Q = \mathbb{Q}^+ \times \mathbb{Q}^+$ ($\mathbb{Q}^+$ being the parasemifield of positive rational numbers) and define a relation $\leq_Q$ on Q by $(a, b) \leq_Q (c, d)$ if and only if either $a < c$ or $a = c$ and $d \leq b$. One checks readily that Q (together with $\leq_Q$) becomes a linearly ordered parasemifield that is additively cancellative.

Clearly, $Q_{ps} = Q$ and $0_Q \notin Q$. If $u_1 = (1, 2)$ and $v_1 = (1, 1)$, then $u_1 < v_1$ and $u_1^2 + v_1^2 = (2, 5) < (2, 4) = 2u_1v_1$. Consequently, the condition 3.6(iv) is not satisfied.

On the other hand, if $u_2 = (1, 1)$ and $v_2 = (2, 1)$, then $u_2 < v_2$ and $2u_2v_2 = (4, 2) <$ $< (5, 2) = u_2^2 + v_2^2$. Thus the condition dual to 3.6(iv) is not satisfied either.

3.15 Remark. It is not clear whether there exists a linearly ordered additively cancellative parasemifield P such that 3.6(iv) is not true for any (compatible) linear ordering defined on P.

4. Parasemifields of fractions

4.1 Lemma. *The following conditions are equivalent:*

(i) *The semiring Q is multiplicatively cancellative (i.e., $ac = bc$ implies $a = b$).*

(ii) *The order $\leq$ is multiplicatively cancellative (i.e., $ac \leq bc$ implies $a \leq b$).*

Proof. Similar to that of 2.1. □

In the rest of this section, we will assume that the equivalent conditions of 4.1 are satisfied. Let P be the parasemifield of fractions of Q.

4.2 Lemma. *Let $u_1, u_2, v_1, v_2, z_1, z_2, w_1, w_2 \in Q$ be such that $u_1/v_1 = u_2/v_2$, $z_1/w_1 = z_2/w_2$ and $u_1w_1 \leq z_1v_1$. Then $u_2w_2 \leq z_2v_2$.*

Proof. Similar to that of 3.1. □

In view of 3.2, define a relation $\leq_P$ on P by $u/v \leq_P z/w$ if and only if $uw \leq_P zv$.

4.3 Lemma. *The relation $\leq_P$ is a linear ordering that is compatible with the multiplication of the parasemifield P.*

Proof. Similar to that of 3.2. □

4.4 Lemma. *The following conditions are equivalent for $a, b \in Q$:*

(i) *$a \leq b$.*

(ii) *$a \leq_P b$.*

(iii) $1 \leq_P b/a$.
(iv) $a/b \leq_P 1$.

Proof. Similar to that of 3.3. □

4.5 Lemma. *If $\alpha, \beta \in P$ and $\alpha \leq_P \beta$, then $\alpha + \gamma \leq_P \beta + \gamma$ for every $\gamma \in P$.*

Proof. We have $\alpha = u/v, \beta = z/w, uw \leq zv$, and $\gamma = a/b$. Then $uwb^2 \leq zvb^2$, $(ub + av)wb = ubwb + avwb \leq zbvb + awvb = (zb + aw)vb$, and hence $u/v + a/b =$ $= (ub + av)/vb \leq_P (zb + aw)/wb = z/w + a/b$. □

In view of 4.5, P becomes a linearly ordered parasemifield.

4.6 Lemma. *If Q is additively cancellative, then P is such.*

Proof. Let $a/b+c/d = a/b+e/f$. Then $adf+cbf = adf+ebd$, and so $cbf = ebd$, $cf = ed$ and $c/d = e/f$. □

4.7 Lemma. *Assume that Q is additively cancellative* (see 4.6) *and denote by S the difference ring of the parasemifield P. Then $\alpha\beta \neq 0_S$ for all $\alpha, \beta \in S\setminus\{0_S\}$ if and only if Q satisfies the condition 3.8(ii).*

Proof. Clearly, S is a domain if and only if $1 + \alpha\beta \neq \alpha + \beta$ for all $\alpha, \beta \in P\setminus\{1\}$. Now, if $\alpha = a/b$ and $\beta = c/d$, then $bd(1 + \alpha\beta) = bd + ac$ and $bd(\alpha + \beta) = ad + bc$. The rest is clear. □

4.8 Lemma. *Assume that Q is additively cancellative. Then P satisfies the equivalent conditions of 3.6 if and only if Q satisfies them.*

Proof. Assume that Q satisfies 3.6(iv). If $a/b < c/d$ and $e/f < g/h$, then $ad < bc, eh < gf$, and so $adgf + bceh \leq adeh + bcgf$. From this, $ag/bh + ce/df \leq$ $\leq ae/bf + cg/dh$. □

4.9 Lemma. *If Q is semisubtractive then P is such.*

Proof. Assume that Q is semisubtractive. If $a/b, c/d \in P$ are such that $a/b \neq$ $\neq c/d$, then $ad \neq bc$ and there is $e \in Q$ such that $ad + e = bc$ ($bc + e = ad$, resp.). Consequently, $a/b + e/bd = c/d$ ($c/d + e/bd = a/b$, resp.). □

4.10 Lemma. *Let $Q_{ps} \neq \emptyset$ ($Q_{ng} \neq \emptyset$, resp.). Then $xy \leq x + xy$ ($x + xy \leq xy$, resp.) for all $x, y \in Q$.*

Proof. Let $a \in Q_{ps}$. We have $ya \leq a + ya$ for every $y \in Q$. Then $xya \leq xa + xya$ and $xy \leq x + xy$ by 4.1. The other case is symmetric. □

4.11 Lemma. *Assume that Q is additively cancellative. Then $0_Q \notin Q$ and $a+b \neq a$ for all $a, b \in Q$.*

Proof. If $0_Q \in Q$ then $0\cdot 0 = (0+0)0 = 0\cdot 0 + 0\cdot 0$, and so $0\cdot 0 = 0$. Now, $a0 = a0\cdot 0$ for every $a \in Q$, and hence $a = a0$ and $0_Q = 1_Q$. From this, $ab = (a+0)b = ab + 0b = $ $= ab + b$ and $b = 0$ for every $b \in Q$. Thus Q is trivial, a contradiction. □

4.12 Lemma. *If Q is additively cancellative then either $Q_{ps} = Q$ and $Q_{ng} = \emptyset$ or $Q_{ng} = Q$ and $Q_{ps} = \emptyset$.*

Proof. Combine 2.3(iii), 4.11 and 4.10. □

4.13 Lemma. *Assume that $0_Q = 1_Q \in Q$. Then Q is additively idempotent and $ab = ab + b$ for all $a, b \in Q$.*

Proof. We have $ab = ab + b$ (see the proof of 4.11), and therefore $b = 1_Q b = $ $= 1_Q b + b = b + b$. □

4.14 Lemma. *Assume that $Q_{ps} \neq \emptyset \neq Q_{ng}$. Then*

(i) *$xy = x + xy$ for all $x, y \in Q$.*

(ii) *If $1_Q \in Q$ then $1_Q = 0_Q$.*

Proof. (i) Use 4.10(i).

(ii) By (i), $y = 1y = 1 + 1y = 1 + y$. □

5. Additively cancellative parasemifields

In this section, let $Q = P$ be a parasemifield (i.e., $P(\cdot)$ is a group).

5.1 Lemma. $0_P \notin P$.

Proof. If $0_P \in P$ then $x + 0 = x$ implies $xy + 0y = xy$ for all $x, y \in P$. Since P is a parasemifield, it follows that $0y = 0$, and hence $1_P = 0^{-1}\cdot 0 = 0^{-1}\cdot 0y = 1y = y$. Thus P is trivial, a contradiction. □

5.2 Lemma. *The following conditions are equivalent:*

(i) *$1_P \in P_{ps}$ ($1_P \in P_{ng}$, resp.).*

(ii) *$P_{ps} \neq \emptyset$ ($P_{ng} \neq \emptyset$, resp.).*

(iii) *$P_{ps} = P$ and $P_{ng} = \emptyset$ ($P_{ng} = P$ and $P_{ps} = \emptyset$, resp.).*

Proof. (i) implies (ii) and (iii) implies (i) trivially.

(ii) implies (iii). If $a \in P_{ps}$ then $x \leq x + a$ and $a^{-1}x \leq a^{-1}x + 1$ for every $x \in P$. Consequently, $1 \in P_{ps}$, $y \leq 1 + y$ and $by \leq b + by$ for all $b, y \in P$. Thus $b \in P_{ps}$ and $P_{ps} = P$. Finally, since $0_P \notin P$ by 5.1, we have $P_{ng} = \emptyset$. □

5.3 Lemma. *Assume that P is additively cancellative. Then either $P_{ps} = P$ and $P_{ng} = \emptyset$ or $P_{ng} = P$ and $P_{ps} = \emptyset$.*

Proof. See 4.12. □

5.4 Lemma. *Assume that P is additively cancellative* (see 5.3).

(i) *The equivalent conditions of 3.6 are satisfied if and only if $u + v \le 1 + uv$ for all $u, v \in P$ such that $1 < u$ and $1 < v$.*

(ii) *The equivalent conditions of 3.8 are satisfied if and only if $u + v \ne 1 + uv$ for all $u, v \in P$ such that $1 < u$ and $1 < v$.*

Proof. It is easy. □

5.5 Remark. Assume that $P_{ps} = P$, put $P_0 = P \cup \{0\}$ and $0 < x$ for every $x \in P$. Then P_0 becomes a linearly ordered semifield.

6. Semifields

In this section, let $Q = F$ be a semifield (i.e., $0_F \in F$ and $F \backslash \{0_F\}$ is a subgroup of $F(\cdot)$).

6.1 Remark. Denote by e the unit element of the multiplicative group $F\backslash\{0\}$. If $e0 = 0$ then $e = 1_F$ is the multiplicatively neutral element of the semifield F. Henceforth, assume that $e0 = f \ne 0$. Then $a = e(a + 0) = ea + e0 = a + f$ for every $a \in F\backslash\{0\}$. Consequently, $ab = ab + fb$ for all $a, b \in F\backslash\{0\}$ and it follows easily that $fb = f$ and $b = f^{-1}fb = f^{-1}f = e$. Thus $|F| = 2$, $F = \{0, e\}$, $e + e = e = e0$ and either $0 \cdot 0 = 0$ or $0 \cdot 0 = e$. Further, if $0 \cdot 0 = 0$ then $0 = 1_F$ and we have either $0 < e$ or $e < 0$. Finally, if $0 \cdot 0 = e$ then $1_F \notin F$ and, again, either $0 < e$ or $e < 0$.

6.2 Remark. Assume that $e0 = 0$ (see 6.1). Then $e = 1_F$ and $0 = 1 \cdot 0 = a^{-1} \cdot a0$ for every $a \in F\backslash\{0\}$ and it follows that $a0 = 0$. Now, if $0 \cdot 0 = b \ne 0$ then $1 = b^{-1}b = b^{-1}0 \cdot 0 = 0 \cdot 0 = b, 0 \cdot 0 = 1$ and $c = 1c = 0 \cdot 0c = 0 \cdot 0 = 1$ for every $c \in F\backslash\{0\}$. Thus $|F| = 2, F = \{0, 1\}$ and $1 + 1 = 0 \cdot 0 + 0 \cdot 0 = 0(0 + 0) = 0 \cdot 0 = 1$. Moreover, $0 = 0 \cdot 1 = 0(0 + 1) = 0 \cdot 0 + 0 \cdot 1 = 1 + 0 = 1$, a contradiction. We have shown that $F \cdot 0 = \{0\}$ anyway.

In the remaining part of this section, assume that $1_F \in F$ and $F \cdot 0 = \{0\}$ (see 6.1 and 6.2).

6.3 Lemma. $\widetilde{F} = \{0\}$ (see 1.8).

Proof. Assume, on the contrary, that $a + b = 0$ for some $a, b \in F\backslash\{0\}$. Then $1 + c = 0$, where $c = a^{-1}b$, and hence $x + xc = 0$ for every $x \in F$. Thus F is a ring and, in fact, F is a field, a contradiction. □

6.4 Lemma. *Either $F_{ps} = F$ and $F_{ng} = \{0\}$ or $F_{ng} = F$ and $F_{ps} = \{0\}$.*

Proof. If $a < 0 < b$ for some $a, b \in F\backslash\{0\}$, then $1 = aa^{-1} < 0 < bb^{-1} = 1$, a contradiction. □

6.5 Remark. Put $P = F\backslash\{0\}$. Then P is a subsemiring of F and either $|P| = 1$ and $|F| = 2$ or P is a (non-trivial) linearly ordered parasemifield. Moreover, either $P_{ps} = P$ and $P_{ng} = \emptyset$ or $P_{ng} = P$ and $P_{ps} = \emptyset$ (cf. 5.5).

7. Norms on semirings

Throughout this section, let $S = S(+, \cdot)$ a non-trivial commutative and associative semiring. Let $\alpha : S \to Q$ be a mapping such that $\alpha(xy) = \alpha(x)\alpha(y)$ for all $x, y \in S$ (i.e., α is a homomorphism of the multiplicative semigroups). Now, consider the following conditions:

(A) $\alpha(x + y) \leq \alpha(x) + \alpha(y)$ for all $x, y \in S$;
(B) $\alpha(x) + \alpha(y) \leq \alpha(x + y)$ for all $x, y \in S$;
(C) $\alpha(x + y) = \alpha(x) + \alpha(y)$ for all $x, y \in S$;
(D) $\alpha(x + y) \leq \max\{\alpha(x), \alpha(y)\}$ for all $x, y \in S$;
(E) $\max\{\alpha(x), \alpha(y)\} \leq \alpha(x + y)$ for all $x, y \in S$;
(F) $\alpha(x + y) = \max\{\alpha(x), \alpha(y)\}$ for all $x, y \in S$;
(G) $\alpha(x + y) \leq \min\{\alpha(x), \alpha(y)\}$ for all $x, y \in S$;
(H) $\min\{\alpha(x), \alpha(y)\} \leq \alpha(x + y)$ for all $x, y \in S$;
(K) $\alpha(x + y) = \min\{\alpha(x), \alpha(y)\}$ for all $x, y \in S$.

7.1 Lemma. (i) *(C) $\Leftrightarrow$ (A) and (B).*
(ii) *(F) $\Leftrightarrow$ (D) and (E).*
(iii) *(K) $\Leftrightarrow$ (G) and (H).*
(iv) *(G) $\Rightarrow$ (D).*
(v) *(E) $\Rightarrow$ (H).*

Proof. It is obvious. □

7.2 Lemma. (i) *If $Q_{ps} = Q$ then (D) $\Rightarrow$ (A) and (B) $\Rightarrow$ (E).*
(ii) *If $Q_{ng} = Q$ then (H) $\Rightarrow$ (B) and (A) $\Rightarrow$ (G).*

Proof. It is easy. □

7.3 Lemma. (i) *(A) $\Rightarrow \alpha(x_1 + \cdots + x_n) \leq \alpha(x_1) + \cdots + \alpha(x_n)$ for all $n \geq 1$ and $x_1, \dots, x_n \in S$.*
(ii) *(B) $\Rightarrow \alpha(x_1) + \cdots + \alpha(x_n) \leq \alpha(x_1 + \cdots + x_n)$ for all $n \geq 1$ and $x_1, \dots, x_n \in S$.*
(iii) *(C) $\Rightarrow \alpha(x_1 + \cdots + x_n) = \alpha(x_1) + \cdots + \alpha(x_n)$ for all $n \geq 1$ and $x_1, \dots, x_n \in S$.*

Proof. Easy (by induction on n). □

7.4 Lemma. (i) *(A)* $\Rightarrow \alpha(nx) \leq n\alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$.
(ii) *(B)* $\Rightarrow n\alpha(x) \leq \alpha(nx)$ *for all* $x \in S$ *and* $n \geq 1$.
(iii) *(C)* $\Rightarrow \alpha(nx) \leq n\alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$.

Proof. An easy consequence of 7.3. □

7.5 Lemma. (i) *(D)* $\Rightarrow \alpha(x_1 + \cdots + x_n) \leq \max\{\alpha(x_1), \ldots, \alpha(x_n)\}$ *for all* $n \geq 1$ *and* $x_1, \ldots, x_n \in S$.
(ii) *(E)* $\Rightarrow \max\{\alpha(x_1), \ldots, \alpha(x_n)\} \leq \alpha(x_1 + \cdots + x_n)$ *for all* $n \geq 1$ *and* $x_1, \ldots, x_n \in S$.
(iii) *(F)* $\Rightarrow \alpha(x_1 + \cdots + x_n) = \max\{\alpha(x_1), \ldots, \alpha(x_n)\}$ *for all* $n \geq 1$ *and* $x_1, \ldots, x_n \in S$.
(iv) *(G)* $\Rightarrow \alpha(x_1 + \cdots + x_n) \leq \min\{\alpha(x_1), \ldots, \alpha(x_n)\}$ *for all* $n \geq 1$ *and* $x_1, \ldots, x_n \in S$.
(v) *(H)* $\Rightarrow \min\{\alpha(x_1), \ldots, \alpha(x_n)\} \leq \alpha(x_1 + \cdots + x_n)$ *for all* $n \geq 1$ *and* $x_1, \ldots, x_n \in S$.
(vi) *(K)* $\Rightarrow \alpha(x_1 + \cdots + x_n) = \min\{\alpha(x_1), \ldots, \alpha(x_n)\}$ *for all* $n \geq 1$ *and* $x_1, \ldots, x_n \in S$.

Proof. Easy (by induction on n). □

7.6 Lemma. (i) *(D)* $\Rightarrow \alpha(nx) \leq \alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$.
(ii) *(E)* $\Rightarrow \alpha(x) \leq \alpha(nx)$ *for all* $x \in S$ *and* $n \geq 1$.
(iii) *(F)* $\Rightarrow \alpha(nx) = \alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$.
(iv) *(G)* $\Rightarrow \alpha(nx) \leq \alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$.
(v) *(H)* $\Rightarrow \alpha(x) \leq \alpha(nx)$ *for all* $x \in S$ *and* $n \geq 1$.
(vi) *(K)* $\Rightarrow \alpha(nx) = \alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$.

Proof. An easy consequence of 7.5. □

7.7 Lemma. *Assume that (A) is true and* $\alpha(nx) \leq \alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$. *Let* $u, v \in S$, $a = \max\{\alpha(u), \alpha(v)\}$. *Then:*
(i) $\alpha((u + v)^m) \leq (m + 1)a^m$ *for every* $m \geq 1$.
(ii) *If* $1_Q \in Q$ *and* $a^{-1} \in Q$ *then* $\alpha((u + v)^m)a^{-m} = (\alpha(u + v)a^{-1})^m \leq (m + 1)1_Q$.

Proof. (i) We have $(u + v)^m = u^m + \binom{m}{1}u^{m-1}v + \cdots + \binom{m}{m-1}uv^{m-1} + v^m$, and hence $\alpha((u + v)^m) \leq \alpha(u^m) + \alpha(u^{m-1}v) + \cdots + \alpha(uv^{m-1}) + \alpha(v^m)$ (use 7.3 and the assumption). Furthemore, $\alpha(u^m) \leq a^m, \alpha(u^{m-1}v) \leq a^m, \ldots \alpha(uv^{m-1}) \leq a^m$ and $\alpha(v^m) \leq a^m$. Thus $\alpha((u + v)^m) \leq (m + 1)a^m$.

(ii) This follows easily from (i).

□

7.8 Remark. Consider the situation from 7.7(ii) and assume that $\alpha(u + v)a^{-1} = 1_Q + b$ for some $b \in Q$ (i.e., $\alpha(u + v) = a + ab$). Furthemore, let $k \geq 3$ be an odd integer such that $1_Q \leq kb$ and $1_Q \leq ((k - 1)/2)b^2$. Put $c = kb + ((k - 1)/2)b^2$ and $d = \binom{k}{3}b^3 + \binom{k}{4}b^4 + \cdots + \binom{k}{k-1}b^{k-1} + b^k$. Then $c + d + 1_Q = (1_Q + b)^k = (\alpha(u + v)a^{-1})^k$ and we have $c + d + 1_Q \leq (k + 1)1_Q$ by 7.7(ii). Moreover, $(k + 1)1_Q = 1_Q + k1_Q \leq kb + ((k - 1)/2)b^2 = c$. Thus $c + d + 1_Q \leq (k + 1)1_Q \leq c$, and hence $c + d + 1_Q \leq c$.

If Q is additively cancellative and $c + d + 1_Q = c$, then $d + 1_Q = 0_Q \in Q$. Consequently, $ed + e = e0_Q = 0_Q$ (see 2.5(i)) for every $e \in Q$ and it follows that Q is a ring.

By 1.8(ii), we have $Q^2 = 0_Q$, i.e., Q is a zero multiplication ring. Then, of course, $\alpha(xy) = \alpha(x)\alpha(y) = 0_Q$ for every $x, y \in S$.

7.9 Lemma. *Assume that $1_S \in S$. Then:*

(i) *$\alpha(1_S)\alpha(x) = \alpha(x)$ for every $x \in S$.*

(ii) *If $1_Q \in Q$ and $\alpha(y)^{-1} \in Q$ for at least one $y \in S$, then $\alpha(1_S) = 1_Q$.*

(iii) *If Q is multiplicatively cancellative then $1_Q \in Q$ and $\alpha(1_S) = 1_Q$.*

Proof. Easy to check. □

7.10 Lemma. *If $0_S \in S$ and $S \cdot 0_S = \{0_S\}$ then $\alpha(x)\alpha(0_S) = \alpha(0_S)$ for every $x \in S$.*

Proof. It is obvious. □

7.11 Lemma. *If (A) is true and $0_S \in S$ then $\alpha(x) \le \alpha(x) + \alpha(0_S)$ for every $x \in S$.*

Proof. It is obvious. □

7.12 Lemma. *Assume that $0_Q \in Q$. Let $v \in S$ be such that $\alpha(v) = 0_Q$.*

(i) *If $Q \cdot 0_Q = \{0_Q\}$ then $\alpha(xv) = 0_Q$ for every $x \in S$.*

(ii) *If (A) is true then $\alpha(x + v) \le \alpha(x)$ for every $x \in S$.*

Proof. It is obvious. □

7.13. Assume that Q is a parasemifield (see 5.1, ..., 5.5).

7.13.1 Lemma. *Assume that $1_S \in S$. Then:*

(i) *$\alpha(1_S) = 1_Q$.*

(ii) *If $x \in S$ is such that $x^{-1} \in S$, then $\alpha(x^{-1}) = \alpha(x)^{-1}$.*

Proof. It is obvious. □

7.13.2 Lemma. *If $v \in S$ is such that $\alpha(v) = 1_Q$, then $\alpha(vx) = \alpha(x)$ for every $x \in S$.*

Proof. It is obvious. □

7.13.3 Lemma. *Assume that $0_S \in S$ and $S \cdot 0_S = \{0_S\}$. Then:*

(i) *$\alpha(x) = 1_Q$ for every $x \in S$.*

(ii) *α satisfies the conditions (D), ..., (K).*

(iii) *α satisfies (A) if and only if $1_Q \le 2_Q$ (e.g., $1_Q \in Q_{ps}$;* see 5.2*).*

(iv) *α satisfies (B) if and only if $2_Q \le 1_Q$ (e.g., $1_Q \in Q_{ng}$;* see 5.2*).*

(v) *If Q is additively cancellative then either α satisfies (A) or (B).*

Proof. It is easy (use 7.10 and 5.3). □

7.13.4 Lemma. *Assume that Q is additively cancellative, semisubtractive and that $Q_{ps} = Q$* (see 2.14, 5.3)*. Assume further that for every $a \in Q$ there is a positive integer m such that $1_Q \le ma$. The following conditions are equivalent:*

(i) *The condition (D) is satisfied.*
(ii) *(A) is satisfied and* $\alpha(nx) \leq \alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$.

Moreover, if $1_S \in S$ *then these conditions are equivalent to:*
(iii) *(A) is satisfied and* $\alpha(n1_S) \leq 1_Q$ *for every* $n \geq 1$.

Proof. (i) implies (ii). Since $Q_{ps} = Q$, we have $\alpha(x) \leq \alpha(x) + \alpha(y)$ and $\alpha(y) \leq \leq \alpha(x) + \alpha(y)$. Thus $\alpha(x + y) \leq \max\{\alpha(x), \alpha(y)\} \leq \alpha(x) + \alpha(y)$. The inequality $\alpha(nx) \leq \alpha(x)$ is clear (see 7.6(i)).

(ii) implies (i). Let $u, v \in S$ and $a = \max\{\alpha(u), \alpha(v)\}$. If $\alpha(u + v)a^{-1} \leq 1_Q$ then $\alpha(u + v) \leq a$. Consequently, assume that $1_Q < \alpha(u + v)a^{-1}$. Then it follows from 2.14 that $\alpha(u + v)a^{-1} = 1_Q + b$ for some $b \in Q$. Furthermore, according to our assumption, there is a positive integer r with $1_Q \leq rb$ and a positive integer s such that $1_Q \leq sb^2$. Choosing an odd integer k such that $\max\{3, r, 2s + 1\} \leq k$, we get $1_Q \leq kb$ and $1_Q \leq ((k - 1)/2)b^2$. Put $c = kb + ((k - 1)/2)b^2$ and $d = = \binom{k}{3}b^3 + \binom{k}{4}b^4 + \cdots + \binom{k}{k-1}b^{k-1} + b^k$. Then $c + d + 1_Q \leq c$ (see 7.8). On the other hand, since $Q_{ps} = Q$, we have $c \leq c + d + 1_Q$. Thus $c = c + d + 1_Q$ and $d + 1_Q = 0_Q$, a contradiction with 5.1.

Finally, assume that $1_S \in S$. We have $\alpha(1_S) = 1_Q$ by 7.13.1, and so (ii) implies (iii). Conversely, if (iii) is true then $\alpha(nx) = \alpha(n1_S \cdot x) = \alpha(n1_S)\alpha(x) \leq 1_Q\alpha(x) = = \alpha(x)$.

□

7.14. Assume that Q is a semifield (see 6.1, ..., 6.5) and put $P = Q\backslash\{0_Q\}$; $P(\cdot)$ is a subgroup of the multiplicative semigroup $Q(\cdot)$ and we denote by e the unit element of P.

7.14.1 Lemma. *Assume that* $1_S \in S$ *and that* $\alpha(x) \neq 0_S$ *for at least one* $x \in S$. *Then* $\alpha(1_S) = e$.

Proof. It is obvious (see 7.9(i)). □

7.14.2 Lemma. *If* $v \in S$ *is such that* $\alpha(v) = e$*, then* $\alpha(vx) = \alpha(x)$ *for every* $x \in S$ *such that* $\alpha(x) \neq 0_S$.

Proof. It is obvious. □

7.14.3 Lemma. *Assume that* $0_S \in S, S \cdot 0_S = \{0_S\}$ *and* $\alpha(0_S) \neq 0_Q$. *Then:*
(i) $\alpha(x)e = e$ *for every* $x \in S$.
(ii) *If* $v \in S$ *is such that* $\alpha(v) \neq 0_Q$ *then* $\alpha(v) = e$.
(iii) $\alpha(0_S) = e$.
(iv) *If* $\alpha(x) \neq 0_Q$ *for every* $x \in S$, *then* $\alpha(x) = \{e\}$ *(and* $e \leq 2e$*).*
(v) *If* $\alpha(u) = 0_Q$ *for at least one* $u \in S$ *then* $0_Qe = e$ *and* $|Q| = 2$ *(and* $0_Q \leq e$*).*

Proof. It is easy (use 7.10 and 6.1). □

7.14.4 Lemma. *Assume that* $0_S \in S, S \cdot 0_S = \{0_S\}$ *and* $\alpha(0_S) = 0_Q$. *Then:*

(i) $\alpha(x)0_Q = 0_Q$ *for every* $x \in S$.

(ii) *If* $e0_Q \neq 0_Q$ *(see 6.1) then* $|Q| = 2$ *and* $\alpha(S) = \{0_S\}$.

Proof. It is easy (use 7.10 and 6.1). □

In the remaining part of this section, assume that $1_Q \in Q$ and $Q \cdot 0_Q = \{0_Q\}$ (see 6.1 and 6.2).

7.14.5 Lemma. (i) *If* $1_S \in S$ *then either* $\alpha(S) = \{0_Q\}$ *or* $\alpha(1_S) = 1_Q$.

(ii) *If* $0_S \in S$ *and* $S \cdot 0_S = \{0_S\}$ *then either* $\alpha(S) = \{1_Q\}$ *(and* $1_Q \leq 2_Q$*) or* $\alpha(0_S) = 0_Q$.

Proof. It is easy (use 7.14.3 and 7.14.4). □

7.14.6 Lemma. *Assume that* $0_Q \leq Q$ (see 6.4) *and put* $T = \{v \in S | \alpha(v) = 0_Q\}$. *Then:*

(i) *Either* $T = \emptyset$ *or* T *is an ideal of the semiring* S.

(ii) *If* $1_S \in T$ *then* $\alpha(S) = \{0_Q\}$.

Proof. Easy (use 7.14.5(i)). □

7.14.7 Lemma. *Assume that* Q *is additively cancellative, semisubtractive and that* $Q_{ps} = Q$ (see 2.14 and 6.4)*. Assume further that for every* $a \in Q \setminus \{0_Q\}$ *there is a positive integer* m *such that* $1_Q \leq ma$*. The following conditions are equivalent:*

(i) *The condition (D) is satisfied.*

(ii) *(A) is satisfied and* $\alpha(nx) \leq \alpha(x)$ *for all* $x \in S$ *and* $n \geq 1$.

Moreover, if $1_S \in S$ *then these conditions are equivalent to:*

(iii) *(A) is satisfied and* $\alpha(n1_S) \leq 1_Q$ *for every* $n \geq 1$.

Proof. Using 6.3, 6.5 and 7.14.6, we can proceed similarly as in the proof of 7.13.4. □

References

[1] El Bashir, R., Hurt, J., Jančařík, A. and Kepka, T.: *Simple commutative semirings*, J. Algebra **236** (2001), 277–306.

[2] El Bashir, R. and Kepka, T.: *Congruence-simple semirings*, Semigroup Forum **75** (2007), 588–608.

[3] Maze, G. and Monico, Ch.: *Public key cryptography based on semigroup actions* Adv. Math. Commun. **1** (2007), 489–507.

[4] Monico, Ch.: *On finite congruence-simple semirings*, J. Algebra **271** (2004), 846–854.