Vítězslav Kala; Tomáš Kepka; Jon D. Phillips

Various subsemirings of the field $\mathbb{Q}$ of rational numbers

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 50 (2009), No. 1, 29--59

Persistent URL: http://dml.cz/dmlcz/142779

Various Subsemirings of the Field $\mathbb{Q}$ of Rational Numbers

V. KALA, T. KEPKA, M. KORBELÁŘ and J. D. PHILLIPS

Praha

Received 15. October 2008

Various subsemirings of the field $\mathbb{Q}$ of rational numbers are studied. For every subsemiring of $\mathbb{Q}^+$ a set of characteristic sequences is presented. All maximal subsemirings of $\mathbb{Q}^+$ are found and classified.

1. Introduction

A (commutative) *semiring* is an algebraic structure with two commutative and associative binary operations (an addition and a multiplication) such that the multiplication distributes over the addition. The notion of semiring seems to have first appeared in the literature in a 1934 paper by Vandiver [4]. Semirings are widely used in various branches of mathematics and computer science and in everyday practice as well (the semiring of natural numbers for instance).

The structure of subrings and subgroups of rational numbers is quite well known. On the other hand, structural properties of subsemirings and subsemigroups of $\mathbb{Q}$ is not well understood, although the concept of semiring is a very basic one. In this paper we present a natural way how to deal with subsemirings of positive rational numbers.

Department of Algebra MFF UK, Sokolovská 83 186 75 Praha 8, Czech Republic
Department of Mathematics & Computer Science Wabash College Crawfordsville, IN 47933 USA

2000 Mathematics Subject Classification. 11A99, 16Y60

Key words and phrases. Semiring, rational number.

Partially supported by the institutional grant MSM 113200007. The first author was supported by the Grant Agency of Charles University #8648/2008 and the second author was supported by the Grant Agency of Czech Republic, No. 201/09/0296.

E-mail address: vita211@gmail.com
E-mail address: kepka@karlin.mff.cuni.cz
E-mail address: miroslav.korbelar@gmail.com
E-mail address: phillipj@wabash.edu

For every subsemiring S of $\mathbb{Q}^+$ and every prime number p we define, using the p-prime valuation function, a characteristic sequence of S. Such sequences can be, on the other hand, used for construction of a semiring that is (in some sense) a good approximation of the original one. Using this idea we find and classify all maximal subsemirings of positive rational numbers. As we will see, there is an uncountable amount of them. In the end, we use this method to present another way of classifying subgroups of $\mathbb{Q}(+)$.

For a more thorough introduction to semirings and a large collection of references, the reader is referred to [1], [2], [3], [5] and [6].

2. Preliminaries

A semiring is called

(i) *unitary* if the multiplicative semigroup $S(\cdot)$ has a neutral element (usually denoted by 1_S or 1);

(ii) *nullary* if the additive semigroup $S(+)$ has a neutral element (usually denoted by 0_S or 0);

(iii) a *ring* if the additive semigroup $S(+)$ is an (abelian) group;

(iv) a *semifield* if it is nullary and the set $S\setminus\{0\}$ is a subgroup of the multiplicative semigroup of S;

(v) a *parasemifield* if the multiplicative semigroup of S is a non-trivial group;

(vi) a *field* if S is both a ring and a semifield.

In the sequel we will use the following notation:

(i) $\mathbb{Z}$, the ring of integers;

(ii) $\mathbb{Q}$, the field of rationals;

(iii) $\mathbb{R}$, the field of reals;

(iv) $\mathbb{Z}^+$ ($\mathbb{Z}_0^+$, respectively), the semiring of positive (non-negative, respectively) integers;

(v) $\mathbb{Q}^+$ ($\mathbb{R}^+$, respectively), the parasemifield of positive rationals (reals, respectively);

(vi) $\mathbb{Q}_0^+$ ($\mathbb{R}_0^+$, respectively), the semifield of non-negative rationals (reals, respectively);

(vii) $\mathbb{Z}_0^-$ (respectively $\mathbb{Q}_0^-, \mathbb{R}_0^-$), the set (and additive semigroup) of non-positive integers (rationals, reals respectively);

(viii) $\mathbb{Q}^*$ ($\mathbb{R}^*$, respectively) the multiplicative group of non-zero rationals (reals, respectively);

(ix) $\mathbb{Q}_1^+ = \{q \in \mathbb{Q} : 1 \leq q\}$ (a unitary subsemiring of $\mathbb{Q}$);

(x) ${}_1\mathbb{Q}^+ = \{q \in \mathbb{Q} : 0 < q < 1\}$ (a subsemigroup of the multiplicative group $\mathbb{Q}^*$);

(xi) ${}_1\mathbb{R}^+ = \{r \in \mathbb{R} : 0 < r < 1\}$ (a subsemigroup of $\mathbb{R}^*$);

(xii) $\mathbb{P}$, the set of (positive) prime integers.

For all $p \in \mathbb{P}$ and $q \in \mathbb{Q}^*$, there exists a uniquely determined integer $v_p(q)$ such that $q = \pm \prod_{p\in\mathbb{P}} p^{v_p(q)}$; (of course, only finitely many of the numbers $v_p(q)$ are non-zero).

Lemma 2.1 *Let $p \in \mathbb{P}$ and $r, s \in \mathbb{Q}^*$. Then*

(i) $v_p(-r) = v_p(r)$;

(ii) $v_p(rs) = v_p(r) + v_p(s)$;

(iii) $v_p(r + s) \geq \min(v_p(r), v_p(s))$, *provided that* $r \neq -s$;

(iv) $v_p(r + s) = \min(v_p(r), v_p(s))$, *provided that* $v_p(r) \neq v_p(s)$.

Proof. (i) and (ii). Easy to check.

(iii) We have $r = r_1 p^k$ and $s = s_1 p^l$ where $k = v_p(r), l = v_p(s), v_p(r_1) = 0 = v_p(s_1)$, and we can assume that $l \leq k$. Then $r + s = p^l t, t = s_1 + r_1 p^{k-l}, k - l \geq 0$. Further, $r_1 = a/b$ and $s_1 = c/d$, where $a, b, c, d \in \mathbb{Z}^*$ and p divides neither b nor d. Now, $t = (ad + bcp^{k-l})/bd, v_p(t) \geq 0$ and $v_p(r + s) = l + v_p(t) \geq l = \min(v_p(r), v_p(s))$.

(iv) We can assume that $v_p(s) < v_p(r)$. Then $v_p(s) = v_p(r + s - r) \geq \min(v_p(r + s), v_p(r))$, and so $v_p(s) \geq v_p(r + s) \geq \min(v_p(r), v_p(s)) = v_p(s)$. Thus $v_p(r + s) = \min(v_p(r), v_p(s))$. □

Lemma 2.2 *For all $m \in \mathbb{Z}^+, p_1, p_2, \dots, p_m \in \mathbb{P}, p_1 < p_2 < \dots < p_m, n_1, n_2, \dots, n_m \in \mathbb{Z}$, and $r, s \in \mathbb{Q}, r < s$, there exists at least one $t \in \mathbb{Q}^*$ such that $r < t < s$, and $v_{p_i}(t) = n_i, 1 \leq i \leq m$.*

Proof. Find $p_0 \in \mathbb{P} \setminus \{p_1, \dots, p_m\}$ such that $a = p_1^{n_1+1} \dots p_m^{n_m+1}/p_0 < (s - r)/2$. Then $2a < s - r$ and $a = p_1 \dots p_m b > b$, where $b = p_1^{n_1} \dots p_m^{n_m}/p_0$. Obviously there is $k \in \mathbb{Z}$ such that $(k - 1)a \leq r < ka$ and we put $t = ka + b = (kp_1 \dots p_m + 1)b$. Clearly, $r < ka < t = (k - 1)a + a + b \leq r + a + b < r + 2a < r + (s - r) = s$; thus $r < t < s$. Moreover, $v_{p_i}(t) = v_{p_i}((kp_1 \dots p_m + 1)b) = v_{p_i}(kp_1 \dots p_m + 1) + v_{p_i}(b) = v_{p_i}(b) = n_i$, for $1 \leq i \leq n$. □

For all $p \in \mathbb{P}, r \in {}_1\mathbb{R}^+$ and $q \in \mathbb{Q}^*$, put $|q|_{p,r} = r^{v_p(q)} \in \mathbb{R}^+$. Put also $|0|_{p,r} = 0$.

Lemma 2.3 *Let $q_1, q_2 \in \mathbb{Q}$. Then:*

(i) $|q_1|_{p,r} = 0$ *if and only if* $q_1 = 0$;

(ii) $|q_1 q_2|_{p,r} = |q_1|_{p,r} \cdot |q_2|_{p,r}$;

(iii) $|q_1 + q_2|_{p,r} \leq \max\{|q_1|_{p,r}, |q_2|_{p,r}\}$; *and*

(iv) $|q_1 + q_2|_{p,r} = \max\{|q_1|_{p,r}, |q_2|_{p,r}\}$, *provided that* $|q_1|_{p,r} \neq |q_2|_{p,r}$.

Proof. Taking into account the definition of the norm $|q|_{p,r}$, the equalities follow from 2.1. □

For every $m \in \mathbb{Z}_0^+$, let $\mathfrak{R}_m$ denote the set of sequences $\boldsymbol{r} = (r_m, r_{m+1}, r_{m+2}, \dots)$ of non-negative real numbers such that

(A) $r_{n+k} \leq r_n \cdot r_k$ whenever $m \leq n$ and $m \leq k$.

Furthermore, let $\overline{\mathfrak{R}}_m$ denote the set of the sequences $\boldsymbol{r} \in \mathfrak{R}_m$ such that

(B) $r_k \leq r_n$ whenever $m \leq n \leq k$.

Lemma 2.4 *Let $m \in \mathbb{Z}_0^+$ and $\boldsymbol{r} \in \mathfrak{R}_m$.*

(i) *If $m_0 \geq m$ is such that $r_{m_0} = 0$, then $r_k = 0$ for every $k \geq m + m_0$;*

(ii) *If $m = 0$ and $r_0 = 0$, then $\boldsymbol{r} = 0$ (i.e., $r_k = 0$ for every $k \in \mathbb{Z}, k \geq m$).*

Proof.

(i) We have $k - m_0 \geq m$ and $r_k = r_{k-m_0+m_0} \leq r_{k-m_0} \cdot r_{m_0} = 0$ by (A). Thus $r_k = 0$.

(ii) This follows immediately from (i).

□

Lemma 2.5 *Let $\boldsymbol{r} \in \mathfrak{R}_0$. If $r_0 = 0$, then $\boldsymbol{r} = 0$. If $r_0 \neq 0$, then $r_0 \geq 1$.*

Proof. We have $r_n \leq r_n \cdot r_0$ and $r_0 \leq r_0^2$. The rest is clear. □

Lemma 2.6 *Let $m \in \mathbb{Z}_0^+$ and $\boldsymbol{r} \in \mathfrak{R}_m$. Then either* $\lim\{r_n : n \geq m\} = \inf\{r_n : n \geq m\} = 0$ *or $r_n \geq 1$ for every $n \geq m$.*

Proof. Assume that $r_k < 1$ for some $k \geq m$. If $k = 0$, then using 2.5 is $r_0 = 0, \boldsymbol{r} = 0$ and our assertion is true. Hence, assume $k > 0$. Now, if $2k \leq n$ then $n = lk + j$ for some $l \geq 2$ and $0 \leq j < k$. We have $r_n \leq r_{k+j} \cdot r_k^{l-1}$, and therefore $r_n \leq r_{k+j} \cdot r_k^{(n-j-k)/k}$ and it follows that $\lim\{r_n : n \geq m\} = 0$. □

Lemma 2.7 *Let $m \in \mathbb{Z}^+$ and $\boldsymbol{r} \in \mathfrak{R}_m$. Then $\lambda(\boldsymbol{r}) = \inf\{r_n^{1/n} : n \geq m\} = \lim\{r_n^{1/n} : n \geq m\}$. Moreover, if $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$, then $\lambda(\boldsymbol{r}) \leq 1$.*

Proof. If $r_{m_0} =$ for some $m_0 \geq m$, then $\lambda(\boldsymbol{r}) = 0$ by 2.4 (i) and there is nothing to prove. Hence, assume that $r_n \neq 0$ for every $n \geq m$. Now, if $m \leq k < n$ then $n = lk + j$ for some $l \geq 1$ and $0 \leq j < k$. We have $r_n \leq r_{k+j} \cdot r_k^{l-1}$, and therefore $r_n^{1/n} \leq r_{k+j}^{1/n} \cdot r_k^{(l-1)/n} = r_{k+j}^{1/n} \cdot (r_k^{1/k})^{(n-j-k)/n}$. Using this, one sees easily that $\limsup\{r_n^{1/n}\} \leq r_k^{1/k}$. Consequently, $\lambda(\boldsymbol{r}) \leq \liminf\{r_n^{1/n}\} \leq \limsup\{r_n^{1/n}\} \leq \lambda(\boldsymbol{r})$, and so $\lambda(\boldsymbol{r}) = \lim\{r_n^{1/n}\}$. Finally, if $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$, then $\lambda(\boldsymbol{r}) \leq 1$ by 2.6. □

Let $\mathfrak{R}_\infty$ denote the set of $\mathbb{Z}$-sequences $\boldsymbol{r} = (\ldots, r_{-2}, r_{-1}, r_0, r_1, r_2, \ldots)$ of non-negative real numbers such that

(A′) $r_{n+k} \leq r_n \cdot r_k$ for all $n, k \in \mathbb{Z}$.

Furthermore, let $\overline{\mathfrak{R}}_\infty$ denote the set of the sequences $\boldsymbol{r} \in \mathfrak{R}_\infty$ such that

(B′) $r_k \leq r_n$ whenever $n, k \in \mathbb{Z}, n \leq k$.

Lemma 2.8 *Let $\boldsymbol{r} \in \mathfrak{R}_\infty, \boldsymbol{r}^+ = (r_1, r_2, r_3, \ldots)$ and $\boldsymbol{r}^- = (r_{-1}, r_{-2}, r_{-3}, \ldots)$. Then:*

(i) *Either $\boldsymbol{r} = 0$ or $r_n \neq 0$ for every $n \in \mathbb{Z}$. In the latter case, $r_0 \geq 1$ and $r_{-m} \geq 1/r_m$ for every $m \geq 1$.*

(ii) $s = \lambda(\boldsymbol{r}^+) = \inf\{r_m^{1/m} : m \geq 1\} = \lim\{r_m^{1/m} : m \geq 1\}$.

(iii) $t = \lambda(\boldsymbol{r}^-) = \inf\{r_{-m}^{1/m} : m \geq 1\} = \lim\{r_{-m}^{1/m} : m \geq 1\}$.

(iv) *$s^m \leq r_m$ and $t^m \leq r_{-m}$ for every $m \geq 1$.*

(v) *$st \geq 1$, provided that $r_0 \neq 0$ (see (i)).*

(vi) *If $0 < r_n < 1$ for at least one $n \geq 1$, then $0 < s < 1 < t$.*

Proof. (i) We have $r_0 = r_{n-n} \le r_n \cdot r_{-n}$ and $r_0 \le r_0^2$.
(ii) and (iii). Clearly, $\boldsymbol{r}^+ \in \mathfrak{R}_1$ and $\boldsymbol{r}^- \in \mathfrak{R}_1$, and 2.7 applies.
(iv) See (ii) and (iii).
(v) We have $1 \le r_0^{1/m} \le r_m^{1/m} \cdot r_{-m}^{1/m}$ for every $m \ge 1$. But $st = \lim\{r_m^{1/m} \cdot r_{-m}^{1/m}\}$.
(vi) We have $s \le r_n^{1/n} < 1$.

□

Lemma 2.9 *Let* $\boldsymbol{r} \in \overline{\mathfrak{R}}_\infty$. *Then:*

(i) $\boldsymbol{r}^+ \in \overline{\mathfrak{R}}_1$.
(ii) *Either* $\lim\{r_m : m \ge 0\} = 0$ *or* $r_n \ge 1$ *for every* $n \in \mathbb{Z}$.
(iii) $\lambda(\boldsymbol{r}^+) \le 1$.
(iv) *If* $r_0 \ne 0$, *then* $\lambda(\boldsymbol{r}^-) \ge 1$.

Proof. See 2.8. □

Remark 2.10 Let $m \in \mathbb{Z}_0^+$ and $\boldsymbol{r} \in \mathfrak{R}_m$ be such that $r_n > 0$ for every $n \ge m$ (see 2.4 (i), (ii)). For every $k \in \mathbb{Z}_0^+$, put $\sigma_k(\boldsymbol{r}) = \sup\{r_{n+k}/r_n : n \ge m\} \in \mathbb{R}^+ \cup \{\infty\}$ and $\rho_k(\boldsymbol{r}) = \sup\{r_n/r_{n+k} : n \ge m\} \in \mathbb{R}^+ \cup \{\infty\}$.

Lemma 2.11

(i) $\sigma_0(\boldsymbol{r}) = 1$ *and* $0 < r_{n+k}/r_n \le \sigma_k(\boldsymbol{r}) \le \sigma_1(\boldsymbol{r})^k$ *for every* $k \in \mathbb{Z}_0^+$ *and* $n \ge m$.
(ii) $\sigma_l(\boldsymbol{r}) \le r_l$ *for every* $l \ge m$.
(iii) *If* $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$, *then* $\sigma_k(\boldsymbol{r}) \le 1$ *for every* $k \in \mathbb{Z}_0^+$.

Proof.

(i) We have $r_{n+k}/r_n = \prod_{i=n}^{n+k-1} r_{i+1}/r_i \le \sigma_1(\boldsymbol{r})^k$ for all $n \ge m$ and $k \ge 1$. The rest is clear.
(ii) We have $r_{n+l}/r_m \le r_l$.
(iii) Easy to see.

□

Lemma 2.12 $\sigma_k(\boldsymbol{r}) < \infty$ *for every* $k \in \mathbb{Z}_0^+$ *in each of the following four cases:*

(i) $\sigma_1(\boldsymbol{r}) < \infty$;
(ii) $m = 0, 1$;
(iii) $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$;
(iv) $r_{n_1} \le r_{n_2}$ *for all* $m \le n_1 \le n_2$.

Proof. If (i) is true, then the result follows from 2.11 (i). If (ii) is true, then from 2.11 (i), (ii). If (iii) is true, then 2.11 takes place. Finally, assume that (iv) is true. If $n \ge 2m - 1 \ge 3$, then $r_{n+1}/r_n \le r_m \cdot r_{n-m+1}/r_n \le r_m$. □

Lemma 2.13 *If* $\sigma_1(\boldsymbol{r}) < \infty$, *then* $\sigma(\boldsymbol{r}) = (\sigma_0(\boldsymbol{r}), \sigma_1(\boldsymbol{r}), \sigma_2(\boldsymbol{r}), \dots) \in \mathfrak{R}_0$.

Proof. By 2.12 (i), $\sigma_k(\boldsymbol{r}) < \infty$ for every $k \ge 0$. Furthermore, $r_{n+k+l}/r_{n+k} \le \sigma_l(\boldsymbol{r}) = \sup\{r_{n_1+l}/r_{n_1} : n_1 \ge m\}$ for all $n \ge m, k \ge 0$ and $l \ge 0$. Thus, $r_{n+k+l}/r_n \le \sigma_l(\boldsymbol{r}) \cdot r_{n+k}/r_n \le \sigma_l(\boldsymbol{r})\sigma_k(\boldsymbol{r})$ and it follows that $\sigma_{k+l}(\boldsymbol{r}) \le \sigma_k(\boldsymbol{r})\sigma_l(\boldsymbol{r})$. That is, $\sigma(\boldsymbol{r}) \in \mathfrak{R}_0$. □

Lemma 2.14 *If* $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$, *then* $\sigma(\boldsymbol{r}) \in \overline{\mathfrak{R}}_0$ *and* $\sigma_k(\boldsymbol{r}) \le 1$ *for every* $k \in \mathbb{Z}_0^+$.

Proof. By 2.11(iii), $\sigma_k(\boldsymbol{r}) \le 1$ and $\sigma(\boldsymbol{r}) \in \mathfrak{R}_0$ by 2.13. If $0 \le k \le l$, then $r_{n+l} \le r_{n+k}$, and so $r_{n+l}/r_n \le r_{n+k}/r_n$. Consequently, $\sigma_l(\boldsymbol{r}) \le \sigma_k(\boldsymbol{r})$ and $\boldsymbol{r} \in \overline{\mathfrak{R}}_0$. □

Lemma 2.15 *If* $m = 0$, *then* $r_0 \ge 1$ *and* $r_k/r_0 \le \sigma_k(\boldsymbol{r}) \le r_k$ *for every* $k \ge 0$. *If, moreover,* $r_0 = 1$, *then* $\sigma_k(\boldsymbol{r}) = r_k$ *(and hence* $\sigma(\boldsymbol{r}) = \boldsymbol{r}$*; see 2.13).*

Proof. We have $r_0 \ge 1$ by 2.5 and $r_k/r_0 \le \sigma_k(\boldsymbol{r}) \le r_k$ by 2.11(i), (ii). □

Lemma 2.16 *Let* $m = 1$, $s \in \mathbb{R}_1^+$ *and* $\boldsymbol{r}' = (s, \boldsymbol{r})$. *Then:*

(i) $\boldsymbol{r}' \in \mathfrak{R}_0$.
(ii) $\sigma_k(\boldsymbol{r}') = \max\{r_k/s, \sigma_k(\boldsymbol{r})\}$ *for every* $k \ge 1$.
(iii) *If* $\boldsymbol{r} \in \overline{\mathfrak{R}}_1$ *and* $s \ge r_1$, *then* $\boldsymbol{r}' \in \overline{\mathfrak{R}}_1$.

Proof. Easy to check. □

Lemma 2.17

(i) $\rho_0(\boldsymbol{r}) = 1$ *and* $0 < r_n/r_{n+k} \le \rho_k(\boldsymbol{r}) \le \rho_1(\boldsymbol{r})^k$ *for every* $k \in \mathbb{Z}_0^+$.
(ii) $1/r_l \le \rho_l(\boldsymbol{r})$ *for every* $l \ge m$.
(iii) *If* $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$, *then* $1 \le \rho_k(\boldsymbol{r})$ *for every* $k \in \mathbb{Z}_0^+$.

Proof.

(i) We have $r_n/r_{n+k} = \prod_{i=n}^{n+k-1} r_i/r_{i+1} \le \rho_1(\boldsymbol{r})^k$ for all $n \ge m$ and $k \ge 1$. The rest is clear.
(ii) We have $r_n/r_{n+l} \ge r_n/r_n r_l = 1/r_l$.
(iii) Easy to see.

□

Lemma 2.18 $\rho_k(\boldsymbol{r}) < \infty$ *for every* $k \in \mathbb{Z}_0^+$ *in each of the following two cases:*

(i) $\rho_1(\boldsymbol{r}) < \infty$;
(ii) $r_{n_1} \le r_{n_2}$ *for all* $m \le n_1 \le n_2$.

Proof. See 2.17(i), (ii). □

Lemma 2.19 *If* $\rho_1(\boldsymbol{r}) < \infty$, *then* $\rho(\boldsymbol{r}) = (\rho_0(\boldsymbol{r}), \rho_1(\boldsymbol{r}), \rho_2(\boldsymbol{r}), \dots) \in \mathfrak{R}_0$.

Proof. By 2.18, $\rho_k(\boldsymbol{r}) < \infty$ for every $k \ge 0$. Furthermore, $r_{n+k}/r_{n+k+l} \le \rho_l(\boldsymbol{r}) = \sup\{r_{n_1}/r_{n_1+l} : n_1 \ge m\}$ for all $n_1 \ge m, k \ge 0$ and $l \ge 0$. Thus $r_n/r_{n+k+l} \le \rho_l(\boldsymbol{r}) \cdot r_n/r_{n+k} \le \rho_l(\boldsymbol{r})\rho_k(\boldsymbol{r})$ and it follows that $\rho_{k+l}(\boldsymbol{r}) \le \rho_k(\boldsymbol{r})\rho_l(\boldsymbol{r})$. That is, $\rho(\boldsymbol{r}) \in \mathfrak{R}_0$. □

Lemma 2.20 *If* $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$, *then* $1 \le \rho_k(\boldsymbol{r}) \le \rho_l(\boldsymbol{r})$ *for all* $0 \le k \le l$.

Proof. Easy to see. □

Lemma 2.21 *Assume that* $\sigma_1(\boldsymbol{r}) < \infty$ *and* $\rho_1(\boldsymbol{r}) < \infty$. *Then* $\sigma_{l-k}(\boldsymbol{r}) \le \sigma_l(\boldsymbol{r})\rho_k(\boldsymbol{r})$ *and* $\rho_{l-k}(\boldsymbol{r}) \le \sigma_k(\boldsymbol{r})\rho_l(\boldsymbol{r})$ *for all* $0 \le k \le l$.

Proof. We have $r_{n+(l-k)}/r_{n+(l-k)+k} \leq \rho_k(\boldsymbol{r})$ for all $n \geq m$. Consequently, $r_{n+l-k}/r_n \leq$ $\leq \rho_k(\boldsymbol{r})r_{n+l}/r_n \leq \rho_k(\boldsymbol{r})\sigma_l(\boldsymbol{r})$, and hence $\sigma_{l-k}(\boldsymbol{r}) \leq \sigma_l(\boldsymbol{r})\rho_k(\boldsymbol{r})$.

Similarly, $r_{n+(l-k)+k}/r_{n+(l-k)} \leq \sigma_k(\boldsymbol{r})$ for all $n \geq m$. Consequently, $r_n/r_{n+l-k} \leq$ $\leq \sigma_k(\boldsymbol{r})r_n/r_{n+l} \leq \sigma_k(\boldsymbol{r})\rho_l(\boldsymbol{r})$, and hence $\rho_{l-k}(\boldsymbol{r}) \leq \sigma_k(\boldsymbol{r})\rho_l(\boldsymbol{r})$. □

Lemma 2.22 *Assume that* $\sigma_1(\boldsymbol{r}) < \infty, \rho_1(\boldsymbol{r}) < \infty$ *and put* $\tau(\boldsymbol{r}) =$ $(\dots, \rho_2(\boldsymbol{r}), \rho_1(\boldsymbol{r}), 1, \sigma_1(\boldsymbol{r}), \sigma_2(\boldsymbol{r}), \dots)$. *Then* $\tau(\boldsymbol{r}) \in \mathfrak{R}_\infty$. *Moreover, if* $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$ *then* $\tau(\boldsymbol{r}) \in \overline{\mathfrak{R}}_\infty$.

Proof. It is enough to combine 2.13, 2.14, 2.19, 2.20, and 2.21. □

Lemma 2.23 *Assume that* $m = 0$ *and* $\rho_1(\boldsymbol{r}) < \infty$. *Then* $\tilde{\tau}(\boldsymbol{r}) = (\dots, \rho_2(\boldsymbol{r}), \rho_1(\boldsymbol{r}), r_0,$ $r_1, r_2, \dots) \in \mathfrak{R}_\infty$ *Moreover:*

(i) If $(\dots, s_2, s_1, r_0, r_1, r_2, \dots) \in \mathfrak{R}_\infty$, *then* $\rho_k(\boldsymbol{r}) \leq s_k$ *for every* $k \geq 1$.

(ii) If $\boldsymbol{r} \in \overline{\mathfrak{R}}_0$ *and* $r_1 \leq 1$, *then* $\tilde{\tau}(\boldsymbol{r}) \in \overline{\mathfrak{R}}_\infty$.

Proof. If $0 \leq k \leq l$, then $r_{k-l}/r_{k-l+l} \leq \rho_l(\boldsymbol{r})$, and therefore $r_{k-l} \leq r_k \cdot \rho_l(\boldsymbol{r})$. Similarly, $r_{n+l} \leq r_{n+(l-k)}r_l$ for every $n \geq 0$, and therefore $r_n/r_{n+(l-k)} \leq r_k \cdot r_n/r_{n+l} \leq r_k\rho_l(\boldsymbol{r})$ and $\rho_{l-k}(\boldsymbol{r}) \leq r_k\rho_l(\boldsymbol{r})$. Now, using 2.19 we conclude that $\tilde{\tau}(\boldsymbol{r}) \in \mathfrak{R}_\infty$.

As concerns (i), if $n \geq 0$ and $k \geq 1$, then $r_n \leq s_k r_{n+k}$, so that $r_n/r_{n+k} \leq s_k$ and it follows that $\rho_k(\boldsymbol{r}) \leq s_k$. Finally, if $\boldsymbol{r} \in \overline{\mathfrak{R}}_0$ and $r_1 \leq 1$, then $\rho_1(\boldsymbol{r}) \geq r_0/r_1 \geq r_0$ and $\tilde{\tau}(\boldsymbol{r}) \in \overline{\mathfrak{R}}_\infty$ by 2.20. □

Lemma 2.24 *Consider the situation from 2.16. Then* $\rho_k(\boldsymbol{r}') = \max\{s/r_k, \rho_k(\boldsymbol{r})\}$ *for every* $k \geq 1$.

Proof. It is easy. □

Lemma 2.25 *Assume that* $m = 1$ *and* $\rho_1(\boldsymbol{r}) < \infty$. *Then* $\tilde{\tau}(\boldsymbol{r}) = (\dots, \rho_2(\boldsymbol{r}), \rho_1(\boldsymbol{r}), 1,$ $r_1, r_2, \dots) \in \mathfrak{R}_\infty$. *Moreover:*

(i) If $(\dots, s_2, s_1, s_0, r_1, r_2, \dots) \in \mathfrak{R}_\infty$, *then* $1 \leq s_0$ *and* $\rho_k(\boldsymbol{r}) \leq s_k$ *for every* $k \geq 1$.

(ii) If $\boldsymbol{r} \in \overline{\mathfrak{R}}_1$ *and* $r_1 \leq 1$, *then* $\tilde{\tau}(\boldsymbol{r}) \in \overline{\mathfrak{R}}_\infty$.

Proof. Combine 2.16 and 2.23. □

Lemma 2.26 *Assume that* $m \geq 2$ *and put* $\kappa(\boldsymbol{r}) = \max\{\sigma_{m-1}(\boldsymbol{r}), r_{2m-2}^{1/2}\}$.

(i) *If* $a \in \mathbb{R}^+$, *then* $(a, \boldsymbol{r}) \in \mathfrak{R}_{m-1}$ *if and only if* $a \geq \kappa(\boldsymbol{r})$.

(ii) *If* $a \in \mathbb{R}^+$ *and* $a \geq \kappa(\boldsymbol{r})$, *then* $\sigma_k((a, \boldsymbol{r})) = \max\{\sigma_k(\boldsymbol{r}), r_{m+k-1}/a\}$ *and* $\rho_k((a, \boldsymbol{r})) =$ $= \max\{\rho_k(\boldsymbol{r}), a/r_{m+k-1}\}$ *for every* $k \geq 1$.

(iii) *If* $a \in \mathbb{R}^+$ *and* $a \geq \kappa(\boldsymbol{r})$, *then* $(a, \boldsymbol{r}) \in \overline{\mathfrak{R}}_{m-1}$ *if and only if* $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$ *and* $a \geq r_m$.

Proof. (i) If $a \geq \kappa(\boldsymbol{r})$, then $r_{n+m-1}/r_n \leq \sigma_{m-1}(\boldsymbol{r}) \leq a$, and hence $r_{n+m-1} \leq r_n a$ for every $n \geq m$. Moreover, $r_{2m-2} \leq a^2$ and we see that $(a, \boldsymbol{r}) \in \mathfrak{R}_{m-1}$. Conversely, if $(a, \boldsymbol{r}) \in \mathfrak{R}_{m-1}$, then $r_{n+m-1}/r_n \leq a$ for every $n \geq m$ and $r_{2m-2} \leq a^2$. Thus, $a \geq \kappa(\boldsymbol{r})$.

(ii) and (iii). It is easy. □

Lemma 2.27 *If* $m \geq 2$ *and* $\sigma_{m-1}(\boldsymbol{r}) < \infty$, *then* $(\kappa(\boldsymbol{r}), \boldsymbol{r}) \in \mathfrak{R}_{m-1}$. *Moreover,* $(\kappa(\boldsymbol{r}), \boldsymbol{r}) \in \overline{\mathfrak{R}}_{m-1}$ *if and only if* $\boldsymbol{r} \in \mathfrak{R}_m$ *and* $\kappa(\boldsymbol{r}) \geq r_m$.

Proof. Use 2.26. □

Remark 2.28 Assume that $m \geq 2$.

(i) If $\sigma_1(\boldsymbol{r}) < \infty$, then $\sigma_{m-1}(\boldsymbol{r}) \leq \sigma_1(\boldsymbol{r})^{m-1}$ and hence $\kappa(\boldsymbol{r}) \leq \max\{\sigma_1(\boldsymbol{r})^{m-1}, r_{2m-2}^{1/2}\}$.

(ii) If $\sigma_{m-1}(\boldsymbol{r}) < \infty$, then $\sigma_1((\kappa(\boldsymbol{r}), \boldsymbol{r})) = \max\{\sigma_1(\boldsymbol{r}), r_m/\kappa(\boldsymbol{r})\}$. Of course, $r_m/\kappa(\boldsymbol{r}) \leq$ $\leq r_n r_m / r_{n+m-1}$ for every $n \geq m$.

(iii) If $\sigma_{m-1}(\boldsymbol{r}) < 1$ (e.g., if $\sigma_1(\boldsymbol{r}) < 1$) and $r_{2m-2} < 1$, then $\kappa(\boldsymbol{r}) < 1$. If, moreover, $r_m < 1$, then we can find $a \in {}_1\mathbb{R}^+$ such that $\kappa(\boldsymbol{r}) \leq a$ and $r_m < a$. We have $(a, \boldsymbol{r}) \in \mathfrak{R}_{m-1}$ and $r_m/a < 1$. By 2.26(ii), $\sigma_1((a, \boldsymbol{r})) = \max\{\sigma_1(\boldsymbol{r}), r_m/a\}$. Consequently, $\sigma_1((a, \boldsymbol{r})) < 1$, provided that $\sigma_1(\boldsymbol{r}) < 1$.

If $r_m^2 < r_{m+1}$, then we can choose a such that $r_m^2/r_{m+1} \leq a$. Then $r_m/a \leq$ $\leq r_{m+1}/r_m \leq \sigma_1(\boldsymbol{r})$, and so $\sigma_1((a, \boldsymbol{r})) = \sigma_1(\boldsymbol{r})$.

Lemma 2.29 *The following conditions are equivalent:*

(i) $\sigma_1(\boldsymbol{r}) < \infty$ *(i.e., there exists* $r \in \mathbb{R}^+$ *such that* $r_{n+1} \leq r \cdot r_n$ *for every* $n \geq m$*).*

(ii) *There exist* $r_0, r_1, \ldots, r_{m-1} \in \mathbb{R}^+$ *such that* $(r_0, \ldots, r_{m-1}, r_m, r_{m+1}, \ldots) \in \mathfrak{R}_0$.

Proof. (i) implies (ii). We will proceed by induction on m. The result is clear for $m = 0$ and follows from 2.16 for $m = 1$. If $m \geq 2$ then $\boldsymbol{r}' = (\kappa(\boldsymbol{r}), \boldsymbol{r}) \in \mathfrak{R}_{m-1}$ and $\sigma_1(\boldsymbol{r}') < \infty$ by 2.26(i),(ii).

(ii) implies (i). Obvious. □

Remark 2.30 Assume that $\sigma_1(\boldsymbol{r}) < \infty$ and consider the situation from 2.29 and put $\boldsymbol{r}' = (r_0, r_1, r_2, \ldots, r_{m-1}, r_m, r_{m+1}, \ldots) \in \mathfrak{R}_0$. We have $\sigma_1(\boldsymbol{r}') < \infty$.

(i) If $\rho_1(\boldsymbol{r}) < \infty$, then $\rho_1(\boldsymbol{r}') < \infty$.

(ii) If $\sigma_1(\boldsymbol{r}) < 1$ and $r_n < 1$ for every $n \geq m$, then the numbers $r_1, \ldots, r_{m-1}$ can be chosen from ${}_1\mathbb{R}^+$.

(iii) If $\boldsymbol{r} \in \overline{\mathfrak{R}_m}$, then the numbers $r_0, r_1, \ldots, r_{m-1}$ can be chosen such that $\boldsymbol{r}' \in \overline{\mathfrak{R}_0}$. If, moreover, $r_n < 1$ for every $n \geq m$ then we can find $r_1, \ldots, r_{m-1} \in {}_1\mathbb{R}^+$.

Lemma 2.31 *The following conditions are equivalent:*

(i) $\sigma_1(\boldsymbol{r}) < \infty$ *and* $\rho_1(\boldsymbol{r}) < \infty$.

(ii) There exist $\ldots, r_{-2}, r_{-1}, r_0, r_1, r_2, \ldots, r_{m-1} \in \mathbb{R}^+$ *such that* $(\ldots, r_{-2}, r_{-1}, r_0, r_1, r_2, \ldots, r_{m-1}, r_m, r_{m+1}, \ldots) \in \mathfrak{R}_\infty$.

Proof. (i) implies (ii). Taking into account 2.29 and 2.30, we can assume that $m = 0$. Now, the result follows from 2.23.

(ii) implies (i). Obvious. □

Example 2.32 We are going to construct a sequence $\boldsymbol{r} \in \mathfrak{R}_2$ such that $\lim\{r_n :$ $: n \geq 2\} = 0$ (see 2.6) and $\sigma_1(\boldsymbol{r}) = \infty = \rho_1(\boldsymbol{r})$. We will do it by induction.

First, choose $r_2, r_3 \in \mathbb{R}^+$ arbitrarily. Then assume that positive real numbers $r_2, r_3, \ldots, r_{2n-1}, n \geq 2$, are found such that $r_{i+j} \leq r_i r_j$ whenever $2 \leq i, j \leq 2n-1$ and $i + j \leq 2n-1$. Now, put $s_1 = \min\{r_i r_{2n-i} : i = 2, \ldots, 2n-2\}$, $s_2 = \min\{r_j r_{2n+1-j} :$ $j = 2, \ldots, 2n-1\}$ and $s = \min\{s_1, s_2, 1/n\}$. Choose $r_{2n}, r_{2n+1} \in \mathbb{R}^+$ such that $0 < r_{2n}, r_{2n+2} < s, n \leq r_{2n}/r_{2n+1}$ for even n and $n \leq r_{2n+1}/r_{2n}$ for n odd. The rest is easy.

Example 2.33 Put $r_n = 1/2^{n^2}$ for every $n \geq 2$. Then $\boldsymbol{r} = (r_2, r_3, r_4, \dots) \in \in \overline{\mathfrak{R}}_2$, $\sigma_1(\boldsymbol{r}) = 1/32$ and $\rho_1(\boldsymbol{r}) = \infty$. Moreover, $\kappa(\boldsymbol{r}) = 1/4$.

Example 2.34 Proceeding similarly as in 2.32 one can construct a sequence $\boldsymbol{r} \in \in \mathfrak{R}_2$ such that $\lim\{r_n : n \geq 2\} = 0, \sigma_1(\boldsymbol{r}) = \infty$ and $\rho_1(\boldsymbol{r}) < \infty$.

3. Subsemirings and subrings of $\mathbb{Q}$—First Observations

Proposition 3.1 *Let S be a subsemigroup of $\mathbb{Q}(+)$ such that $S \cap \mathbb{Q}^+ \neq \emptyset \neq S \cap \mathbb{Q}^-$. Then S is a subgroup of $\mathbb{Q}^+$.*

Proof. Let $a, b, c, d \in \mathbb{Z}^+$ be such that $a/b \in S$ and $-c/d \in S$. Then $bc - 1 \in \in \mathbb{Z}_0^+, ad \in \mathbb{Z}^+$ and hence, $-a/b = (bc - 1)a/b + ad(-c/d) \in S$. Similarly, $bc \in \in \mathbb{Z}^+, ad - 1 \in \mathbb{Z}_0^+$ and $c/d = bc(a/b) + (ad - 1)(-c/d) \in S$. □

Proposition 3.2 *Let S be a subsemiring of $\mathbb{Q}$ such that $S \cap \mathbb{Q}^- \neq \emptyset$. Then S is a subring of $\mathbb{Q}$.*

Proof. If $a \in S \cap \mathbb{Q}^-$, then $a^2 \in S \cap \mathbb{Q}^+$ and $S(+)$ is a subgroup of $\mathbb{Q}(+)$ by 3.1. Thus S is a subring. □

Proposition 3.3 *Let S be a non-zero nullary subsemiring of $\mathbb{Q}_0^+$ and $T = S\setminus\{0\}$. Then:*

(i) *T is a (non-nullary) subsemiring of $\mathbb{Q}^+$.*
(ii) *T is unitary if and only if S is so.*
(iii) *T is a (proper) maximal subsemiring of $\mathbb{Q}^+$ if and only iff S is a maximal subsemiring of $\mathbb{Q}_0^+$.*

Proof. It is obvious. □

Proposition 3.4 *Let T be a subsemigroup of $\mathbb{Q}^+$ and $S = T \cup \{0\}$. Then:*

(i) *S is a non-zero nullary subsemiring of $\mathbb{Q}_0^+$.*
(ii) *S is unitary if and only if T is so.*
(iii) *S is a maximal subsemiring of $\mathbb{Q}_0^+$ if and only if T is a maximal subsemiring of $\mathbb{Q}^+$*

Proof. It is obvious. □

Proposition 3.5 *Let S be a subsemiring of $\mathbb{Q}$ and let $T = S \cup \mathbb{Z}^+ \cup (S + \mathbb{Z}^+)$. Then:*

(i) *T is a unitary subsemiring of $\mathbb{Q}$ and $S \subseteq T$.*
(ii) *S is an ideal of T and $S = T$ if and only if $1 \in S$.*
(iii) *$S \cup (S + \mathbb{Z}^+)$ is a bi-ideal of T (i.e., it is an ideal of both the semigroups $T(+)$ and $T(\cdot)$).*
(iv) *T is a subring of $\mathbb{Q}$ if and only if S is a non-zero subring.*
(v) *$T = \mathbb{Q}$ if and only if $S = \mathbb{Q}$.*

Proof. (i), (ii), and (iii). Easy to check.

(iv). First, assume that T is a subring of $\mathbb{Q}$. Then $-1 \in T$ and, since $-1 \notin \mathbb{Z}^+$, we have $-1 \in S \cup (S + \mathbb{Z}^+)$. If $-1 \in S$, then S is subring by 3.2. If $-1 \in S + \mathbb{Z}^+$, then $S \cap \mathbb{Z}^- \neq \emptyset$ and we use 3.2 again. Conversely, if S is a non-zero subring, then $-a/b \in S \subseteq T$, and T is a subring by 3.2.

(v) If $S = \mathbb{Q}$, then, apparently, $T = \mathbb{Q}$. Now, assume that $T = \mathbb{Q}$. Then S is a non-zero subring of $\mathbb{Q}$ by (iv). Consequently, $S \cap \mathbb{Z}^+ \neq \emptyset$ and we put $n = \min(S \cap \mathbb{Z}^+)$. If $n = 1$, then $1 \in S$ and $S = T = \mathbb{Q}$ by (ii). Finally, if there is a $p \in \mathbb{P}$ such that p divides n, then $1/p \in T$ and we conclude easily that $1/p \in S + \mathbb{Z}^+$. Thus, $1/p = a + m$ for some $m \in \mathbb{Z}^+$ and then $(pm-1)/p = -a \in S, pm - 1 \in S \cap \mathbb{Z}^+ = n\mathbb{Z}^+$ and p divides $pm - 1$, a contradiction.

□

Remark 3.6 Let S be a subsemiring of $\mathbb{Q}$. Then $S_0 = S \cup \{0\}$ is the smallest nullary subsemiring containing S (see 3.2, 3.3, and 3.4). Clearly, $S_0 \neq \mathbb{Q}$ if and only if $S \neq \mathbb{Q}$. Furthermore, by 3.5, $S_1 = S \cup \mathbb{Z}^+ \cup (S + \mathbb{Z}^+)$ is the smallest unitary subsemiring containing S. Again, $S_1 \neq \mathbb{Q}$ if and only if $S \neq \mathbb{Q}$. Finally, $S_{0,1} = \mathbb{Z}_0^+ \cup (S + \mathbb{Z}_0^+)$ is the smallest nullary and unitary subsemiring of $\mathbb{Q}$ containing S. We have $S_{0,1} \neq \mathbb{Q}$ if and only if $S \neq \mathbb{Q}$. In particular, if S is a (proper) maximal subsemiring of $\mathbb{Q}$, then S is both nullary and unitary.

Remark 3.7 (i) For every $p \in \mathbb{P}$ put $\mathbb{U}(p) = \{a/b : \ a \in \mathbb{Z}, b \in \mathbb{Z}^+, p$ does not divide $b\}$. It is easy to check that $\mathbb{U}(p)$ is a maximal subring of $\mathbb{Q}$. Of course, $\mathbb{U}(p)$ is unitary.

(ii) Let R be a proper subring of $\mathbb{Q}$. By 3.5 (iv), (v), $R_1 = (R + \mathbb{Z}^+) \cup \mathbb{Z}^+$ is a proper unitary subring of $\mathbb{Q}$ and there is at least one prime $p \in \mathbb{P}$ such that $1/p \notin R_1$. If $a/b \in R_1$, where $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = 1$ and p divides b, then $b = mp$ and $na + kp = 1$ for some $m, n, k \in \mathbb{Z}$. Now, $1/p = na/p + kp/p = nma/b + k \in R_1$, a contradiction. We have proved that $R_1 \subseteq \mathbb{U}(p)$. Consequently, $R \subseteq \mathbb{U}(p)$, too.

(iii) It follows from (i) and (ii) that the subrings $\mathbb{U}(p), p \in \mathbb{P}$, are just all maximal subrings of the field $\mathbb{Q}$. According to 3.2, these subrings are maximal as subsemirings as well.

Remark 3.8 If S is a proper subsemiring of $\mathbb{Q}$ such that $S \nsubseteq \mathbb{Q}_0^+$, then S is a subring by 3.2, and hence $S \subseteq \mathbb{U}(p)$ for a prime $p \in \mathbb{P}$ by 3.7 (ii). Using this (and 3.7 (iii)), we conclude easily that the subsemiring $\mathbb{Q}_0^+$ and the sub(semi)rings $\mathbb{U}(p), p \in \mathbb{P}$, are just all maximal subsemirings of $\mathbb{Q}$. Notice that $\mathbb{Q}_0^+ = \{q \in \mathbb{Q} : \ |q| \leq q\} = \{q \in \mathbb{Q} : \ |q| = q\}$ and $\mathbb{U}(p) = \{q \in \mathbb{Q}^* : \ \mathrm{v}_p(q) \geq 0\} \cup \{0\} = \{q \in \mathbb{Q} : \ |q|_{p,r} \leq 1\}, r \in {}_1\mathbb{R}^+$.

Remark 3.9 If S is a subsemiring of $\mathbb{Q}$, then $S - S = \{a - b : \ a, b \in S\}$ is the difference ring of S. That is, it is just the smallest subring of $\mathbb{Q}$ containing S.

Remark 3.10 Let S_1 and S_2 be subsemirings of $\mathbb{Q}$ and let $\varphi : S_1 \to S_2$ be a homomorphism (i.e., φ is a mapping such that $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in S_1$).

(i) First, assume that $S_1 \subseteq \mathbb{Z}_0^+$. If $0 \in S_1$, then $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$, so that $\varphi(0) = 0 \in S_2$. If $m \in S_1 \backslash \{0\}$ then $\varphi(m)\varphi(m) = \varphi(m^2) = m\varphi(m)$, and hence either $\varphi(m) = 0$ or $\varphi(m) = m$. If $m, n \in S_1 \backslash \{0\}$ are such that $\varphi(m) = 0$ and $\varphi(n) \neq 0$, then $\varphi(n) = n, \varphi(m+n) = \varphi(n) = n \neq 0$, and hence $\varphi(m+n) = m+n$ and $m = 0$, a contradiction. We have shown that either $0 \in S_2$ and $\varphi = 0$ or $S_1 \subseteq S_2$ and $\varphi = \mathrm{id}_{S_1}$.

(ii) Next, assume that $S_1 \subseteq \mathbb{Q}_0^+$. Again, if $0 \in S_1$, then $\varphi(0) = 0$. If $a/b \in S_1, a, b, \in \in \mathbb{Z}^+$, then $a = b \cdot a/b \in T = S_1 \cap \mathbb{Z}^+$ and $\varphi(a) = b\varphi(a/b), \varphi(a/b) = \varphi(a)/b$. Put $\psi = \varphi|T$. According to (i), either $0 \in S_2$ and $\psi = 0$ or $T \subseteq S_2$ and $\psi = \mathrm{id}_T$. In the former case, we get $\varphi(a) = 0$ and $\varphi(a/b) = 0$. In the latter case, we get $\varphi(a) = a$ and $\varphi(a/b) = a/b$. We have thus shown again that either $0 \in S_2$ and $\varphi = 0$ or $S_1 \subseteq S_2$ and $\varphi = \mathrm{id}_{S_1}$.

(iii) Assume, finally, that $S_1 \nsubseteq \mathbb{Q}_0^+$. By 3.2, S_1 is a subring of $\mathbb{Q}$. If $a \in S_1 \cap \mathbb{Q}^-$, then $-a \in S_1 \cap \mathbb{Q}^+$ and $0 = \varphi(a-a) = \varphi(a) + \varphi(-a)$ and $\varphi(a) = -\varphi(-a)$. Using (ii), we see that either $0 \in S_2$ and $\varphi = 0$ or $S_1 \subseteq S_2$ and $\varphi = \mathrm{id}_{S_1}$.

(iv) Combining (ii) and (iii), we conclude that either $0 \in S_2$ and $\varphi = 0$ or $S_1 \subseteq S_2$ and $\varphi = \mathrm{id}_{S_1}$.

(v) It follows immediately from (iv) that different subsemirings of $\mathbb{Q}$ are non-isomorphic.

Remark 3.11 Let S be a subsemiring of $\mathbb{Q}$. If $m \in S \cap \mathbb{Z}^+$, then the set $S + m$ is again a subsemiring. Moreover, if $r \in S \cup \mathbb{Z}^+, r \neq 0$, then the set Sr is a subsemiring.

4. Subsemirings of $\mathbb{Q}^+$—First Steps

Throughout this section, let S be a subsemiring of $\mathbb{Q}^+$ and let $p \in \mathbb{P}, \mathrm{v} = \mathrm{v}_p$.

Lemma 4.1 *If $m = \mathrm{v}(a) \geq 0$ for some $a \in S$, then for every $n \geq m$ there is at least one $b \in S$ with $\mathrm{v}(b) = n$.*

Proof. Put $b = p^{n-m} \cdot a$. □

Lemma 4.2 *If $m = \mathrm{v}(a) < 0$ for some $a \in S$, then for every $n \in \mathbb{Z}$ there is at least one $b \in S$ with $\mathrm{v}(b) = n$.*

Proof. First, $\mathrm{v}(c) = -1$, where $c = p^{-m-1} \cdot a \in S$. If $n \geq 0$, then $p^{n+1} \cdot c \in S$ and $\mathrm{v}(p^{n+1} \cdot c) = n$. If $n < 0$, then $c^{-n} \in S$ and $\mathrm{v}(c^{-n}) = n$. □

Definition 4.3 *If $\mathrm{v}(a) \geq 0$ for every $a \in S$ (see 4.1 and 4.2), then we put $(\mathtt{w}_p(S) =)\ \mathtt{w}(S) = \min\{\mathrm{v}(a) : a \in S\}$. If $\mathrm{v}(b) < 0$ for at least one $b \in S$ (see 4.2), then we put $(\mathtt{w}_p(S) =)\ \mathtt{w}(S) = -\infty$.*

Definition 4.4 *For every $n \in \mathbb{Z}$ such that $n \geq \mathtt{w}(S)$, (see 4.3) we put $(\mathbf{u}_{p,n}(S) =)$ $\mathbf{u}_n(S) = \inf\{c \in S : \mathrm{v}(c) \leq n\}$ $(\in \mathbb{R}_0^+)$. Moreover, if $m = \mathtt{w}(S) \geq 0$, then $(\boldsymbol{u}_p(S) =)\ \boldsymbol{u}(S) = (\mathbf{u}_m(S), \mathbf{u}_{m+1}(S), \mathbf{u}_{m+2}(S), \dots)$. If $\mathtt{w}(S) = -\infty$, then $(\boldsymbol{u}_p(S) =)$ $(\boldsymbol{u}(S) = (\dots \mathbf{u}_{-2}(S), \mathbf{u}_{-1}(S), \mathbf{u}_0(S), \mathbf{u}_1(S), \mathbf{u}_2(S), \dots)$.*

Lemma 4.5

(i) *If* $m = \mathtt{w}(S) \geq 0$, *then* $\boldsymbol{u}(S) \in \overline{\mathfrak{R}}_m$.

(ii) *If* $\mathtt{w}(S) = -\infty$, *then* $\boldsymbol{u}(S) \in \overline{\mathfrak{R}}_\infty$.

Proof. Let $n, k \in \mathbb{Z}$ be such that $n \geq \mathtt{w}(S)$ and $k \geq \mathtt{w}(S)$. It follows easily from 4.4 that $\mathbf{u}_n(S) \in \mathbb{R}_0^+$ and $\mathbf{u}_k(S) \leq \mathbf{u}_n(S)$ if $n \leq k$. To show the condition (A) ((A′), respectively), consider sequences $\boldsymbol{a} = (a_1, a_2, a_3, \ldots)$ and $\boldsymbol{b} = (b_1, b_2, b_3, \ldots)$ of numbers from S such that $a_1 \geq a_2 \geq a_3 \geq \cdots, \mathrm{v}(a_i) \leq n, \lim(\boldsymbol{a}) = \mathbf{u}_n(S), b_1 \geq b_2 \geq$ $\geq b_3 \geq \cdots, \mathrm{v}(b_i) \leq k$, and $\lim(\boldsymbol{b}) = \mathbf{u}_k(S)$. Then $\mathrm{v}(a_i b_i) \leq n + k, a_i b_i \in S, \lim(\boldsymbol{ab}) =$ $= \mathbf{u}_n(S) \cdot \mathbf{u}_k(S)$ and $a_i b_i \geq \mathbf{u}_{n+k}(S)$. Thus $\lim(\boldsymbol{ab}) \geq \mathbf{u}_{n+k}(S)$. □

Definition 4.6 *If* $\mathtt{w}(S) \geq 0$, *then we put* $(\lambda_p(S) =)\ \lambda(S) = \lambda(\boldsymbol{u}(S))$ *(see* 4.5 *(i) and* 2.7*). If* $\mathtt{w}(S) = -\infty$, *then* $(\lambda_p^+(S) =)\ \lambda^+(S) = \lambda(\boldsymbol{u}(S)^+)$ *and* $(\lambda_p^-(S) =)$ $\lambda^-(S) = \lambda(\boldsymbol{u}(S)^-)$*(see* 4.5 *(ii) and* 2.8*).*

Lemma 4.7 *Assume that* $\mathtt{w}(S) = m \geq 0$. *Then:*

(i) *Either* $\lim(\boldsymbol{u}(S)) = 0$ *or* $\mathbf{u}_n(S) \geq 1$ *for every* $n \geq m$.

(ii) *If* $\mathbf{u}_{m_0}(S) = 0$ *for some* $m_0 \geq m$, *then* $\mathbf{u}_k(S) = 0$ *for every* $k \geq m + m_0$.

(iii) *If* $m = 0$ *and* $\mathbf{u}_0(S) = 0$, *then* $\boldsymbol{u}(S) = 0$.

(iv) *If* $m = 0$ *and* $\mathbf{u}_0(S) \neq 0$, *then* $\mathbf{u}_0(S) \geq 1$.

(v) $\lambda(S)^n \leq \mathbf{u}_n(S)$ *for every* $n \geq m$, $n \neq 0$.

(vi) $0 \leq \lambda(S) \leq 1$.

Proof. By 4.5(i), $\boldsymbol{u}(S) \in \overline{\mathfrak{R}}_m$. Now, we use 2.6, 2.4 (i), 2.4 (iii), 2.5, and 2.7. □

Lemma 4.8 *Assume that* $\mathtt{w}(S) = -\infty$. *Then:*

(i) *Either* $\lim(\boldsymbol{u}(S)^+) = 0$ *or* $\mathbf{u}_n(S) \geq 1$ *for every* $n \in \mathbb{Z}$.

(ii) *If* $\mathbf{u}_{m_0}(S) = 0$ *for some* $m_0 \in \mathbb{Z}$, *then* $\boldsymbol{u}(S) = 0$.

(iii) *If* $\mathbf{u}_0(S) \neq 0$, *then* $\mathbf{u}_0(S) \geq 1$ *and* $\lambda^-(S) \geq 1$.

(iv) $0 \leq \lambda^+(S) \leq 1$ *and* $\lambda^+(S) \leq \mathbf{u}_1(S) \leq \mathbf{u}_0(S)$.

(v) $\lambda^+(S)^m \leq \mathbf{u}_m(S)$ *and* $\lambda^-(S)^m \leq \mathbf{u}_{-m}(S)$ *for every* $m \leq 1$.

(vi) *If* $0 < \mathbf{u}_{m_0}(S) < 1$ *for at least one* $m_0 \geq 1$, *then* $0 < \lambda^+(S) < 1 < \lambda^-(S)$.

Proof. By 4.5 (ii), $\boldsymbol{u}(S) \in \overline{\mathfrak{R}}_\infty$. Now, we use 2.6, 2.8 (i), 2.9 (iii), 2.8 (iv), and 2.8 (vi). □

Lemma 4.9 *If* $S \not\subseteq \mathbb{Q}_1^+$, *then* $\lim(\boldsymbol{u}(S)) = 0$ $(\lim(\boldsymbol{u}(S)^+) = 0$, *respectively).*

Proof. We use 4.7 (i) and 4.8(i). □

Remark 4.10 Let S_1 and S_2 be subsemirings of $\mathbb{Q}^+$ such that $S_1 \subseteq S_2$. Then $\mathtt{w}_p(S_2) \leq \mathtt{w}_p(S_1)$, $\mathbf{u}_{p,m}(S_2) \leq \mathbf{u}_{p,m}(S_1)$ for every $m \in \mathbb{Z}, m \geq \mathtt{w}_p(S_1)$, and $\lambda^+(S_2) \leq$ $\leq \lambda^+(S_1)$.

Lemma 4.11 *Let* S *be a proper subsemiring of* $\mathbb{Q}^+$. *Then* $S_1 = S \cup \mathbb{Z}^+ \cup (S + \mathbb{Z}^+)$ *is a proper unitary subsemiring of* $\mathbb{Q}^+$.

Proof. By 3.5 (i), S_1 is a unitary subsemiring of $\mathbb{Q}^+$. If $p \in \mathbb{P}$ is such that $1/p \in S_1$, then either $1/p \in S$ or $1/p \in S + \mathbb{Z}^+$. In the latter case, $1/p = a + m, a \in S, m \in \mathbb{Z}^+$, a contradiction. □

Remark 4.12 Let T be a subset of ${}_1\mathbb{Q}^+$ such that $ab \in T$ for all $a, b \in T$ and $c + d \in T$ for all $c, d \in T, c + d < 1$. Denote by S_1 the set of $s \in \mathbb{Q}_1^+$ such that $sd \in T$ whenever $d \in T$ and $sd < 1$. Then $1 \in S_1$ and we put $S = T \cup S_1$.

If $r, s \in T$, then $rs \in T \subseteq S$. Assume, for a while, that $r \in T$ and $s \in S_1$. If $rs < 1$, then $rs \in T$. If $rs \geq 1$ and $d \in T$ is such that $rsd < 1$, then $rd \in T$ and $rsd \in T$, since $s \in S_1$. We have shown that $rs \in S_1 \subseteq S$. Assume, finally, that $r, s \in S_1$. If $d \in T$ is such that $rsd < 1$, then $rd < 1$ (since $s \geq 1$), and so $rd \in T$ and, since $s \in S_1$, we have $rsd \in T$. Thus $rs \in S_1$ and, altogether, $rs \in S$.

Let $r, s \in S$. If $r + s < 1$, then $r, s \in T$ and $r + s \in T \subseteq S$. If $r + s \geq 1$ and $d \in T$ is such that $(r + s)d < 1$, then $rd < 1$, $sd < 1$ and by previous part (S is multiplicatively closed) are $rd \in T$ and $sd \in T$. Then $(r + s)d \in T$ and we have proved that $r + s \in S_1$. It follows that $r + s \in S$.

We have checked that S is a unitary subsemiring of $\mathbb{Q}^+$. Clearly, $T = S \cap {}_1\mathbb{Q}^+$. Moreover, if R is a subsemiring of $\mathbb{Q}^+$ with $R \cap {}_1\mathbb{Q}^+ = T$, then $R \subseteq S$.

Remark 4.13 Let T be a non-empty subset of ${}_1\mathbb{Q}^+$ such that $a + b \in T$ and $ab/(a + b) \in T$ for all $a, b \in T$. Then the set $\{a^{-1} : a \in T\}$ is a subsemiring of $\mathbb{Q}_1^+$.

5. Maximal Subsemirings of $\mathbb{Q}^+$—First Steps

Lemma 5.1 *Let $a, b, c \in \mathbb{Z}^+$ be such that $a < b$, $c < b$ and* $\gcd(a, c) = 1$. *Then $1/b \in S$, where $S = \langle a/b, c/b \rangle$ denotes the subsemiring generated by the numbers a/b and c/b (we have $S \subseteq \mathbb{Q}^+$).*

Proof. First, find $m \in \mathbb{Z}^+$ such that $m \geq 2$ and $\binom{m}{2} \geq (m + 1)(b - 1)^4$. We are going to construct a sequence $k_0, k_1, \dots, k_m$ of integers such that $0 \leq k_i \leq c$. Since $\gcd(a^{m+1}, c) = 1$, there is $0 \leq k_0 < c$ with $b^m \equiv k_0 a^{m+1} \pmod c$. Similarly, $\gcd(a^m, c) = 1$, $(b^m - k_0 a^{m+1})/c \equiv k_1 a^m \pmod c$ for some $0 \leq k_1 < c$ and $b^m \equiv (k_0 a^{m+1} + k_1 a^m c) \pmod{c^2}$. Proceeding by induction, we find the remaining numbers $k_2, \dots, k_m$ such that $b^m \equiv (k_0 a^{m+1} + k_1 a^m c + \dots + k_i a^{m+1-i} c^i) \pmod{c^{i+1}}$ for every $0 \leq i \leq m$. Now, put $l = \sum_{i=0}^{m} k_i a^{m+1-i} c^i$. Since $a < b$ and $c < b$, we have $l \leq (m + 1)(b - 1)^{m+2} \leq \binom{m}{2}(b - 1)^{m-2} \leq b^m$, and hence $b^m - l \geq 0$. On the other hand, $b^m - l = k_{m+1} c^{m+1}$ and $b^m = l + k_{m+1} c^{m+1}$. Finally, it follows from the definition of l that $1/b = (l + k_{m+1} c^{m+1})/b^{m+1} \in S$. □

Lemma 5.2 *Let $a, b, c, d \in \mathbb{Z}^+$ be such that $a < b$, $c < d$ and* $\gcd(a, b) = \gcd(c, d) = \gcd(a, c) = 1$. *Then* $1/\mathrm{lcm}(b, d) \in \langle a/b, c/d \rangle$.

Proof. We have $a/b = e/g$, $c/d = f/g$ and $\gcd(e, f) = 1$, where $g = \mathrm{lcm}(b, d)$. It remains to use 5.1. □

In the rest of this section, let S be a subsemiring of $\mathbb{Q}^+$.

Lemma 5.3 *Let $p_1, \dots, p_m$, $m \geq 1$, be pairwise different prime integers and let $a_1, \dots, a_m \in S \cap {}_1\mathbb{Q}^+$ be such $\mathrm{v}_{p_i}(a_i) \leq 0$ for every $1 \leq i \leq m$. Then there is $b \in S$ such that $b < 1$ and $\mathrm{v}_{p_i}(b) \leq 0$ for all $i = 1, \dots, m$.*

Proof. First of all, find an integer n such that $m < n$ and $a_i^n < 1/(m(p_1 \dots p_m)^m)$, $i = 1, 2, \dots, m$. Put $b_i = (p_1 \dots p_{i-1} p_{i+1} \dots p_m)^i a_i^n$ and $b = \sum_i b_i$. We have $b_i < < (p_1 \dots p_m)^i a_i^n \leq (p_1 \dots p_m)^m a_i^m < 1/m$ and $b < 1$. Clearly, $b \in < a_1, \dots, a_m > \subseteq S$. Moreover, $\mathrm{v}_{p_i}(b_i) = n\mathrm{v}_{p_i}(a_i) \leq 0$ and $\mathrm{v}_{p_i}(b_j) = n\mathrm{v}_{p_i}(a_j) + j$ for $j \neq i$. If $\mathrm{v}_{p_i}(b_{j_1}) = = \mathrm{v}_{p_i}(b_{j_2})$ for $j_1 < j_2$, $j_1 \neq i \neq j_2$, then $n(\mathrm{v}_{p_i}(a_{j_1}) - \mathrm{v}_{p_i}(a_{j_2})) = j_2 - j_1$, $1 \leq \leq j_2 - j_1 < m$, a contradiction with $m < n$. Similarly, if $\mathrm{v}_{p_i}(b_i) = \mathrm{v}_{p_i}(b_j)$ for $i \neq j$, then $n(\mathrm{v}_{p_i}(a_i) - \mathrm{v}_{p_i}(a_j)) = j$, $1 \leq j < m$, again a contradiction. We see that the numbers $\mathrm{v}_{p_i}(b_1), \dots, \mathrm{v}_{p_i}(b_m)$ are pair-wise different, and hence $\mathrm{v}_{p_i}(b) = \min\{\mathrm{v}_{p_i}(b_j) : 1 \leq j \leq \leq m\} \leq \mathrm{v}_{p_i}(b_i) \leq 0$. □

Definition 5.4 *Put* $\mathrm{p}(S) = \{p \in \mathbb{P} : \mathrm{w}_p(S) = -\infty\}$. *That is, $p \in \mathrm{p}(S)$ if and only if $\mathrm{v}_p(a) < 0$ for at least one $a \in S$.*

Lemma 5.5 $\mathrm{p}(S) = \emptyset$ *if and only if* $S \subseteq \mathbb{Z}^+$.

Proof. It is obvious. □

Lemma 5.6 $\mathrm{p}(S) = \mathbb{P}$ *if and only if for every prime $p \in \mathbb{P}$ there are positive integers a_p and b_p such that p divides b_p, p does not divide a_p and $a_p/b_p \in S$.*

Proof. It is obvious. □

Definition 5.7 *Let $p \in \mathbb{P}$. The semiring S will be called p-paradivisible if $S \cap \cap {}_1\mathbb{Q}^+ \neq \emptyset$ and $\mathrm{v}_p(a) > 0$ for every $a \in S \cap {}_1\mathbb{Q}^+$. We denote by* $\mathrm{pd}(S)$ *the set of $p \in \mathbb{P}$ such that S is p-paradivisible.*

Lemma 5.8 *Assume that $S \cap {}_1\mathbb{Q}^+ \neq \emptyset$.*

(i) *If $p \in \mathrm{p}(S)$ is such that S is not p-paradivisible, then $\mathrm{v}_p(a) < 0$ for at least one $a \in S \cap {}_1\mathbb{Q}^+$.*

(ii) *If $p \in \mathbb{P} \setminus \mathrm{p}(S)$, then S is p-paradivisible if and only if $\mathrm{v}_p(a) \neq 0$ for every $a \in S \cap {}_1\mathbb{Q}^+$.*

Proof. (i) There are $b \in S$ and $c \in S \cap {}_1\mathbb{Q}^+$ such that $\mathrm{v}_p(b) < 0$ and $\mathrm{v}_p(c) \leq 0$. Now, $c^m b < 1$ for suitable $m \in \mathbb{Z}^+$ and we have $c^m b \in S \cap {}_1\mathbb{Q}^+$ and $\mathrm{v}_p(c^m b) < 0$.

(ii) This is obvious. □

Proposition 5.9 *Assume that $S \cap {}_1\mathbb{Q}^+ \neq \emptyset$ and that* $\mathrm{pd}(S) = \emptyset$. *Then $S = < 1/p : p \in \mathrm{p}(S) > = \{a \in \mathbb{Q}^+ : \mathrm{v}_{p_1}(a) \geq 0$ for every $p_1 \in \mathbb{P} \setminus \mathrm{p}(S)\}$.*

Proof. Put $T = < 1/p : p \in \mathrm{p}(S) >$ (notice that $\mathrm{p}(S) \neq \emptyset$ by 5.5). Clearly, $S \subseteq T$ and $T = \{a : \mathrm{v}_{p_1}(a) \geq 0, p_1 \in \mathbb{P} \setminus \mathrm{p}(S)\}$. If $p \in \mathrm{p}(S)$, then there are positive integers b, c such that $b < c$, $\gcd(b, c) = 1$, p divides c, p does not divide b and $b/c \in S$ (see 5.8(i). If $b = 1$, then $1/p \in S$ follows easily. If $b > 1$, then there are positive integers $m, k_1, \dots, k_m$ and primes $p_1, \dots, p_m$ such that $p_1 < p_2 < \dots < p_m$ and $b = p_1^{k_1} \dots p_m^{k_m}$. According to our assumption, we can find numbers $f_1, \dots, f_m \in S \cap {}_1\mathbb{Q}^+$ with $\mathrm{v}_{p_i}(f_i) \leq 0$. By 5.3, there are positive integers d, e such that $d < e$, $\gcd(d, e) = 1$, $d/e \in S$ and none of the primes $p_1, \dots, p_m$ divides d. Then, of course, $\gcd(b, d) = 1$. Consequently, by 5.2, $1/g \in S$, where $g = \mathrm{lcm}(c, e)$. Since p divides c, we conclude that $1/p \in S$, Thus $S = T$. □

Remark 5.10 Let S_1 and S_2 be subsemirings of $\mathbb{Q}^+$ such that $S_1 \subseteq S_2$. Then $\mathsf{p}(S_1) \subseteq \mathsf{p}(S_2)$. Moreover, if $S_1 \cap {}_1\mathbb{Q}^+ \neq \emptyset$, then $\mathsf{pd}(S_2) \subseteq \mathsf{pd}(S_1)$.

6. Maximal Subsemirings of $\mathbb{Q}^+$—Some Of Them

Remark 6.1 It follows immediately from 4.11 that every maximal subsemiring of $\mathbb{Q}^+$ is unitary.

Proposition 6.2

(i) $\mathbb{Q}_1^+$ *is a (proper, unitary) maximal subsemiring of* $\mathbb{Q}^+$ *and* $\mathbb{Q}_1^+ = \{q \in \mathbb{Q} : 1 \leq |q| \leq q\}$.

(ii) $\mathtt{w}_p(\mathbb{Q}_1^+) = -\infty$ *for every* $p \in \mathbb{P}$. *Consequently,* $\mathsf{p}(\mathbb{Q}_1^+) = \mathbb{P}$.

(iii) $\mathbf{u}_{p,m}(\mathbb{Q}_1^+) = 1$ *for all* $p \in \mathbb{P}$ *and* $m \in \mathbb{Z}$.

(iv) $\lambda_p^+(\mathbb{Q}_1^+) = 1 = \lambda_p^-(\mathbb{Q}_1^+)$ *for all* $p \in \mathbb{P}$.

(v) $\mathsf{pd}(\mathbb{Q}_1^+) = \emptyset$.

(vi) *The difference ring* $\mathbb{Q}_1^+ - \mathbb{Q}_1^+$ *is the field* $\mathbb{Q}$.

Proof. For all $a, b \in {}_1\mathbb{Q}^+$ there is a positive integer n such that $c = b/a^n \geq 1$. Then $c \in \mathbb{Q}_1^+$, $b = ca^n$ and $b \in < \mathbb{Q}_1^+, a >$. It means that $< \mathbb{Q}_1^+, a > = \mathbb{Q}^+$ for every $a \in {}_1\mathbb{Q}^+ = \mathbb{Q}^+ \setminus \mathbb{Q}_1^+$ and we conclude that $\mathbb{Q}_1^+$ is a maximal subsemiring of $\mathbb{Q}^+$. The rest is clear. □

Proposition 6.3 *Let* $p \in \mathbb{P}$ *and* $\mathbb{S}_p = \{q \in \mathbb{Q}^+ : \mathrm{v}_p(q) \geq 0\} = \mathbb{Q}^+ \cap \mathbb{U}_p = \{q \in \mathbb{Q}^+ : |q|_{p,r} \leq 1\}$, $r \in {}_1\mathbb{R}^*$. *Then:*

(i) $\mathbb{S}_p$ *is a maximal subsemiring of* $\mathbb{Q}^+$.

(ii) $\mathtt{w}_p(\mathbb{S}_p) = 0$ *and* $\mathtt{w}_{p_1}(\mathbb{S}_{p_1}) = -\infty$ *for every* $p_1 \in \mathbb{P} \setminus \{p\}$.

(iii) $\mathbf{u}_{p,m}(\mathbb{S}_p) = 0$ *for all* $m \geq 0$.

(iv) $\lambda_p(\mathbb{S}_p) = 0$.

(v) $\mathbf{u}_{p_1,n}(\mathbb{S}_p) = 0$ *for all* $p_1 \in \mathbb{P} \setminus \{p\}$ *and* $n \in \mathbb{Z}$.

(vi) $\lambda_{p_1}^+(\mathbb{S}_p) = 0 = \lambda_{p_1}^-(\mathbb{S}_p)$ *for every* $p_1 \in \mathbb{P} \setminus \{p\}$.

(vii) $\mathsf{p}(\mathbb{S}_p) = \mathbb{P} \setminus \{p\}$ *and* $\mathsf{pd}(\mathbb{S}_p) = \emptyset$.

(viii) *The difference ring* $\mathbb{S}_p - \mathbb{S}_p$ *is the ring* $\mathbb{U}(p)$ *(see* 3.7 *(i))*

Proof. Clearly, $\mathbb{S}_p$ is a unitary subring of $\mathbb{Q}^+ \cap \mathbb{U}(p)$. Now, if $a \in \mathbb{Q}^+$ is such that $\mathrm{v}_p(a) < 0$, then $a = b/p^k c$ for some positive integers b, c, k, where p does not divide b. We have $c/b \in \mathbb{S}_p$ and $1/p = p^{k-1} \cdot a \cdot c/b \in < \mathbb{S}_p, a >$. Consequently, $\mathbb{Q}^+ = < 1/p_1 : p_1 \in \mathbb{P} > \subseteq < \mathbb{S}_p, a >$ and $< \mathbb{S}_p, a > = \mathbb{Q}^+$. The remaining assertions are easy to check. □

Lemma 6.4 *If S is a subsemiring of $\mathbb{Q}^+$, then $\mathbb{P} \setminus \mathrm{p}(S) = \{p \in \mathbb{P} : S \subseteq \mathbb{S}_p\}$.*

Proof. It is obvious. □

Proposition 6.5 *The following conditions are equivalent for a subsemiring S of $\mathbb{Q}^+$:*

(i) $S = \mathbb{Q}^+$ *(i.e., $S \subseteq \mathbb{Q}^+$ and $S = \bigcap \mathbb{S}_p$, $p \in \emptyset$).*
(ii) $\mathrm{p}(S) = \mathbb{P}$ *and $1/p \in S$ for at least one $p \in \mathbb{P}$.*
(iii) $\mathrm{p}(S) = \mathbb{P}$ *and $1/m \in S$ for at least one $m \in \mathbb{Z}^+$, $m \geq 2$.*
(iv) *For every prime $p \in \mathbb{P}$ there exist positive integers a_p, b_p, c_p, d_p such that p divides b_p, p divides neither a_p nor c_p, $c_p < d_p$ and $a_p/b_p \in S$, $c_p/d_p \in S$.*

Proof. (i) implies (ii), (ii) implies (iii) and (iii) implies (iv). These implications are easy.

(iv) implies (i). Since $c_p/d_p \in S$, we have $c_p/d_p \in S \cap {}_1\mathbb{Q}^+$, $\mathrm{v}_p(c_p/d_p) \leq 0$ and $p \notin \mathrm{pd}(S)$. Consequently, $\mathrm{pd}(S) = \emptyset$. Further, $a_p/b_p \in S$ and $\mathrm{v}_p(a_p/b_p) < 0$. Consequently, $\mathrm{p}(S) = \mathbb{P}$ and it follows from 5.9 that $S = \mathbb{Q}^+$. □

Proposition 6.6 $\bigcap_{p \in \mathbb{P}} \mathbb{S}_p = \mathbb{Q}_1^+ \cap \bigcap_{p \in \mathbb{P}} \mathbb{S}_p = \mathbb{Z}^+$.

Proof. It is obvious. □

Proposition 6.7 *The following conditions are equivalent for a subsemiring S of $\mathbb{Q}^+$:*

(i) $S = \mathbb{Z}^+$.
(ii) $S = \bigcap \mathbb{S}_p, p \in \mathbb{P}$.
(iii) S *is unitary and* $\mathrm{p}(S) = \emptyset$.

Proof. Combine 5.5 and 6.6. □

Proposition 6.8 *(cf. 6.5 and 6.7). The following conditions are equivalent for a subsemiring S of $\mathbb{Q}^+$:*

(i) $S = \bigcap \mathbb{S}_{p_1}, p_1 \in P_1$, *for a non-empty proper subset P_1 of $\mathbb{P}$.*
(ii) $\emptyset \neq \mathrm{p}(S) \neq \mathbb{P}$ *and $S = \bigcap \mathbb{S}_p, p \in \mathbb{P} \setminus \mathrm{p}(S)$.*
(iii) $\mathrm{p}(S) \neq \mathbb{P}$ *and $1/p_2 \in S$ for at least one $p_2 \in \mathbb{P}$.*
(iv) $\mathrm{p}(S) \neq \mathbb{P}$ *and $1/m \in S$ for at least one $m \in \mathbb{Z}^+$, $m \geq 2$.*
(v) $\mathrm{p}(S) \neq \mathbb{P}$ *and for every prime $p \in \mathbb{P}$ there exist positive integers a_p, b_p such that $a_p < b_p$, p does not divide a_p and $a_p/b_p \in S$.*

Proof. (i) implies (ii). Combining 5.10 and 6.3(vii), we get $\mathrm{p}(S) \in \mathbb{P} \setminus P_1$ and $P_1 \subseteq \mathbb{P} \setminus \mathrm{p}(S)$ (see also 6.4). In particular, $\mathrm{p}(S) \neq \mathbb{P}$. Furthermore, since $P_1 \neq \mathbb{P}$, we have $1/p_3 \in S$, $p_3 \in \mathbb{P} \setminus P_1, S \nsubseteq \mathbb{Z}^+$ and $\mathrm{p}(S) \neq \emptyset$ by 5.5. Finally, $S = \bigcap \mathbb{S}_p, p \in \mathbb{P} \setminus \mathrm{p}(S)$ by 6.4.

(ii) implies (iii), (iii) implies (iv) and (iv) implies (v). These implications are easy.

(v) implies (i). We have $a_p/b_p \in S \cap {}_1\mathbb{Q}^+$ and $\mathrm{v}_p(a_p/b_p) \leq 0$. Consequently, $\mathrm{pd}(S) = \emptyset$. Now, $S = \bigcap \mathbb{S}_p, p \in \mathbb{P} \setminus \mathrm{p}(S)$ by 5.9. □

Corollary 6.9 *Let S be a subsemiring of $\mathbb{Q}^+$. Then $S = \cap\, \mathbb{S}_p, p \in P$ for a subset P of $\mathbb{P}$ if and only if either S is unitary and* $\mathrm{p}(S) = \emptyset$ *or $1/m \in S$ for at least one $m \in \mathbb{Z}^+$, $m \geq 2$.*

Proof. Follows from 6.5, 6.7 and 6.8. □

Remark 6.10 Every proper subsemiring of $\mathbb{Q}^+$ is contained in a maximal subsemiring of $\mathbb{Q}^+$.

Indeed, let S be a proper subsemiring of $\mathbb{Q}^+$. If $S \cap {}_1\mathbb{Q}^+ = \emptyset$, then $S \subseteq \mathbb{Q}_1^+$ and our result is true (see 6.2(i)). Henceforth, we can assume that $S \cap {}_1\mathbb{Q}^+ \neq \emptyset$. Further, due to 6.4 and 6.3(i), we can assume that $\mathrm{p}(S) = \mathbb{P}$. Since S is a proper subsemiring of $\mathbb{Q}^+$, we have $\mathrm{pd}(S) \neq \emptyset$ by 5.9.

Let $\mathscr{T}$ denote the set of proper subsemirings T of $\mathbb{Q}^+$ such that $S \subseteq T$. Then $S \in \mathscr{T}$ and the set $\mathscr{T}$ is ordered by inclusion. Since $S \subseteq T$, we have $\mathbb{P} = \mathrm{p}(S) \subseteq \mathrm{p}(T)$, and so $\mathrm{p}(T) = \mathbb{P}$. Now, again, $\mathrm{pd}(T) \neq \emptyset$ follows from 5.9. Taking into account that $\mathrm{v}_p(1/2) \leq 0$ for all primes $p \in \mathbb{P}$, we conclude that $1/2 \notin T$ for every $T \in \mathscr{T}$. Consequently, the ordered set $\mathscr{T}$ is upwards inductive and it contains at least one maximal subsemiring.

Remark 6.11 For all $p_1, p_2 \in \mathbb{P}$, $p_1 \neq p_2$, we have $(p_1 + 1)/p_1 \in \mathbb{Q}_1^+ \setminus \mathbb{S}_{p_1}$ and $1/p_2 \in \mathbb{S}_{p_1} \setminus (\mathbb{S}_{p_2} \cup \mathbb{Q}_1^+)$. Consequently, $\mathbb{Q}_1^+ \nsubseteq \mathbb{S}_{p_1} \nsubseteq \mathbb{Q}_1^+$ and $\mathbb{S}_{p_1} \nsubseteq \mathbb{S}_{p_2}$. Moreover, $p_1\mathbb{Q}_1^+ \neq \mathbb{Q}_1^+$, $p_1\mathbb{S}_{p_1} \neq \mathbb{S}_{p_1}$ and $p_1\mathbb{S}_{p_2} = \mathbb{S}_{p_2}$. From this, we conclude that the semirings $\mathbb{Q}_1^+$ and $\mathbb{S}_p$, $p \in \mathbb{P}$, are pair-wise nonisomorphic (see also 3.10(v)).

Remark 6.12

(i) Notice that $\mathbb{Q}_1^+ + \mathbb{Q}_1^+ = \{q \in \mathbb{Q} : q \geq 2\}$, and so $1 \notin \mathbb{Q}_1^+ + \mathbb{Q}_1^+$. If $a, b \in \mathbb{Q}_1^+$ are such that $ab = 1$, then $a = 1 = b$. Moreover, let $1 < q \in \mathbb{Q}$. Put $a = (q + 1)/2$ and $b = 2q/(q + 1)$. Then $a, b > 1$ and $ab = q$. Hence $(\mathbb{Q}_1^+ \setminus \{1\}) \cdot (\mathbb{Q}_1^+ \setminus \{1\}) = \mathbb{Q}_1^+ \setminus \{1\}$.

(ii) Let $p \in \mathbb{P}$. If $p_1 \in \mathbb{P}$, $p_1 \neq p$ then $1/p_1 \in \mathbb{S}_p$ and $(p_1 - 1)/p_1 \in \mathbb{S}_p$. Thus $1 \in \mathbb{S}_p + \mathbb{S}_p$ and it follows that $a = a/p_1 + a(p_1 - 1)/p_1$ for every $a \in \mathbb{S}_p$. Consequently, $\mathbb{S}_p + \mathbb{S}_p = \mathbb{S}_p$. Moreover, $a/p_1, p_1 \in \mathbb{S}_p$ and $p_1 \cdot a/p_1 = a$, if $a \neq p_1$, and $1/p_1, p_1^2 \in \mathbb{S}_p$ and $p_1^2 \cdot 1/p_1 = a$, if $a = p_1$. Hence $(\mathbb{S}_p \setminus \{1\}) \cdot (\mathbb{S}_p \setminus \{1\}) = \mathbb{S}_p$.

Remark 6.13

(i) It is easy to see that for a maximal subsemiring S of $\mathbb{Q}^+$ the following is true: S is (additively) semisubtractive iff $S - S \neq \mathbb{Q}$.

Indeed, if S is semisubtractive then for every $a, b \in \mathbb{Q}_1^+$, $a > b$, is $a - b \in S$ and hence $S - S = (-S) \cup \{0\} \cup S \neq \mathbb{Q}$. On the other hand, if S isn't semisubtractive, then there are $a_1, b_1 \in S$, $a_1 > b_1$, such that $a_1 - b_1 \notin S$. Hence $S \subsetneq (S - S) \cap \mathbb{Q}^+$ and $(S - S) \cap \mathbb{Q}^+ = \mathbb{Q}^+$. Thus $S - S = \mathbb{Q}$.

(ii) $\mathbb{Q}_1^+$ is not semisubtractive (see (i)). On the other hand, for all $c, d \in \mathbb{Q}_1^+$ there exists $m \in \mathbb{Z}^+$ with $mc - d \in \mathbb{Q}_1^+$. That is, $\mathbb{Q}_1^+$ is (additively) archimedian.

(iii) Let $p \in \mathbb{P}$. The semiring $\mathbb{S}_p$ is semisubtractive (see (i)) (and hence archimedean as well).

Remark 6.14 Let $p \in \mathbb{P}$. Then $p\mathbb{S}_p$ is a proper ideal of the semiring $\mathbb{S}_p$ (clearly, $1 \notin p\mathbb{S}_p$), and so $\mathbb{S}_p$ is not ideal-simple. Now, let I be a non-empty subset of $\mathbb{S}_p$ such that $I + \mathbb{S}_p \subseteq I$ and $II \subseteq I$. If $a \in I$ and $b \in \mathbb{S}_p$ is such that $a < b$, then $b - a \in \mathbb{S}_p$, and so $b = (b - a) + a \in I$. Put $r = \inf(I)$. If $r < 1$, then $r = 0$ and $I = \mathbb{S}_p$. If $r \geq 1$, then $I = \{q \in \mathbb{S}_p : q \geq r\}$. Using this, we conclude easily that the semiring $\mathbb{S}_p$ is bi-ideal-simple.

7. More Subsemirings of $\mathbb{Q}^+$

Proposition 7.1 *For all $p \in \mathbb{P}$, $m \in \mathbb{Z}_0^+$ and $\boldsymbol{r} \in \overline{\mathfrak{R}}_m$, put $\mathbb{V}(p, m, \boldsymbol{r}) = \{a \in \mathbb{Q}^+ :$ $: m \leq \mathrm{v}_p(a)$ and $r_{\mathrm{v}_p(a)} \leq a\}$. Then:*

(i) *$V = \mathbb{V}(p, m, \boldsymbol{r})$ is a proper subsemiring of $\mathbb{Q}^+$.*
(ii) *V is unitary if and only if $m = 0$ and $r_0 \leq 1$.*
(iii) *$\mathtt{w}_p(V) = m$.*
(iv) *$\mathbf{u}_{p,n} = r_n$ for every $n \geq m$.*
(v) *$\lambda_p(V) = \inf\{r_n^{1/n} : n \geq m\}$.*
(vi) *$\mathtt{w}_{p_1}(V) = -\infty$ for every $p_1 \in \mathbb{P} \setminus \{p\}$.*
(vii) *$\mathsf{p}(V) = \mathbb{P} \setminus \{p\}$.*
(viii) *$\mathsf{pd}(V) \subseteq \{p\}$ and $\mathsf{pd}(V) = \{p\}$ if and only if $r_k < 1$ for at least one $k \geq m$ and either $m \geq 1$ or $m = 0$ and $r_0 \geq 1$.*

Proof. For all $a, b \in V$, we have $m \leq \min(\mathrm{v}_p(a), \mathrm{v}_p(b)) \leq \mathrm{v}_p(a + b)$, and therefore $r_{\mathrm{v}_p(a+b)} \leq r_{\mathrm{v}_p(a)} \leq a \leq a + b$, provided that $\mathrm{v}_p(a) \leq \mathrm{v}_p(b)$. The other case is symmetric and we see that $a + b \in V$. Further, $m \leq 2m \leq \mathrm{v}_p(a) + \mathrm{v}_p(b) = \mathrm{v}_p(ab)$ and $r_{\mathrm{v}_p(ab)} =$ $= r_{\mathrm{v}_p(a)+\mathrm{v}_p(b)} \leq r_{\mathrm{v}_p(a)} \cdot r_{\mathrm{v}_p(b)} \leq ab$. Thus $ab \in V$.

By 2.2, for all $m \leq n \in \mathbb{Z}$ and $s \in \mathbb{R}^+$, there is $c \in \mathbb{Q}^+$ with $r_n < c < r_n + s$ and $\mathrm{v}_p(c) = n$. Then $c \in V$ and we see that $V \neq \emptyset$, V is a subsemiring of $\mathbb{Q}^+$ and $\mathtt{w}_p(V) = m$. Moreover, since s was arbitrary, we also see that $\mathbf{u}_{p,n}(V) \leq r_n$. On the other hand, if $d \in V$ and $\mathrm{v}_p(d) \leq n$, then $r_n \leq r_{\mathrm{v}_p(d)} \leq d$ and it follows that $\mathbf{u}_{p,n}(V) = r_n$.

If $p_1 \in \mathbb{P} \setminus \{p\}$ and $k \in \mathbb{Z}^+$, then $r_m \leq e = p^l/p_1^k$ for some $l \in \mathbb{Z}^+$, $m \leq l$, and we have $m \leq l = \mathrm{v}_p(e)$, $r_l \leq r_m \leq e$, $e \in V$ and $\mathrm{v}_{p_1}(e) = -k$. Consequently, $\mathtt{w}_{p_1}(V) = -\infty$ and $\mathsf{p}(V) = \mathbb{P} \setminus \{p\}$.

The assertion (ii) is obvious, (v) follows from (iv), and it remains to show (viii). If $r_n \geq 1$ for every $n \geq m$, then $V \subseteq \mathbb{Q}_1^+$ and $\mathsf{pd}(V) = \emptyset$ trivially. Hence, assume that $r_k < 1$ for at least one $k \geq m$. If $p_1 \in \mathbb{P} \setminus \{p\}$, then, by 2.2, there is $a \in {}_1\mathbb{Q}^+$ such that $r_k < a < 1$, $\mathrm{v}_p(a) = k$ and $\mathrm{v}_{p_1}(a) = 0$. Then $a \in V \cap {}_1\mathbb{Q}^1$ and it follows that $p_1 \notin \mathsf{pd}(V)$. Then $\mathsf{pd}(V) \subseteq \{p\}$ and $\mathsf{pd}(V) = \{p\}$ if $m \geq 1$ or $m = 0$ and $r_0 \geq 1$. □

Proposition 7.2 *Assume that* $\inf\{r_n : n \geq m\} = 0$ *($= r \geq 1$, resp.) (see 2.6). Let $p_1 \in \mathbb{P} \setminus \{p\}$. Then:*

(i) *$\mathbf{u}_{p_1,n_1} = 0$ ($\mathbf{u}_{p_1,n_1} = r$, resp.) for every $n_1 \in \mathbb{Z}$.*

(ii) $\lambda^+_{p_1}(V) = 0 = \lambda^-_{p_1}(V)$ *(*$\lambda^+_{p_1}(V) = 1 = \lambda^-_{p_1}(V)$*, resp.).*

Proof. Let $s = \inf\{r_n\}$ and $n_1 \in \mathbb{Z}$. For every $\varepsilon \in \mathbb{R}^+$, there is $k \geq m$ with $r_k < s + \varepsilon$. By 2.2, there exists $b \in \mathbb{Q}^+$ such that $r_k < b < s + \varepsilon$, $\mathrm{v}_p(b) = k$ and $\mathrm{v}_{p_1}(b) = n_1$. Then $b \in V$ and it is now clear that $\mathbf{u}_{p_1,n_1}(V) = s$. □

Lemma 7.3

(i) $V \subseteq \mathbb{S}_p$ *and* $V = \mathbb{S}_p$ *if and only if* $m = r_0 = r_1 = r_2 = \cdots = 0$.

(ii) $V \nsubseteq \mathbb{S}_{p_1}$ *for every* $p_1 \in \mathbb{P} \setminus \{p\}$.

(iii) $V \subseteq \mathbb{Q}^+_1$ *(equivalently,* $V \subseteq \mathbb{Q}^+_1 \cap \mathbb{S}_p$*) if and only if* $\inf\{r_n : n \geq m\} \geq 1$.

Proof. It is easy (use 7.1). □

Lemma 7.4 $\mathbb{V}(p_1, m_1, \boldsymbol{r}) \subseteq \mathbb{V}(p_2, m_2, \boldsymbol{s})$ *if and only if* $p_1 = p_2$*,* $m_2 \leq m_1$*, and* $s_n \leq r_n$ *for every* $n \geq m_1$.

Proof. Only the direct implication needs a proof. First, the equality $p_1 = p_2 = p$ follows by combination of 7.3(i),(ii). Further, the inequality $m_2 \leq m_1$ follows from 4.10 and 7.1(iii). Finally, if $r_n < s_n$ for some $n \geq m_1$, then, by 2.2, $\mathrm{v}_p(a) = n$ for some $a \in \mathbb{Q}^+$ such that $r_n < a < s_n$. Then $a \in \mathbb{V}(p_1, m_1, \boldsymbol{r})$ and $a \notin \mathbb{V}(p_2, m_2, \boldsymbol{s})$, a contradiction. □

Remark 7.5 It follows immediately from 7.4 that the subsemirings $\mathbb{V}(p, m, \boldsymbol{r})$, $p \in \mathbb{P}, m \in \mathbb{Z}^+_0, \boldsymbol{r} \in \overline{\mathfrak{R}}_m$, are pair-wise different. Due to 3.10, they are pair-wise non-isomorphic as well.

Lemma 7.6 *Let* S *be a subsemiring of* $\mathbb{Q}^+$ *and let* $p \in \mathbb{P}$ *be such that* $m = \mathtt{w}_p(S) \geq$ ≥ 0 *(i.e.,* $p \in \mathbb{P} \setminus \mathrm{p}(S)$*). Then* $S \subseteq \mathbb{V}(p, m, \boldsymbol{u}_p(S))$.

Proof. See 4.3, 4.4 and 4.5(i). □

Proposition 7.7 *For all* $p \in \mathbb{P}$ *and* $\boldsymbol{r} \in \overline{\mathfrak{R}}_\infty$*, put* $\mathbb{V}(p, \infty, \boldsymbol{r}) = \{a \in \mathbb{Q}^+ : r_{\mathrm{v}_p(a)} \leq a\}$. *Then:*

(i) $V = \mathbb{V}(p, \infty, \boldsymbol{r})$ *is a subsemiring of* $\mathbb{Q}^+$.

(ii) $V \neq \mathbb{Q}^+$ *if and only if* $r_0 \neq 0$ *(then* $r_0 \geq 1$*).*

(iii) V *is unitary if and only if* $r_0 \leq 1$ *(then* $r_0 = 0, 1$*).*

(iv) $\mathtt{w}_{p_1}(V) = -\infty$ *for every* $p_1 \in \mathbb{P}$.

(v) $\mathbf{u}_{p,n}(V) = r_n$ *for every* $n \in \mathbb{Z}$.

(vi) $\lambda^+_p(V) = \inf\{r_n^{1/n} : n \geq 1\} \leq 1$ *and* $\lambda^-_p(V) = \inf\{r_{-n}^{1/n} : n \geq 1\}$.

(vii) $\mathrm{p}(V) = \mathbb{P}$.

(viii) $\mathsf{pd}(V) \subseteq \{p\}$ *and* $\mathsf{pd}(V) = \{p\}$ *if and only if* $r_0 \neq 0$ *(see (ii)) and* $r_k < 1$ *for at least one* $k \in \mathbb{Z}$.

Proof. Similar to that of 7.1 (use 2.1, 2.2, 2.8 and 2.9). □

Proposition 7.8 *Assume that* $\inf\{r_n : n \geq 1\} = 0$ *(*$= r \geq 1$*, resp.) (see 2.6). Let* $p_1 \in \mathbb{P} \setminus \{p\}$*. Then:*

(i) $\mathbf{u}_{p_1,n_1}(V) = 0$ *(*$\mathbf{u}_{p_1,n_1}(V) = r$*, resp.) for every* $n_1 \in \mathbb{Z}$.

(ii) $\lambda^+_{p_1}(V) = 0 = \lambda^-_{p_1}(V)$ *(*$\lambda^+_{p_1}(V) = 1 = \lambda^-_{p_1}(V)$*, resp.).*

Proof. Similar to that of 7.2. □

Lemma 7.9

(i) $V \not\subseteq \mathbb{S}_{p_1}$ *for every* $p_1 \in \mathbb{P}$.

(ii) $V \subseteq \mathbb{Q}^+_1$ *if and only if* $r_n \geq 1$ *for every* $n \in \mathbb{Z}$ *(see 2.6). Moreover,* $V = \mathbb{Q}^+_1$ *if and only if* $r_n = 1$ *for every* $n \in \mathbb{Z}$.

Proof. It is easy. □

Lemma 7.10 *Let* $p_1, p_2 \in \mathbb{P}$ *and* $\boldsymbol{r}, \boldsymbol{s} \in \overline{\mathfrak{R}}_\infty$. *Then* $\mathbb{V}(p_1, \infty, \boldsymbol{r}) \subseteq \mathbb{V}(p_2, \infty, \boldsymbol{s})$ *if and only if at least (and then just) one of the following three conditions holds:*

(1) $s_0 = 0$ *(then* $\boldsymbol{s} = 0$*);*

(2) $p_1 = p_2$, $s_0 \neq 0$, $s_n \leq r_n$ *for every* $n \in \mathbb{Z}$*;*

(3) $p_1 \neq p_2$, $s_0 \neq 0$, $r_n \geq 1$ *and* $s_n \leq \inf\{r_k : k \geq 0\}$ *for every* $n \in \mathbb{Z}$.

Proof. Let $V_1 = \mathbb{V}(p_1, \infty, \boldsymbol{r}) \subseteq \mathbb{V}(p_2, \infty, \boldsymbol{s}) = V_2$, $p_1 \neq p_2$ and $s_0 \neq 0$. Suppose, for contradiction, that $r_k < 1$ for some $k \in \mathbb{Z}$. Then $\emptyset \neq V_1 \cap (0, 1) \subseteq V_2 \cap (0, 1)$ and thus there is $m \in \mathbb{Z}$ such that $s_m < 1$. By 7.7(viii) and 5.10 we have $\{p_2\} \subseteq \mathrm{pd}(V_2) \subseteq$ $\subseteq \mathrm{pd}(V_1) \subseteq \{p_1\}$, a contradiction.

The rest is easy (use 2.2). □

Remark 7.11 It follows easily from 7.10 that the subsemirings $\mathbb{V}(p, \infty, \boldsymbol{r})$, $\boldsymbol{r} \in$ $\in \overline{\mathfrak{R}}_\infty$, $\boldsymbol{r}$ not constant, are pair-wise different. Due to 3.10, they are pair-wise nonisomorphic as well. Notice that if $\boldsymbol{r} = (\dots, r, r, r, \dots)$, $r = 0$ or $r \geq 1$, is constant, then $\mathbb{V}(p, \infty, \boldsymbol{r}) = \{q \in \mathbb{Q}^+ : r \leq q\}$.

Proposition 7.12 *Let* S *be a subsemiring of* $\mathbb{Q}^+$ *and let* $p \in \mathbb{P}$ *be such that* $\mathtt{w}_p(S) =$ $= -\infty$ *(i.e.,* $p \in \mathrm{p}(S)$*). Then* $S \subseteq \mathbb{V}(p, \infty, \boldsymbol{u}_p(S))$.

Proof. See 4.3, 4.4 and 4.5(ii). □

Lemma 7.13 *Let* S *be a proper subsemiring of* $\mathbb{Q}^+$ *such that* $S \not\subseteq \mathbb{Q}^+_1$ *and* $S \not\subseteq \mathbb{S}_p$ *for every* $p \in \mathbb{P}$. *Then:*

(i) $S \cap {}_1\mathbb{Q}^+ \neq \emptyset$.

(ii) $\mathrm{p}(S) = \mathbb{P}$ *(i.e.,* $\mathtt{w}_p(S) = -\infty$ *for every* $p \in \mathbb{P}$*).*

(iii) $\mathrm{pd}(S) \neq \emptyset$.

(iv) $S \subseteq \mathbb{V}(p, \infty, \boldsymbol{u}_p(S))$ *for every* $p \in \mathbb{P}$.

Proof. Since $S \not\subseteq \mathbb{Q}^+_1$, we have $S \cap {}_1\mathbb{Q}^+ \neq \emptyset$. The equality $\mathrm{p}(S) = \mathbb{P}$ follows from 6.4. Further, $\mathrm{pd}(S) \neq \emptyset$ by 5.9. Finally, $S \subseteq \mathbb{V}(p, \infty, \boldsymbol{u}_p(S))$ by 7.12. □

8. Maximal Subsemirings of $\mathbb{Q}^+$—All Found

Proposition 8.1 *For* $p \in \mathbb{P}$ *and* $r \in {}_1\mathbb{R}^+$, *put* $\mathbb{W}(p, r) = \{a \in \mathbb{Q}^+ : |a|_{p,r} \leq a\}$. *Then:*

(i) *$W = \mathbb{W}(p, r)$ is a proper unitary subsemiring of $\mathbb{Q}^+$ and $\mathbb{Q}_1^+ \cap \mathbb{S}_p \subseteq W$.*
(ii) *$W = \mathbb{V}(p, \infty, \boldsymbol{r})$, where $r_m = r^m$ for every $m \in \mathbb{Z}$.*
(iii) *$\mathsf{w}_{p_1}(W) = -\infty$ for every $p_1 \in \mathbb{P}$.*
(iv) *$\mathbf{u}_{p,n}(W) = r^n$ for every $n \in \mathbb{Z}$.*
(v) *$\mathsf{p}(W) = \mathbb{P}$.*
(vi) *$\lambda_p^+(W) = r = \lambda_p^-(W)$.*
(vii) *$\mathsf{pd}(W) = \{p\}$.*
(viii) *The difference ring $W - W$ is the field $\mathbb{Q}$.*

Proof. Put $r_m = r^m$ for every $m \in \mathbb{Z}$. Then $\boldsymbol{r} \in \overline{\mathfrak{R}_\infty}$ and it is clear that $W = \mathbb{V}(p, \infty, \boldsymbol{r})$. Now, the assertions (i),..., (vii) follow from 7.7. To show (viii), put $A = W - W$. Let $a \in \mathbb{Q}^+$ be such that $\mathrm{v}_p(a) < 0$. If $p_1 \in \mathbb{P}$ is such that $|a|_{p,r} < p_1$, then $\mathrm{v}_p(p_1 + a) = \mathrm{v}_p(a)$ and $p_1 + a \in W$. Of course, $p_1 \in W$ and $p_1 + a - p_1 = a$. It is easy to see that $A = \mathbb{Q}$. □

Proposition 8.2 *Let $p_1 \in \mathbb{P} \setminus \{p\}$. Then:*
(i) *$\mathbf{u}_{p_1,n}(W) = 0$ for every $n \in \mathbb{Z}$.*
(ii) *$\lambda_{p_1}^+(W) = 0 = \lambda_{p_1}^-(W)$.*

Proof. Combine 8.1(ii) and 7.8. □

Lemma 8.3 *Let $p_1, p_2 \in \mathbb{P}$ and $r_1, r_2 \in {}_1\mathbb{R}^+$ be such that $\mathbb{W}(p_1, r_1) \subseteq \mathbb{W}(p_2, r_2)$. Then $p_1 = p_2$ and $r_1 = r_2$.*

Proof. Combining 8.1(ii) and 7.10, we get $p_1 = p_2$ and $r_2^n \le r_1^n$ for every $n \in \mathbb{Z}$. In particular, $r_2 \le r_1$ and $r_2^{-1} \le r_1^{-1}$, i.e., $r_1 \le r_2$. Then $r_1 = r_2$. □

Lemma 8.4 *Let $p \in \mathbb{P}$ and let $\boldsymbol{r} \in \overline{\mathfrak{R}_\infty}$ be such that $0 < r_k < 1$ for at least one $k \in \mathbb{Z}$. Put $r = \lambda(\boldsymbol{r}^+)$ (see 2.8). Then $r \in {}_1\mathbb{R}^+$ and $\mathbb{V}(p, \infty, \boldsymbol{r}) \subseteq \mathbb{W}(p, r)$.*

Proof. By 2.8(vi), $0 < r < 1$ (in fact, $k \ge 1$). Let $a \in \mathbb{V}(p, \infty, \boldsymbol{r})$ and $m = \mathrm{v}_p(a)$. If $m = 0$, then $r_0 = r_m \le a$. But $r_0 \ge 1$ by 2.8(i), and hence $|a|_{p,r} = 1 \le a$. If $m \ge 1$, then $r^m \le r_m$ by 2.8(iv), and so $|a|_{p,r} = r^m \le r_m \le a$. If $m \le -1$, then $t^{-m} \le r_m$, $t = \lambda(\boldsymbol{r}^-)$, by 2.8(iv), and $t^{-\mathrm{v}_p(a)} = t^{-m} \le r_m \le a$. But $rt \ge 1$, by 2.8(v), so that $t \ge r^{-1}$ and $t^{-m} \ge r^m$. Thus $|a|_{p,r} = r^m \le t^{-m} \le a$. We have checked that $a \in \mathbb{W}(p, r)$. □

Lemma 8.5 *Let S be a proper subsemiring of $\mathbb{Q}^+$ such that $S \nsubseteq \mathbb{Q}_1^+$ and $S \nsubseteq \mathbb{S}_p$ for every $p \in \mathbb{P}$. Then:*
(i) *$\mathsf{pd}(S) \ne \emptyset$.*
(ii) *If $p_1 \in \mathsf{pd}(S)$, then $s = \lambda(\mathbf{u}_{p_1}(S)^+) \in {}_1\mathbb{R}^+$ and $S \subseteq \mathbb{W}(p_1, s)$.*

Proof. (i) See 7.13(iii).
(ii) By 7.13(iv), $S \subseteq V = \mathbb{V}(p_1, \infty, \boldsymbol{u}_{p_1}(S))$. Since $p_1 \in \mathsf{pd}(S)$, we have $\boldsymbol{u}_{p_1,0}(S) \ge 1$. By 4.8(ii), $\mathbf{u}_{p_1,m}(S) \ne 0$ for every $m \in \mathbb{Z}$. Since $S \nsubseteq \mathbb{Q}_1^+$, we have $V \nsubseteq \mathbb{Q}_1^+$ and then $0 < \mathbf{u}_{p_1,k}(S) < 1$ for at least one $k \in \mathbb{Z}$ (in fact, $k \ge 1$) by 7.9(ii). Now, by 8.4, $V \subseteq \mathbb{W}(p_1, s)$. □

Proposition 8.6 *For all $p \in \mathbb{P}$ and $r \in {}_1\mathbb{R}^+$, the subsemiring $\mathbb{W}(p,r)$ is maximal in $\mathbb{Q}^+$.*

Proof. By 8.1(v),(vii) we have $\mathsf{p}(W) = \mathbb{P}$ and $\mathsf{pd}(W) = \{p\}$, $W = \mathbb{W}(p,r)$. Consequently, $W \nsubseteq \mathbb{Q}_1^+$ and $W \nsubseteq \mathbb{S}_{p_1}$ for every $p_1 \in \mathbb{P}$. Now, let S be a proper subsemiring of $\mathbb{Q}^+$ such that $W \subseteq S$. By 8.5, $S \subseteq \mathbb{W}(p_2,s)$, $p_2 \in \mathsf{pd}(S)$ and $s \in {}_1\mathbb{R}^+$. Thus $\mathbb{W}(p,r) \subseteq \mathbb{W}(p_2,s)$ and we get $p = p_2$ and $r = s$ by 8.3 and it means that $\mathbb{W}(p,r)$ is a maximal subsemiring of $\mathbb{Q}^+$. □

Theorem 8.7 *The semirings $\mathbb{Q}_1^+$, $\mathbb{S}_p$ and $\mathbb{W}(p,r)$, $p \in \mathbb{P}$, $r \in {}_1\mathbb{R}^+$ are just all (proper) maximal subsemirings of $\mathbb{Q}^+$. These subsemirings are pair-wise different (and hence non-isomorphic). Every proper subsemiring of $\mathbb{Q}^+$ is contained in (at least) one of them.*

Proof. By 6.2(i), 6.3(i) and 8.6, all the indicated subsemirings are maximal in $\mathbb{Q}^+$. If S is a maximal subsemiring of $\mathbb{Q}^+$ such that $S \neq \mathbb{Q}_1^+$ and $S \neq \mathbb{S}_p$ for every $p \in \mathbb{P}$, then $\mathsf{p}(S) = \mathbb{P}$ and $\mathsf{pd}(S) \neq \emptyset$ by 7.13. According to 8.5, we have $S = \mathbb{W}(p_1,s)$, $p_1 \in \mathsf{pd}(S)$, $s \in {}_1\mathbb{R}^+$.

By 6.11, the subsemirings $\mathbb{Q}_1^+$ and $\mathbb{S}_p$ are pair-wise different. By 8.3, the same is true for the subsemirings $\mathbb{W}(p,r)$. Moreover, $\mathbb{W}(p,r) \neq \mathbb{Q}_1^+$ (compare 6.2(v) and 8.1(vii)) and $\mathbb{W}(p,r) \neq \mathbb{S}_{p_1}$ (compare 6.3(viii) and 8.1(viii)). Finally, by 3.10, all these subsemirings are pair-wise non-isomorphic.

The rest follows from 8.5. □

Remark 8.8 The same result as in 6.10 follows (independently) also from 8.5, 8.6 and 8.7.

Remark 8.9 Let $p \in \mathbb{P}$ and $r \in {}_1\mathbb{R}^+$. If $a, b \in \mathbb{W}(p,r)$ are such that $a < 1$ and $b < 1$, then $\mathrm{v}_p(a) \geq 1$, $\mathrm{v}_p(b) \geq 1$, and hence $\mathrm{v}_p(a+b) \geq 1$. In particular, $a + b \neq 1$. Thus $1 \notin \mathbb{W}(p,r) + \mathbb{W}(p,r)$ and $\mathbb{W}(p,r) + \mathbb{W}(p,r) \neq \mathbb{W}(p,r)$.

Now, assume that $1 = cd$ for some $c, d \in \mathbb{W}(p,r)$. If $c = 1$, then $d = 1$ and conversely, and hence let $c \neq 1 \neq d$, $c < 1$ and $1 < d = 1/c$. We have $r^m \leq c < 1$ and $r^{-m} \leq c^{-1}$, $m = \mathrm{v}_p(c) = -\mathrm{v}_p(d)$. Consequently, $m \geq 1$ and $r^m = c = p^m c_1/d_1$, $c_1, d_1 \in \mathbb{Z}^+$,$p^m c_1 < d_1$, p divides neither c_1 nor d_1. From this, $r = pe^{1/m}$, $e = c_1/d_1$, $e \in {}_1\mathbb{Q}^+$, $\mathrm{v}_p(e) = 0$, $e < 1/p^m$, $e = (r/p)^m$.

Conversely, assume that r^m is rational and $\mathrm{v}_p(r^m) = m$ for some $m \in \mathbb{Z}^+$. Then $c = r^m = p^m c_1/d_1$, where $c_1, d_1 \in \mathbb{Z}^+$, $p^m c_1 < d_1$ and p divides neither c_1 nor d_1. We have $m = \mathrm{v}_p(c)$, $c \in \mathbb{W}(p,r)$, $-m = \mathrm{v}_p(c^{-1})$ and $c^{-1} \in \mathbb{W}(p,r)$. Of course, $c \neq 1 \neq c^{-1}$.

We have shown that $cd = 1$ for some $c, d \in \mathbb{W}(p,r)$ such that $c \neq 1 \neq d$ if and only if there exists $f \in {}_1\mathbb{Q}^+$ such that $\mathrm{v}_p(f) = m \geq 1$ and $r = f^{1/m}$.

Remark 8.10 From 6.13(i) follows that $\mathbb{W}(p,r)$ is not (additively) semisubtractive.

Let $a, b \in \mathbb{W}(p,r)$. There are $k_1, k_2 \in \mathbb{Z}^+$ with $\mathrm{v}_p(b) - \mathrm{v}_p(a) < k_1$ and $r^{\mathrm{v}_p(b)} \leq$ $\leq p^{k_2}a - b$. Put $k = k_1 + k_2$ and $c = p^k a - b$. Then $\mathrm{v}_p(p^k a) = k + \mathrm{v}_p(a) > \mathrm{v}_p(b)$,

$v_p(c) = v_p(b)$ and $r^{v_p(c)} = r^{v_p(b)} \leq p^k a - b = c$. Thus $c \in \mathbb{W}(p,r)$ and we have proved that the semiring $\mathbb{W}(p,r)$ is (additively) archimedean.

Remark 8.11 Let S be a subsemiring of $\mathbb{Q}$ such that $S - S = \mathbb{Q}$. If $S \cap \mathbb{Q}^- \neq \emptyset$, then S is a subring of $\mathbb{Q}$ by 3.2, and hence $S = S - S = \mathbb{Q}$. Now, assume that $S \subseteq \mathbb{Q}_0^+$ and put $T = S \cap \mathbb{Q}^+$. Then T is a subsemiring of $\mathbb{Q}^+$ and $T - T = \mathbb{Q}$. Assume, finally, that $1 \in T + T$. We are going to show that $T = \mathbb{Q}^+$.

Let, on the contrary, T be a proper subsemiring of $\mathbb{Q}^+$. Since $T - T = \mathbb{Q}$ we get $T \nsubseteq \mathbb{S}_p$ for any $p \in \mathbb{P}$ (use 6.3(viii)). Since $1 \in T + T$, we have $T \nsubseteq \mathbb{Q}_1^+$. Now, it follows from 8.7 that $T \subseteq \mathbb{W}(p,r)$ for some $p \in \mathbb{P}$ and $r \in {}_1\mathbb{R}^+$. But $1 \notin \mathbb{W}(p,r) + \mathbb{W}(p,r)$ by 8.9, a contradiction.

We have proved the following assertion (see also 6.9): Let S be a subsemiring of $\mathbb{Q}$ such that $S - S = \mathbb{Q}$ and $1 = a + b$ for some $a, b \in S$, $a \neq 0 \neq b$. Then either $S = \mathbb{Q}$ or $S = \mathbb{Q}_0^+$ or $S = \mathbb{Q}^+$.

As a corollary, we get such an assertion: Let S be a subsemiring of $\mathbb{Q}$ such the $S - S = \mathbb{Q}$ and $1/m \in S$ for at least one $m \in \mathbb{Z}$, $m \geq 2$. Then either $S = \mathbb{Q}$ or $S = \mathbb{Q}_0^+$ or $S = \mathbb{Q}^+$.

9. Unitary and non-unitary subgroups of $\mathbb{Q}(+)$

Definition 9.1 *Let A be a unitary subgroup of $\mathbb{Q}(+)$, (i.e., $1 \in A$). For every prime $p \in \mathbb{P}$ let* $\mathrm{ch}(A,p) = \sup\{k \in \mathbb{Z}_0^+ : p^{-k} \in A\} \in \mathbb{Z}_0^+ \cup \{\infty\}$. *Furthermore, put* $\mathrm{ch}(A) = (\mathrm{ch}(A,p) : p \in \mathbb{P})$.

Lemma 9.2 *Let A be a unitary subgroup of $\mathbb{Q}(+)$. If $a/b \in A$ where $a, b \in \mathbb{Z}, b \neq 0$ and* $\gcd(a,b) = 1$, *then $1/b \in A$.*

Proof. We have $1/b = ma/b + nb/b \in A$, where $m, n \in \mathbb{Z}$ are such that $1 = \gcd(a,b) = ma + nb$. □

Lemma 9.3 *Let A be a unitary subgroup of $\mathbb{Q}(+)$ and let $p \in \mathbb{P}$. If $c/d \in A$ and $k \in \mathbb{Z}_0^+$, where $c, d \in \mathbb{Z}, d \neq 0$, p does not divide c and p^k divides d, then $k \leq$* $\mathrm{ch}(A,p)$.

Proof. We have $d = p^k l$, $c/p^k = lc/d \in A$, $\gcd(c, p^k) = 1$ and 9.2 applies. □

Lemma 9.4 *Let A be a unitary subgroup of $\mathbb{Q}(+)$ and let $p_1, p_2, \dots, p_m, m \geq 1$, be pair-wise different primes. Then $a/p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} \in A$ for all $a \in \mathbb{Z}$ and $1 \leq k_i \leq$* $\leq \mathrm{ch}(A, p_i)$, $i = 1, 2, \dots, m$.

Proof. Put $b = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ and $c = \sum_{j=1}^m p_1^{k_1} p_2^{k_2} \cdots p_{j-1}^{k_{j-1}} p_{j+1}^{k_{j+1}} \dots p_m^{k_m}$ ($c = 1$ if $m = 1$). Then $c/b = \sum_{i=1}^m 1/p^{k_i} \in A$ and $\gcd(c,b) = 1$. By 9.2, $1/b \in A$, and hence $a/b \in A$, too. □

Proposition 9.5 *Let A be a unitary subgroup of $\mathbb{Q}(+)$. Then $A = \{q \in \mathbb{Q}^* : v_p(q) \geq -\mathrm{ch}(A,p)$ for every $p \in \mathbb{P}\} \cup \{0\}$ and* $\mathrm{ch}(A,p) = \sup\{-v_p(x) : 0 \neq x \in A\}$ *for every $p \in \mathbb{P}$.*

Proof. First, take $q \in A, q \neq 0$. We have $q = a/b, a, b \in \mathbb{Z}^*, \gcd(a, b) = 1$. If $p \in \mathbb{P}$ and $v_p(q) \geq 0$, then $-\mathrm{ch}(A, p) \leq 0 \leq v_p(q)$ trivially. If $m = v_p(q) < 0$, then $m \geq -\mathrm{ch}(A, p)$ by 9.3.

Conversely, if $q \in \mathbb{Q}^*$ is such that $v_p(q) \geq -\mathrm{ch}(A, p)$ for every $p \in \mathbb{P}$, then $q = a/b, a, b \in \mathbb{Z}^*, \gcd(a, b) = 1$ and either $b = \pm 1$ and $q \in A$ trivially or $b \neq \pm 1$ and $q = a/b \in A$ by 9.4. □

Corollary 9.6 *Let A_1 and A_2 be unitary subgroups of $\mathbb{Q}(+)$. Then:*

(i) $A_1 \subseteq A_2$ *if and only if* $\mathrm{ch}(A_1) \leq \mathrm{ch}(A_2)$ *(i.e.,* $\mathrm{ch}(A_1, p) \leq \mathrm{ch}(A_2, p)$ *for every* $p \in \mathbb{P}$*).*

(ii) $A_1 = A_2$ *if and only if* $\mathrm{ch}(A_1) = \mathrm{ch}(A_2)$.

Remark 9.7 Let A_1 be a unitary subgroup of $\mathbb{Q}(+)$ and let φ be a (group) homomorphism of A_1 into a subgroup A_2 of $\mathbb{Q}(+)$. Then $\varphi(0) = 0$ and, if $a, b \in \mathbb{Z} \setminus \{0\}$ are such that $a/b \in A_1$, then $\varphi(1)a = \varphi(a) = \varphi(b \cdot a/b) = b\varphi(a/b)$ and $\varphi(a/b) = \varphi(1)a/b$. Thus $\varphi(q) = \varphi(1)q$ for every $q \in A_1$. In particular, either $\varphi(1) = 0$ and $\varphi = 0$ or $\varphi(1) \neq 0$ and φ is injective. If $\varphi(1) \neq 0$, then $A_3 = \varphi(1)A_1$ is a subgroup of A_2 and $A_3 \cong A_1$. Clearly, A_3 is unitary if and only if $\varphi(1)^{-1} \in A_1$. Finally, φ is an isomorphism of A_1 onto A_2 if and only if $\varphi(1) \neq 0$ and $A_2 = \varphi(1)A_1$.

Remark 9.8 Let A_1 be a unitary subgroup of $\mathbb{Q}(+)$ and let $r \in \mathbb{Q}^*$ be such that $r^{-1} \in A_1$. Put $A_2 = rA_1$. Then A_2 is a unitary subgroup of $\mathbb{Q}(+)$ and the mapping $a \to ra$ is an isomorphism of A_1 onto A_2 (cf, 9.7). Moreover, $v_p(ra) = v_p(r) + v_p(a)$ for every $p \in \mathbb{P}$. Now, is clear that $\mathrm{ch}(A_2, p) = \mathrm{ch}(A_1, p) - v_p(r)$.

Consequently, the following two conditions are satisfied:

(1) For every $p \in \mathbb{P}, \mathrm{ch}(A_1, p) = \infty$ if and only if $\mathrm{ch}(A_2, p) = \infty$;

(2) The set $\{p \in \mathbb{P} : \mathrm{ch}(A_1, p) \neq \mathrm{ch}(A_2, p)\}$ is finite.

Remark 9.9 Let A_1 and A_2 be unitary subgroups of $\mathbb{Q}(+)$. Then the following are equivalent:

(i) $A_1 \cong A_2$.

(ii) $A_2 = rA_1$ for some $r \in \mathbb{Q}(+)$ (then $r \neq 0$ and $r^{-1} \in A_1$).

(iii) The conditions 9.8 (1), (2) are satisfied.

Indeed, the first two conditions are equivalent by 9.7 and 9.8 and they imply the third one by 9.8. Now, assume that the conditions 9.8 (1), (2) are satisfied. Put $s_p = \mathrm{ch}(A_1, p) - \mathrm{ch}(A_2, p)$ for every $p \in \mathbb{P}$ (here, $\infty - \infty = 0$) and $r = \prod p^{s_p}$ (use 9.8 (1), (2)). Then $r \in \mathbb{Q}^*$ and $v_p(r) = s_p$ for every $p \in \mathbb{P}$. If $A_3 = rA_1$, then $\mathrm{ch}(A_3, p) = \mathrm{ch}(A_1, p) - s_p = \mathrm{ch}(A_2, p)$ for every $p \in \mathbb{P}$ (see 9.8). Now, $rA_1 = A_2$ follows from 9.6.

Remark 9.10 Let $\alpha : \mathbb{P} \to \mathbb{Z}_0^+ \cup \{\infty\}$ be a mapping. Put $\mathrm{A}(\alpha) = \{q \in \mathbb{Q}^* : v_p(q) \geq -\alpha(p)$ for every $p \in \mathbb{P}\} \cup \{0\}$. Then $\mathrm{A}(\alpha)$ is a unitary subgroup of $\mathbb{Q}(+)$ and $\mathrm{ch}(\mathrm{A}(\alpha)) = \alpha$.

Proposition 9.11 *There exists a biunique correspondence between unitary additive subgroups of* $\mathbb{Q}(+)$ *and mappings* $\alpha : \mathbb{P} \to \mathbb{Z}_0^+ \cup \{\infty\}$. *The correspondence is given by* $A \to \mathrm{ch}(A)$ *and* $\alpha \to \mathrm{A}(\alpha)$ *(see* 9.1 *and* 9.10*). Moreover:*

(i) *If* A_1 *and* A_2 *are unitary subgroups of* $\mathbb{Q}(+)$, *then* $A_1 \subseteq A_2$ *if and only if* $\mathrm{ch}(A_1) \le \mathrm{ch}(A_2)$ *and* $A_1 \cong A_2$ *if and only if the conditions* 9.8 (1), (2) *are satisfied (see* 9.9*).*

(ii) *If* A *is a unitary subgroup of* $\mathbb{Q}(+)$, *then* A *is finitely generated if and only if the set* $\{p \in \mathbb{P} : \mathrm{ch}(A, p) \neq 0\}$ *is finite. In such a case,* A *is cyclic and* $A = \mathbb{Z}/m$ *for some* $m \in \mathbb{Z}^+$.

(iii) $\mathrm{ch}(\mathbb{Z}) = (0, 0, \dots)$ *and* $\mathrm{ch}(\mathbb{Q}) = (\infty, \infty, \dots)$.

Proof. See and combine 9.1, ..., 9.10. □

Proposition 9.12 *Let* A *be a non-zero subgroup of* $\mathbb{Q}(+)$. *Then:*

(i) $A \cap \mathbb{Z}^+ \neq \emptyset$ *and* $A \cap \mathbb{Z} = \chi(A) \cdot \mathbb{Z}$, *where* $\chi(A) = \min(A \cap \mathbb{Z}^+)$.

(ii) $A/\chi(A)$ *is a unitary subgroup of* $\mathbb{Q}(+)$ *isomorphic to* A.

(iii) A *is unitary if and only if* $\chi(A) = 1$.

(iv) *If* $p \in \mathbb{P}$ *divides* $\chi(A)$, *then* $\mathrm{ch}(A/\chi(A), p) = 0$.

(v) *If* $a, b \in \mathbb{Z}, b \neq 0$ *are such that* $a/b \in A$, *then* $\chi(A)$ *divides* a.

Proof. It is easy (if $1/p \in A/\chi(A)$, then $\chi(A)/p \in A$, and so p does not divide $\chi(A)$). □

Definition 9.13 *Let* A *be a non-zero subgroup of* $\mathbb{Q}(+)$. *We put* $\mathrm{ch}(A, p) = \mathrm{ch}(A/\chi(A), p)$ *for every prime* $p \in \mathbb{P}$ *and* $\mathrm{ch}(A) = \mathrm{ch}(A/\chi(A))$ *(see* 9.12*).*

Lemma 9.14 *Let* A *be a non-zero subgroup of* $\mathbb{Q}(+)$ *and let* $p \in \mathbb{P}$.

(i) If p *divides* $\chi(A)$, *then* $\mathrm{ch}(A, p) = 0$.

(ii) If p *does not divide* $\chi(A)$, *then* $\mathrm{ch}(A, p) = \sup\{k \in \mathbb{Z}_0^+ : \chi(A)/p^k \in A\} (\in \mathbb{Z}_0^+ \cup \{\infty\})$.

Proof. (i) See 9.13 and 9.12 (iv).

(ii) For every $k \in \mathbb{Z}_0^+$, we have $1/p^k \in A/\chi(A)$ if and only if $\chi(A)/p^k \in A$. □

Lemma 9.15 *Let* A *be a non-zero subgroup of* $\mathbb{Q}(+)$ *and let* $p \in \mathbb{P}$.

(i) If $a/b \in A$, *where* $a, b \in \mathbb{Z}, b \neq 0$, *and* $\gcd(a, b) = 1$, *then* $\chi(A)/b \in A$.

(ii) If $c/d \in A$ *and* $k \in \mathbb{Z}_0^+$, *where* $c, d \in \mathbb{Z}, d \neq 0$, p *does not divide* c *and* p^k *divides* d, *then* $k \le \mathrm{ch}(A, p)$.

Proof. (i) We have $a \in A \cap \mathbb{Z}$, and so $a = \chi(A)e$ for some $e \in \mathbb{Z}$. Consequently, $e/b \in A/\chi(A)$, $1/b \in A/\chi(A)$, by 9.2 and, finally, $\chi(A)/b \in A$.

(ii) Using 9.3, we can proceed similarly as in the proof of (i). □

Lemma 9.16 *Let* A *be a non-zero subgroup of* $\mathbb{Q}(+)$ *and let* $p_1, p_2, \dots, p_m, m \ge 1$, *be pair-wise different primes. Then* $a/p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m} \in A$ *for all* $a \in \mathbb{Z}$ *such that* $\chi(A)$ *divides* a *and all* $1 \le k_i \le \mathrm{ch}(A, p_i)$, $i = 1, 2, \dots, m$.

Proof. Use 9.4 (see the proof of 9.15(i)). □

Proposition 9.17 *Let A be a non-zero subgroup of $\mathbb{Q}(+)$. Then $A = \{q \in \mathbb{Q}^* : \mathrm{v}_p(q) \geq \mathrm{v}_p(\chi(A)) - \mathrm{ch}(A, p)$ for every $p \in \mathbb{P}\} \cup \{0\}$.*

Proof. If $q \in A, q \neq 0$, then $q/\chi(A) \in A/\chi(A)$ and $\mathrm{v}_p(q) - \mathrm{v}_p(\chi(A)) \geq -\mathrm{ch}(A, p)$ by 9.5. Conversely, if $q \in \mathbb{Q}^*$ is such that $\mathrm{v}_p(q) \geq \mathrm{v}_p(\mathrm{ch}(A)) - \mathrm{ch}(A, p)$ for every $p \in \mathbb{P}$, then $\mathrm{v}_p(q/\chi(A)) \geq -\mathrm{ch}(A, p), q/\chi(A) \in A/\chi(A)$ by 9.5, and so $q \in A$. □

Lemma 9.18 *Let A_1 and A_2 be non-zero subgroups of $\mathbb{Q}(+)$. Then $A_1 \subseteq A_2$ if and only if $\chi(A_2)$ divides $\chi(A_1)$ and $\mathrm{ch}(A_1, p) \leq \mathrm{ch}(A_2, p) + \mathrm{v}_p(\chi(A_1)) - \mathrm{v}_p(\chi(A_2))$ for every $p \in \mathbb{P}$.*

Proof. If $A_1 \subseteq A_2$, then $A_1 \cap \mathbb{Z} \subseteq A_2 \cap \mathbb{Z}$ and it follows easily that $\chi(A_2)$ divides $\chi(A_1), \chi(A_1) = m\chi(A_2)$ for some $m \in \mathbb{Z}^+$. Moreover, $A_1/\chi(A_1) \subseteq A_2/\chi(A_1) = (A_2/\chi(A_2))/m$ and $\mathrm{ch}(A_1/\chi(A_1), p) \leq \mathrm{ch}(A_2/\chi(A_1), p)$ by 9.6(i). But $\mathrm{ch}(A_2/\chi(A_1), p) = \mathrm{ch}(A_2/\chi(A_2), p) + \mathrm{v}_p(m) = \mathrm{ch}(A_2/\chi(A_2), p) + \mathrm{v}_p(\chi(A_1)) - \mathrm{v}_p(\chi(A_2))$ follows from 9.8. The rest follows from 9.17. □

Corollary 9.19 *Let A_1 and A_2 be non-zero subgroups of $\mathbb{Q}(+)$. Then $A_1 = A_2$ if and only if $\chi(A_1) = \chi(A_2)$ and $\mathrm{ch}(A_1) = \mathrm{ch}(A_2)$.*

Remark 9.20 Let A_1 and A_2 be non-zero subgroups of $\mathbb{Q}(+)$. Then $A_1 \cong A_1/\chi(A_1)$ and $A_2 \cong A_2/\chi(A_2)$. Using this and 9.9, we conclude that $A_1 \cong A_2$ if and only if the conditions 9.8 (1), (2) are satisfied.

Remark 9.21 Let $m \in \mathbb{Z}^+$ and let $\alpha : \mathbb{P} \to \mathbb{Z}_0^+ \cup \{\infty\}$ be a mapping such that $\alpha(p) = 0$ whenever p divides m. Put $\mathrm{A}(\alpha, m) = m\mathrm{A}(\alpha) = \{q \in \mathbb{Q}^* : \mathrm{v}_p(q) \geq \mathrm{v}_p(m) - \alpha(p)$ for every $p \in \mathbb{P}\} \cup \{0\}$ (see 9.10). Then $\mathrm{A}(\alpha, m)$ is a non-zero subgroup of $\mathbb{Q}(+), \chi(\mathrm{A}(\alpha, m)) = m$ and $\mathrm{ch}(\mathrm{A}(\alpha, m)) = \alpha$.

Proposition 9.22 *There exists a biunique correspondence between non-zero additive subgroups of $\mathbb{Q}(+)$ and ordered pairs (α, m), where $m \in \mathbb{Z}^+$ and $\alpha : \mathbb{P} \to \mathbb{Z}_0^+ \cup \{\infty\}$ is a mapping such that $\alpha(p) = 0$ for every p dividing m. The correspondence is given by $A \to (\mathrm{ch}(A), \chi(A))$ and $(\alpha, m) \to \mathrm{A}(\alpha, m)$ (see 9.12, 9.13, and 9.21). Moreover:*

(i) If A_1 and A_2 are non-zero subgroups of $\mathbb{Q}(+)$, then $A_1 \subseteq A_2$ if and only if $\chi(A_2)$ divides $\chi(A_1)$ and $\mathrm{ch}(A_1, p) \leq \mathrm{ch}(A_2, p) + \mathrm{v}_p(\chi(A_1)) - \mathrm{v}_p(\chi(A_2))$ for every $p \in \mathbb{P}$ and $A_1 \cong A_2$ if and only if the conditions 9.8 (1), (2) are satisfied (see 9.20).

(ii) If A is non-zero subgroup of $\mathbb{Q}(+)$, then A is finitely generated if and only if the set $\{p \in \mathbb{P} : \mathrm{ch}(A, p) \neq 0\}$ is finite. In such a case, A is cyclic and $A = \mathbb{Z}q$ for some $q \in \mathbb{Q}^+$.

Proof. See and combine 9.18, ..., 9.21 and 9.11. □

10. Unitary and Non-unitary Subrings of $\mathbb{Q}$

Proposition 10.1 *Let $A (= A(+))$ be a unitary subgroup of $\mathbb{Q}(+)$. Then A is a (unitary) subring of $\mathbb{Q}$ if and only if $\mathrm{ch}(A(+), p) \in \{0, \infty\}$ for every $p \in \mathbb{P}$ (see 9.1).*

Proof. Use 9.5 and 9.1. □

Proposition 10.2 *There exists a biunique correspondence between unitary subrings of* $\mathbb{Q}$ *and subsets of* $\mathbb{P}$. *If* A *is a unitary subring of* $\mathbb{Q}$, *then the corresponding subset is* $\mathrm{p}_A = \{p \in \mathbb{P} : 1/p \in A\}$. *If* P *is a subset of* $\mathbb{P}$, *then the corresponding unitary subring is* $\mathrm{A}_P = \{q \in \mathbb{Q}^* : \mathrm{v}_p(q) \geq 0$ *for every* $p \in \mathbb{P} \setminus P\} \cup \{0\}$. *Moreover:*

(i) *If* A_1 *and* A_2 *are unitary subrings of* $\mathbb{Q}$, *then* $A_1 \subseteq A_2$ *if and only if* $\mathrm{p}_{A_1} \subseteq \mathrm{p}_{A_2}$ *and* $A_1 \cong A_2$ *if and only if* $A_1 = A_2$.

(ii) *If* A *is a unitary subring of* $\mathbb{Q}$, *then* A *is a finitely generated ring if and only if the set* p_A *is finite.*

(iii) $\mathrm{p}_{\mathbb{Z}} = \emptyset$.

(iv) $\mathrm{p}_{\mathbb{Q}} = \mathbb{P}$.

Proof. It is easy (see 10.1, 9.5 and 3.10). □

Proposition 10.3 *Let* $A(= A(+))$ *be a non-zero subgroup of* $\mathbb{Q}(+)$. *Then* A *is a subring of* $\mathbb{Q}$ *if and only if* $\mathrm{ch}(A(+), p) \in \{0, \infty\}$ *for every* $p \in \mathbb{P}$ *(see* 9.1, 9.12, 9.13 *and* 10.1*).*

Proof. Put $m = \chi(A)$ (see 9.12). If A is a subring of $\mathbb{Q}$ and $p \in \mathbb{P}$ is such that $\mathrm{ch}(A(+), p) \geq 1$, then p does not divide m (9.12(iv)), $1/p \in A/m$ and $m/p \in A$. Consequently, $m^n/p^n \in A$ and $m^{n-1}/p^n \in A/m$ for every $n \in \mathbb{Z}^+$ and it follows from 9.3 that $\mathrm{ch}(A(+), p) = \mathrm{ch}(A(+)/m, p) = \infty$.

Now, if $\mathrm{ch}(A(+), p) \in \{0, \infty\}$ for every $p \in \mathbb{P}$, then A/m is a subring of $\mathbb{Q}$ by 10.1, and hence $ab/m^2 \in A/m$ and $ab/m \in A$ for all $a, b \in A$. Then, of course, $ab \in A$ and A is a subring. □

Proposition 10.4 *There exists a biunique correspondence between (non-zero) subrings of* $\mathbb{Q}$ *and ordered pairs* (P, m), *where* $m \in \mathbb{Z}^+$ *and* P *is a subset of* $\mathbb{P}$ *such that* $p \in \mathbb{P} \setminus P$ *whenever* $p \in \mathbb{P}$ *divides* m. *If* A *is a subring of* $\mathbb{Q}$, *then the corresponding pair is* $(\mathrm{p}_A, \chi(A(+)))$, *where* $\mathrm{p}_A = \{p \in \mathbb{P} : \chi(A(+))/p \in A\}$. *If* (P, m) *is a pair as above, then the corresponding subring is* $\mathrm{A}_{(P,m)} = \{q \in \mathbb{Q}^* : \mathrm{v}_p(q) \geq$ $\geq \mathrm{v}_p(m)$ *for every* $p \in \mathbb{P} \setminus P\} \cup \{0\}$. *Moreover:*

(i) *If* A_1 *and* A_2 *are subrings of* $\mathbb{Q}$, *then* $A_1 \subseteq A_2$ *if and only if* $\chi(A_2(+))$ *divides* $\chi(A_1(+))$ *and* $\mathrm{p}_{A_1} \subseteq \mathrm{p}_{A_2}$ *and* $A_1 \cong A_2$ *if and only if* $A_1 = A_2$.

(ii) *If* A *is a subring of* $\mathbb{Q}$, *then* A *is a finitely generated ring if and only if the set* p_A *is finite.*

Proof. It is easy (see 9.14, 9.22, 10.2, 10.3 and 3.10). □

11. Subsemigroups of $\mathbb{Q}(+)$ — First Observations

Proposition 11.1 *(see* 3.1*) Let* S *be a subsemigroup of* $\mathbb{Q}(+)$ *such that* $S \cap \mathbb{Q}^+ \neq$ $\neq \emptyset \neq S \cap \mathbb{Q}^-$. *Then* S *is a subgroup of* $\mathbb{Q}(+)$.

Proposition 11.2 *Let S be a subsemigroup of $\mathbb{Q}_0^-(+)$ ($\mathbb{Q}_0^+(+)$, resp.). Then $-S =$ $= \{-q : q \in S\}$ is a subsemigroup of $\mathbb{Q}_0^+(+)$ ($\mathbb{Q}_0^-(+)$, resp.) and the mapping $q \mapsto -q$ is an isomorphism of $S(+)$ onto $(-S)(+)$.*

Proof. It is obvious. □

Proposition 11.3 *Let S be a subsemigroup of $\mathbb{Q}_0^+(+)$ such that $0 \in S$. Then:*

(i) *0 is a neutral element of $S(+)$.*
(ii) *If S is non-zero, then $T = S \setminus \{0\}$ is a subsemigroup of $\mathbb{Q}^+(+)$; the semigroup $T(+)$ has no neutral element.*

Proof. It is obvious. □

Proposition 11.4 *Let S be a subsemigroup of $\mathbb{Q}^+(+)$ such that $r \in \mathbb{Q}^+$, where $r = \inf(S)$. Then $r^{-1}S$ is a subsemigroup of $\mathbb{Q}^+(+)$, $\inf(r^{-1}S) = 1$ and the mapping $q \mapsto r^{-1}q$ is an isomorphism of $S(+)$ onto $(r^{-1}S)(+)$.*

Proof. It is obvious. □

Proposition 11.5 *Let S be a non-zero subsemigroup of $\mathbb{Q}(+)$. If $r \in S$, $r \neq 0$, then $r^{-1}S$ is a unitary subsemigroup of $\mathbb{Q}(+)$ and the mapping $q \mapsto r^{-1}q$ is an isomorphism of $S(+)$ onto $(r^{-1}S)(+)$.*

Proof. It is obvious. □

Lemma 11.6 *Let S be a subsemigroup of $\mathbb{Q}(+)$ and let $a, b, c, d \in \mathbb{Z}$ be such that $b \geq 1$, $d \neq 0$, $a/b \in S$ and $a/b - c/d \in S$.*
Then:

(i) *$a \in S$, $(ad - bc)/d \in S$.*
(ii) *$a - c/d = (ad - c)/d \in S$.*
(iii) *If $d \geq 1$, then $ad \in S$, $ad - bc \in S$ and $ad - c \in S$.*

Proof. (i) We have $a = b \cdot a/b \in S$, $(ad - bc)/bd = a/b - c/d \in S$ and hence $a - bc/d = (ad - bc)/d \in S$.

(ii) If $b \geq 2$, then $a - a/b = (b-1)a/b \in S$ and $(ad - c)/d = a - c/d =$ $= (a - a/b) + (a/b - c/d) \in S$.

(iii). Use (i) and (ii). □

Lemma 11.7 *Let S be a subsemigroup of $\mathbb{Q}(+)$ such that $S - S = \mathbb{Q}$ and $T =$ $= S \cap \mathbb{Q}^+ \neq \emptyset$. Then for every $n \in \mathbb{Z}^+$ there are $a_n, a'_n \in T \cap \mathbb{Z}^+$ such that $a_n - 1/n =$ $= (na_n - 1)/n \in T$, $na_n - 1 \neq 0$, and $a'_n - 1/(na_n - 1) = ((na_n - 1)a'_n - 1)/(na_n - 1) \in T$. Moreover, $r = na_n - 1 \in T \cap \mathbb{Z}^+$, $s = ra'_n - 1 \in T \cap \mathbb{Z}^+$ and* $\gcd(r, ns) = 1$.

Proof. Clearly, T is a subsemigroup of $\mathbb{Q}(+)$. If $S \cap \mathbb{Q}^- \neq \emptyset$, then S is a subgroup of $\mathbb{Q}(+)$ by 11.1, and therefore $S = S - S = \mathbb{Q}$ and $T = \mathbb{Q}^+$. If $S \cap \mathbb{Q}^- = \emptyset$, then $S \subseteq \mathbb{Q}_0^+$ and $T = S \setminus \{0\}$. Now, we see that $T - T = \mathbb{Q}$ anyway.

By 11.6, there are $a_n, b_n \in \mathbb{Z}^+$ such that $a_n/b_n \in T$, $a_n \in T \cap \mathbb{Z}^+$, $a_n/b_n - 1/n \in T$ and $a_n - 1/n = r/n \in T$. Then $r \in T \cap \mathbb{Z}^+$, too. In particular, $r \neq 0$ and, by 11.6

again, there are $a'_n, b'_n \in \mathbb{Z}^+$ such that $a'_n/b'_n \in T$, $a'_n \in T \cap \mathbb{Z}^+$, $a'_n/b'_n - 1/r \in T$ and $a'_n - 1/r = s/r \in T$. Then $s \in T \cap \mathbb{Z}^+$, too, and hence $ns \in T \cap \mathbb{Z}^+$.

Now, if $p \in \mathbb{P}$ divides both r and ns, then p divides $na_n - 1$ and p does not divide n. Consequently, p divides $s = ra'_n - 1$ and p divides 1, a contradiction. Thus $\gcd(r, ns) = 1$. □

Lemma 11.8 *Let S be a subsemigroup of $\mathbb{Q}(+)$ such that $T = S \cap \mathbb{Q}^+ \neq \emptyset$. The following conditions are equivalent:*

(i) $S - S = \mathbb{Q}$.

(ii) *For every $n \in \mathbb{Z}^+$ there is $m_n \in \mathbb{Z}^+$ such that $k/n \in T$ for every $k \in \mathbb{Z}$, $k \geq m_n$.*

(iii) *For all $t \in T$ and $q \in \mathbb{Q}$ there is $l \in \mathbb{Z}^+$ with $lt - q \in T$.*

Proof. (i) implies (ii). By 11.7, there are $r, s \in T \cap \mathbb{Z}^+$ such that $r/n \in T$, $s/r \in T$ and $\gcd(r, ns) = 1$. We have $r, ns \in T$ and we put $T_1 = \{ur + vns : u, v \in \mathbb{Z}_0^+, u+v \neq 0\}$. Clearly, T_1 is a subsemigroup of $(T \cap \mathbb{Z}^+)(+)$ and $r, ns \in T_1$. Using the equality $\gcd(r, ns) = 1$, we find $m_n \in \mathbb{Z}^+$ such that $m_n, m_n + 1, m_n + 2, \ldots \in T_1$ (see 12.1). Now, if $k \in \mathbb{Z}^+$ is such that $k \geq m_n$, then $k = u_1 r + v_1 ns$ for some $u_1, v_1 \in \mathbb{Z}_0^+$, $u_1 + v_1 \neq 0$, and $k/n = u_1 r/n + v_1 ns/n = u_1 \cdot r/n + v_1 r \cdot s/r \in T$.

(ii) implies (iii). We have $t = a/b$ and $q = c/d$, where $a, b, d \in \mathbb{Z}^+$ and $c \in \mathbb{Z}$. By (ii), there is $m \in \mathbb{Z}^+$ such that $k/bd \in T$ for every $k \in \mathbb{Z}^+$, $k \geq m$. Now, find $l \in \mathbb{Z}^+$ with $lad - bc \geq m$. Then $lt - q = la/b - c/d = (lad - bc)/bd \in T$.

(iii) implies (i). It follows immediately that $\mathbb{Q} = T - T \subseteq S - S$. □

Remark 11.9 Let S be a subsemigroup of $\mathbb{Q}(+)$ such that $T = S \cap \mathbb{Q}^- \neq \emptyset$. Considering the subsemigroup $-S$ and using 11.8, we see that the conditions 11.8(i),(iii) remain equivalent and, moreover, they are equivalent to:

(ii2) For every $n \in \mathbb{Z}^+$ there is $m_n \in \mathbb{Z}^-$ such that $k/n \in T$ for every $k \in \mathbb{Z}$, $k \leq m_n$.

Remark 11.10 Let S be a subsemigroup of $\mathbb{Q}(+)$ such that $S - S = \mathbb{Q}$ and $1/t \in S$ for some $t \in \mathbb{Z}^+$, $t \geq 2$.

Clearly, S is unitary and we show that for every $q \in \mathbb{Q}^+$ there exists $l \in \mathbb{Z}^+$ with $t^l q \in S$.

Put $T = S \cap \mathbb{Q}^+$ and $R = T \cup T/t \cup T/t^2 \cup \cdots$. Then $T - T = \mathbb{Q}$ and R is a subsemigroup of $\mathbb{Q}^+(+)$. If $n \in \mathbb{Z}^+$, then it follows from 11.8 that $t^l/n \in T_1$ for some $l \in \mathbb{Z}^+$. We have $t^l/n = a \in T$, $l_1 \in \mathbb{Z}_0^+$, and so $1/n = a/t^l \in R$. We have shown that $1/n \in R$ for every $n \in \mathbb{Z}^+$ and it follows easily that $R = \mathbb{Q}^+$.

Remark 11.11 (cf. 8.11). Let S be a subsemiring of $\mathbb{Q}$ such that $S - S = \mathbb{Q}$. Then $T = S \cap \mathbb{Q}^+$ is a subsemiring of $\mathbb{Q}^+$ and $T - T = \mathbb{Q}$.

(i) Assume that $1/t \in T$ for some $t \in \mathbb{Z}^+$, $t \geq 2$. If $q \in \mathbb{Q}^+$, then $t^l q \in T$ for some $l \in \mathbb{Z}^+$ (by 11.10). But $1/t^l \in T$, and hence $q \in T$. Thus $T = \mathbb{Q}^+$ and either $S = \mathbb{Q}^+$ or $S = \mathbb{Q}_0^+$ or $S = \mathbb{Q}$.

(ii) Assume that $1 \in T + T$. Then $1 = a/b + c/d$ for some $a, b, c, d \in \mathbb{Z}^+$ such that $a/b \in T$, $c/d \in T$ and $\gcd(a, b) = 1 = \gcd(c, d)$. We have $1 = (ad + bc)/bd$, and hence $\gcd(a, c) = 1$ as well. Now, using 5.2, we get $1/t \in T$, where $t = \operatorname{lcm}(b, d) \geq 2$. By (i), $T = \mathbb{Q}^+$.

Lemma 12.1 *Let S be a subsemigroup of $\mathbb{Z}^+(+)$ such that* $\gcd(S) = 1$. *Then there exists at least one positive integer s such that $s, s+1, s+2, \ldots \in S$.*

Proof. Let m denote the smallest positive integer such that $m + n \in S$ for some $n \in S \cup \{0\}$. If $m_1 \in \mathbb{Z}^+$ and $n_1 \in S \cup \{0\}$ are such that $m_1 + n_1 \in S$, then $m_1 = = km + l, k \in \mathbb{Z}^+, l \in \mathbb{Z}, 0 \leq l < m$, and both $km + kn + n_1 = k(m + n) + n_1$ and $km + kn + n_1 + l = m_1 + n_1 + kn$ are in S. Since $l < m$, we get $l = 0$ and it follows that $m \mid m_1$. Consequently, $m \mid a$ for all $a \in S$, and hence $m \mid \gcd(S) = 1$, $m = 1$. Thus $n + 1 \in S$; if $n = 0$, then $1 \in S$ and $S = \mathbb{Z}^+$.

We have shown that $t \in S$ and $t + 1 \in S$ for at least one $t \in S$. If $r_1 \geq t$ and $0 \leq r_2 < t$, then $r_1 t + r_2 = (r_1 - r_2)t + r_2(t + 1) \in S$. We can put $s = t^2$. □

Proposition 12.2 *Let S be a subsemigroup of $\mathbb{Z}^+$ and let $r = \gcd(S)$. Then there exists a uniquely determined positive integer $s = \sigma(S)$ such that $(s-1)r \notin S$ and $sr, (s+1)r, (s+2)r, \ldots \in S$.*

Proof. $T = r^{-1}S$ is a subsemigroup of $\mathbb{Z}^+(+)$ and $\gcd(T) = 1$. Now, the result follows from 12.1. □

Proposition 12.3 *Every subsemigroup of $\mathbb{Z}(+)$ is finitely generated.*

Proof. Let S be a subsemigroup of $\mathbb{Z}(+)$. If S is a non-zero group, then $S(+)$ is a cyclic group and it is, as a semigroup, generated by the two-element subset $\{a, -a\}$, where $a = \min(S \cap \mathbb{Z}^+)$. If S is not a group, then, taking into account 11.1, 11.2 and 11.3, we may restrict ourselves to the case $S \subseteq \mathbb{Z}^+$. If $r = \gcd(S)$, then the semigroups $S(+)$ and $T(+)$ are isomorphic, $T = r^{-1}S \subseteq \mathbb{Z}^+$, $\gcd(T) = 1$, and therefore we can assume that $r = 1$. Put $s = \sigma(S)$ (see 12.2) and $m = \min(S)$. Now, denote by R the subsemigroup of $\mathbb{Z}(+)$ generated by the set $\{n \in S : n \leq s + m - 1\}$. Clearly, $R \subseteq S$, $\{n_1 \in S : n_1 \leq s\} \subseteq R$, $m \in R$, $s \in R$ and $R(+)$ is a finitely generated semigroup. If $m = 1$, then $R = S = \mathbb{Z}^+$. If $m \geq 2$, then $s, s+1, \ldots, s+m-1 \in R$, and hence $s + km, s + km + 1, \ldots, s + (k+1)m - 1 \in R$ for every $k \geq 1$. Consequently, $\{s_1 : s \leq s_1\} \subseteq R$ and we conclude that $R = S$. □

Example 12.4 The set $A_m = \{m, m+1, m+2, \ldots\}$, $m \geq 1$, is a subsemigroup of $\mathbb{Z}^+(+)$ and the set $\{m, m+1, \ldots, 2m-1\}$ is the smallest generator set of $A_m(+)$. Consequently, the semigroup $A_m(+)$ cannot be generated by less than m elements. Notice also that $S = A_m$ when S is a subsemigroup of $\mathbb{Z}^+(+)$ such that $\gcd(S) = 1$ and $\sigma(S) = \min(S)$.

Remark 12.5 Let S be a finitely generated subsemigroup of $\mathbb{Q}(+)$. Then the difference subgroup $A = S - S$ is finitely generated, and hence it is a cyclic group.

Remark 12.6 Let S be a subsemigroup of $\mathbb{Q}(+)$ such that $S \cap \mathbb{Q}^+ \neq \emptyset$ (see 11.2). Then $S \cap \mathbb{Z}^+ \neq \emptyset$ and, if $r = \gcd(S \cap \mathbb{Z}^+)$, then there exists $s \in \mathbb{Z}^+$ such that $sr, (s+1)r, (s+2)r, \ldots \in S$.

References

[1] Głazek, K.: *A Guide to the Literature on Semirings and their Applications in Mathematics and Information Sciences*, Kluwer Academic Publishers, Dordrecht, 2002.

[2] Golan, J. S.: *Semirings and their Applications*, Kluwer Academic Publishers, Dordrecht, 1999.

[3] Golan, J. S.: *Semirings and Affine Equations over Them: Theory and Applications*, Kluwer Academic Publishers, Dordrecht, 2003.

[4] Vandiver, H. S.: *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.

[5] Hebisch, U., Weinert, H. J.: *Semirings and semifields*. In: *Handbook of Algebra* **Vol. 1**, Elsevier, Amsterdam, 1996.

[6] Hebisch, U., Weinert, H. J.: *Semirings: Algebraic Theory and Applications in Computer Science*, World Scientific Publishing. Co. Pte. Ltd., Singapore, 1998.