

On residuals in partially ordered semigroups*

By O. STEINFELD (Budapest)

Dedicated to Professor L. Kalmár on his 60th birthday

§ 1. Introduction

Let L be a residuated lattice-ordered semigroup and S a closed interval of L which has a maximum element s . In this paper we prove a lemma and a theorem which give some sufficient conditions in order that the mapping

$$x \rightarrow x:s \quad (x \in S)$$

be an isomorphism with respect to the order relation and the operations of L .

The results of §§ 2 and 3 are needed in the proof of the lemma and the theorem. First we consider a naturally ordered semigroup in which unique prime factorization holds. In § 2, some consequences of these hypotheses are enumerated. In § 3, we prove two lemmas concerning the residuals $p:s$ ($q:s$), where p (q) is a prime (primary) element in S . These lemmas generalize some previous results of the author.

In § 5 we apply the results of § 4 to the residuated lattice-ordered semigroup of all ideals of an associative ring.

§ 2. Some consequences of unique prime factorization

Let S be a *partially ordered semigroup*, i. e. a set with an associative multiplication and with a partial order \cong such that, for all $a, b, c (\in S)$ $a \cong b$ implies $ac \cong bc$ and $ca \cong cb$. S will be called *negatively ordered* if, for all $a, b (\in S)$, $ab \cong a$ and $ab \cong b$ hold.

We shall say that S is *naturally ordered*¹⁾ if it is negatively ordered and

$$(2.1) \quad a < b \text{ implies } a = bx = yb \text{ for some } x, y \in S.$$

Assume that S is a partially ordered semigroup (with at least three elements) satisfying:

*) On the 6th Austrian Mathematical Congress the author lectured on some results of this paper.

¹⁾ In FUCHS [2] a positively ordered semigroup satisfying (2.1) is called naturally ordered.

(i) S is naturally ordered and has a minimum element²⁾ 0 and a maximum element²⁾ s ;

(ii) every element $a \in S$ ($0 < a < s$) may be represented as the product of a finite number of prime elements³⁾

$$(2.2) \quad a = p_1 p_2 \dots p_k$$

and two representations of an element a can differ only in the order of prime factors, that is, in S the unique prime factorization holds;

(iii) in S there exists an element z ($0 < z < s$) which is not a zero-divisor.

From hypotheses (i), (ii), (iii) we conclude in turn:

(A) *The element s is the identity of S .*

The element s is idempotent because $s^2 < s$ would imply the existence of a prime element $p (\in S)$ with $s^2 \cong p < s$, which is impossible.

It suffices to prove that $sp = ps = p$ for all primes $p \in S$. By (2.1) and $p < s$ there exists $q (\in S)$ with $p = sq$. This implies, because of $s^2 = s$

$$sp = s^2 q = sq = p.$$

Naturally $ps = p$ holds too.

(B) *Every prime p of S is a maximal element⁴⁾ in S .*⁵⁾

Let m be an element of S with $p < m < s$. The property (2.1) guarantees the existence of an element h such that $p = mh$. Because of the primeness of p this implies

$$h \cong p$$

and because of the negative order in S

$$p \cong h.$$

Thus $p = mp$ which contradicts hypothesis (ii).

(C) *S is commutative.*⁶⁾

In view of (A) and (ii) it suffices to prove that the prime elements of S commute. Let p, q be different primes of S . By (2.1) there exists an element $x (\in S)$ such that $qx = pq (< p)$. The prime property of p and (B) show that $x \cong p$. Therefore $pq \cong qp$. Changing the roles of p and q we get the converse inequality, whence $pq = qp$, in fact.

Because of (C) every element $a \in S$ ($0 < a < s$) can be written up to the order of factors *uniquely* in the form

$$(2.3) \quad a = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

with prime powers $p_i^{k_i}$ belonging to different (pairwise commuting) bases p_i .

²⁾ We use the term „minimum element” to mean an element which is smaller than any other element. Obviously the minimum element 0 is unique and satisfies $0 \cdot a = a \cdot 0 = 0$ for all $a \in S$. The meaning of „maximum element” is clear. The maximum element s is in general not an identity in S .

³⁾ An element $p \in S$ ($0 \cong p < s$) is said to be *prime* if $ab \cong p$ ($a, b \in S$) implies either $a \cong p$ or $b \cong p$.

⁴⁾ An element m is called *maximal* in S if $m \cong m' < s$ ($m' \in S$) implies $m' = m$.

⁵⁾ Here we follow the argument of ŠULGEIFER [5].

⁶⁾ Here we follow the argument of FUCHS—STEINFELD [3].

(D) S is free of divisors of zero.

The assumption $xy=0$ ($0 < x, y < s$) implies that 0 has at least one prime factorization. Among the prime factorizations of 0 let us consider a shortest one:

$$0 = p_1 \dots p_r,$$

that is $p_1 \dots p_{i-1} p_{i+1} \dots p_r \neq 0$ holds for $1 \leq i \leq r$. Let p denote a prime element of S satisfying $z \leq p$ where z is no divisor of zero. As $p_1 \dots p_r = 0 \leq z \leq p$ holds, by (B) the prime element p must occur among p_1, \dots, p_r . E. g. let $p = p_1$. Thus $zp_2 \dots p_r \leq p_1 p_2 \dots p_r = 0$, which contradicts hypothesis (iii).

(E) Every prime power p^k ($k = 1, 2, \dots$) is a primary element⁷⁾ in S .

Let a, b be two elements of S such that $ab \leq p^k$. We can assume that $0 < a, b < s$ and $ab \neq 0$. Because of (i) and (A) there exists an element d with $ab = p^k d$. If $a \not\leq p^k$ then by (ii) the prime element p must occur among the prime factors of b . Thus $b \leq p$ and so $b^k \leq p^k$.

§ 3. Some results on residuals

Let L be a residuated partially ordered semigroup, i. e. a partially ordered semigroup having the following property: for every pair of elements $a, b \in L$ there exists a right-residual $a:b \in L$ and a left-residual $a::b \in L$ defined by

$$(3.1) \quad xb \leq a \text{ (if and only if } x \leq a:b \text{ (} x \leq a::b \text{))}.$$

We need to know:

(a) If L is a residuated partially ordered semigroup and $\inf(a, b) = a \cap b$ ($a, b \in L$) exists in L , then so do $(a:x) \cap (b:x)$, $(a::x) \cap (b::x)$ for all $x \in L$ and

$$(3.2) \quad (a:x) \cap (b:x) = (a \cap b):x, \quad (a::x) \cap (b::x) = (a \cap b)::x$$

(See FUCHS [2].)

(b) A residuated partially ordered semigroup L which is at the same time a lattice is a lattice-ordered semigroup, that is,

$$(3.3) \quad (a \cup b)c = ac \cup bc \quad \text{and} \quad c(a \cup b) = ca \cup cb$$

hold for all $a, b, c \in L$ (See FUCHS [2].)

(c) If the maximum element e of a lattice-ordered semigroup L is an identity in L , then

$$(3.4) \quad a \cup b = e \text{ implies } a \cap b = ab \cup ba \quad (a, b \in L),$$

$$(3.5) \quad a \cup b = e, a \cup c = e \text{ imply } a \cup bc = e \quad (a, b, c \in L)$$

and

$$(3.6) \quad a_1 a_2 \dots a_r \leq a_1 \cap a_2 \cap \dots \cap a_r \quad (a_i \in L).$$

(See BIRKHOFF [1] or FUCHS [2].)

⁷⁾ An element $q \in S$ ($0 \leq q < s$) is called primary if $ab \leq q$ and $a \leq q$ ($a, b \in S$) imply $b^r \leq q$ and if $ab \leq q$ and $b \leq q$ imply $a^t \leq q$ for suitable positive integers r, t .

We remark that (3. 6) implies that L is negatively ordered.

Let L be a lattice-ordered semigroup with the minimum element 0 and maximum element e which is an identity in L . For every element $s (\in L)$ the interval $[0, s] = S$ (consisting of all elements $x (\in L)$ with $0 \leq x \leq s$) is a lattice-ordered subsemigroup of L .

Lemma 3.1. (cf. STEINFELD [4]). *Let L be a residuated lattice-ordered semigroup with the minimum element 0 and maximum element e which is an identity in L . Let $[0, s] = S$ denote an interval of L . If $p (\in S, p \neq s)$ is a prime element in S then $p:s$ is a prime element in L and*

$$(3. 7) \quad (p:s) \cap s = p,$$

$$(3. 8) \quad p:s = p::s$$

hold.

Furthermore $p:s$ is the only prime element in L whose intersection with s is equal to p . For every $r \in L$, $r \cap s = p$ implies $r \leq p:s$. The prime p of S is a prime element in L too if and only if $p = p:s$ holds.

PROOF. First we show that $p:s$ is a prime element in L . Let m, n be elements of L satisfying $mn \leq p:s$. By the definition of $p:s$ we have

$$ms \cdot ns \leq mns \leq p.$$

As $ms \leq s, ns \leq s$, the prime property of p in S implies $ms \leq p$ or $ns \leq p$. Therefore $m \leq p:s$ or $n \leq p:s$.

$p \leq (p:s) \cap s$ holds trivially, so instead of (3. 7) it suffices to prove $(p:s) \cap s \leq p$. The relations

$$((p:s) \cap s)s \leq (p:s)s \leq p \text{ and } s \not\leq p$$

imply $(p:s) \cap s \leq p$, in fact.

Let r be an element of L such that $r \cap s = p$. This implies $rs \leq r \cap s \leq p$, thus, $r \leq p:s$.

If r is a prime element in L with $r \cap s = p$, then because of

$$(p:s)s \leq p \leq r \text{ and } s \not\leq r$$

the relation $p:s \leq r$ must hold. Thus $r = p:s$.

For the left residual $p::s$ the same statements hold, thus $p:s = p::s$, that is (3. 8) is true.

If $p = p:s$, then p is a prime element in L . If however $p \neq p:s$, then because of $(p:s)s \leq p, p:s \not\leq p$ and $s \not\leq p$ the element p is not prime in L .

For the primary elements an analogous result is true.

Lemma 3. 2. *Let L be a residuated lattice-ordered semigroup with the minimum element 0 and maximum element e which is an identity in L . Let s denote an element in the center of L . If q is a primary element of the interval $[0, s] = S$ such that $s^i \not\leq q$*

for $i=1, 2, \dots$, then $q:s$ is a primary element in L and

$$(3.9) \quad (q:s) \cap s = q,$$

$$(3.10) \quad q:s = q::s$$

hold. $q:s$ is the only primary element in L whose intersection with s is q .

From $r \cap s = q$ ($r \in L$) it follows $r \leq q:s$. A primary element q of S is primary in L too if and only if $q = q:s$.

PROOF. First we show that $q:s$ is primary in L . Let m, n be elements of L such that $mn \leq q:s$. By the definition of $q:s$ we obtain

$$ms \cdot ns \leq mns \leq q.$$

If $n \not\leq q:s$, that is $ns \not\leq q$, the primary property of q implies $(ms)^k \leq q$ for a suitable integer $k \geq 1$. As s commutes with the elements of L we can write $(ms)^k = m^k s^k \leq q$. In the case $k=1$ we get $m \leq q:s$. If $k > 1$, then $m^k s s^{k-1} \leq q$ holds. Hence $s^{k-1} \not\leq q$ implies $m^k s \leq q$, that is $m^k \leq q:s$.

Similarly $mn \leq q:s$ and $m \not\leq q:s$ imply $n^l \leq q:s$ for a suitable integer $l \geq 1$. Thus $q:s$ is primary indeed.

Because s belongs to the center, statement (3.10) is trivial.

As $q \leq (q:s) \cap s$ is always true, we have to prove only $(q:s) \cap s \leq q$. The relations

$$((q:s) \cap s)s \leq (q:s)s \leq q \text{ and } s^i \not\leq q \quad (i=1, 2, \dots)$$

imply $(q:s) \cap s \leq q$.

Let r be an element of L such that $r \cap s = q$. This implies $rs \leq r \cap s \leq q$ and so $r \leq q:s$.

Furthermore if r is primary in L , then from $r \cap s = q$ and $s^i \not\leq q$ it follows $s^i \not\leq r$ ($i=1, 2, \dots$). Hence $(q:s)s \leq q \leq r$ implies $q:s \leq r$, and so $r = q:s$.

If $q = q:s$ holds, then q is a primary element in L . If $q \neq q:s$, then because of $(q:s)s \leq q$, $s^i \not\leq q$ ($i=1, 2, \dots$) and $q:s \not\leq q$, the element q is not primary in L .

§ 4. The mapping $x \rightarrow x:s$

First we shall prove

Lemma 4.1. *Let L be a residuated lattice-ordered semigroup with a minimum element 0 and a maximum element e which is the identity of L . Let s be an element of L satisfying the following conditions*

(α) $s^2 = s$ and for every element $x \in S = [0, s]$ the relation $(x:s)s = s(x:s) = (x:s) \cap s$ holds,

(β) $(0:s) \cup s = e$.

Then

$$(4.1) \quad x \rightarrow x:s \quad (\text{for } x \in S)$$

is a one-to-one mapping from the lattice-ordered subsemigroup $S = [0, s]$ onto the set Q of all right-residuals $x:s$ ($x \in S$) which preserves intersections and products. ⁸⁾

⁸⁾ We remark that condition (β) implies $x \neq x:s$ for all $x \in [0, s]$.

PROOF. As L is negatively ordered, $x \cong (x:s) \cap s$ holds for every $x \in S$. On the other hand, condition (α) implies $(x:s) \cap s = (x:s)s \cong x$. Therefore

$$(4.2) \quad (x:s) \cap s = x \quad (\text{for every } x \in S).$$

The implication

$$(4.3) \quad a \cong b \Rightarrow (a:s) \cong (b:s) \quad (0 \cong a, b \cong s)$$

follows immediately from the definition of right-residuals. Conversely, because of (4.2), the implication

$$(4.4) \quad a:s \cong b:s \Rightarrow a = (a:s) \cap s \cong (b:s) \cap s = b \quad (0 \cong a, b \cong s)$$

holds too. (4.3) and (4.4) imply that (4.1) is a one-to-one mapping from S onto Q .

In view of (a) we get

$$a \cap b \rightarrow (a \cap b):s = (a:s) \cap (b:s) \quad (0 \cong a, b \cong s)$$

and so (4.1) is a homomorphic mapping with respect to the operation \cap .

Now we can verify

$$(4.5) \quad (ab):s = (a:s)(b:s) \quad (0 \cong a, b \cong s).$$

(4.2) and (α) imply

$$(4.6) \quad ab = ((a:s) \cap s)((b:s) \cap s) = (a:s)s(b:s)s = (a:s)(b:s)s^2 = (a:s)(b:s)s.$$

Hence in view of (3.1)

$$(4.7) \quad (a:s)(b:s) \cong (ab):s.$$

On the other hand, $((ab):s)(b:s) \cong (a:s)(b:s)$, therefore

$$(4.8) \quad ((a:s)(b:s))::((ab):s) \cong b:s.$$

Furthermore $((ab):s)s \cong ab \cong (a:s)(b:s)$ implies

$$(4.9) \quad ((a:s)(b:s))::((ab):s) \cong s.$$

From (4.8), (4.9) and (β) we obtain

$$(4.10) \quad ((a:s)(b:s))::((ab):s) \cong (b:s) \cup s = e$$

and hence

$$(4.11) \quad ab:s \cong (a:s)(b:s).$$

(4.7) and (4.11) complete the proof of (4.5) and Lemma 4.1.

We say that in a partially ordered semigroup S the *strict unique prime factorization* holds, if in S conditions (i), (ii), (iii) are fulfilled.

Theorem 4.2. *Let L be a residuated lattice-ordered semigroup with a minimum element 0 and a maximum element e which is the identity of L . Let s be an element of L satisfying the following conditions:*

- (I) the strict unique prime factorization holds in the interval $[0, s] = S$,
- (II) $(0:s) \cup s = e$,
- (III) s is in the center of L .

Then

$$(4.12) \quad x \rightarrow x:s \quad (\text{for } x \in S)$$

is an isomorphic mapping from the lattice-ordered semigroup S onto the set Q of all right-residuals $x:s$ ($x \in S$); thus the strict unique prime factorization holds in Q too.

PROOF. As in S the assumptions (i), (ii), (iii) are fulfilled, we can use the results (A)–(E). From the conditions and (A), (C), it follows that S is a commutative lattice-ordered subsemigroup of L with the identity s . Thus (B), (3.4), (3.5) and (I) imply that every element x ($0 < x < s$) of S can be written uniquely in the form

$$(4.13) \quad x = p_1^{k_1} \dots p_r^{k_r} = p_1^{k_1} \cap \dots \cap p_r^{k_r} \quad (k_i \geq 1)$$

with different prime elements p_1, \dots, p_r of S . In view of (E) the prime powers $p_i^{k_i}$ ($i = 1, 2, \dots, r$) are primary elements in S .

By making use of Lemma 3.2, (E), (a) and (4.13) we obtain $x = p_1^{k_1} \cap \dots \cap p_r^{k_r} = ((p_1^{k_1}:s) \cap s) \cap \dots \cap ((p_r^{k_r}:s) \cap s) = (p_1^{k_1}:s) \cap \dots \cap (p_r^{k_r}:s) \cap s = ((p_1^{k_1} \cap \dots \cap p_r^{k_r}):s) \cap s = (x:s) \cap s$, that is,

$$(4.14) \quad (x:s) \cap s = x \quad (\text{for all } 0 < x < s).$$

Because of (D), 0 is a prime element of S , therefore from Lemma 3.1 it follows $0:s = 0::s$. Hence $s(0:s) = s(0::s) = 0 = (0:s)s$. In view of (a), this and (II) imply

$$(4.15) \quad (0:s) \cap s = (0:s)s = 0.$$

Because of $(s:s) \cap s = s$ one can write instead of (4.14) more generally

$$(4.14') \quad (a:s) \cap s = a \quad (\text{for all } 0 \leq a \leq s).$$

Now we can prove that (I), (II) and (III) imply (α) and (β) .

Let y denote an element $y = a:s \in Q$ ($a \in S$). (4.14'), (III) and (3.6) imply $a = (a:s) \cap s = y \cap s \cong ys = sy = b$. Hence $y \leq b:s$. By making use of (4.14') again we obtain $b = (b:s) \cap s \cong y \cap s = (a:s) \cap s = a$. Thus

$$sy = ys = b = a = y \cap s \quad (y \in Q)$$

holds. Because (A) implies $s^2 = s \cap s = s$, the implication

$$(I), (II) \text{ and } (III) \Rightarrow (\alpha) \text{ and } (\beta)$$

is proved.

In view of Lemma 4.1 we have to show only

$$(4.16) \quad (a \cup b):s = (a:s) \cup (b:s) \quad (a, b \in S).$$

The cases $a=0$ or $b=0$ and $a=s$ or $b=s$, respectively, are trivial. Let us consider the elements a, b ($0 < a, b < s$) satisfying

$$(4.17) \quad \begin{aligned} a &= p_1^{m_1} \dots p_r^{m_r} = p_1^{m_1} \cap \dots \cap p_r^{m_r}, \\ b &= p_1^{n_1} \dots p_r^{n_r} = p_1^{n_1} \cap \dots \cap p_r^{n_r} \end{aligned} \quad (m_i + n_i \geq 1; p_i^0 = s).$$

First we shall prove

$$(4.18) \quad a \cup b = \prod_{i=1}^r p_i^{\min(m_i, n_i)}.$$

(4.17) implies

$$a \cup b = \prod_{i=1}^r p_i^{m_i} \cup \prod_{i=1}^r p_i^{n_i} = \prod_{i=1}^r p_i^{\min(m_i, n_i)} (a' \cup b'),$$

where

$$a' = \prod_{i=1}^r p_i^{m_i - \min(m_i, n_i)} \quad \text{and} \quad b' = \prod_{i=1}^r p_i^{n_i - \min(m_i, n_i)}$$

are elements of S . As a' and b' cannot have common prime factors, because of (B) and (3.5) $a' \cup b' = s$ holds. Thus (4.18) is proved.

By using (4.18) and (4.5) we get

$$(4.19) \quad (a \cup b):s = \left(\prod_{i=1}^r p_i^{\min(m_i, n_i)} \right):s = \prod_{i=1}^r (p_i:s)^{\min(m_i, n_i)}.$$

On the other hand, there results

$$(4.20) \quad (a:s) \cup (b:s) = \prod_{i=1}^r (p_i:s)^{m_i} \cup \prod_{i=1}^r (p_i:s)^{n_i} = \prod_{i=1}^r (p_i:s)^{\min(m_i, n_i)} (A' \cup B')$$

where $A' = \prod_{i=1}^r (p_i:s)^{m_i - \min(m_i, n_i)}$ and $B' = \prod_{i=1}^r (p_i:s)^{n_i - \min(m_i, n_i)}$. By virtue of (II)

this implies as above $A' \cup B' = e$. So statement (4.16) has been verified.

Let us consider an element $x \in S$ ($0 < x < s$) written in the form (4.13). We can write

$$x:s = (p_1^{k_1} \dots p_r^{k_r}):s = (p_1^{k_1}:s) \dots (p_r^{k_r}:s) = (p_1:s)^{k_1} \dots (p_r:s)^{k_r},$$

where because of Lemma 3.1 the elements $p_i:s$ ($i=1, 2, \dots, r$) are different prime elements in L .

Because (4.12) is an isomorphic mapping of S onto Q the properties (i), (ii) and (iii) are fulfilled in Q too.

The proof of Theorem 4.2 is thereby completed.

§ 5. Application to ideal theory

It is known that the set of all ideals of an associative ring is a residuated lattice-ordered semigroup. (See FUCHS [2], Third Part.) Thus we can apply the results of § 4 to the ideals of an associative ring.⁹⁾

Lemma 5. 1. *Let α be an ideal of an associative ring R satisfying the following conditions*

(α') $\alpha^2 = \alpha$ and for every ideal γ of α the relation $(\gamma:\alpha)\alpha = \alpha(\gamma:\alpha) = \alpha \cap (\gamma:\alpha)$ holds,

(β') $(0:\alpha) + \alpha = R$.

Then

$$(5. 1) \quad \gamma \rightarrow \gamma:\alpha \quad (\text{for ideals } \gamma \text{ of } \alpha)$$

is a one-to-one mapping from the lattice-ordered semigroup S of all ideals of α onto the set Q of all right ideal quotients $\gamma:\alpha$ ($\gamma \in S$) which preserves intersections and products.

For the proof it is enough to remark that because of (β') the ideals of α are ideals of R too.

We shall say that *strict unique prime factorization holds* for the ideals of an associative ring A if the following conditions are fulfilled:

(i') for the ideals a, b of A

$a \subset b$ implies $a = bc = db$ for some ideals c, d of A ;

(ii') every ideal γ of A ($0 \subset \gamma \subset A$) may be represented as the product of a finite number of prime ideals of A and two representations of γ can differ only in the order of the factors,

(iii') 0 is a prime ideal of A .

Now we can apply Theorem 4. 2 to the ideals.

Theorem 5. 2. *Let α be an ideal of an associative ring R satisfying the following conditions:*

(I') the strict unique prime factorization holds for the ideals γ of α .

(II') $(0:\alpha) + \alpha = R$,

(III') α commutes with every ideal η of R and $R\eta = \eta R = \eta$ holds.

Then

$$\gamma \rightarrow \gamma:\alpha \quad (\text{for ideals } \gamma \text{ of } \alpha)$$

is an isomorphic mapping from the lattice-ordered semigroup S of all ideals γ of α onto the set Q of all (right) ideal quotients $\gamma:\alpha$ ($\gamma \in S$).

⁹⁾ Naturally it would be possible to extend these results to the ideals of a semigroup or a semiring.

Bibliography

- [1] G. BIRKHOFF, *Lattice Theory*, New York, 1948.
- [2] L. FUCHS, *Partially ordered algebraic systems*, Oxford—London—New York—Paris, 1963.
- [3] L. FUCHS—O. STEINFELD, Principal components and prime factorization in partially ordered semigroups, *Ann. Univ. Sci. Budapestensis, R. Eötvös*, **6** (1963), 103—111.
- [4] O. STEINFELD, On ideal-quotients and prime ideals, *Acta Math. Acad. Sci. Hungar.* **4** (1953), 289—298.
- [5] (E. G. ŠULGEĬFER) Е. Г. Шульге йфер, Разложение на простые множители в структурах с умножением, *Украинский Математический Журнал*, **2** (1950), 100—111.

(Received June 28, 1964.)