数理解析研究所講究録
第 292 巻 1977 年 160-167

ON DIVISOR THEORY IN AN ARCHIMEDIAN LATTICE-ORDERED SEMIGROUP

Dedicated to Emeritus Professor Mchio Nagumo on his 70th birthday

KENTARO MURATA and KUMIE SHIRAI

The main purpose of this note is to consider a divisor theory of lattice-ordered semigroups (abbr. l-semigroups), and to show that an l-semigroup S is Artinian if and only if the cone of S has the divisor theory.

1. Introduction. Let L be an l-semigroup (not necessarily commutative), and let Σ be any multiplicatively closed subset of L such that for each element $a \in L$ there is an element $x \in \Sigma$ with $x \leqslant a$. Let Δ be a commutative l-semigroup with unity quantity ε such that (1) ε is the greatest element of Δ, (2) Δ contains primes and (3) each element of Δ is uniquely decomposed into primes apart from its commutativity.

An l-semigroup epimorphism f: $a \longmapsto f(a)$ from L to Δ is called a right divisor theory of L if it satisfies the following conditions:

(1°) If for x, $y \in \Sigma$, f(x) is divisible by f(y) in Δ, then x is divisible by y on the right-hand side in L, i.e. if there is an element $\gamma \in \Delta$ such that $f(x) = \gamma f(y)$, then there is an element c $\in$ L such that x = cy.

(2°) $\Sigma(\alpha) = \Sigma(\beta)$ implies $\alpha = \beta$, where $\Sigma(\alpha)$ is the set of the elements of $x \in \Sigma$ such that f(x) is divisible by $\alpha \in \Sigma$.

A left divisor theory is defined analogously.

A main purpose of this note is to prove the following

THEOREM. Let S be a conditionally complete lattice-ordered semigroup (abbr. cl-semigroup) with unity quantity e. Assume that the cone $C = \{a \in S;\ a \leqslant e\}$ satisfies the ascending chain condition in the sense of quasi-equality (cf. DEFINITION 3) and has a join-generator system Σ such that (a) Σ is closed under multiplication (b) every element of Σ is invertible in S and (c) every element $s \in S$ is written as $s = ax^{-1} = y^{-1}b$ where $a, b \in C$ and $x, y \in \Sigma$. Then the following conditions are equivalent:

(1_r) C has a right divisor theory.

(1_l) C has a left divisor theory.

(2) C is archimedian.

(3) S is Artinian.

Let G be the group generated by Σ in S. Then S is a quotient semigroup of C by $G \wedge C$ in the sense of [2], where $\wedge$ will denote the intersection. The cone C of S is said to be archimedian, if whenever $z^n x \leq e$ for $n = 1, 2, \ldots (x \in \Sigma,\ z \in G)$ imply $z \leq e$. Since $z^n x \leq e \Longleftrightarrow z^n \leq x \Longleftrightarrow xz^n \leq e$, there needs no distinction of "right" and "left" for archimedesness. An Artinian l-semigroup is considered in the next section.

2. Artinian l-semigroups. Let S be a cl- semigroup whose cone C has a join-generator system Σ with the conditions (a), (b) and (c) in the theorem mentioned above.

LEMMA 1. The group G generated by Σ in S is a join-generator system of S.

Proof. The any element $a \in S$ there is an element $x \in \Sigma$ such that $ax \in C$. That $ax = \sup N$ for a subset N of Σ. Hence we have $a = (\sup N)x^{-1} = \sup(Nx^{-1})$ where $Nx^{-1} = \{ux^{-1};\ u \in N\}$. This means that G is a join-generator system of S.

LEMMA 2. For any two elements a and b of S, $X(a,b) = \{u \in G;\ ub \leq a\}$ is non-void. The set $F(a,b) = \{s \in S;\ sb \leq a\}$ has an upper bound, and $\sup F(a,b) = \sup X(a,b)$.

Proof. Take an element $x \in G$ such that $x \leq a$, and take $y \in \Sigma$ such that $yb \leq e$. Then putting $u = xy$ we have $ub \leq a$. It is easy to see that av^{-1} is an upper bound of F(a,b) for any $v \in G$ with $v \leq b$. Let $s = cx^{-1}$ be any element of F(a,b) where $c \in C$, $x \in \Sigma$; and put $J = \{z \in \Sigma\ ;\ z \leq c\}$. Then since $zx^{-1}b \leq cx^{-1}b = sb \leq a$ and zx^{-1}

$\in G$, we have $s = cx^{-1} = (\sup J)x^{-1} = \sup(Jx^{-1}) \leqslant \sup X(a,b)$. Hence $\sup F(a,b) \leqslant \sup X(a,b)$. The converse inequality is evident.

DEFINITION 1. $a/b = \sup F(a,b)$ is called a right residual of a by b.

LEMMA 3. If $a \in S$ and $u \in G$, then $a/u = au^{-1}$. In particular $e/u = u^{-1}$.

Proof. There is a subset A of G such that $a/u = \sup A$. Then for any $z \in A$ we have $zu \leqslant a$, $z \leqslant au^{-1}$, $a/u \leqslant au^{-1}$. The converse inequality is evident.

The residual has thr following properties:

(1) $a/(bc) = (a/c)/b$.

(2) $(\inf A)/b = \inf \{a/b;\ a \in A\}$, if either inf A or the right-hand side exists.

(3) $a/(\sup B) = \inf \{a/b;\ b \in B\}$, if either sup B or the right-hand side exists.

It is clear that $U(a) = \{u \in G;\ a \leqslant u\}$ is non-void for any $a \in S$.

DEFINITION 2. $a^* = \inf U(a)$ is called a closure of a. a is said to be closed if $a^* = a$.

The following properties are immediate:

(4) $a \leqslant a^*$.

(5) $a \leqslant b$ implies $a^* \leqslant b^*$.

LEMMA 4. If a is closed, then a/b is closed for any $b \in S$.

Proof. Let $b = \sup B$ for a subset B of G. Then since $a = \inf U(a)$ we have $a/b = \inf U(a)/\sup B = \inf \{u/v;\ u \in U(a),\ v \in B\} = \inf \{uv^{-1}\} \geqslant \inf U(a/b) \geqslant a/b$ (by (2), (3) and LEMMA 3). Hence we obtain $a/b = \inf U(a/b)$ as desired.

We have the following properties:

(6) $a^* = e/(e/a)$.

(7) $e/a = e/a^*$.

(8) $a^{**} = a^*$.

(9) $a^*b^* \leqslant (a^*b^*)^* = (ab)^*$.

(10) $(\sup A)^* = \sup(A^*)^*$, if either sup A or sup A^* exists, where $A^* = \{a^*;\ a \in A\}$. In particular $(a \cup b)^* = (a^* \cup b^*)^*$.

(11) $(\inf A^*)^* = \inf A^*$, if $\inf A^*$ exists. In particular $(a^* \cap b^*)^* = a^* \cap b^*$.

We define an operation "$\circ$" by $a^* \circ b^* = (ab)^*$.

(12) $(\sup A)^* \circ b^* = (\sup(A^* \circ b^*))^*$, $b^* \circ (\sup A)^* = (\sup(b^* \circ A^*))^*$, if sup A exists.

Proof. Ad (6): For any $u \in U(a)$ we have $e/a \geqslant e/u = u^{-1}$, $e/(e/a) \leqslant e/u^{-1} = u$. Hence $e/(e/a) \leqslant \inf U(a) = a^*$. Conversely since $a = \sup A$ for a suitable subset A of G, we have $x^{-1} = e/x \geqslant e/a$ for any $x \in A$. Hence $x = e/x^{-1} = e/(e/x) \leqslant e/(e/a)$ and hence $a = \sup A \leqslant e/(e/a)$. Thus we obtain $a^* \leqslant e/(e/a)$ by LEMMA 4 and (5). Ad (7): By (6) we have $e/a^* = e/(e/(e/a)) = (e/a)^* \geqslant e/a$. The converse inequality is evident. (8) is immediate by (6) and (7). Ad (9): Since $e/(ab)^* = e/(ab) = (e/b)/a = (e/b^*)/a = e/(ab^*)$, we have $(ab)^* = (ab)^{**} = e/(e/(ab)^*) = e/(e/(ab^*)) = (ab^*)^*$. Now we can define left residuals and argue symmetrically as above. If $u \in G$ then $ua \leqslant e \Longleftrightarrow a \leqslant u^{-1} \Longleftrightarrow au \leqslant e$. Hence we have $e/a = a\backslash e$, the left residual of e by a. This yield $(ab)^* = (a^*b)^*$, and the identity of (9) holds. (10), (11) and (12) are checked easily.

DEFINITION 3. Two elements $a, b \in S$ are said to be quasi-equal, if $a^* = b^*$. In symbol: $a \sim b$.

(13) $a \sim b$ implies $e/a = e/b$, and conversely.

(14) $a^* \sim a$.

(15) $a^* \sim c$ implies $a^* \geqslant c$.

The above three are immediate. Put $S^* = \{s^*;\ s \in S\}$, and define $a^* \vee b^* = (a^* \cup b^*)^* = (a \cup b)^*$, $a^* \wedge b^* = (a^* \cap b^*)^* = a^* \cap b^*$ and $a^* \mathbin{\bar{\wedge}} b^* = (a \cap b)^*$. Then by using (8) $\sim$ (12) we can show that $(S^*, \circ, \vee, \wedge)$ is cl-semigroup, and similarly for $(S^*, \circ, \vee, \mathbin{\bar{\wedge}})$.

DEFINITION 4. If the semlgroup $(S^*, \circ)$ is a group, S is called an Artinian l-semigroup [3].

We can show that if S is Artinian, $(S^*, \circ, \vee, \wedge)$ is an cl-group. Hence $(S^*, \circ)$ is a commutative group, and $(S^*, \vee, \wedge)$ is a distributive lattice. In this case e is maximally integral (cf. p, 12 in [1]). For it can be shown that C is archimedian if and only if the above two meet operations coinside (cf. pp 13-14 in [1]).

3. Proof of THEOREM. $(1_r) \Rightarrow (2)$; Let (C, Δ, f) be a given divisor theory of the cone C of S, and let H be the restricted direct product of infinite cyclic groups, each of which is generated by a prime divisor in Δ. Then it can be show that f: $C \longrightarrow \Delta$ extends to a map f: $S \longrightarrow H$ by f: $cz^{-1} \longmapsto f(c)f(z)^{-1}$ where $cz^{-1} \in S$, $c \in C$, $z \in \Sigma$. $f(cz^{-1})$ does not depend on the choice of the fractional representations.

Suppose that $xu^n \leqslant e$, $x \in \Sigma$, $u \in G$ for $n = 1,2,\ldots$, and let $f(x) = \pi_1^{\lambda_1} \ldots \pi_r^{\lambda_r} . \pi_{r+1}^{\lambda_{r+1}} \ldots \pi_m^{\lambda_m} (\lambda_i > 0)$, $f(u) = \pi_1^{\mu_1} \ldots \pi_r^{\mu_r} . \rho_{r+1}^{\mu_{r+1}} \ldots \rho_t^{\mu_t}$ ($\mu_i > 0$ or < 0) be the prime factorizations in H, where $\pi_1, \ldots, \pi_r$ are the common prime divisors. The since $f(xc^n) \in \Delta$ we have $\lambda_i + n\mu_i \geqslant 0$ $(i = 1,\ldots, r)$ and $n\mu_j \geqslant 0$ $(j = r+1,\ldots, t)$ for all positive integers n. This implies $\mu_i > 0$ for $i = 1,\ldots, r,\ldots,t$. Hence we have $f(u) \leqslant f(e)$, $f(u) \in \Delta$. Since u is written as $u = yz^{-1}$ for some $y, z \in \Sigma$, we have $y = uz$, $f(y) = f(u)f(z)$. By using the condition (1°) we can choose an element $c \in C$ such that $y = cz$. Thus we obtain $u = c \leqslant e$ as desired.

$(2) \Rightarrow (3)$: Let a be an arbitrary element of S^*, and let $b = az \in C$, $z \in \Sigma$. Then since $e/b \geqslant e$, we have $b^* = e/(e/b) \leqslant e/e = e$ Hence we obtain $a \circ z = b^* \in C^* = \{c^*; c \in C\} = S^* \wedge C$. Thus in order to prove that $(S^*, \circ)$ is a group, it is sufficient to show that every element of C^* is invertible with respect to the operation "$\circ$". Let $a \in C^*$, and let $u \in G$ be an element such that $a(e/a) \leqslant u$. Then $u^{-1}a(e/a) \leqslant e$, $u^{-1}a \leqslant e/(e/a) = a^* = a$. Hence we have $a \leqslant ua$, $a \leqslant u^n a$ for $n = 1,2,\ldots$. If we take an element $x \in \Sigma$ such that $x \leqslant a$, then $x \leqslant u^n a$. Hence $u^{-n}x \leqslant a \leqslant e$ for $n = 1,2,\ldots$. This implies $u^{-1} \leqslant e$, $e \leqslant u$. Thus we get $e \leqslant \inf U(a(e/a)) = (a(e/a))^* \leqslant e^* = e$. We obtain therefore $a \circ (e/a) = e$.

$(3) \Rightarrow (1_r)$: Suppose that S is Artinian. Then $(S^*, \circ, \vee, \curlywedge)$ is cl-group and so $(S^*, \circ, \vee, \curlywedge)$ is commutative l- group. For an element p^* of S^*, p^* is irreducible if and only if p^* is prime. Since C satisfies the ascending chain condition in the sense of quasi-equality, each element of C* is uniquely decomposed into primes apart from its commutativity. Now we show that $(C, C^*, *)$ is a divisor theory of C. Suppose that $x^* = a^* \circ y^*$ for $x, y \in \Sigma$ and $a^* \in C^*$. Then since $x^* = x$, $y^* = y$ we have $x = a^* \circ y$, $xy^{-1} = x \circ y^{-1} = a^*$, $x = a^* y$. This shows that the condition (1°) holds for C. Let $\Sigma(a^*)$ be the set of the elements $x \in \Sigma$ which are divisible by a^*, i.e., $x \leqslant a^*$. If $\Sigma(a^*) = \Sigma(b^*)$ we obtain $a^* = \sup \Sigma(a^*) = \sup \Sigma(b^*) = b^*$. That is, the condition (2°) holds for C.

Similarly we can show the implications: $(1_1) \Longrightarrow (2) \Longrightarrow (3) \Longrightarrow (1_1)$.

4. Uniqueness for divisor theory. Let (L, Δ, f) be a (right) divisor theory of L. An element α is called a principal divisor, if there is an element $x \in \Sigma$ such that $\alpha = f(x)$. It is easily shown that $\Sigma(\alpha)$ is not vacuous for each divisor α.

UNIQUENESS THEOREM. For any two right divisor theories (L, Δ, f) and (L, Γ, g) of L there exists an isomorphism φ from Δ to Γ, under which the principal divisors in Δ and in Γ correspond.

Proof. We shall show first that for each prime $\pi \in \Delta$ there is a prime $\rho \in \Gamma$ such that $\Sigma(\rho) \subseteq \Sigma(\pi)$. For, if not, there is a prime $\pi \in \Delta$ for which there is no prime $\rho \in \Gamma$ with $\Sigma(\rho) \subseteq \Sigma(\pi)$. Take an element $x \in \Sigma(\pi)$, and let $g(x) = \rho_1^{k_1} \dots \rho_n^{k_n}$ be the prime factorization of $g(x)$ in Γ. Then since each $\Sigma(\rho_i)$ is not contained in $\Sigma(\pi)$, we can choose x_i which is contained in $\Sigma(\rho_i)$ and not contained in $\Sigma(\pi)$. Hence there are $\gamma_i \in \Gamma$ such that $g(x_i) = \rho_i \gamma_i$ for $i = 1, \dots, n$. Then we have $g(x_1^{k_1} \dots x_n^{k_n}) = g(x)\gamma$, where $\gamma = \gamma_1^{k_1} \dots \gamma_n^{k_n}$. Hence by (1°) $x_1^{k_1} \dots x_n^{k_n}$ is divisible by x on the right-hand side in L, hence $f(x_1^{k_1} \dots x_n^{k_n})$ is divisible by $f(x)$, and hence $f(x_1)^{k_1} \dots f(x_n)^{k_n}$ is divisible by π. Therefore $\Sigma(\pi)$ contains some x_i, which is a contradiction. Symmetrically for the prime $\rho \in \Gamma$, there is a prime $\pi' \in \Delta$ such that $\Sigma(\pi') \subseteq \Sigma(\rho)$.

Next we show that $\pi = \pi'$. Since Δ is a semigroup with the unique factorization theorem, we have $\pi\pi' \neq \pi'$. By using (2°) we can see that $\Sigma(\pi\pi')$ is strictly contained in $\Sigma(\pi')$ and hence in $\Sigma(\pi)$. Then we can take an element $y \in \Sigma$ such that f(y) is divisible by π' and not divisible by $\pi\pi'$. If $\pi \neq \pi'$, f(y) is divisible by $\pi\pi'$, since f(y) is divisible by π. This is imposible. We have therefore $\pi = \pi'$, $\Sigma(\pi) = \Sigma(\rho)$. By using (2°) we can see easily that for each prime $\pi \in \Delta$, the prime $\rho \in \Gamma$ with $\Sigma(\rho) = \Sigma(\pi)$ is uniquely determined. Hence we can define the map $\varphi : \pi \longmapsto \rho = \varphi(\pi)$. It is evident that φ extends uniquely to an isomorphism from Δ to Γ.

In order to prove the last part of the theorem we suppose that f(x) is exactly divisible by π^k. Since $\Sigma(\pi^2)$ is, by (2°), strictly contained in $\Sigma(\pi)$, we can choose an element x_0 such that $f(x_0) = \pi\alpha$ and α is not divisible by π. Hence again by (2°) we can take an element u which is contained in $\Sigma(\alpha^k)$ and not in $\Sigma(\pi\alpha^k)$. Then of course g(u) is not divisible by $\varphi(\pi)$. Since $f(xu) = f(x)f(u) = \pi^k\alpha^k\beta = (\pi\alpha)^k\beta = f(x_0)^k\beta = f(x_0^k)\beta$ for some $\beta \in \Delta$, we get $xu = bx_0^k$ for some $b \in L$. Hence we have $g(x)g(u) = g(x_0)^k g(b)$. On the other hand since $g(x_0)$ is divisible by $\varphi(\pi)$ and g(u) is not divisible by $\varphi(\pi)$, g(x) is divisible by $\varphi(\pi)^k$. By a symmetrical argument we can show that f(x) is exactly divisible by π^k if and only if g(x) is exactly divisible by $\varphi(\pi)^k$. This completes the proof.

COROLLARY 1. Suppose that S is an Artinian l-semigroup, and C the cone of S. Then the divisor theory (C,C*,*) is uniquely determined apart from isomorphism.

COROLLARY 2. S and C are as same as in Corollary 1. Assume that the ascending chain condition holds for elements of C, and any prime element is maximal (in C). Then S forms a commutative l-group.

Proof. It can be proved that quasi-equality implies equality, which is similar to the proof of Theorem 2.6 in [1].

REFERENCES

[1] K.Asano and K.Murata, Arithmetical ideal yheory in semigroups, Journal Institute of Polytec., Osaka City Univ. 4 (1953), 9-33.

[2] K.Murata, On the quotient semigroup of a noncommutative semigroup, Osaka Math. J.2 (1950), 1-5.