Mh. Math. 119, 217–221 (1995)

Monatshefte für
Mathematik
© Springer-Verlag 1995
Printed in Austria

A Note on Subsemigroups with Divisor Theory

By

Krzysztof Kuzara, Poznań

(Received 25 January 1993; in revised form 13 December 1993)

Abstract. The paper is concerned with the problem of describing those subsemigroups of a semigroup with divisor theory which have a divisor theory as well.

1. Introduction and Statement of Results

In this paper, a semigroup is a commutative cancellative multiplicative semigroup with identity, usually denoted by 1. For the readers convenience we list below some basic facts on semigroups with divisor theory. For more details we refer to the recent paper by F. HALTER-KOCH [4]. Let S be a semigroup, we use here the standard notation used in a divisor theory. In particular, $a|b$ $(a, b \in S)$ means that a divides b, and $a^k \| b$ is equivalent to $a^k | b$ and $a^{k+1} \nmid b$. Moreover, $b = \gcd(B)$ means that b is the greatest common divisor of $B \subset S$. We denote by $Ir(S)$ the set of irreducible elements of S and by $P(S)$ the set of prime elements of S.

Let D be a free abelian semigroup. Then $P(D) = Ir(D)$ is the uniquely determined basis of D. Every element $d \in D$ has a unique representation

$$d = \prod_{p \in P(D)} p^{v_p(d)}$$

with $v_p(d) \in \mathbb{N}_0$, $v_p(d) = 0$ for almost all $p \in P(D)$.

A *divisor theory* for a semigroup S is a semigroup homomorphism $\partial: S \to D$ from S into a free abelian semigroup D with the following properties:

(D1) If $a, b \in S$ and $\partial a | \partial b$ (in D), then $a|b$ (in S).

1991 Mathematics Subject Classification: 20M14, 11R27.

(D2) For every $d \in D$ there exists $s_1, \ldots, s_n \in S$ with
$d = \gcd(\partial s_1, \ldots, \partial s_n)$.

It is easy to see (cf. [6]) that condition (D2) in the definition is equivalent to

(D2′) For every $p \in P(D)$ there exist $s_1, \ldots, s_n \in S$ with
$p = \gcd(\partial s_1, \ldots, \partial s_n)$.

Let $\partial : S \to D$ be a divisor theory for a semigroup S. For $d_1, d_2 \in D$ we write $d_1 \sim_\partial d_2$ when there exist $s_1, s_2 \in S$ with $d_1 \partial s_1 = d_2 \partial s_2$. Of course $\sim_\partial$ is an equivalence relation. We denote by $[d]_\partial$ the equivalence class of d. It can easily be seen that the quotient set $D/\sim_\partial$ with the multiplication defined by $[d_1]_\partial [d_2]_\partial = [d_1 d_2]_\partial$ is an abelian group with identity $1 = \partial S$. We call $Cl(S) = D/\sim_\partial$ the *divisor class group of* S. For $X \in Cl(S)$ and $d \in D$ we write

$$\Omega_X(d) = \sum_{p \in P(D) \cap X,\, p^k \| d} k.$$

The most classical examples of semigroups with divisor theory are multiplicative semigroups of Dedekind rings and so-called Hilbert's semigroups (cf. [4]). Let us observe that a subsemigroup of a semigroup with a divisor theory does not need to have a divisor theory. Indeed, let $\Gamma_2 = \{1\} \cup \{2n : n \in \mathbb{N}\}$. Then Γ_2 is a subsemigroup of the multiplicative semigroup $\mathbb{N}$ and it is easy to see Γ_2 has no divisor theory [4, Beispiel 3]. Hence we have the following:

Problem. Given a semigroup S with a divisor theory, describe the set of all subsemigroups $S' \subset S$ having a divisor theory as well.

Our principal goal is to give a partial solution of this problem. We proceed as follows. Let $\partial : S \to D$ be a divisor theory and $\mathscr{A} = (m_X)_{X \in Cl(S)}$ be a family of positive integers. Then the set

$$S_{\mathscr{A}} = \{s \in S : \Omega_X(\partial s) \equiv 0 \,(\operatorname{mod} m_X) \text{ for all } X \in Cl(S)\}$$

is a subsemigroup of S. Moreover, let $\partial_{\mathscr{A}} = \partial|_{S_{\mathscr{A}}} : S_{\mathscr{A}} \to D$ be the restriction of ∂ to $S_{\mathscr{A}}$. We shall explain in which circumstances the operation $(S, \partial) \mapsto (S_{\mathscr{A}}, \partial_{\mathscr{A}})$ leads to a subsemigroup with a divisor theory. It turns out that for a large class of families $\mathscr{A}$ this is really the case. Moreover, we explain the basic connections between divisor class groups of S and $S_{\mathscr{A}}$.

Theorem. *Let* $\partial : S \to D$ *be a divisor theory,* $P = P(D)$, $B = \{X \in Cl(S) : X \cap P(D) \neq \varnothing\}$, $C = \{X \in Cl(S)\colon \operatorname{card}(X \cap P(D)) > 1\}$.

Let $\mathscr{A} = (m_X)_{X \in Cl(S)}$ *be a family of positive integers,*

$$S_{\mathscr{A}} = \{s \in S: \Omega_X(\partial s) \equiv 0 \,(\operatorname{mod} m_X) \text{ for all } X \in Cl(S)\}$$

and

$\partial_{\mathscr{A}} = \partial|_{S_{\mathscr{A}}}: S_{\mathscr{A}} \to D$ *be the restriction of* ∂ *to* $S_{\mathscr{A}}$.

i) *The mapping* $\partial_{\mathscr{A}}$ *is a divisor theory for* $S_{\mathscr{A}}$ *if and only if the following conditions are satisfied:*

(A1) $m_X = 1$ *for all* $X \in B \backslash C$.

(A2) $X^{-1} \in [\{Y^{m_Y}: Y \in B, Y \neq X\}]$ *for all* $X \in B \backslash C$.

(*where* $[A]$ *denotes the semigroup generated by* A)

ii) *Let* $\partial_{\mathscr{A}}: S_{\mathscr{A}} \to D$ *be a divisor theory for* $S_{\mathscr{A}}$. *Then there is a group monomorphism*

$$\Phi_{\mathscr{A}}: Cl(S_{\mathscr{A}}) \to Cl(S) \times \prod_{x \in B} \mathbb{Z}/(m_X)$$

such that

$$\Phi_{\mathscr{A}}([d]_{\partial_{\mathscr{A}}}) = ([d]_{\partial}, (\Omega_X(d) (\operatorname{mod} m_X))_{X \in B}).$$

iii) *Suppose that* $Cl(S)$ *is finite,* $Cl(S) = h$, $m_X = 1$ *for all* $X \in B \backslash C$ *and* $\gcd(m_X, h) = 1$ *for all* $X \in C$. *Then* $\partial_{\mathscr{A}}$ *is a divisor theory and* $\Phi_{\mathscr{A}}$ *is an isomorphism.*

Our theorem describes a general method for construction of semigroups with a given divisor class group. As an example we give a simple proof of the following result.

Corollary. *For every finite abelian group G there exists a subsemigroup S of the multiplicative semigroup* $\mathbb{N}$ *having the divisor class group isomorphic to G.*

Indeed, let $m_1, \ldots, m_k \in \mathbb{N}$ and $S_i = \{n \in \mathbb{N}: \Omega(n) \equiv 0 \,(\operatorname{mod} m_i)\}$ for $i \in \{1, \ldots, k\}$. Then, according to our theorem $S_1 \times \cdots \times S_k$ is a subsemigroup of $\mathbb{N}^k \cong \mathbb{N}$ with the divisor class group isomorphic to $\prod_{i=1}^k \mathbb{Z}/(m_i)$, corollary therefore follows. For other realization theorem see SKULA [6], GEROLDINGER and KACZOROWSKI [2], and LETTL [5].

Acknowledgement. The author wishes to thank the anonymous referee for his valuable remarks concerning the first version of this paper.

2. Proof of the Theorem

i) The mapping $\partial_{\mathscr{A}}$ is obviously a semigroup homomorphism and of course satisfies (D1).

Suppose first, that $\partial_{\mathscr{A}}$ is a divisor theory, and let $X\in B\backslash C$ be given. Then $X\cap P=\{p\}$, and from (D2′) there exists some $s\in S$ such that $v_p(\partial s)=1$. Since $v_p(\partial s)=\Omega_X(\partial s)\equiv 0 \pmod{m_X}$, we conclude $m_X=1$. Using (D2′) again we have that there exist $p_1,\ldots,p_n\in P$ with $pp_1\cdot\cdots\cdot p_n\in\partial S_{\mathscr{A}}$ and $p\notin\{p_1,\ldots,p_n\}$. Hence

$$1=\partial S_{\mathscr{A}}=X\cdot Y_1^{n_1}\cdot\cdots\cdot Y_r^{n_r}\quad\text{where } n_i\equiv 0 \pmod{m_{Y_i}}\quad\text{for all } 1\leqslant i\leqslant r$$

and consequently $X^{-1}\in[\{Y^{m_Y}:Y\in B,\ Y\neq X\}]$ as required in (A2).

Now we prove that the conditions (A1) and (A2) are sufficient. Suppose that $m_X=1$ and $X^{-1}\in[\{Y^{m_Y}:Y\in B,\ Y\neq X\}]$ for all $X\in B\backslash C$, and let $p\in P$ be given. We must produce $s_1,\ldots,s_n\in S$ with $p=\gcd(\partial s_1,\ldots,\partial s_n)$.

Case 1: Suppose $X=[p]_\partial\in C$. Then there exists some $q\in P\cap X$ such $p\neq q$. Since $Cl(S)=[B]$, there exist $Y_1,\ldots,Y_r\in B$ such that $X^{-1}=Y_1\cdot\cdots\cdot Y_r$. Let $q_i\in Y_i\cap P$ be arbitrary and $a,a_1,\ldots,a_r\in D$ such that $pa\in\partial S$ and $q\nmid a$, $pa_i\in\partial S$ and $q_i\nmid a_i$ for all $1\leqslant i\leqslant r$. Then there exist some $m\in\mathbb{N}$ such that $(pq_1\cdot\cdots\cdot q_r)^m\in\partial S_{\mathscr{A}}$, $(pa)^m\in\partial S_{\mathscr{A}}$ and $(pa_i)^m\in\partial S_{\mathscr{A}}$ for all $1\leqslant i\leqslant r$. Then we also have $pq^{m-1}q_1^m\cdot\cdots\cdot q_r^m\in\partial S_{\mathscr{A}}$ and

$$p=\gcd(pq^{m-1}q_1^m\cdot\cdots\cdot q_r^m,(pa)^m,(pa_1)^m,\ldots,(pa_r)^m).$$

Case 2: Suppose, $X=[p]_\partial\in B\backslash C$. By assumption, there exist $Y_1,\ldots,Y_r\in B\backslash\{X\}$ such that

$$X^{-1}=Y_1^{n_1}\cdot\cdots\cdot Y_r^{n_r}\quad\text{where } n_i\equiv 0 \pmod{m_{Y_i}}\quad\text{for all } 1\leqslant i\leqslant r.$$

Let $q_i\in Y_i\cap P$ be arbitrary and $a_i\in D$ such that $pa_i\in\partial S$ and $q_i\nmid a_i$ for all $1\leqslant i\leqslant r$. Then $pq_1^{n_1}\cdot\cdots\cdot q_r^{n_r}\in\partial S_{\mathscr{A}}$ and there exist some $m\in\mathbb{N}$ such that $(pa_i)^m\in\partial S_{\mathscr{A}}$ for all $1\leqslant i\leqslant r$. Then we have

$$p=\gcd(pq_1^{n_1}\cdot\cdots\cdot q_r^{n_r},(pa_1)^m,\ldots,(pa_r)^m).$$

ii) We define the mapping $\Phi: D\to Cl(S)\times\prod_{X\in B}\mathbb{Z}/(m_X)$,

$$\Phi(d)=([d]_\partial,(\Omega_X(d) \pmod{m_X}))_{X\in B}).$$

The mapping Φ is obviously a semigroup homomorphism. It easy to see that $d_1\sim_{\partial_{\mathscr{A}}}d_2$ implies $d_1\sim_\partial d_2$ and $\Omega_X(d_1)\equiv\Omega_X(d_2) \pmod{m_X}$ for all $X\in Cl(S)$.

Hence Φ induces the group homomorphism $\Phi_{\mathscr{A}}: Cl(S_{\mathscr{A}}) \to Cl(S) \times \times \prod_{X\in B} \mathbb{Z}/(m_X)$, $\Phi_{\mathscr{A}}([d]_{\partial_{\mathscr{A}}}) = \Phi(d)$. Its kernel is trivial and $\Phi_{\mathscr{A}}$ is an injection.

iii) If $\gcd(m_X, h) = 1$ for all $X \in B$, then we find $l_X \in \mathbb{N}$ with $m_X \cdot l_X \equiv 1 \pmod{h}$. Hence $X = X^{l_X m_X}$ and $[\{Y^{m_Y}: Y \in B, Y \neq X\}] = = [\{Y: Y \in B, Y \neq X\}]$ for all $X \in B$. Since ∂ is a divisor theory, hence applying i) to $\mathscr{A}' = (m'_X)_{X \in Cl(S)}$ with $m'_X = 1$ for all $X \in B$, we have that $X^{-1} \in [\{Y: Y \in B, Y \neq X\}]$ for all $X \in B \setminus C$. Hence $\partial_{\mathscr{A}}$ is a divisor theory. In order to prove that $\Phi_{\mathscr{A}}$ is surjective, let $Y \in Cl(S)$ and a family $(\varepsilon_X)_{X\in B} \in \mathbb{N}_0^B$ be given. Since $Cl(S) = [B]$, also we have

$$Y = \prod_{X \in B} X^{e_X}, \quad \text{where } e_X \in \mathbb{N}_0.$$

By the Chinese remainder theorem, for all $X \in B$ we can find $r_X \in \mathbb{N}$ such that

$$r_X \equiv \varepsilon_X \pmod{m_X}, \qquad r_X \equiv e_X \pmod{h}.$$

Now we set $d = \prod_{X\in B} \prod_{i=1}^{r_X} p_{X,i}$ where $p_{X,1}, \ldots, p_{X,r_X} \in X \cap P$ (not necessarily different). Then it is easy to see that

$$\Phi_{\mathscr{A}}([d]_{\partial})_{\mathscr{A}} = (Y, (\varepsilon_X \pmod{m_X}))_{X\in B}).$$

This completes the proof.

References

[1] Clifford, A. H.: Arithmetic and ideal theory of commutative semigroups. Ann. of Math. **39**, 594–610 (1938).

[2] Geroldinger, A., Kaczorowski, J.: Analytic and arithmatic theory of semigroups with divisor theory. Seminaire de théorie des nombres de Bordeaux **4**, 199–238 (1992).

[3] Gundlach, K. B.: Einführung in die Zahlentheorie. Mannheim: B.I.

[4] Halter-Koch, F.: Halbgruppen mit Divisorentheorie. Expo. Math. **8**, 27–66 (1990)

[5] Lettl, G.: Subsemigroups of finitely generated groups with divisor theory. Mh. Math. **106**, 205–210 (1988).

[6] Skula, L.: Divisorentheorie einer Halbgruppe. Math. Z. **114**, 113–120 (1970).

K. Kuzara
Faculty of Mathematics and Computer Science
Adam Mickiewicz University
UL. Matejki 48/49
PL-60-769 Poznań, Poland.