Bibliography

[1] P. Erdös and R. L. Graham, *On a linear diophantine problem of Frobenius*, Acta Arith. 21 (1972), pp. 399–408.

[2] G. H. Hardy and E. M. Wright, *The Theory of Numbers*, 4th ed., Oxford University Press, 1960.

[3] B. R. Heap and M. S. Lynn, *A graph theoretic algorithm for the solution of a linear diophantine equation*, Numerische Math. 6 (1964), pp. 346–354.

[4] S. M. Johnson, *A linear diophantine problem*, Canad. J. Math. 12 (1960), pp. 390–398.

[5] N. S. Mendelsohn, *A linear diophantine equation with applications to nonnegative matrices*, Ann. N. Y. Acad. Sci. 175. art. 1 (1970), pp. 287–294.

Received on 23. 1. 1975 (666)

ACTA ARITHMETICA
XXXI (1976)

On c-semigroups

by

LADISLAV SKULA (Brno)

A semigroup with a divisor theory in which all factorizations into irreducibles of a given element have the same length is called a *c-semigroup*.

In his paper [1] L. Carlitz has proved that *the multiplicative semigroup of the ring of all algebraic integers of a number field is a c-semigroup if and only if that ring has class number* $\leqslant 2$.

In Narkiewicz's book [3] the following problem (no. 29) is posed: *Characterize Dedekind domains in which all factorizations into irreducibles of a given element have the same length.*

In this paper it is shown that the property *to be a c-semigroup* depends on the so-called *c-characteristic* of a semigroup (with a divisor theory) that is equal to the pair consisting of its divisor class group and of the image of the canonical mapping of all prime divisors into that group (Proposition 2.3).

From Claborn's Realization Theorem ([2], Theorem 15.18) it follows that *for every pair consisting of a commutative group and its any strong systems of generators there exists a Dedekind domain for which that pair is its c-characteristic* (Theorem 2.4).

For a subset of a commutative group the notion of *c-set* is introduced by means of the properties of that group only. It is shown (Proposition 2.3, Theorems 2.6, 2.7) that *the c-characteristics of c-semigroups are just the commutative groups and their strong systems of generators which are c-sets of those groups.*

In Section 3 the c-sets of elements of finite orders of a commutative group are characterized by Theorem 3.1, from which the characterization of all c-sets of the cyclic group of order p^n (p a prime, n a positive integer) is derived (Proposition 3.4). An analogous characterization of all c-sets of a finite cyclic group remains an open question.

1. Fundamental concepts

1.1. In this paper all groups considered are commutative and additive notation is employed. For semigroups multiplicative notation is employed. (If a semigroup is a group, then we use additive and multiplicative notation when speaking about the group and the semigroup, respectively.)

1.2. Let Γ be a group. The zero of Γ will be denoted by 0_Γ and the order of 0_Γ will be the number 1.

A subset M of Γ will be said to be a *strong system of generators of the group* Γ if for each $g \in \Gamma$, $g \neq 0_\Gamma$, there exist $g_1, \ldots, g_k \in M$ $(k > 0)$ and positive integers $n_1, \ldots, n_k$ such that $g = n_1 g_1 + \ldots + n_k g_k$.

Let I be a set and, for each $\iota \in I$, let $a_\iota \in \Gamma$, where almost all a_ι are equal to 0_Γ, which means that the set $\{\iota \in I : a_\iota \neq 0_\Gamma\}$ is finite. By the symbol $\sum a_\iota$ $(\iota \in I)$ we understand the finite sum $\sum a_\iota$ $(\iota \in \{\iota \in I :\ a_\iota \neq 0_\Gamma\})$. In case $I = \emptyset$ the symbol $\sum a_\iota$ $(\iota \in I)$ means the element 0_Γ.

1.3. Let $\mathfrak{D}$ be a commutative semigroup with identity element. An element $\mathfrak{r} \in \mathfrak{D}$ is called an *irreducible of the semigroup* $\mathfrak{D}$ if it is not a unit of $\mathfrak{D}$ and the equality $\mathfrak{r} = \mathfrak{a} \cdot \mathfrak{b}$ $(\mathfrak{a} \in \mathfrak{D}, \mathfrak{b} \in \mathfrak{D})$ implies that $\mathfrak{a}$ or $\mathfrak{b}$ is a unit of $\mathfrak{D}$, whence $\mathfrak{b}$ and $\mathfrak{r}$ or $\mathfrak{a}$ and $\mathfrak{r}$ are associated.

The semigroup $\mathfrak{D}$ is called a *UF-semigroup* (abbreviation for a unique factorization semigroup) if the identity element is an only unit of $\mathfrak{D}$ and every element $\mathfrak{d} \in \mathfrak{D}$ different from the identity element may be written uniquely (with the exception of the order of factors) in the form

$$\mathfrak{d} = \mathfrak{r}_1 \ldots \mathfrak{r}_k \quad (k > 0),$$

where $\mathfrak{r}_i$ $(1 \leqslant i \leqslant k)$ are the irreducibles of the semigroup $\mathfrak{D}$.

UF-semigroups are Gaussian semigroups with an only unit and they are free abelian semigroups. The sets of generators are equal to the sets of irreducibles.

The set of all irreducibls of a UF-semigroup will be denoted by $\mathfrak{P}(\mathfrak{D})$. Every element $\mathfrak{d}$ of $\mathfrak{D}$ may be uniquely written in the form of the formally infinite product

$$\mathfrak{d} = \prod \mathfrak{p}^{a_\mathfrak{p}} \quad (\mathfrak{p} \in \mathfrak{P}(\mathfrak{D}))(^1),$$

where $a_\mathfrak{p}$ are non-negative integers almost all equal to the number 0.

1.4. A semigroup G is called a *δ-semigroup* if it has a *divisor theory*, i.e., if there exists a UF-semigroup cG in which G is embedded and

1° for $g_1 \in G$, $g_2 \in G$ we have $g_1 \underset{G}{|} g_2$ if and only if $g_1 \underset{cG}{|} g_2$(²),

2° for each $\mathfrak{d} \in cG$ there exist elements $g_1, \ldots, g_k$ $(k > 0)$ of G such that $\mathfrak{d} = (g_1, \ldots, g_k)$(³).

[1] If the index set is empty, then under the product over this set we understand the identity element of the semigroup $\mathfrak{D}$.

[2] The symbol $\underset{G}{|}$ denotes the relation of divisibility in the semigroup G.

[3] Here the symbol $(g_1, \ldots, g_k)$ denotes the greatest common divisor of the elements $g_1, \ldots, g_k$ in cG.

The semigroup G is then commutative, it has an identity element that is the only unit of G and in G the cancellation law holds. *The semigroup cG is uniquely defined with the exception of the G-isomorphism.*

For elements $\mathfrak{d}_1 \in cG$, $\mathfrak{d}_2 \in cG$ we put $\mathfrak{d}_1 \sim_G \mathfrak{d}_2$ if there exist $g_1 \in G$, $g_2 \in G$ such that $g_1 \cdot \mathfrak{d}_1 = g_2 \cdot \mathfrak{d}_2$. The relation $\sim_G$ is a congruence on the semigroup cG and the semigroup of the classes of this congruence is a group that is called a *divisor class group of the semigroup* G and is denoted by Γ_G (additive notation is employed). The canonical mapping of cG onto Γ_G is denoted by φ_G.

1.5. Let $R = (R, +, \cdot)$ be an integral domain (i.e., a commutative ring with an identity element and without zero divisors). By the symbol R^* we shall denote the semigroup of principal ideals of R different from the zero ideal. This semigroup can be considered as the multiplicative semigroup of R.

The integral domains R for which R^* is a δ-semigroup (i.e., has a divisor theory) are just *Krull domains.*

1.6. The Realization Theorem introduced below is due to Claborn and is taken from Fossum's book [2] (Theorem 15.18).

A subsemigroup G of a UF-semigroup $\mathfrak{D}$ is said to be a *dense subsemigroup of* $\mathfrak{D}$ if for each $Y \subseteq \mathfrak{P}(\mathfrak{D})$, $\operatorname{card} Y < \operatorname{card} \mathfrak{P}(\mathfrak{D})$, and each $\mathfrak{d} \in \mathfrak{D}$, $\mathfrak{d} = \prod \mathfrak{p}^{d_\mathfrak{p}}$ $(\mathfrak{p} \in \mathfrak{P}(\mathfrak{D}))$ ($d_\mathfrak{p}$ being non-negative integers almost all equal to 0), there exists a $g \in G$, $g = \prod \mathfrak{p}^{a_\mathfrak{p}}$ $(\mathfrak{p} \in \mathfrak{P}(\mathfrak{D}))$ ($a_\mathfrak{p}$ being non-negative integers almost all equal to 0) such that $a_\mathfrak{p} = d_\mathfrak{p}$ for each $\mathfrak{p} \in Y$.

THEOREM (Realization Theorem). *Let $\mathfrak{D}$ be a UF-semigroup, and G a dense subsemigroup of $\mathfrak{D}$ such that for $g_1 \in G$, $g_2 \in G$ we have*

$$g_1 \underset{G}{|} g_2 \text{ if and only if } g_1 \underset{\mathfrak{D}}{|} g_2.$$

Then there exist a Dedekind domain R and an isomorphism σ of the semigroup cR^* onto the semigroup $\mathfrak{D}$ such that $\sigma(R^*) = G$.

1.7. Let m be a positive integer and let $b, a_1, \ldots, a_k$ $(k > 0)$ be integers. We say that $(x_1, \ldots, x_k)$ is a *minimal solution of the congruence*

$$\sum_{j=1}^{k} \xi_j a_j \equiv b \pmod{m}$$

if $x_1, \ldots, x_k$ are non-negative integers, at least one x_j $(1 \leqslant j \leqslant k)$ is different from zero, $\sum_{j=1}^{k} x_j a_j \equiv b \pmod{m}$ and if $y_1, \ldots, y_k$ are non-negative integers such that $\sum_{j=1}^{k} y_j a_j \equiv b \pmod{m}$ and $y_j \leqslant x_j$ for each $1 \leqslant j \leqslant k$, we have $y_1 = \ldots = y_k = 0$ or $y_j = x_j$ for each $1 \leqslant j \leqslant k$.

Lemma. *Let* $n, n_1, \ldots, n_k$ $(k > 0)$ *be non-negative integers,* $n > n_j$ $(1 \leqslant j \leqslant k)$, *$p$ a prime number, and b, t integers, where* $tp^n < b \leqslant (t+1)p^n$.

Then for the minimal solution $(x_1, \ldots, x_k)$ *of the congruence*

$$\sum_{j=1}^{k} \xi_j p^{n_j} \equiv b \pmod{p^n}$$

we have

$$\sum_{j=1}^{k} x_j p^{n_j} = b - tp^n.$$

Proof. We prove the lemma inductively with regard to k.

I. Let $k = 1$ and let (x_1) be a minimal solution of the congruence $\xi_1 p^{n_1} \equiv b \pmod{p^n}$. Then $0 < x_1 \leqslant p^{n-n_1}$, whence

$$-(t+1)p^n \leqslant -b < x_1 p^{n_1} - b < p^n - tp^n = -(t-1)p^n,$$

which implies $x_1 p^{n_1} - b = -tp^n$.

II. Let the assertion hold for each $1 \leqslant k' \leqslant k-1$ and let $(x_1, \ldots, x_k)$ be a minimal solution of the congruence

$$\sum_{j=1}^{k} \xi_j p^{n_j} \equiv b \pmod{p^n}.$$

We can suppose that $x_1 \cdot \ldots \cdot x_k \neq 0$ and $n_k \leqslant n_j$ for each $1 \leqslant j \leqslant k$.

Then $p^{n_k} | b$. Put

$$y_k = \frac{b}{p^{n_k}} - tp^{n-n_k}, \qquad y_j = 0 \text{ for } 1 \leqslant j \leqslant k-1.$$

Then $y_k > 0$ and $\sum_{j=1}^{k} y_j p^{n_j} \equiv b \pmod{p^n}$, whence $y_k > x_k$, from which we obtain $b - x_k p^{n_k} > tp^n$. Put $b' = b - x_k p^{n_k}$. Since $x_1 \cdot \ldots \cdot x_{k-1} \neq 0$, $(x_1, \ldots, x_{k-1})$ is a minimal solution of the congruence $\sum_{j=1}^{k-1} x_j p^{n_j} \equiv b' \pmod{p^n}$. As $tp^n < b' < b \leqslant (t+1)p^n$, we obtain from the inductive supposition $\sum_{j=1}^{k-1} x_j p^{n_j} = b' - tp^n$; hence $\sum_{j=1}^{k} x_j p^{n_j} = b - tp^n$ and the proof of the lemma is complete.

1.8. Definition. A mapping f of a set M into the set of negative integers is said to be a *divisor map of M*, or briefly a *d-map of M*, if $M - f^{-1}(0)$ is a finite set. If $M = f^{-1}(0)$, then f is called the *zero divisor map of M*, or briefly the *zero d-map of M*. (The empty mapping which we can speak about in case $M = \emptyset$ is supposed to be zero divisor map of M.)

Let M be a subset of a group Γ. The divisor map f of M is called a *principal divisor map of M in Γ*, or briefly a *pd-map of M in Γ*, if

$$\sum f(\mu)\mu \ (\mu \in M) = 0_\Gamma.$$

A pd-map f of M in Γ is called a *minimal principal divisor map of M in Γ*, or briefly a *minimal pd-map of M in Γ*, if f is not a zero d-map of M and, for every pd-map g of M in Γ with the property $g(\mu) \leqslant f(\mu)$ for each $\mu \in M$, $g = f$ or g is the zero d-map of M.

2. c-characteristic

2.1. Definition. Let G be a δ-semigroup. The pair $[\Gamma_G, \varphi_G(\mathfrak{P}(\mathfrak{c}G))]$ is called the *c-characteristic of G* and denoted by $c(G)$.

If σ is an isomorphism of the group Γ_G onto a group Γ, then we consider the pair $[\Gamma, \sigma\varphi_G(\mathfrak{P}(\mathfrak{c}G))]$ equal to the pair $[\Gamma_G, \varphi_G(\mathfrak{P}(\mathfrak{c}G))]$.

Under the *c-characteristic of a Krull domain R* we understand the c-characteristic of the semigroup R^*.

Evidently:

2.1.1. *If $[\Gamma, M]$ is the c-characteristic of a δ-semigroup, then M is a strong system of generators of the group Γ.*

2.2. Definition. A δ-semigroup G is said to be a *c-semigroup* if for the irreducibles $P_1, \ldots, P_n$ $(n > 0)$ of G and non-negative integers $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, the equality

$$\prod_{i=1}^{n} P_i^{a_i} = \prod_{i=1}^{n} P_i^{b_i} \quad \text{implies} \quad \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i.$$

2.3. Proposition. *Let G_1, G_2 be δ-semigroups such that $c(G_1) = c(G_2)$ Then G_1 is a c-semigroup if and only if G_2 is a c-semigroup.*

Proof. For simplification we put $\mathfrak{P}(\mathfrak{c}G_j) = \mathscr{P}_j$, $\varphi_{G_j} = \varphi_j$ and $\Gamma_{G_j} = \Gamma$ for $j = 1, 2$. Further, we put $\varphi_2(\mathscr{P}_2) = M$. Since $c(G_1) = c(G_2)$, there exists an isomorphism σ of the group Γ_1 onto the group Γ_2 such that $\sigma\varphi_1(\mathscr{P}_1) = M$.

Let G_1 be a c-semigroup and let $Q_1, \ldots, Q_n$ $(n > 0)$ be the irreducibles of G_2 and $a_1, \ldots, a_n$, $b_1, \ldots, b_n$ non-negative integers such that

$$\sum_{i=1}^{n} Q_i^{a_i} = \sum_{i=1}^{n} Q_i^{b_i}.$$

For each $1 \leqslant i \leqslant n$ there exist non-negative integers $d_{i\mathfrak{q}}$ $(\mathfrak{q} \in \mathscr{P}_2$ almost all equal to zero and such that

$$Q_i = \prod \mathfrak{q}^{d_{i\mathfrak{q}}} \quad (\mathfrak{q} \in \mathscr{P}_2).$$

Therefore we obtain for each $\mathfrak{q} \in \mathscr{P}_2$

$$\sum_{i=1}^{n} a_i d_{i\mathfrak{q}} = \sum_{i=1}^{n} b_i d_{i\mathfrak{q}}.$$

Further, let $1 \leqslant i \leqslant n$.

For each $\mathfrak{q} \in \mathscr{P}_2$ there exists a $\mathfrak{p}_\mathfrak{q} \in \mathscr{P}_1$ such that

$$\sigma\varphi_1(\mathfrak{p}_\mathfrak{q}) = \varphi_2(\mathfrak{q}).$$

Then we put $d_{i\mathfrak{q}} = c_{i\mathfrak{p}_\mathfrak{q}}$. For a $\mathfrak{p} \in \mathscr{P}_1$ for which there does not exist a $\mathfrak{q} \in \mathscr{P}_2$ such that $\mathfrak{p} = \mathfrak{p}_\mathfrak{q}$, we put $c_{i\mathfrak{p}} = 0$.

$c_{i\mathfrak{p}}$ $(\mathfrak{p} \in \mathscr{P}_1)$ are non-negative integers almost all equal to zero. Then $P_i \in \mathfrak{c}G_1$, where

$$P_i = \prod \mathfrak{p}^{c_{i\mathfrak{p}}} \quad (\mathfrak{p} \in \mathscr{P}_2).$$

We have

$$\prod_{i=1}^{n} P_i^{a_i} = \prod \mathfrak{p}^{u_\mathfrak{p}} \ (\mathfrak{p} \in \mathscr{P}_1) \quad \text{and} \quad \prod_{i=1}^{n} P_i^{b_i} = \prod \mathfrak{p}^{v_\mathfrak{p}} \ (\mathfrak{p} \in \mathscr{P}_1),$$

where

$$u_\mathfrak{p} = \sum_{i=1}^{n} a_i c_{i\mathfrak{p}} \quad \text{and} \quad v_\mathfrak{p} = \sum_{i=1}^{n} b_i c_{i\mathfrak{p}}.$$

Since $c_{i\mathfrak{p}_\mathfrak{q}} = d_{i\mathfrak{q}}$ for $\mathfrak{q} \in \mathscr{P}_2$ and $c_{i\mathfrak{p}} = 0$ otherwise, we have $u_\mathfrak{p} = v_\mathfrak{p}$ for each $\mathfrak{p} \in \mathscr{P}_1$; hence

$$\prod_{i=1}^{n} P_i^{a_i} = \prod_{i=1}^{n} P_i^{b_i}.$$

For $\mu \in M$ we put $f_i(\mu) = \sum d_{i\mathfrak{q}}$ $(\mathfrak{q} \in \varphi_2^{-1}(\mu))$. The mapping f_i is a minimal pd-map of M in Γ_2. If we put $g_i(\nu) = f_i(\sigma(\nu))$ for $\nu \in \sigma^{-1}(M)$, then g_i is a minimal pd-map of $\sigma^{-1}(M)$ in Γ_1. Since $g_i(\nu) = \sum c_{i\mathfrak{p}}$ $(\mathfrak{p} \in \varphi_1^{-1}(\nu))$ for $\nu \in \sigma^{-1}(M)$, P_i is an irreducible of G_1. Since G_1 is a c-semigroup, we have

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i;$$

therefore G_2 is a c-semigroup, too. The proposition is proved.

2.4. THEOREM. *Let M be a strong system of generators of a group Γ. Then there exists a Dedekind domain whose c-characteristic is the pair $[\Gamma, M]$.*

Proof. Let $M \neq \emptyset$ be a strong system of generators of a group Γ. (In case $M = \emptyset$ the theorem holds.)

Let $\mathfrak{m}$ be an infinite cardinal number such that $\mathfrak{m} > \operatorname{card} M$, and for $\mu \in M$ let X_μ denote an arbitrary set with the property that $\operatorname{card} X_\mu = \mathfrak{m}$ and for $\alpha \in M$, $\beta \in M$, $\alpha \neq \beta$ the sets X_α, X_β are disjoint.

Let $\mathfrak{D}$ be a UF-semigroup such that $\mathfrak{P}(\mathfrak{D}) = \bigcup X_\mu$ $(\mu \in M)$. For simplification we shall further write $\mathfrak{P}(\mathfrak{D}) = \mathscr{P}$. Then $\operatorname{card}\mathscr{P} = \mathfrak{m}$. For $\mathfrak{p} \in X_\mu$ we put $\varphi(\mathfrak{p}) = \mu$ and for $\mathfrak{d} \in \mathfrak{D}$, $\mathfrak{d} = \prod \mathfrak{p}^{a_\mathfrak{p}}$ $(\mathfrak{p} \in \mathscr{P})$ $(a_\mathfrak{p} \geqslant 0)$ we put $\varphi(\mathfrak{d}) = \sum a_\mathfrak{p}\varphi(\mathfrak{p})$ $(\mathfrak{p} \in \mathscr{P})$. φ is a homomorphism of $\mathfrak{D}$ onto Γ.

We put $G = \{\mathfrak{d} \in \mathfrak{D} \colon \varphi(\mathfrak{d}) = 0_\Gamma\}$. Clearly, G is a subsemigroup of $\mathfrak{D}$ and for $g_1 \in G$, $g_2 \in G$ we have $g_1 \underset{G}{|} g_2$ if and only if $g_1 \underset{\mathfrak{D}}{|} g_2$.

We show that G is a dense subsemigroup of $\mathfrak{D}$. Let $Y \subseteq \mathscr{P}$, $\operatorname{card} Y < \operatorname{card}\mathscr{P}$, and let $\mathfrak{d} = \prod \mathfrak{p}^{d_\mathfrak{p}}$ $(\mathfrak{p} \in \mathscr{P}) \in \mathfrak{D}$. We put $\mathfrak{a}^* = \prod \mathfrak{p}^{d_\mathfrak{p}}$ $(\mathfrak{p} \in Y)$. If $\varphi(\mathfrak{a}^*) = 0_\Gamma$, we put $\mathfrak{a} = \mathfrak{a}^*$. Otherwise there exist $\mu_1, \ldots, \mu_k \in M$ $(k > 0)$ and positive integers $a_1, \ldots, a_k$ such that $\sum_{i=1}^{k} a_i\mu_i = -\varphi(\mathfrak{a}^*)$. Since $\operatorname{card} X_\mu > \operatorname{card} Y$, there exist $\mathfrak{p}_i \in X_{\mu_i} - Y$ $(1 \leqslant i \leqslant k)$. We set $\mathfrak{a} = \mathfrak{a}^* \prod_{i=1}^{k} \mathfrak{p}_i^{a_i}$. In both cases $\varphi(\mathfrak{a}) = 0_\Gamma$; hence $\mathfrak{a} \in G$ and if $\mathfrak{a} = \prod \mathfrak{p}^{a_\mathfrak{p}}$ $(\mathfrak{p} \in \mathscr{P})$, then for $\mathfrak{p} \in Y$ we have $a_\mathfrak{p} = d_\mathfrak{p}$. Therefore G is a dense subsemigroup of $\mathfrak{D}$.

By Claborn's Realization Theorem 1.6 there exists a Dedekind domain R and an isomorphism σ of the semigroup $\mathfrak{c}R^*$ onto the semigroup $\mathfrak{D}$ such that $\sigma(R^*) = G$. Hence G is a δ-semigroup and we can suppose that $\mathfrak{c}G = \mathfrak{D}$. There exists an isomorphism $\bar{\sigma}$ of the divisor class group Γ_{R^*} onto the divisor class group Γ_G such that $\bar{\sigma}\circ\varphi_{R^*} = \varphi_G\circ\sigma$.

Let $\mathfrak{d}_1 \in \mathfrak{D}$, $\mathfrak{d}_2 \in \mathfrak{D}$. Then there exist $\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3 \in \mathfrak{D}$ such that $\mathfrak{d}_1\cdot\mathfrak{c}_1 = \mathfrak{d}_2\cdot\mathfrak{c}_2$ and $\varphi(\mathfrak{c}_3) = -\varphi(\mathfrak{c}_1)$. Put $g_1 = \mathfrak{c}_1\cdot\mathfrak{c}_3$, $g_2 = \mathfrak{c}_2\cdot\mathfrak{c}_3$. If $\varphi(\mathfrak{d}_1) = \varphi(\mathfrak{d}_2)$, then $\varphi(\mathfrak{c}_1) = \varphi(\mathfrak{c}_2)$; hence $g_1 \in G$, $g_2 \in G$, whence $\mathfrak{d}_1 \sim_G \mathfrak{d}_2$. If, on the other hand, $\mathfrak{d}_1 \sim_G \mathfrak{d}_2$, then clearly $\varphi(\mathfrak{d}_1) = \varphi(\mathfrak{d}_2)$. Therefore there exists an isomorphism τ of the divisor class group Γ_G onto the group Γ such that $\tau\circ\varphi_G = \varphi$. The situation is demonstrated by the following diagram:

$$\begin{tikzcd}
 & & \Gamma & \\
G \arrow[r] & \mathfrak{D} = \mathfrak{c}G \arrow[ur, "\varphi"] \arrow[rr, "\varphi_G"'] & & \Gamma_G \arrow[ul, dashed, "\tau"'] \\
R^* \arrow[u, "\sigma|_{R^*}"] \arrow[r] & \mathfrak{c}R^* \arrow[u, "\sigma"'] \arrow[rr, "\varphi_{R^*}"'] & & \Gamma_{R^*} \arrow[u, dashed, "\bar{\sigma}"']
\end{tikzcd}$$

Here $\sigma|_{R^*}$ denotes the restriction of σ to $R^*(\sigma/R^* \colon R^* \to G)$ and the undenoted morphisms denote the identity embeddings.

We have

$$c(R^*) = [\Gamma_{R^*}, \varphi_{R^*}(\mathfrak{P}(\mathfrak{c}R^*))] = [\Gamma, \tau\bar{\sigma}\varphi_{R^*}(\mathfrak{P}(\mathfrak{c}R^*))].$$

Further,

$$\tau\bar{\sigma}\varphi_{R^*}(\mathfrak{P}(\mathfrak{c}R^*)) = \tau\varphi_G\sigma(\mathfrak{P}(\mathfrak{c}R^*)) = \tau\varphi_G(\mathscr{P}) = \varphi(\mathscr{P}) = M.$$

Therefore, $c(R^*) = [\Gamma, M]$ and the theorem is proved.

2.5. DEFINITION. A subset M of a group Γ is called a *c-set of the group Γ* if for minimal principal divisor maps $f_1, \ldots, f_n$ $(n > 0)$ of M in Γ and integers $x_1, \ldots, x_n$ the equality $\sum_{i=1}^{n} x_i f_i(\mu) = 0$ for each $\mu \in M$ implies $\sum_{i=1}^{n} x_i = 0$.

2.6. THEOREM. *Let M be a strong system of generators of a group Γ. Then the following statements are equivalent:*

(a) *M is a c-set of the group Γ,*

(b) *there exists a c-semigroup whose c-characteristic is the pair $[\Gamma, M]$.*

Proof. I. Let M be a c-set of the group Γ. By 2.4 we can suppose that there exists a δ-semigroup G such that

$$\Gamma = \Gamma_G \quad \text{and} \quad M = \varphi_G(\mathfrak{P}(\mathfrak{c}G)).$$

We show that G is a c-semigroup. Let $P_1, \ldots, P_n$ $(n > 0)$ be the irreducibles of G and $a_1, \ldots, a_n, b_1, \ldots, b_n$ integers such that

$$\sum_{i=1}^{n} P_i^{a_i} = \sum_{i=1}^{n} P_i^{b_i}.$$

For each $1 \leqslant i \leqslant n$ let $c_{i\mathfrak{p}}$ $(\mathfrak{p} \in \mathfrak{P}(\mathfrak{c}G))$ be non-negative integers almost all equal to zero and such that

$$P_i = \prod \mathfrak{p}^{c_{i\mathfrak{p}}} \quad (\mathfrak{p} \in \mathfrak{P}(\mathfrak{c}G)).$$

For each $\mu \in M$ we set $f_i(\mu) = \sum c_{i\mathfrak{p}}$ $(\mathfrak{p} \in \varphi_G^{-1}(\mu))$. The mappings f_i are minimal pd-maps of M in Γ.

For each $\mathfrak{p} \in \mathfrak{P}(\mathfrak{c}G)$ we get $\sum\limits_{i=1}^{n} a_i c_{i\mathfrak{p}} = \sum\limits_{i=1}^{n} b_i c_{i\mathfrak{p}}$; hence for each $\mu \in M$ we have $\sum\limits_{i=1}^{n} (a_i - b_i) f_i(\mu) = 0$, from which it follows that $\sum\limits_{i=1}^{n} a_i = \sum\limits_{i=1}^{n} b_i$. Therefore G is a c-semigroup.

II. Let G be a c-semigroup, $c(G) = [\Gamma, M]$. We can suppose that $\Gamma = \Gamma_G$, $M = \varphi_G(\mathfrak{P}(\mathfrak{c}G))$. Let $f_1, \ldots, f_n$ $(n > 0)$ be minimal pd-maps of M in Γ and $x_1, \ldots, x_n$ integers with the property $\sum\limits_{i=1}^{n} x_i f_i(\mu) = 0$ for each $\mu \in M$.

For each $\mu \in M$ there exists a $\mathfrak{p}_\mu \in \mathfrak{P}(\mathfrak{c}G)$ such that $\varphi_G(\mathfrak{p}_\mu) = \mu$. We put

$$P_i = \prod \mathfrak{p}^{f_i(\mu)} \quad (\mu \in M)$$

for $1 \leqslant i \leqslant n$. The elements P_i are the irreducibles of G. There exist non-negative integers $a_1, \ldots, a_n, b_1, \ldots, b_n$ such that $x_i = a_i - b_i$. Then

$$\prod_{i=1}^{n} P_i^{a_i} = \prod_{i=1}^{n} P_i^{b_i};$$

hence $\sum\limits_{i=1}^{n} a_i = \sum\limits_{i=1}^{n} b_i$, from which it follows that $\sum\limits_{i=1}^{n} x_i = 0$. Therefore M is a c-set of the group Γ.

The proof is complete.

From 2.3 and 2.6 we get

2.7. THEOREM. *Let the pair $[\Gamma, M]$ be the c-characteristic of a δ-semigroup G. Then G is a c-semigroup if and only if M is a c-set of the group Γ.*

2.8. COROLLARY. *In a Dedekind domain all factorizations into irreducibles of a given element have the same length if and only if the set of all ideal classes containing at least one prime ideal is a c-set of the ideal class group of that domain.*

3. c-sets of elements of finite orders

3.1. THEOREM. *Let $\mu_1, \ldots, \mu_k$ $(k > 0)$ be different elements of a group Γ with finite orders $m_1, \ldots, m_k$. Then the set $M = \{\mu_1, \ldots, \mu_k\}$ is a c-set of the group Γ if and only if for every minimal principal divisor map f of M in Γ the equation*

$$\sum_{j=1}^{k} \frac{f(\mu_j)}{m_j} = 1$$

holds.

Proof. I. Let M be a c-set of the group Γ and let f be a minimal pd-map of M in Γ. For $1 \leqslant j \leqslant k$ we put $f_j(\mu) = 0$ for $\mu \in M - \{\mu_j\}$ and $f_j(\mu_j) = m_j$. Then f_j are minimal pd-maps of M in Γ. We put $x_0 = m_1 \cdot \ldots \cdot m_k$, $x_j = -(m_1 \cdot \ldots \cdot m_k / m_j) f(\mu_j)$ $(1 \leqslant j \leqslant k)$. For each $1 \leqslant s \leqslant k$ we get

$$x_0 f(\mu_s) + \sum_{j=1}^{k} x_j f_j(\mu_s) = 0.$$

Since M is a c-set of Γ, we have $\sum\limits_{j=0}^{k} x_j = 0$, from which it follows that $\sum\limits_{j=1}^{k} \dfrac{f(\mu_j)}{m_j} = 1$.

II. Let $\sum\limits_{j=1}^{k} \dfrac{f(\mu_j)}{m_j} = 1$ hold for every minimal pd-map f of M in Γ. Let $f_1, \ldots, f_n$ $(n > 0)$ be minimal pd-maps of M in Γ, and let $x_1, \ldots, x_n$ be integers with the property $\sum\limits_{i=1}^{n} x_i f_i(\mu) = 0$ for each $\mu \in M$. Then we have

$$0 = \sum_{j=1}^{k} \frac{1}{m_j} \sum_{i=1}^{n} x_i f_i(\mu_j) = \sum_{i=1}^{n} x_i \sum_{j=1}^{k} \frac{f_i(\mu_j)}{m_j} = \sum_{i=1}^{n} x_i;$$

hence M is a c-set of Γ.

Thus the proof is complete.

3.2. PROPOSITION. *Let M be a subgroup of a group Γ and let each element of M have a finite order. Then M is a c-set if and only if* card $M \leqslant 2$.

Proof. If card $M \leqslant 2$, then clearly M is a c-set of Γ. Let M be a c-set of Γ.

If there exists in M an element μ with order $m > 2$, we put $f(\mu) = f(-\mu) = 1$. Then f is a minimal pd-map of the set $\{\mu, -\mu\}$ in Γ and

$$\frac{f(\mu)}{m}+\frac{f(-\mu)}{m} = \frac{2}{m} \neq 1.$$

Hence the set $\{\mu, -\mu\}$ is not a c-set of Γ; therefore even the set M is not a c-set of Γ. Consequently all non zero elements of M have order 2.

If card $M \geqslant 3$, then there exist $\alpha \in M$, $\beta \in M$ such that $0_\Gamma \neq \alpha \neq \beta \neq 0_\Gamma$. Then for $\gamma = \alpha+\beta$ we have $\gamma \notin \{0_\Gamma, \alpha, \beta\}$. We put $f(\alpha) = f(\beta) = f(\gamma) = 1$. Then f is a minimal pd-map of the set $\{\alpha, \beta, \gamma\}$ in Γ and

$$\frac{f(\alpha)}{2}+\frac{f(\beta)}{2}+\frac{f(\gamma)}{2} \neq 1.$$

Therefore, $\{\alpha, \beta, \gamma\}$ is not a c-set of Γ; hence even the set M is not a c-set of Γ.

Thus the proposition is proved.

3.3. Remark. Proposition 3.2 generalizes Carlitz's result [1] concerning a ring of algebraic integers. Here the fact is used that the c-characteristic of such a ring is $[\Gamma, \Gamma]$, where Γ is a finite group.

The proof of 3.2 is a modification of Carlitz's proof from [1].

3.4. Proposition. *Let Γ be a cyclic group of order p^n, where p is a prime number and n a positive integer. Let $\mu_1, \ldots, \mu_k$ $(k > 0)$ be elements of the group Γ with orders $p^{n_1} \geqslant p^{n_2} \geqslant \ldots \geqslant p^{n_k} \geqslant 1$. Then the following statements are equivalent*:

(a) *$\{\mu_1, \ldots, \mu_k\}$ is a c-set of the group Γ,*

(b) $1 \leqslant i \leqslant j \leqslant k \Rightarrow \mu_j = p^{n_i-n_j}\mu_i$,

(c) $1 \leqslant j \leqslant k \Rightarrow \mu_j = p^{n_1-n_j}\mu_1$[4].

Proof. We can suppose that Γ is the additive group of the ring of rest classes modulo p^n. Then there exist integers $1 \leqslant b_j < p^{n_j}$, $p \nmid b_j$ such that $b_j p^{n-n_j} \in \mu_j$ $(1 \leqslant j \leqslant k)$.

I. Let (a) hold and let $1 \leqslant i \leqslant j \leqslant k$, $\mu_j \neq \mu_i$. The set $A = \{\mu_i, \mu_j\}$ is a c-set of Γ. There exists just one integer $1 \leqslant x < p^{n_i}$ such that

$$xb_i + b_j p^{n_i-n_j} \equiv 0 \,(\mathrm{mod}\, p^{n_i}).$$

Then $x\mu_i + \mu_j = 0_\Gamma$. We put $f(\mu_i) = x$, $f(\mu_j) = 1$. Then f is a minimal pd-map of A in Γ, whence according to 3.1 we have

$$1 = \frac{f(\mu_i)}{p^{n_i}}+\frac{f(\mu_j)}{p^{n_j}} = \frac{x}{p^{n_i}}+\frac{1}{p^{n_j}},$$

[4] Proposition 3.4 has been proved independently by J. Śliwa.

from which we get $p^{n_i} = x + p^{n_i-n_j}$; therefore

$$\mu_j = -x\mu_i = p^{n_i-n_j}\mu_i - p^{n_i}\mu_i = p^{n_i-n_j}\mu_i.$$

Thus statement (b) holds.

II. Implication (b) $\Rightarrow$ (c) is evident.

III. Let (c) hold. Then $b_j \equiv b_1 (\mathrm{mod}\, p^{n_j})$. We can suppose that the elements $\mu_1, \ldots, \mu_k$ are different.

Let f be a minimal pd-map of $\{\mu_1, \ldots, \mu_k\}$ in Γ. Then $\big(f(\mu_1), \ldots, f(\mu_k)\big)$ is a minimal solution of the congruence $\sum_{j=1}^{k} \xi_j b_j p^{n-n_j} \equiv 0 \,(\mathrm{mod}\, p^n)$. Since $b_j p^{n-n_j} \equiv b_1 p^{n-n_j} (\mathrm{mod}\, p^n)$, $\big(f(\mu_1), \ldots, f(\mu_k)\big)$ is a minimal solution of the congruence $\sum_{j=1}^{k} \xi_j p^{n-n_j} \equiv 0\,(\mathrm{mod}\, p^n)$ and by Lemma 1.7 we have $\sum_{j=1}^{k} f(\mu_j) p^{n-n_j} = p^n$, thus $\sum_{j=1}^{k} \frac{f(\mu_j)}{p^{n_j}} = 1$. Then Theorem 3.1 implies that $\{\mu_1, \ldots, \mu_k\}$ is a c-set of Γ.

The proposition is proved.

3.5. Remark. In the case of elements of infinite orders we can prove the following result:

If α, β, γ are rational integers, $\alpha > 0$, $\beta < 0$, $\gamma < 0$, then the set $\{\alpha, \beta, \gamma\}$ is a c-set of the additive group of rational integers if and only if

$$\beta(\alpha, \gamma) \equiv \gamma(\alpha, \beta)\big(\mathrm{mod}\, \alpha(\beta, \gamma)\big)\text{[5]}.$$

There remains the open problem of how to characterize all c-sets of the infinite cyclic group.

[5] The symbol (φ, ψ) means the greatest common divisor of rational integers φ, ψ.

References

[1] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11 (1960), pp. 391–392.

[2] R. M. Fossum, *The Divisor Class Group of a Krull Domain*, Berlin–Heidelberg–New York 1973.

[3] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Warszawa 1974.

Received on 31. 1. 1975
and in revised form on 31. 5. 1975

(664)