Ladislav Skula

On δn-semigroups

Archivum Mathematicum, Vol. 17 (1981), No. 1, 43--52

Persistent URL: http://dml.cz/dmlcz/107089

ARCH. MATH. 1, SCRIPTA FAC. SCI. NAT. UJEP BRUNENSIS
XVII: 43—52, 1981

ON δn - SEMIGROUPS

LADISLAV SKULA, Brno

(Received March 9, 1980)

A *divisor theory of a commutative semigroup G* with identity element is a homomorphism h of G into a unique factorization semigroup $\mathfrak{D}$ which preserves the divisibility relation in both directions and for each $\mathfrak{d} \in \mathfrak{D}$ there exist a positive integer n and $g_1, \ldots, g_n \in G$ such that $\mathfrak{d}$ is the greatest common divisor of the set $\{h(g_1), \ldots, h(g_n)\}$.

This paper deals with the question when this integer n depends only on the semigroup G and not on the element $\mathfrak{d}$. It is shown (Theorem 1.5) that then n depends on the divisor class group Γ of G, the image of prime divisors of G in Γ, and the subset of this image containing all divisor classes which are images of at least two different prime divisors of G.

If this integer n depends only on the divisor class group of G, then we call this group an *n-group* whose basic properties are mentioned in Section 2.

The problem, when a cyclic group is an n-group, is fully solved in Section 3 by Theorem 3.6.

0. BASIC CONCEPTS AND ASSERTIONS

In this paper the *semigroup* is always commutative with identity element and multiplicative notation is employed. If g_1, g_2 are elements of a semigroup G, then

$$g_1 \mid g_2 = g_1 \underset{G}{\mid} g_2$$

denotes the existence of $g \in G$ such that $g_1 g = g_2$.

The *groups* are also commutative, and additive notation is employd. The *zero element* of a group Γ is denoted by $0_\Gamma = 0$. A subset M of Γ is said to be a *strong system of generators of the group* Γ if for each $\gamma \in \Gamma$, $\gamma \neq 0_\Gamma$ there exist $\gamma_1, \ldots, \gamma_k \in M (k > 0)$ and positive integers $n_1, \ldots, n_k$ such that

$$\gamma = n_1\gamma_1 + \ldots + n_k\gamma_k.$$

The semigroup $\mathfrak{D}$ is called a *UF-semigroup* (a *unique factorization semigroup*) if the identity element is the only unit of $\mathfrak{D}$ and each 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

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

where $\mathfrak{r}_i (1 \leqq i \leqq k)$ are the irreducibles of $\mathfrak{D}$. The set of all irreducibles of $\mathfrak{D}$ will be denoted by $\mathfrak{P}(\mathfrak{D})$. For $\mathfrak{d}_1, \dots, \mathfrak{d}_k \in \mathfrak{D} (k > 0)$ the symbol

$$(\mathfrak{d}_1, \dots, \mathfrak{d}_k)$$

denotes the *greatest common divisor* of the elements $\mathfrak{d}_1, \dots, \mathfrak{d}_k$ in $\mathfrak{D}$.

UF-semigroups are Gaussian semigroups with one unit and they are free abelian semigroups. The sets of generators are equal to those of irreducibles.

The greatest common divisor of a subset M of the set of integers $\mathbf{Z}$ will be abbreviated to the g.c.d. of M.

Let G be a semigroup, $\mathfrak{D}$ a UF-semigroup and h a homomorphism of G into $\mathfrak{D}$. We say that $h: G \to \mathfrak{D}$ is a *divisor theory* if it holds:

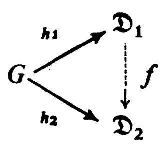
1° $g_1 \underset{G}{|} g_2 \Leftrightarrow h(g_1) \underset{\mathfrak{D}}{|} h(g_2)$ for $g_1, g_2 \in G$,

2° for each $\mathfrak{d} \in \mathfrak{D}$ there exist a positive integer n and elements $g_1, \dots, g_n \in G$ such that

$$\mathfrak{d} = (h(g_1), \dots, h(g_n)).$$

We recall that the homomorphism h is uniquely defined with the exception of the "*G-isomorphism*" (*Clifford* [1]), more exactly:

if $h_1: G \to \mathfrak{D}_1$, $h_2: G \to \mathfrak{D}_2$ are divisor theories, then there exists an isomorphism f of $\mathfrak{D}_1$ onto $\mathfrak{D}_2$ such that $fh_1 = h_2$ is valid.



If $h: G \to \mathfrak{D}$ is a divisor theory, we put $\mathfrak{d}_1 \sim \mathfrak{d}_2$ for $\mathfrak{d}_1, \mathfrak{d}_2 \in \mathfrak{D}$ if there exist $g_1, g_2 \in G$ such that $h(g_1)\,\mathfrak{d}_1 = h(g_2)\,\mathfrak{d}_2$. The relation $\sim$ is a congruence on the semigroup $\mathfrak{D}$ and the semigroup of the classes of $\sim$ is a group called a *divisor class group of G* and denoted by Γ. (For this group Γ we shall use additive notation.) The canonical mapping of $\mathfrak{D}$ onto Γ is denoted by φ.

The situation is demonstrated by the diagram:

$$G \xrightarrow{h} \underset{\sim}{\mathfrak{D}} \xrightarrow{\varphi} \Gamma.$$

If for a semigroup G there exists a divisor theory $h\colon G \to \mathfrak{D}$, we call G a *δ-semigroup*.

Then it holds

0.1. Proposition (*Skula* [2], 3.3). *Let $h\colon G \to \mathfrak{D}$ be a divisor theory. Then for each $\mathfrak{p}_0 \in \mathfrak{P}(\mathfrak{D})$ the set $\varphi(\mathfrak{P}(\mathfrak{D}) - \{\mathfrak{p}_0\})$ is a strong system of generators of the divisor class group Γ of G.*

A certain "converse" proposicion also holds:

0.2. Proposition. (*Skula* [2], 3.6.) *Let $\mathfrak{D}$ be a UF-semigroup, Γ be a group which is defined by means of a congruence relation $\sim$ on $\mathfrak{D}$ and φ be a canonical mapping of $\mathfrak{D}$ onto Γ with the following property: for each $\mathfrak{p}_0 \in \mathfrak{P}(\mathfrak{D})$ the set $\varphi(\mathfrak{P}(\mathfrak{D}) - \{\mathfrak{p}_0\})$ is a strong system of generators of the group Γ.*

Then there exists just one divisor theory $h\colon G \to \mathfrak{D}$ such that G is a subsemigroup of $\mathfrak{D}$, h is the identity of G in $\mathfrak{D}$ and for $\mathfrak{d}_1, \mathfrak{d}_2 \in \mathfrak{D}$ we have $\mathfrak{d}_1 \sim \mathfrak{d}_2$ if and only if there exist $g_1, g_2 \in G$ such that $g_1\mathfrak{d}_1 = g_2\mathfrak{d}_2$. Then Γ is the divisor class group of G and $G = 0_\Gamma$.

1. δn - SEMIGROUPS

1.1. Definition. Let $h\colon G \to \mathfrak{D}$ be a divisor theory, n a positive integer. The semigroup G is said to be a *δn-semigroup* if for each $\mathfrak{d} \in \mathfrak{D}$ there exist $g_1, \ldots, g_n \in G$ such that

$$\mathfrak{d} = (h(g_1), \ldots, h(g_n)).$$

1.2. Remark. For $n = 1$ the notion of δn-semigroup $= \delta 1$ – semigroup coincides with the notion of "a *semigroup with a unique factorization*" (or with more units) which is equivalent to *the divisor class group of G being trivial.*

1.3. Definition. Let $h\colon G \to \mathfrak{D}$ be a divisor theory. Then we call the set

$$\{\gamma \in \Gamma : \exists\, \mathfrak{p}_1, \mathfrak{p}_2 \in \mathfrak{P}(\mathfrak{D}), \mathfrak{p}_1 \neq \mathfrak{p}_2, \varphi(\mathfrak{p}_1) = \varphi(\mathfrak{p}_2) = \gamma\}$$

the *doubled set of G.*

1.4. Definition. Let Γ be a group. For $X \subseteq \Gamma$ we put $L(X) = \{x_1\xi_1 + \ldots + x_k\xi_k\colon x_i$ non-negative integers, $\xi_i \in X (k \geqq 1)\}$. (For $X = \emptyset$ we put $L(X) = L(\emptyset) = \{0_\Gamma\}$.)

In this notation *the set X is a strong system of generators of Γ if and only if $L(X) = \Gamma$.*

Let M be a strong system of generators of the group Γ. An element $\alpha \in M$ is said to be a *necessary element of* (*the strong system of generators*) M if $M - \{\alpha\}$ is not a strong system of generators of the group Γ.

Let n be a positive integer. We say that $N \subseteq M$ is an *n-suitable subset of M* if for each $\omega \in \Gamma$ there exist $N_1, \ldots; N_n \subseteq M$ such that

$$\omega \in L(N_1) \cap \ldots \cap L(N_n) \qquad \text{and} \qquad N_1 \cap \ldots \cap N_n \subseteq N.$$

It is clear that *any subset of M which contains an n-suitable subset of M is an n-suitable subset of M.*

1.5. Theorem. *Let* h: $G \to \mathfrak{D}$ *be a divisor theory,* n *an integer* $\geqq 2$. *Then* G *is a* δn*-semigroup if and only if the doubled set of* G *is an* n*-suitable subset of* $\varphi(\mathfrak{P}(\mathfrak{D}))$.

Proof. I. Let G be a δn-semigroup and let $\omega \in \Gamma$, $\omega \neq 0$. There exist $\mathfrak{d} \in \mathfrak{D}$ and $g_1, \ldots, g_n \in G$ such that

$$\varphi(\mathfrak{d}) = -\omega,$$
$$\mathfrak{d} = (h(g_1), \ldots, h(g_n)).$$

Let $\mathfrak{d}_1, \ldots, \mathfrak{d}_n \in \mathfrak{D}$, $h(g_i) = d \,.\, d_i (1 \leqq i \leqq n)$. Then $\mathfrak{d}_i$ is not the identity element of $\mathfrak{D}$ and let

$$\mathfrak{d}_i = \prod_{j=1}^{k(i)} \mathfrak{p}_{ij}^{a_{ij}}$$

be the canonical form of $\mathfrak{d}_i$. Put

$$N_i = \{\varphi(\mathfrak{p}_{ij}) \colon 1 \leqq j \leqq k(i)\}.$$

Then $\omega = \varphi(\mathfrak{d}_i) \in L(N_i)$, thus $\omega \in L(N_1) \cap \ldots \cap L(N_n)$.

Let $\gamma \in N_1 \cap \ldots \cap N_n$. Then for each $1 \leqq i \leqq n$ there exists an integer $1 \leqq u(i) \leqq$ $\leqq k(i)$ such that

$$\gamma = \varphi(\mathfrak{p}_{iu(i)}).$$

Since $(\mathfrak{d}_1, \ldots, \mathfrak{d}_n) = 1$, there exists an integer $2 \leqq a \leqq n$ such that $\mathfrak{p}_{1u(1)} = \mathfrak{p}_{au(a)}$. Hence the element γ belongs to the doubled set of G.

II. Let the doubled set N of G be an n-suitable subset of $\varphi(\mathfrak{P}(\mathfrak{D}))$ and let $\mathfrak{d} \in \mathfrak{D} -$ $- h(G)$, $\varphi(\mathfrak{d}) = \omega \neq 0$. Then there exist $N_1, \ldots, N_n \subseteqq \varphi(\mathfrak{P}(\mathfrak{D}))$ such that

$$-\omega \in L(N_1) \cap \ldots \cap L(N_n) \quad \text{and} \quad N_1 \cap \ldots \cap N_n \subseteqq N.$$

For each $1 \leqq i \leqq n$ there exist a positive integer $k(i)$, $\mathfrak{p}_{ij} \in \mathfrak{P}(\mathfrak{D})$ and positive integers $a_{ij} (1 \leqq j \leqq k(i))$ such that $\varphi(\mathfrak{p}_{ij}) \in N_i$ and

$$-\omega = \sum_{j=1}^{k(i)} a_{ij} \varphi(\mathfrak{p}_{ij}).$$

Since $N_1 \cap \ldots \cap N_n$ is a subset of the doubled set N of G, we can suppose

$$\bigcap_{i=1}^{n} \{\mathfrak{p}_{ij} : 1 \leqq j \leqq k(i)\} = \emptyset.$$

Put for each $1 \leqq i \leqq n$

$$\mathfrak{d}_i = \prod_{j=1}^{k(i)} \mathfrak{p}_{ij}^{a_{ij}}.$$

Then $\mathfrak{d}_i \in \mathfrak{D}$, $(\mathfrak{d}_1, \ldots, \mathfrak{d}_n) = 1$, $\varphi(\mathfrak{d}_i) = -\omega$, therefore $\varphi(\mathfrak{d}\mathfrak{d}_i) = 0$. Thus, there exist $g_1, \ldots, g_n \in G$ with the property $\mathfrak{d}\mathfrak{d}_i = h(g_i)$. Clearly,

$$\mathfrak{d} = (h(g_1), \ldots, h(g_n)).$$

The proof is complete.

2. n-GROUP

2.1. Definition. A group Γ is said to be an *n-group*, where n denotes a positive integer, if for each strong system of generators M of the group Γ the set of the necessary elements of M is an n-suitable subset of M.

From 0.1, 0.2 and 1.5 we obtain

2.2. Theorem. *For an integer $n \geqq 2$ a group Γ is an n-group if and only if every δ-semigroup, whose divisor class group is isomorphic to Γ, is a δn-semigroup.*

For $n = 1$ we immediately get the following

2.3. **Proposition.** *A group Γ is a* 1*-group if and only if for each strong system of generators M of Γ the set of necessary elements of M is also a strong system of generators of Γ.*

Obviously there holds

2.4. Proposition. *The trivial group is an n-group for each positive integer n.*

2.5. Proposition. *Let n be a positive integer, Γ an n-group. Then for every subgroup H of Γ the factor group Γ/H is also an n-group.*

Proof. Let $\mathfrak{M}$ be a strong system of generators of the factor group Γ/H and f be the canonical mapping of Γ onto Γ/H. For each $X \in \mathfrak{M}$ let $x(X) \in X$. Put

$$M = \{x(X) : X \in \mathfrak{M}\} \cup H.$$

Obviously, M is a strong system of generators of Γ.

Let $s \in M - H$ be a necessary element of M. Then there exists $\omega \in \Gamma$ such that $\omega \notin L(M - \{s\})$. Let $X_i \in \mathfrak{M}(1 \leqq i \leqq k)$ such that $f(\omega) \in L(X_1, \ldots, X_k)$. Thus there exist positive integers a_i and $h \in H$ such that

$$\omega = a_1 x(X_1) + \ldots + a_k x(X_k) + h,$$

which implies the existence of an integer $i(1 \leqq i \leqq k)$ such that $x(X_i) = s$. Hence $f(s) = X_i$ and $f(s)$ is a necessary element of $\mathfrak{M}$.

Let $X \in \Gamma/H$ and $x \in X$. Then there exist $N_1, \ldots, N_n \subseteqq M$ such that

$$x \in L(N_1) \cap \ldots \cap L(N_n)$$

and $N_1 \cap \ldots \cap N_n$ is a subset of the set of necessary elements of M. For $1 \leqq i \leqq n$ put $\mathrm{N}_i = f(N_i) - \{H\}$. Then $\mathrm{N}_i \subseteqq \mathfrak{M}$ and $X = f(x) \in L(\mathrm{N}_1) \cap \ldots \cap L(\mathrm{N}_n)$. For

$S \in \bigcap_{i=1}^{n} N_i$ we have $x(S) \in \bigcap_{i=1}^{n} N_i - H$, whence we obtain that $x(S)$ is a necessary element of M, therefore $S = f(x(S))$ is a necessary element of the system $\mathfrak{M}$.

The Proposition is proved.

3. CYCLIC n-GROUP

In this Section we give an equivalent condition in Theorem 3.6, when a cyclic group is an n-group for positive integer n. The following Definition has a helpful function.

3.1. Definition. Let k, n be positive integers. We denote by $P(k)$ the system of all mapping π of a non-empty finite set A into the system 2^P of all subsets of a non-empty set P, card $P \leqq k$ with the following property: for each $p \in P$ there exist $a \in A$, $b \in A$, $a \neq b$ such that $p \in \pi(a) \cap \pi(b)$.

The set A is denoted by d(p) and the set P by $c(\pi)$.

We say that $\pi \in P(k)$ has the property $\alpha(k, n)$ if there exist $A_1, \ldots, A_n \subseteqq d$(p) such that $\bigcap_{i=1}^{n} A_i = \emptyset$ and $\bigcup \pi(a)\,(a \in A_i) = c(\pi)$ for each $1 \leqq i \leqq n$. (Here, under the union over empty set we understand again the empty set.)

Further, we put $k\varrho n$ if each $\pi \in P(k)$ has the property $\alpha(k, n)$.

3.2. Lemma. *Let k, n be positive integers. If each injective mapping from $P(k)$ has the property $\alpha(k, n)$, then $k\varrho n$.*

Proof. Let $\pi \in P(k)$. Put

$$\begin{aligned} B &= \{a \in d(\pi) : \exists\, a' \in d(\pi), a' \neq a, \pi(a) = \pi(a')\},\\ R &= \bigcup \pi(a)\,(a \in B),\\ C &= \{a \in d(\pi) : \pi(a) \cap (c(\pi) - R) \neq \emptyset\},\\ P' &= \bigcup \pi(a)\,(a \in C),\\ A' &= C \cup \{\alpha\}, \end{aligned}$$

where α is a symbol which does not belong to $d(\pi)$.

If $C = \emptyset$, put $C_i = \emptyset (1 \leqq i \leqq n)$. In case $C \neq \emptyset$ the set P' is non-empty and card $P' \leqq k$. For $a \in A'$ put

$$\pi'(a) = \begin{cases} \pi(a) & \text{for } a \neq \alpha,\\ P' \cap R & \text{for } a = \alpha. \end{cases}$$

Then $\pi' \in P(k)$, $d(\pi') = A'$, $c(\pi') = P'$ and π' is injective. Therefore there exist $C_1, \ldots, C_n \subseteqq A'$ such that $\bigcap_{i=1}^{n} C_i = \emptyset$ and $\bigcup \pi'(a)\,(a \in C_i) = P'(1 \leqq i \leqq n)$.

There exist disjoint subsets U, V of B such that

$$\bigcup \pi(u)\,(u \in U) = \bigcup \pi(v)\,(v \in V) = R.$$

We can suppose $n \geqq 2$ and put

$$A_i = \begin{cases} U \cup (C_i - \{\alpha\}) & \text{for } 1 \leqq i \leqq n-1, \\ V \cup (C_n - \{\alpha\}) & \text{for } i = n. \end{cases}$$

Then $\bigcap_{i=1}^{n} A_i = \emptyset$ and $\bigcup \pi(a)\,(a \in A_i) = c(\pi)$ for each $1 \leqq i \leqq n$. Thus $k\varrho n$.

3.3. Lemma. *Let k, n be positive integers. If each $\pi \in P(k)$ with the properties*

(1) $a, b, c \in d(\pi), a \neq b \neq c \neq a \Rightarrow \pi(a) \cap \pi(b) \cap \pi(c) = \emptyset$,

(2) $a, b \in d(\pi) \Rightarrow \pi(a) \cap \pi(b) \neq \emptyset$

has the property $\alpha(k, n)$, then $k\varrho n$.

Proof. I. For $\pi, \pi' \in P(k)$ put $\pi \leqq \pi'$ if $d(\pi) = d(\pi')$, $c(\pi) = c(\pi')$ and $\pi(a) \subseteqq \pi'(a)$ for each $a \in d(\pi)$. It is clear that if π has the property $\alpha(k, n)$, then π' has also the property $\alpha(k, n)$. Therefore, if each $\pi \in P(k)$ with the property (1) has the property $\alpha(k, n)$, then $k\varrho n$.

II. Denote the set of all mappings from $P(k)$ with the property (1) by $\bar{P}(k)$. For $\pi \in \bar{P}(k)$ which does not satisfy (2) let $a, b \in d(\pi)$ such that $\pi(a) \cap \pi(b) = \emptyset$. Put $d(\pi') = d(\pi) - \{b\}$, $c(\pi') = c(\pi)$ and

$$\pi'(x) = \begin{cases} \pi(a) \cup \pi(b) & \text{for } x = a, \\ \pi(x) & \text{for } x \in d(\pi') - \{a\}. \end{cases}$$

Then $\pi' \in \bar{P}(k)$ and if π' has the property $\alpha(k, n)$, then π has also the property $\alpha(k, n)$.

From this there follows Lemma.

3.4. Lemma. *Let m, n be positive integers greater than 1, $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be the canonical form of the integer m. Then the cyclic group of order m is an n-group if and only if $k\varrho n$.*

Proof. We can suppose that the cyclic group of order m is the additive group $\Gamma = \mathbf{Z}/m\mathbf{Z}$, where $\mathbf{Z}$ denotes the additive group of integers. Let f be the canonical homomorphism of $\mathbf{Z}$ onto Γ. Then for $M \subseteqq \mathbf{Z}$ the set $f(M)$ is a strong system of generators of Γ if and only if the g.c.d. of $M \cup \{m\}$ is 1. Then an element $\alpha \in f(M)$ is a necessary element of $f(M)$ if and only if there exists a prime p such that $p \mid m$, $p \nmid a$, where $a \in M$, $f(a) = \alpha$, and for each $b \in M$, $b \not\equiv a \pmod m$ the relation $p \mid b$ is satisfied.

I. First, we suppose that $k\varrho n$. Let $M \subseteqq \mathbf{Z}$, $f(M)$ be a strong system of generators of Γ, the integers from M be mutually incongruent mod m and let $f(S)$ be the set of necessary elements of $f(M)$, where $S \subseteqq M$.

Put $A = M - S$ and let P denote the set of all primes p with the properties: $p \mid m$, there exists $a \in A$ such that $p \,.\, a$ and $p \nmid s$ for each $s \in S$.

If $P = \emptyset$, the g.c.d. of $S \cup \{m\}$ is equal to 1, hence $f(S)$ is a strong system of generators of Γ.

Let $P \neq \emptyset$. Then card $P \leqq k$. For $a \in A$ put

$$\pi(a) = \{p \in P : p \nmid a\}.$$

Then $\pi \in P(k)$, $d(\pi) = A$, $c(\pi) = P$. Therefore there exist sets $A_1, \ldots, A_n \subseteqq A$ such that $\bigcap_{i=1}^{n} A_i = \emptyset$ and $\bigcup \pi(a)\ (a \in A_i) = P$ for each $1 \leqq i \leqq n$.

Put $N_i = f(A_i) \cup f(S)$ for $1 \leqq i \leqq n$. Then $N_i \subseteqq f(M)$ and $\bigcap_{i=1}^{n} N_i = f(S)$.

Since $\bigcup \pi(a)\ (a \in A_i) = P$, the g.c.d. of $A_i \cup S \cup \{m\}$ is equal to 1, thus N_i is a strong system of generators of Γ which implies that Γ is an n-group.

II. Assume that Γ is an n-group. Let $\pi \in P(k)$ injective.

We can suppose that $c(\pi) = P = \{p_1, \ldots, p_h\}$, where $1 \leqq h \leqq k$. Then we can consider $d(\pi) = A$ a subset of positive integers, where for $a \in A$ we have

$$a = \prod p(p \in P - \pi(a)).$$

(In case $P - \pi(a) = \emptyset$, under the mentioned product we understand the integer 1.)

The integers from A are mutually incongruent mod m and the g.c.d. of $(A - \{a\}) \cup \cup \{m\}$ is equal to 1 for each $a \in A$. Thus $f(A)$ is a strong system of generators of Γ whose set of necessary elements is empty.

Hence there exist $N_1, \ldots, N_n \subseteqq f(A)$ such that $f(1) \in L(N_i)\ (1 \leqq i \leqq n)$ and $\bigcap_{i=1}^{n} N_i = \emptyset$. Let $A_i \subseteqq A, f(A_i) = N_i$. Then $\bigcap_{i=1}^{n} A_i = \emptyset$ and the g.c.d. of $A_i \cup \{m\} = 1$, therefore for each $p \in P$ there exists $a \in A_i$ such that $p \in \pi(a)$. Then we have

$$\bigcup \pi(a)\ (a \in A_i) = \mathrm{P}$$

for each $1 \leqq i \leqq n$, hence $k\varrho n$ according to 3.2.

The Lemma is proved.

3.5. Lemma. *Let k, n be positive integers. Then*

$$k\varrho n \Leftrightarrow k < \frac{n(n+1)}{2}.$$

Proof. I. Suppose $k < \dfrac{n(n+1)}{2}$ and $\pi \in P(k)$ with the properties (1), (2) from 3.3. For $p \in c(\pi)$ set $f(p) = \{a, b\}$, where $a, b \in d(\pi)$, $a \neq b$, $p \in \pi(a) \cap \pi(b)$. Then f is a surjection of $c(\pi)$ onto the system of all two-elemented subsets of $d(\pi)$. Therefore

$$k \geqq \operatorname{card} c(\pi) \geqq \frac{m(m-1)}{2},$$

where $m = \text{card}\, d(\pi)$. Hence $n \geqq m$. Put

$$A_i = \begin{cases} d(\pi) - \{a_i\} & \text{for } 1 \leqq i \leqq m, \\ d(\pi) - \{a_m\} & \text{for } m \leqq i \leqq n, \end{cases}$$

where $d(\pi) = \{a_1, \ldots, a_m\}$. Then

$$\bigcap_{i=1}^{n} A_i = \emptyset \qquad \text{and} \qquad \bigcup \pi(a)\,(a \in A_i) = c(\pi)\,(1 \leqq i \leqq n).$$

From Lemma 3.3. we get $k \varrho n$.

II. Let $n \geqq 2$, $k \geqq \frac{n(n+1)}{2}$, P be a k-elemented set, A an $(n+1)$-elemented set and $\mathfrak{S}$ the system of all $(n-1)$-elemented subsets of A. Since card $\mathfrak{S} \leqq k$, there exists an injection p of $\mathfrak{S}$ into P. For $a \in A$ put

$$\pi(a) = \{p(X) : X \in \mathfrak{S}, a \notin X\} \cup (P -- p(\mathfrak{S})).$$

Then $\pi \in P(k)$, $d(\pi) = A$ and $c(\pi) = P$. If $B \subseteqq A$, card $B \leqq n - 1$, then for $X \in \mathfrak{S}$, $X \supseteqq B$ we have $p(X) \notin \bigcup \pi(a)\,(a \in B)$.

If $A_1, \ldots, A_n \subseteqq A$, card $A_i \geqq n(1 \leqq i \leqq n)$, then $\bigcap_{i=1}^{n} A_i \neq \emptyset$.

Therefore k non ϱn.

The Lemma is proved.

3.6. Theorem. *An infinite cyclic group is not an n-group for any positive integer n.*

A non-trivial cyclic group is a 1*-group if and only if it has order* 2.

A cyclic group of order m, where m is an integer > 1, *whose canonical form contains just k primes, is an n-group for an integer* $n > 1$ *if and only if*

$$k < \frac{n(n+1)}{2}.$$

Proof. Let γ be a generator of a cyclic group Γ of order m, where m is an integer > 2. Then there exists an integer $1 < x < m$ such that $(x, m) = 1$. The set $M = \{\gamma, x\gamma\}$ is a strong system of generators of Γ and the set of all necessary elements of M is empty. According to 2.3 the group Γ is not a 1-group.

On the other hand we obtain immediately from 2.3 that a cyclic group of order 2 is a 1-group.

The other parts of the Theorem follow from 2.5, 3.4 and 3.5.

REFERENCES

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

[2] Skula, L.: *Divisorentheorie einer Halbgruppe*, Math. Zeitschrift, 114 (1970), 113—120.

Skula L.
662 95 Brno, Janáčkovo nám. 2a
Czechoslovakia