Josef Zapletal

Distinguishing subsets of semi-groups and groups

Archivum Mathematicum, Vol. 4 (1968), No. 4, 241--251

Persistent URL: `http://dml.cz/dmlcz/104672`

DISTINGUISHING SUBSETS OF SEMI-GROUPS AND GROUPS

JOSEF ZAPLETAL

Received March 25, 1968

1. DEFINITIONS AND SYMBOLS

Let A be a non-void set. We shall call every finite sequence $x = x_1x_2 \dots x_n$ where $x_1, x_2, \dots, x_n \in A$ a string over A. We shall denote the void sequence by Λ, and the set of all strings by A^*. We shall call $| x | = | x_1x_2 \dots x_n | = n$ the length of the string x. The length $| \Lambda |$ of the void string is 0. We identify strings of the length 1 with elements of A.

We define an operation of binary composition $xy = x_1x_2 \dots x_ny_1y_2 \dots y_m$ for the strings $x = x_1x_2 \dots x_n$, $y = y_1y_2 \dots y_m$ where x_i, $y_j \in A$ for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, m$. For $x = \Lambda$, we put $\Lambda y = y\Lambda = y$. We write x^n instead of $\underbrace{x \dots . x}_{\text{n-times}}$.

The operation of binary composition is associative. We shall call the set A^* with the unit (neutral element) Λ together with the operation of binary composition a free monoid. (See [3], pages 3 and 18).

The language is intended to mean a free monoid A^* with an unary relation L in A^*. We shall denote the language as an ordered pair (A^*, L) where $L \subseteqq A^*$.

Let (A^*, L) be a language. Let $x \in A^*$, $y \in A^*$. Let $axb \in L$ be equivalent to $ayb \in L$ for each $a \in A^*$, $b \in A^*$. Then we put $x \underset{L}{\Xi} y$. The relation $\underset{L}{\Xi}$ is a congruence on the free monoid A^*.

2. ON NOVOTNÝ'S PROBLEM

Prof. M. Novotný put the following question:
Let A^* be a free monoid. Let Θ be a congruence on A^*. What property must Θ have in order that the language (A^*, L) might exist for which $\Theta = \underset{L}{\Xi}$ holds true?

2.1 Remark. *There exist such a set A and such a congruence Θ on A^* that $\Theta \neq \underset{L}{\Xi}$ for every subset $L \subseteqq A^*$.*

2.2 Example. Let $A = \{a, b, c\}$. Let $\{\Lambda\}, \{a\}, \{b\}, \{c\}, \pi = \{x \mid x \in A^*, |x| \geqq 2\}$ be the classes of the equivalence relation Θ on A^*. Then Θ is a congruence relation and $\Theta \neq \underset{L}{\Xi}$ for every $L \subseteqq A^*$.

Proof. We shall show that Θ is a congruence. Let $x \,\Theta\, y$. Let $u \in A^*$, $v \in A^*$. If $x = \Lambda$ then $y = \Lambda$ and clearly $uxv = uyv$ and hence $uxv \,\Theta\, uyv$. Let $x \neq \Lambda$, then $y \neq \Lambda$. It suffices to assume the case that at least one of the elements u, v is non-void. (If $u = v = \Lambda$, then $uxv = x$, $uyv = y$ implies $uxv \,\Theta\, uyv$). Then $|uxv| > 1$, $|uyv| > 1$ and hence $uxv \in \pi$, $uyv \in \pi$. We have $uxv \,\Theta\, uyv$.

We shall prove that $\Theta \neq \underset{L}{\Xi}$ for every $L \subseteqq A^*$. To prove that $\Theta \neq \underset{L}{\Xi}$ we assume conversely that there exists a set $L \subseteqq A^*$ such that $\Theta = \underset{L}{\Xi}$.

Let L contain at least two distinct elements of A^*, of the length 1 for instance a and b. Let $uav \in L$. If $u = v = \Lambda$ then $ubv = b \in L$ and conversely. In other cases $uav \in \pi$, and also $ubv \in \pi$. The strings uav and ubv belong simultaneously to L or to $A^* - L$. Therefore $a \underset{L}{\Xi} b$ and hence $a \,\Theta\, b$, which contradicts the assumption that $\{a\}$ and $\{b\}$ are classes.

Let L contain at most one element of A^* of the length 1. Then there exist two elements in A^*, for intance a and b which do not belong to L. The proof for $a \underset{L}{\Xi} b$ and hence $a \,\Theta\, b$, which contradicts the assumption that $\{a\}$ and $\{b\}$ are classes, is analogous.

2.3 Example. Let A be a finite set containing at least two elements. Let $L = \{x^2 \mid x \in A^*\}$. If $x \underset{L}{\Xi} y$ then $x = y$.

Proof. Let $x \underset{L}{\Xi} y$; we have $x^2 \in L$ and hence $\Lambda\, xx \in L$; therefore $yx = \Lambda\, yx \in L$. There exists an element $t \in A^*$ with the property $yx = t^2$.

Let $|x| = |y|$. Then $2\,|t| = |t^2| = |yx| = |y| + |x| = 2\,|x|$ and $|t| = |x| = |y|$. It follows $y = t = x$.

Let $|x| < |y|$. Then $2|x| < |y| + |x| = |yx| = |t^2| = 2|t|$ and $2|t| = |t^2| = |yx| = |y| + |x| < 2\,|y|$. Thus $|x| < |t| < |y|$. From the equation $yx = t^2$ there follows the existence of a string $u \neq \Lambda$ with the property $y = tu$, $t = ux$. It implies $y = uxu$. We choose an arbitrary $v \in A^*$, $v \neq u$, $|v| = |u|$. Clearly $vxvx \in L$. From $x \underset{L}{\Xi} y$ follows $vxvy \in L$. It implies the existence of an element $s \in A^*$ with the property $vxvx = s^2$. We have $2|s| = |s^2| = |vxvy| = |vxv| + |y| = |uxu| + |y| = |y| + |y| = 2|y|$ and $|s| = |y| = |vxv|$. Thus $vxv = s = y = uxu$. As we have $|v| = |u|$ it follows $v = u$ which is a contradiction with the assumption $v \neq u$. Thus the case $|x| < |y|$ is impossible and the assertion is proved.

2.4 Definition Let G be a semi-group, u, v elements in G. A mapping t

defined in G by the equation $t(x) = uxv$ is called a *translation determined by an ordered pair* (u, v). (See [1] page 297). Let T be the set of all translations in G, L a subset of G. We say that L *distinguishes* G if for any pair of distinct elements x, y in G there exists an element $t \in T$ such that $t(x) \in L$, $t(y) \bar{\in} L$ or conversely.

2.5 Remark. *Let Θ be any congruence relation of A^*. Consider the set A^*/Θ of all Θ — classes of A^* and denote by $\bar{x}(x \in A^*)$ the Θ — class including the element x. We define the operation of binary composition on the set A^*/Θ by the aid of the operation on A^*. We assign to every pair $\bar{x}$, $\bar{y} \in A^*/\Theta$ the Θ — class of A^* including the element xy; in symbols* $\bar{x}\bar{y} = \overline{xy}$. (See [7] page 170).

2.6 Theorem. *Let A^* be a free monoid, Θ a congruence on A^*. Then the following statements are equivalent:*

1. *There exists a subset $L \subseteq A^*$ such that $\Theta = \underset{L}{\Xi}$.*

2. *There exists a subset $\bar{L}$ in A^*/Θ such that A^*/Θ is distinguished by $\bar{L}$.*

Proof. Let (1) hold. From the assumptions $x \in L$, and $x \underset{L}{\Xi} y$ it follows that $\Lambda \,.\, x \,.\, \Lambda \in L$ hence $y = \Lambda \,.\, y \,.\, \Lambda \in L$ and hence $L = \bigcup_{x \in L} \bar{x}$ where $x \in \bar{x} \in A^*/\Theta$. Let us denote the set $\{\bar{x} \mid \bar{x} \in A^*/\Theta,\ \bar{x} \subseteq L\}$ by $\bar{L}$. Let $\bar{x} \in A^*/\Theta$ and $\bar{y} \in A^*/\Theta$ where $\bar{x} \neq \bar{y}$. Then for $x \in \bar{x}$, $y \in \bar{y}$ the formula $x\Theta y$ does not hold. (1) holds true, therefore $x \operatorname{non} \underset{L}{\Xi} y$. There exist $u \in A^*$, $v \in A^*$ such that $uxv \in L$, $uyv \bar{\in} L$ (or conversely). Since L contains with every element x from L the whole class $\bar{x} \in A^*/\Theta$ in which x lies too, $\bar{u}\bar{x}\bar{v} = \overline{uxv} \in \bar{L}$ follows from $uxv \in L$ and similarly $\bar{u}\bar{y}\bar{v} = \overline{uyv} \bar{\in} \bar{L}$ follows from $uyv \bar{\in} L$ (or conversely). Therefore A^*/Θ is distinguished by the set $\bar{L}$.

Suppose (2). Let us put $L = \bigcup B$, where $B \in \bar{L}$, and let $x \in A^*$, $y \in A^*$.

(α) We shall prove that $x\Theta y$ implies $x\underset{L}{\Xi}y$. Let $x\Theta y$; then $uxv\, \Theta\, uyv$ and hence $\overline{uxv} = \overline{uyv}$. If $uxv \in L$ we have $\overline{uxv} \subseteq L$ therefore also $\overline{uyv} \subseteq L$ and we obtain $uyv \in L$. Similarly if $uyv \in L$ we have $uxv \in L$. Hence $x\underset{L}{\Xi}y$.

(β) We shall prove that $x\underset{L}{\Xi}y$ implies $x\Theta y$. We shall carry out the proof (β) by the contradiction. Let us suppose that there exist x, $y \in A^*$ such that $x\underset{L}{\Xi}y$ but $x \operatorname{non} \Theta y$. According to (2) there exists a translation $t \in T$ such that $t(\bar{x}) \in \bar{L}$, $t(\bar{y}) \bar{\in} \bar{L}$ or conversely. Let the first case occur. There exist u, $v \in A^*/\Theta$ such that $t(\bar{x}) = \bar{u}\bar{x}\bar{v} = \overline{uxv}$, $t(\bar{y}) = \bar{u}\bar{y}\bar{v} = \overline{uyv}$ and it holds $\overline{uxv} \in \bar{L}$, $\overline{uyv} \in \bar{L}$. Let $u \in \bar{u}$, $v \in \bar{v}$ be

arbitrary. Consequently there is $uxv \in \overline{uxv} \in L$ and similarly $uyv \in \overline{uyv} \,\overline{\in}\, L$. Since $\overline{uxv} \subseteqq L$ and $\overline{uyv} \cap L = \emptyset$ it follows $uxv \in L$ and $uyv \,\overline{\in}\, L$. But this is the contradiction with the assumption $x \underset{L}{\Xi} y$. Hence it holds (β).
From (α) and (β) we shall get that (1) holds true.

2.7 Theorem. *Let L' be the complement of L in the free monoid A^*. Then $\underset{L}{\Xi} = \underset{L'}{\Xi}$.*

Proof. For $x, y \in A^*$ there holds $x \underset{L}{\Xi} y$ exactly when $uxv \in L$ is equivalent with $uyv \in L$ for arbitrary $u, v \in A^*$. Let be $uxv \in L'$. Let us suppose $uyv \,\overline{\in}\, L'$. Consequently $uyv \in L$ and that is the contradiction with the assumption $x \underset{L}{\Xi} y$.

2.8 Theorem. *Let A and B be semi-groups, L a subset in A. Let φ be a homomorphism of A onto B for which $\varphi^{-1}(\varphi(L)) = L$ holds true. Let L distinguish A. Then $\varphi(L)$ distinguishes B.*

Proof. Let $r, s \in B$, $r \neq s$, let us choose $x \in \varphi^{-1}(r)$, $y \in \varphi^{-1}(s)$ arbitrarily. It is $x \neq y$ and there exist $u, v \in A$ such that $uxv \in L$ and $uyv \,\overline{\in}\, L$ or conversely. It is $\varphi^{-1}(\varphi(L)) = L$ and therefore $\varphi(uxv) = \varphi(u) \,.\, r \,.\, \varphi(v) \in \varphi(L)$ and $\varphi(uyv) = \varphi(u)\, s\, \varphi(v) \,\overline{\in}\, \varphi(L)$ or conversely.

2.9 Remark. *The converse statement of the theorem 2.8 does not hold true.*

2.10 Example. Let A be additive semi-group of nonnegative integers. Let us denote by L the subset of even numbers. Let B be additive semi-group which has two elements 0 and 1 for which $1 + 1 = 0$. Let φ be a homomorphism of A onto B for which $\varphi(L) = 0$, $\varphi(L') = 1$. Then the subset $\varphi(L)$ distinguishes B, but L does not distinguish A.

Proof. It is sufficient to choose two arbitrary even numbers $a, b \in A$. For every translation $t \in T$ there holds $t(a) \in L$ if and only if $t(b) \in L$.

2.11 Definition. Let G be a semi-group, $I \subseteqq G$. We shall call the set I *an ideal of the semi-group G* when $ab \in I$ and $ba \in I$ hold for $a \in I$, $b \in G$. If I is a proper non-void subset in G, then we shall call I a *proper ideal*. The proper ideal which has at least two elements is called a *non-trivial ideal.*

2.12 Theorem. *Let G be a semi-group, I a non-trivial ideal in G. Then I does not distinguish G.*

Proof. The ideal I is non-trivial, it has hence at least two elements. Let $x, y \in I$, $x \neq y$. For all $u \in G$ there is $ux \in I$, $uy \in I$ and for all $v \in G$ there is $uxv \in I$, $uyv \in I$. For a chosen pair of the elements x, y there does not exist a translation $t \in T$ such that $t(x) \in I$, $t(y) \,\overline{\in}\, I$ or conversely. Thus I does not distinguish G.

2.13 Corollary. *Let G be a semi-group, L a subset in G. In order that L*

distinguishes G, there is necessary that neither L nor L' contain a non-trivial ideal.

2.14 Definition. (2°) A non-void subset R of a semigroup G is said to be a *normal complex,* if for arbitrary $u, v \in G$ and for arbitrary $x, y \in R$ always $uyv \in R$ follows from $uxv \in R$.

A normal complex is said to be *a non-trivial one,* if it contains at least two different elements.

2.15 Remark. *From the definition of the non-trivial complex there follows that it does not distinguish the semi-group G. It is sufficient to take $x, y \in R$, $x \neq y$.*

2.16 Theorem (2°) *Let G be a semi-group, R a subset in G. The following statements are equivalent.*

(1) *R is the normal complex.*

(2) *There exists a homomorphism φ of the semi-group G such that R is a complete counter image of one element at the homomorphism φ.*

2.17 Remark. *Let G be a group and H its normal divisor, then every class of the decomposition of the group G modulo H is a normal complex.*

2.18 Theorem. *Let G be a group, H its normal divisor containing at least two different elements. Then no class of the decomposition modulo H* (especially H) *distinguishes G.*

Proof. The statement follows from the remarks 2.15 and 2.17.

2.19 Theorem. (2°) *The semi-group G is a group if and only if it does not contain proper ideals.*

2.20 Remark. *Regarding the theorem* 2.12 *the condition for the distinguishing is not a sufficient condition.*

Proof. A group does not contain a non-trivial ideal. Let us put $L = aH$ where $a \in G$ and where H is a normal divisor containing at least two elements. According to the theorem 2.18 the set L does not distinguish G. Simultaneously, neither L nor L' contain a proper ideal.

2.21 Agreement. Let G be a semi-group, L a non-void proper subset in G. Let T be the set of all translations. For arbitrary $t \in T$ put $T_t^0 = \{x | x \in G, t(x) \in L\}$ and $T_t^1 = \{x | x \in G,\ t(x) \in G - L\}$. Let us denote by $G_t = \{T_t^\circ, T_t'\}$ the decomposition corresponding to the translation t and to the subset L. Let us denote by $\bar{G}_T = \bigwedge_{t \in T} \bar{G}_t$. the least common refinement of the decompositions $\bar{G}_t$, $t \in T$ (See [2]).

2.22 Theorem. *Let G be a semi-group, $L \subset G$ a subset. Then L distinguishes the semi-group G if and only if $\bar{G}_T$ is the least decomposition.*

Proof. Let $\bar{G}_T$ be the least decomposition. Consequently every class $\bar{G}_T$ contains exactly one element. Let $x, y \in G$, $x \neq y$. There exists

(2°) The definitions and statements see for example Ljapin [4].

$t_0 \in T$ such that $t_0(x) \in L$ and $t_0(y) \overline{\in} L$ (or conversely). The set L distinguishes G.

Let L distinguish G. Let $x, y \in G$, $x \neq y$. There exists $t_0 \in T$ such that $t_0(x) \in L$ and $t_0(y) \overline{\in} L$ (or conversely). The elements x, y are not in the same class of the decomposition $\bar{G}_T$.

3. EXAMPLES

3.1 Example. Let R be the multiplicative group of the positive rational numbers, $N \subset R$ the set of the natural numbers; then N distinguishes R.

Proof. Let $x, y \in R$, $x \neq y$. Without loss of generality it is possible to assume that $x > y$.

Let $x = \frac{p}{q}$, $y = \frac{p'}{q'}$. We put $u = 1$, $v = \frac{q}{p}$; then $uxv = 1 \cdot \frac{p}{q} \cdot \frac{q}{p} = 1 \in N$ and $uyv = 1 \cdot \frac{p'}{q'} \cdot \frac{q}{p} = \frac{p'}{q'} : \frac{p}{q} = \frac{y}{x} < 1$ and hence $uyv \overline{\in} N$.

3.2 Example. Let $G = \{a^0, a^1, a^2, a^3, a^4, a^5 = a^0\}$ be a cyclic group of the order 5. Let $L = \{a^2, a^3\}$. Then L distinguishes G.

Proof. The cyclic group is a commutative multiplicative group. The system of all translations T is determined by the elements a^0, a^1. a^2, a^3, a^4 indeed, $t(x) = uxv = uvx = a^k x$ for a suitable k. Let t_k be the translation determined by the element $a^k \in G$. Let G_{t_k} be the decomposition corresponding to the translation t_k, (k $= 0, 1, 2, 3, 4$).

We shall construct $\bar{G}_{t_k}$ corresponding to the subset L.

$$\begin{aligned}
\bar{G}_{t_0} &= \{T^0_{t_0} = \{a^2, a^3\}, \quad T^1_{t_0} = \{a^0, a^1, a^4\}\} \\
\bar{G}_{t_1} &= \{T^0_{t_1} = \{a^1, a^2\}, \quad T^1_{t_1} = \{a^0, a^3, a^4\}\} \\
\bar{G}_{t_2} &= \{T^0_{t_2} = \{a^0, a^1\}, \quad T^1_{t_2} = \{a^2, a^3, a^4\}\} \\
\bar{G}_{t_3} &= \{T^0_{t_3} = \{a^0, a^4\}, \quad T^1_{t_3} = \{a^1, a^2, a^3\}\} \\
\bar{G}_{t_4} &= \{T^0_{t_4} = \{a^3, a^4\}, \quad T^1_{t_4} = \{a^0, a^1, a^2\}\}
\end{aligned}$$

Let $\bar{G}_T = \bigwedge_{t_k \in T} \bar{G}_{t_k}$. Let us put $T^{i_0 i_1 i_2 i_3 i_4} = T^{i_0}_{t_0} \cap T^{i_1}_{t_1} \cap T^{i_2}_{t_2} \cap T^{i_3}_{t_3} \cap T^{i_4}_{t_4}$.

The non-void sets $T^{i_0 i_1 i_2 i_3 i_4}$ where i_k has the values zero and one for $k = 0, 1, 2, 3, 4$ are the classes of the decomposition $\bar{G}_T$. The exponents form a five-element sequence of the zeros and ones. The intersection of more than two sets $T^0_{t_k}$ is void. For the sequences $i_0 i_1 i_2 i_3 i_4$, which contain more than two zeros the sets $T^{i_0 i_1 i_2 i_3 i_4}$ are void. Similarly the sets $T^{i_0 i_1 i_2 i_3 i_4}$ whose sequences contain more than three ones are void. Therefore it is sufficient to consider the sequences containing exactly two zeros and the sets $T^{i_0 i_1 i_2 i_3 i_4}$ corresponding to them.

$$\begin{array}{ll} T^{00111} = \{a^2\} & T^{10101} = \emptyset \\ T^{01011} = \emptyset & T^{10110} = \emptyset \\ T^{01101} = \emptyset & T^{11001} = \{a^0\} \\ T^{01110} = \{a^3\} & T^{11010} = \emptyset \\ T^{10011} = \{a^1\} & T^{11100} = \{a^4\} \end{array}$$

$\bar{G}_T = \{\{a^0\}, \{a^1\}, \{a^2\}, \{a^3\}, \{a^4\}\}$. According to the theorem 2.21 the set L distinguishes G.

3.3 Example. Let G be a cyclic group of the order 9. Let $L = \{a^2, a^5, a^8\}$.

Then L does not distinguish G.

Proof. The set $H = \{a^0, a^3, a^6\}$ is a subgroup of the group G. Since G is cyclic, H is a normal divisor. But $L = a^2H$. Thus L is a class modulo H. According to the theorem 2.17 the set L does not distinguish G.

4. DISTINGUISHING SUBSETS OF GROUPS

4.1 Lemma. *Let G be a group, L a proper subset in G. Let x, y be elements in G. Then the following statements are equivalent.*

(1) For all u, v G the condition $uxv \in L$ is equivalent with $uyv \in L$.

(2) For all u, $v \in G$ the condition $ux^{-1}yv \in L$ is equivalent with $uv \in L$.

Proof. Let (1) hold. Let us now choose u_0, $v_0 \in G$ arbitrarily but fixed and further let us choose $u_1 = u_0x^{-1}$, $v_1 = v_0$. Then $u_0v_0 = u_0x^{-1}xv_0 = uxv \in L$ exactly when $u_0x^{-1}yv_0 = uyv \in L$. Hence $u_0x^{-1}yv_0 \in L$ is equivalent with $u_0v_0 \in L$ for all u_0, $v_0 \in G$, that means, there holds (2).

Similarly the statement (1) can be proved from the statement (2).

4.2 Remark. *In this paragraph we denote the unit of a group by 1.*

4.3 Lemma. *Let G be a group, L a proper subset in G. Then the following statement are equivalent.*

(1) *L does not distinguish G.*

(2) *There exists an element $z \in G$, $z \neq 1$ such that for all, u $v \in G$, $uv \in L$ is equivalent with $uzv \in L$.*

Proof. Let (1) hold. There exist x, $y \in G$ $x \neq y$ such that for all u, $v \in G$ there holds $uxv \in L$ exactly when $uyv \in L$. This is, however, according to lemma 4.1 equivalent with the statement, that $ux^{-1}yv \in L$ axactly when $uv \in L$. If we put $x^{-1}y = z$ in the last equivalence then $z \neq 1$ and we shall get (2).

Let (2) hold. Then the statement (1) follows directly from the definiton 2.4.

4.4 Definition. Let G be a group, L a proper subset in G, $z \neq 1$ an element in G. Let $uv \in L$ be equivalent with $uzv \in L$ for all $u, v \in G$. We shall denote by $Q(z)$ the cyclic group generated by the element z and we shall call it *the α-group of the set L in G.*

4.5 Lemma. *Let $Q(z)$ be an α-group of the set L in G. Then $L = \bigcup_{a \in L} aQ(z)$ holds true.*

Proof. Let $a \in L$. Let us denote $K = a^{-1}L$. Then $z^n \in K$ for all integers n.

Obviously $1 \in K$. We shall prove that $z^k \in K$ is equivalent with $z^{k+1} \in K$ For all $u, v \in G$ it holds true that $uv \in L$ is equivalent with $uzv \in L$. Let us put $u = a$, $v = 1$. We obtain that $a \in L$ is equivalent with $az \in L$ and hence $z \in K$. Let us denote the last equivalence by $(+)$. If $z^k \in K = a^{-1}L$ then $az^k \in L$. According to $(+)$ the relations $az^k \in L$, $az^kz \in L$ are equivalent. It is further $az^kz = az^{k+1} \in L$. The last relation is equivalent with $z^{k+1} \in a^{-1}L = K$. From the preceding equivalences we shall get that $z^k \in K$ is equivalent with $z^{k+1} \in K$. Considering that $z \in K$, there holds $z^n \in K$ for all integers.

It follows that $Q(z) \subseteqq K$, hence $aQ(z) \subseteqq L$. From this $\bigcup_{a \in L} aQ(z) \subseteqq L$. Since, however $a \in aQ(z)$ we have $\bigcup_{a \in L} aQ(z) = L$.

4.6 Definition. Let G be a group, L a non-void subset in G. Then we define the set $W(L) \subseteqq G$ as follows: $W(L) = \{z | z \in G$ with the property $uzv \in L$ if and only if $uv \in L$ for all $u, v \in G\}$.

4.7 Theorem. *Let G be a group, L a proper non-void subset in G. Then $W(L)$ is a normal divisor of the group G.*

Proof. I. We shall show that $W(L)$ is a subgroup of the group G.

α) From the definition of $W(L)$ follows that $1 \in W(L)$.

β) Let $z_1, z_2 \in W(L)$. We shall show that z_1z_2 belongs to $W(L)$. Since z_1 and z_2 belong $W(L)$ the relation $uv \in L$ for all $u, v \in G$ is equivalent with $uz_1v \in L$ and similarly $uv \in L$ is equivalent with $uz_2v \in L$. Now let us choose $u_0, v_0 \in G$ arbitrary but fixed and let us put further $u_1 = u_0$, $v_1 = z_2v_0$. Then it holds $u_0v_0 \in L$ if and only if $u_0z_2v_0 = u_1v_1 \in L$, which is equivalent with $u_0z_1z_2v_0 = u_1z_1v_1 \in L$. From this $uv \in L$ is equivalent with $uz_1z_2v \in L$ for all $u, v \in G$. Hence $z_1z_2 \in W(L)$.

γ) Let $z \in W(L)$. We shall show that z^{-1} is an element of $W(L)$. Since $z \in W(L)$, $uv \in L$ is equivalent with $uzv \in L$. Let us choose $u_0, v_0 \in G$ arbitrary but fixed and let us put $u_1 = u_0$, $v_1 = z^{-1}v_0$, Consequently it holds: $u_0v_0 = u_1zv_1 \in L$ exactly when $u_0z^{-1}v_0 = u_1v_1 \in L$. Hence $uv \in L$ is equivalent with $uz^{-1}v \in L$ for all $u, v \in G$. Hence $z^{-1} \in W(L)$.

II. We shal show that $W(L)$ is a normal divisor of the group G, that means, for $z \in W(L)$ and arbitrary element $a \in G$ there holds $aza^{-1} \in W(L)$. Let us choose $u_0, v_0 \in G$ arbitrary but fixed and let us choose further $u_1 = u_0a$ and $v = a^{-1}v_0$. Since there is $z \in W(L)$ and it holds $u_0v_0 = u_0a \,.\, a^{-1} = u_1v_1 \in L$ the relation $u_0v_0 \in L$ is equivalent with $u_1zv_1 = u_0(aza^{-1})\, v_0 \in L$. Hence $uv \in L$ is equivalent with $uaza^{-1}v \in L$ for all $u, v \in G$ and it holds $aza^{-1} \in W(L)$.

4.8 Theorem. *Let G be a group, L a proper non-void subset in G. Then* $L = \bigcup\limits_{a \in L} aW(L)$.

Proof. $W(L)$ is a normal divisor. We shall show that with the element a from the set L the whole class $aW(L)$ is a subset of L. Let $z \in W(L)$ and choose $a \in L$ arbitrarily, then $a \,.\, 1 \in L$ is equivalent with $a \,.\, z \,.\, 1 \in L$. Thus for all $z \in W(L)$ there is $az \in L$ and therefore $aW(L) \subseteqq L$. Hence $\bigcup\limits_{a \in L} aW(L) \subseteqq L$. Conversely if $a \in L$ then $a \in aW(L)$ so that $L \subseteqq \bigcup\limits_{a \in L} aW(L)$.

4.9 Definition. Let H be a normal divisor of a group G. We say that H is *a proper normal divisor* if $1 \neq H \neq G$ holds true.

4.10 Lemma. *Let H be a proper normal divisor of a group G. If $L = \bigcup\limits_{a \in L} aH$, then L does not distinguish G.*

Proof. We shall prove that for $h \in H$, $h \neq 1$ holds that $uv \in L$ is equivalent with $uhv \in L$. Let $uv \in L$ then $uvH \subseteqq L$ but $uvH = u(vH) = u(Hv)$ and hence $uhv \in uHv \subseteqq L$. Let $uhv \in L$ then $uv \in uvH = uHv = u(hH)v = uhvH \subseteqq L$.

4.11 Theorem. *Let G be a group, L a proper nonvoid subset in G. Then the following statements are equivalent:*

(1) *L does not distinguish G.*

(2) *There exists an α-group $Q(z)$ such that*

$$L = \bigcup_{a \in L} aQ(z).$$

(3) *There exists a proper normal divisor H such that*

$$L = \bigcup_{a \in L} aH.$$

Proof. Let (1) hold. According to the lemma 4.3 there exists an α-group $Q(z)$ generated by an element z, $z \neq 1$ for which according to the lemma 4.5 $L = \bigcup\limits_{a \in L} aQ(z)$ holds.

Let (2) hold. Then there exists the set $W(L) \neq \{1\}$ in G which is a normal divisor (theorem 4.7) with the property $L = \bigcup\limits_{a \in L} aW(L)$ (theorem

4.8). It is $L \neq G$ and thus also $W(L) \neq G$ because if $W(L) = G$ held true then $L = \bigcup_{a \in L} aW(L) = G$ would be. If we put $H = W(L)$ then holds (3).

Let (3) hold, then according to the lemma 4.10 the statement will hold.

4.12 Corollary. *If G is a simple group (containing no proper normal divisor), then an arbitrary proper non-void subset L of the group G distinguishes G.*

4.13 Corollary. *If G is a cyclic group of the prime number order, then every proper non-void subset L of the group G distinguishes G.*

4.14 Corollary. *Let G be a group, L a proper subset in G containing the unit. Let L contain no proper normal divisor of the group G. Then L distinguishes G.*

4.15. Corollary. *Let G be a group, L a proper nonvoid subset in G. Let L contain no class modulo a proper normal divisor of the group G. Then L distinguishes G.*

4.16 Theorem. *Let G be a group, L a proper non-void subset in G. Then $\mathscr{L} = \{aW(L) \mid a \in L\}$ distinguishes $G/W(L)$.*

Proof. We shall carry out the proof by the contradiction. Let $\mathscr{L}$ do not distinguish $G/W(L)$. Then there exist different elements $\bar{x} = xW(L)$, $\bar{y} = yW(L)$ in $G/W(L)$ such that the condition $\bar{u}\bar{x}\bar{v} \in \mathscr{L}$ is equivalent with $\bar{u}\bar{x}\bar{v} \in \mathscr{L}$ for all $\bar{u}$, $\bar{v} \in G/W(L)$. The relation $\bar{u}\bar{x}\bar{v} = uxv\, W(L) \in \mathscr{L}$ is equivalent with $uxv\, W(L) \subseteqq L$ according to the theorem 4.8. Hence $uxv \in L$. Conversely if $uxv \in L$ then $uxv\, W(L) \subseteqq L$ and this is equivalent with $\bar{u}\bar{x}\bar{v} = uxv\, W(L) \in \mathscr{L}$. We obtain that $\bar{u}\bar{x}\bar{v} = uxv\, W(L) \in \mathscr{L}$ is equivalent with $uxv \in L$. From the preceeding equivalences there follows that $uxv \in L$ is equivalent with $uyv \in L$. The last equivalence is, however, according to the lemma 4.1 equivalent with the statement $ux^{-1}yv \in L$ if and only if $uv \in L$. Then xy^{-1} is an element of $W(L)$ and it holds $xy^{-1}W(L) = W(L)$. It holds now that $yW(L) = W(L)y = (xy^{-1}W(L))\, y = x(y^{-1}W(L)\, y) = x(y^{-1}yW(L)) = xW(L)$. In this way we shall get the equality $\bar{x} = xW(L) = yW(L) = \bar{y}$. This is, however, the contradiction. Therefore $\mathscr{L}$ distinguishes the factor-group $G/W(L)$.

The results of the theorems 4.11 and 4.16 may be formulated as follows.

4.17 Theorem. *Let G be a group, L a proper non-void subset in G. Let L do not distinguish G. Then there exist a group G_1 and a homomorphism $\varphi : G \to G_1$ which is not an isomorphism such that $L = \varphi^{-1}[\varphi(L)]$ and $\varphi(L)$ distinguishes the group G_1.*

REFERENCES

[1] Birkhoff G., *Teorija struktur (Lattice theory)*, Moskva 1952.
[2] Borůvka O., *Grundlagen der Gruppoid und Gruppentheorie*, Berlin 1960.
[3] Chevalley C., *Fundamental Concepts of Algebra*, New York 1956.
[4] Ljapin E. S., *Polugruppy*, GIFML Moskva 1960.
[5] Novotný M., *Über endlich charakterisierbare Sprachen*, Publ. Fac. Sci. Univ. J. E. Purkyně, Brno (1965), No. 468, 495—502.
[6] Novotný M., *Bemerkung über ableitbare Sprachen*, 503—507.
[7] Szász G., *Introduction to Lattice Theory*, Budapest 1963.

Department of Mathematics
Technical University, Brno,
Hilleho 6