Czechoslovak Mathematical Journal

Jaroslav Ježek; Tomáš Kepka

Varieties of quasigroups determined by short strictly balanced identities

Czechoslovak Mathematical Journal, Vol. 29 (1979), No. 1, 84–96

Persistent URL: http://dml.cz/dmlcz/101580

Czechoslovak Mathematical Journal, 29 (104) 1979, Praha

VARIETIES OF QUASIGROUPS DETERMINED BY SHORT STRICTLY BALANCED IDENTITIES

JAROSLAV JEŽEK and TOMÁŠ KEPKA, Praha

(Received March 11, 1977)

In this paper we find all varieties of quasigroups determined by a set of strictly balanced identities of length $\leqq 6$ and study their properties. There are eleven such varieties: the variety of all quasigroups, the variety of commutative quasigroups, the variety of groups, the variety of abelian groups and, moreover, seven varieties which have not been studied in much detail until now. In Section 1 we describe these varieties. A survey of some significant properties of arbitrary varieties is given in Section 2; in Sections 3, 4 and 5 we assign these properties to the eleven varieties mentioned above and in Section 6 we give a table summarizing the results.

1. STRICTLY BALANCED QUASIGROUP IDENTITIES OF LENGTH $\leqq 6$

Quasigroups are considered as universal algebras with three binary operations $\cdot, /, \backslash$ (the class of all quasigroups is thus a variety).

A quasigroup term t (i.e. a formal expression consisting of variables and the three binary operation symbols $\cdot, /, \backslash$) is called balanced if every variable has at most one occurrence in t; it is called strictly balanced if it is balanced and contains neither $/$ nor $\backslash$. A quasigroup identity $t = s$ (i.e. a pair of quasigroup terms) is called balanced or strictly balanced, if the terms t, s are both balanced or strictly balanced, respectively, and contain the same variables. The length of a term t is the number of occurrences of variables in t. The length of an identity $t = s$ is the sum of the lengths of t and s. Evidently, the length of a balanced identity is an even number.

Consider the following identities:

(1) $x . yz = x . yz$, (7) $x . yz = xy . z$, (13) $xy . z = xy . z$,

(2) $x . yz = x . zy$, (8) $x . yz = yx . z$, (14) $xy . z = yx . z$,

(3) $x \,.\, yz = y \,.\, xz$, (9) $x \,.\, yz = xz \,.\, y$, (15) $xy \,.\, z = xz \,.\, y$,

(4) $x \,.\, yz = y \,.\, zx$, (10) $x \,.\, yz = zx \,.\, y$, (16) $xy \,.\, z = zx \,.\, y$,

(5) $x \,.\, yz = z \,.\, xy$, (11) $x \,.\, yz = yz \,.\, x$, (17) $xy \,.\, z = yz \,.\, x$,

(6) $x \,.\, yz = z \,.\, yx$, (12) $x \,.\, yz = zy \,.\, x$, (18) $xy \,.\, z = zy \,.\, x$.

For every $i = 1, 2, \ldots, 18$ we denote by $\mathscr{V}_i$ the variety of quasigroups determined by the identity (i).

1.1. Proposition. *Let $t = s$ be a strictly balanced quasigroup identity of length $\leqq 6$. Then the variety of quasigroups determined by $t = s$ is equal to some of the varieties $\mathscr{V}_1, \mathscr{V}_2, \ldots, \mathscr{V}_{18}$. If $i \in \{1, 2, \ldots, 6\}$ then $\mathscr{V}_{i+12}$ is the dual of $\mathscr{V}_i$.*

Proof. Obvious.

Now we define eleven significant varieties of quasigroups:

$\mathscr{R} = \mathscr{V}_1 = \mathrm{Mod}\,(x = x) =$ the variety of all quasigroups;
$\mathscr{C} = \mathscr{V}_2 = \mathrm{Mod}\,(xy = yx) =$ the variety of commutative quasigroups;
$\mathscr{G} = \mathscr{V}_7 = \mathrm{Mod}\,(x \,.\, yz = xy \,.\, z) =$ the variety of groups;
$\mathscr{A} = \mathscr{C} \cap \mathscr{G} =$ the variety of abelian groups;
$\mathscr{D}_1 = \mathscr{V}_3 = \mathrm{Mod}\,(x \,.\, yz = y \,.\, xz)$;
$\mathscr{D}_2 = \mathscr{V}_{15} = \mathrm{Mod}\,(xy \,.\, z = xz \,.\, y) =$ the dual of $\mathscr{D}_1$;
$\mathscr{E}_1 = \mathscr{V}_6 = \mathrm{Mod}\,(x.\, yz = z \,.\, yx)$;
$\mathscr{E}_2 = \mathscr{V}_{18} = \mathrm{Mod}\,(xy \,.\, z = zy \,.\, x) =$ the dual of $\mathscr{E}_1$;
$\mathscr{F}_1 = \mathscr{D}_1 \cap \mathscr{E}_2$;
$\mathscr{F}_2 = \mathscr{D}_2 \cap \mathscr{E}_1 =$ the dual of $\mathscr{F}_1$;
$\mathscr{H} = \mathscr{E}_1 \cap \mathscr{E}_2$.

1.2. Proposition. *The following relations hold*:

(i) $\mathscr{V}_1 = \mathscr{V}_{13} = \mathscr{R}$;
(ii) $\mathscr{V}_2 = \mathscr{V}_{11} = \mathscr{V}_{12} = \mathscr{V}_{14} = \mathscr{C}$;
(iii) $\mathscr{V}_4 = \mathscr{V}_5 = \mathscr{V}_8 = \mathscr{V}_9 = \mathscr{V}_{10} = \mathscr{V}_{16} = \mathscr{V}_{17} = \mathscr{A}$.

Proof. (i) is obvious. In (ii) only $\mathscr{V}_{12} = \mathscr{C}$ is not immediate. However, quasigroups from $\mathscr{V}_{12}$ satisfy $xx = x(x(x \setminus x)) = ((x \setminus x)\, x)\, x$, $x = (x \setminus x)\, x$, $yx = y((x \setminus x)\, x) = (x(x \setminus x))\, y = xy$. We are going to prove (iii).

If Q is a quasigroup from $\mathscr{V}_5$ and $a, b \in Q$, then $a = (a / b)\, b = (a / b)\,(b(b \setminus b)) = (b \setminus b)\,((a / b)\, b) = (b \setminus b)\, a$, so that $a / a = b \setminus b$ and Q has a unit element e. Thus $ab = e \,.\, ab = b \,.\, ea = ba$ and $Q \in \mathscr{C} \cap \mathscr{V}_5 = \mathscr{A}$.

Quasigroups from $\mathscr{V}_4$ satisfy $x \,.\, yz = y \,.\, zx$ and $y \,.\, zx = z \,.\, xy$, so that $\mathscr{V}_4 \subseteq \mathscr{V}_5 = \mathscr{A}$.

If Q is a quasigroup from $\mathscr{V}_8$ and $a, b \in Q$, then $ab = a((b \mathbin{/} b)\, b) = ((b \mathbin{/} b)\, a)\, b$, so that $a \mathbin{/} a = b \mathbin{/} b$ and Q contains a left unit e. In particular, $ab = e \,.\, ab = ae \,.\, b$ and e is a unit. Hence $ab = a \,.\, be = ba \,.\, e = ba$ and so $x \,.\, yz = xy \,.\, z$.

If $Q \in \mathscr{V}_9$ and $a, b \in Q$, then $a = (a \mathbin{/} b)\, b = (a \mathbin{/} b)\,((b \mathbin{/} b)\, b) = ((a \mathbin{/} b)\, b) \,.$ $.\, (b \mathbin{/} b) = a(b \mathbin{/} b)$, so that $a \setminus a = b \mathbin{/} b$ and Q contains a unit. Now we have $\mathscr{V}_9 \subseteq \mathscr{C}$ and $\mathscr{V}_9 \subseteq \mathscr{V}_4 = \mathscr{A}$.

If $Q \in \mathscr{V}_{10}$ and $a, b \in Q$, then $ab = a(b(b \setminus b)) = ((b \setminus b)\, a)\, b$, so that $a \mathbin{/} a =$ $= b \setminus b$ and Q contains a unit. Now $\mathscr{V}_{10} \subseteq \mathscr{C}$ and $\mathscr{V}_{10} \subseteq \mathscr{V}_4 = \mathscr{A}$.

The varieties $\mathscr{V}_{16}$ and $\mathscr{V}_{17}$ are dual to $\mathscr{V}_4$ and $\mathscr{V}_5$ and thus also equal to $\mathscr{A}$.

1.3. Proposition. *The following conditions are equivalent for a quasigroup Q:*

(i) $Q \in \mathscr{D}_1$ ($Q \in \mathscr{D}_2$, *respectively*).

(ii) *There exists an abelian group $Q(+)$ and a permutation p of the set Q such that $p(0) = 0$ and $ab = p(a) + b$ for all $a, b \in Q$ ($ab = a + p(b)$ for all $a, b \in Q$, respectively).*

Proof. See Theorem 13 of [8].

1.4. Proposition. *The following conditions are equivalent for a quasigroup Q:*

(i) $Q \in \mathscr{E}_1$ ($Q \in \mathscr{E}_2$, *respectively*).

(ii) *There exists an abelian group $Q(+)$, its automorphism f and an element $g \in Q$ such that $ab = f^2(a) + f(b) + g$ for all $a, b \in Q$ ($ab = f(a) + f^2(b) + g$ for all $a, b \in Q$, respectively).*

Proof. See Theorems 17 and 18 of [12].

1.5. Proposition. *The following conditions are equivalent for a quasigroup Q:*

(i) $Q \in \mathscr{F}_1$ ($Q \in \mathscr{F}_2$, *respectively*).

(ii) *There exists an abelian group $Q(+)$ and its automorphism f such that $f^2 = \mathrm{id}_Q$ and $ab = f(a) + b$ for all $a, b \in Q$ ($ab = a + f(b)$ for all $a, b \in Q$, respectively).*

Proof. It is an easy combination of 1.3 and 1.4.

1.6. Proposition. *The following conditions are equivalent for a quasigroup Q:*

(i) $Q \in \mathscr{H}$.

(ii) *There exists an abelian group $Q(+)$, its automorphism f and an element $g \in Q$ such that $f^3 = \mathrm{id}_Q$ and $ab = f^2(a) + f(b) + g$ for all $a, b \in Q$.*

Proof. Apply 1.4.

1.7. Proposition. *We have* $\mathscr{C} \cap \mathscr{G} = \mathscr{C} \cap \mathscr{D}_1 = \mathscr{C} \cap \mathscr{D}_2 = \mathscr{C} \cap \mathscr{E}_1 = \mathscr{C} \cap \mathscr{E}_2 =$ $= \mathscr{G} \cap \mathscr{D}_1 = \mathscr{G} \cap \mathscr{D}_2 = \mathscr{G} \cap \mathscr{E}_1 = \mathscr{G} \cap \mathscr{E}_2 = \mathscr{D}_1 \cap \mathscr{D}_2 = \mathscr{D}_1 \cap \mathscr{E}_1 = \mathscr{D}_2 \cap \mathscr{E}_2 =$ $= \mathscr{A}$.

Proof. Some equalities are obvious and the rest follows from 1.3.

1.8. Theorem. *Every quasigroup variety determined by a set of strictly balanced identites of length* $\leqq 6$ *is equal to one of the varieties* $\mathcal{R}, \mathcal{C}, \mathcal{G}, \mathcal{A}, \mathcal{D}_1, \mathcal{D}_2, \mathcal{E}_1, \mathcal{E}_2, \mathcal{F}_1, \mathcal{F}_2, \mathcal{H}$. *These eleven varieties are pairwise different. If* V *is any of them, then* $A \subseteq V \subseteq \mathcal{R}$. *Moreover,* $\mathcal{F}_1 \subset \mathcal{D}_1$, $\mathcal{F}_1 \subset \mathcal{E}_2$, $\mathcal{F}_2 \subset \mathcal{D}_2$, $\mathcal{F}_2 \subset \mathcal{E}_1$, $\mathcal{H} \subset \mathcal{E}_1$, $\mathcal{H} \subset \mathcal{E}_2$ *and there are no other non-trivial inclusions.*

Proof. It follows from the above results.

2. PROPERTIES OF VARIETIES

Let V be a variety of universal algebras. (The similarity type is considered to be finitary but not necessarily finite or countable; all agebras are considered to be non-empty.) We shall consider the following conditions on V:

SAP (strong amalgamation property): If $A, B, C \in V$, $A = B \cap C$ and A is a subalgebra of both B, C, then there exists an algebra $D \in V$ such that both B, C are subalgebras of D.

EXT (extensivity): For every two algebras $A, B \in V$ there exists an algebra $C \in V$ and two monomorphisms $f : A \to C$, $g : B \to C$.

IDE Every algebra from V contains an idempotent, i.e. an element a such that the one-element set $\{a\}$ is a subalgebra.

CEP (congruence extension property): If r is a congruence of a subalgebra A of an algebra $B \in V$, then there exists a congruence s of B such that $r = s \cap (A \times A)$.

RSM (residual smallness): There exists only a set of non-isomorphic subdirectly irreducible algebras from V.

FEP (finite embeddability property): If $A \in V$, then for any finite subset B of A there exists a finite algebra $C \in V$ and an injective homomorphism of B (considered as a partial algebra) into C.

SFG Subalgebras of finitely generated algebras from V are finitely generated.

EFG Every countable algebra from V can be embedded into a finitely generated algebra from V.

SBL Every subalgebra of an algebra $A \in V$ is a block of a congruence of A.

SCH (Schreier property): Every non-trivial subalgebra of a V-free algebra is V-free.

If V is a variety of quasigroups, then we shall be concerned, moreover, with the following two conditions on V:

NCP (normal congruences property): If $Q(\cdot, /, \backslash) \in V$ and if r is a congruence of the groupoid $Q(\cdot)$, then r is a congruence of the quasigroup $Q(\cdot, /, \backslash)$.

GCC If $Q(\cdot, /, \backslash) \in V$ and if r, s are two congruences of the groupoid $Q(\cdot)$, then $r \circ s = s \circ r$.

Let V be a variety of universal algebras and K a class of algebras. If there exists a set $M \subseteq V \cap K$ such that every algebra from $V \cap K$ is isomorphic to precisely one algebra from M, then we say that V has few K-algebras and put $\nu(K, V) = \langle \alpha, \beta \rangle$ where α is the cardinality of M and β is the smallest cardinal number such that no algebra of cardinality $\geqq \beta$ belongs to $V \cap K$. If V is non-trivial and every algebra from V is isomorphic to a subalgebra of an algebra from $V \cap K$, then we say that V has enough K-algebras and write $\nu(K, V) = \text{en}$. Finally, if V has neither few nor enough K-algebras, we write $\nu(K, V) = \text{pr}$. We shall be concerned with the determination of $\nu(\text{Sim}, V)$ and $\nu(\text{Sir}, V)$; here Sim is the class of simple algebras and Sir is the class of subdirectly irreducible algebras. A variety is residually small iff it has few subdirectly irreducible algebras.

For every variety V we denote by $v(V)$ the cardinality of the set of subvarieties of V and by $m(V)$ the cardinality of the set of minimal subvarieties of V.

In the following sections we shall be concerned with varieties of quasigroups determined by strictly balanced identities of length $\leqq 6$ and for every such variety V we shall try to decide which of the above twelve conditions are satisfied by V and, moreover, to describe $\nu(\text{Sim}, V)$, $\nu(\text{Sir}, V)$, $v(V)$ and $m(V)$.

2.1. Lemma. *Let V be a non-trivial variety. Then:*

(i) *V has enough simple algebras iff for every $A \in V$ and every triple a, b, c of pairwise different elements of A there exists an algebra $B \in V$ such that A is a subalgebra of B and $\langle a, c \rangle$ belongs to the congruence generated in B by $\langle a, b \rangle$.*

(ii) *If V has enough simple algebras then it has neither* CEP *nor* SBL.

(iii) *If the similarity type of V is finite and V has* EFG, *then it does not have* SFG.

(iv) *V is extensive iff every algebra $A \in V$ can be embedded into an algebra $B \in V$ having an idempotent.*

(v) IDE *implies* EXT.

Proof. It is well-known and easy

2.2. Lemma. *Let V be a variety of quasigroups. If V satisfies* NCP, *then it satisfies* GCC.

Proof. It is easy.

Let V be a variety of universal algebras. Then V^* denotes the variety of pointed V-algebras, i.e. of V-algebras with an added nullary operation. Thus elements of V^* are algebras $A(f_1, f_2, \ldots, u)$ such that $A(f_1, f_2, \ldots) \in V$ and u is an element of A.

2.3. Lemma. *Let V be a variety. Then:*

(i) *If P is one of the properties* SAP, CEP, RSM, FEP, SFG, EFG, SBL *then V has P iff V^* has P.*

(ii) *If K is either* Sim *or* Sir, *then* $v(K, V) = \mathrm{en} \Leftrightarrow v(K, V^*) = \mathrm{en}$ *and* $v(K, V) = \mathrm{pr} \Leftrightarrow v(K, V^*) = \mathrm{pr}$; *if* $v(K, V) = \langle \alpha, \beta \rangle$ *and* $v(K, V^*) = \langle \gamma, \delta \rangle$ *then* $\beta = \delta$.

Proof. It is easy.

3. THE VARIETIES $\mathscr{R}$, $\mathscr{C}$, $\mathscr{G}$, $\mathscr{A}$

3.1. Theorem. *The varieties $\mathscr{R}$ and $\mathscr{C}$ have the properties* SAP, EXT, FEP, EFG, SCH. *They do not have the properties* IDE, CEP, RSM, SFG, SBL, NCP, GCC. *We have* $v(\mathrm{Sim}, \mathscr{R}) = v(\mathrm{Sim}, \mathscr{C}) = v(\mathrm{Sir}, \mathscr{R}) = v(\mathrm{Sir}, \mathscr{C}) = \mathrm{en}$ *and* $\upsilon(\mathscr{R}) = \upsilon(\mathscr{C}) = m(\mathscr{R}) = m(\mathscr{C}) = 2^{\aleph_0}$.

Proof. It can be easily proved (see also [4]) that every halfquasigroup can be embedded into a quasigroup and every commutative halfquasigroup can be embedded into a commutative quasigroup. (By a halfquasigroup we mean a partial groupoid G such that if $a, b, c \in G$, ab and ac are defined and $ab = ac$ then $b = c$ and if ba and ca are defined and $ba = ca$ then $b = c$.) From this SAP, EXT, $v(\mathrm{Sim}, \mathscr{R}) = v(\mathrm{Sim}, \mathscr{C}) = \mathrm{en}$ follow. (The fact that the variety of all quasigroups has enough simple members was proved by many authors, see e.g. [9]; almost every proof of this case can be adopted for $\mathscr{C}$ as well.) FEP is easy. The validity of EFG and SCH is proved in [4] (Theorems I.2.4, I.2.8) for $\mathscr{R}$; the proofs for $\mathscr{C}$ are in fact the same. By 2.1, $\mathscr{R}$ and $\mathscr{C}$ do not have CEP, SFG and SBL; evidently they do not have IDE, RSM. In [14] a commutative quasigroup with two noncommuting groupoid congruences is constructed. Hence $\mathscr{R}$, $\mathscr{C}$ do not satisfy GCC and by 2.2 they do not satisfy NCP. It is proved in [2] that there are uncountably many minimal varieties of totally symmetric quasigroups; hence $m(\mathscr{C}) = 2^{\aleph_0}$.

3.2. Theorem. *The variety $\mathscr{G}$ has the properties* SAP, EXT, IDE, EFG, SCH, NCP, GCC; *it does not have the properties* CEP, RSM, FEP, SFG, SBL. *We have* $v(\mathrm{Sim}, \mathscr{G}) = v(\mathrm{Sir}, \mathscr{G}) = \mathrm{en}$, $\upsilon(\mathscr{G}) = 2^{\aleph_0}$ *and* $m(\mathscr{G}) = \aleph_0$.

Proof. Since every group has a unit, $\mathscr{G}$ has IDE and EXT. The validity of SAP, SCH and EFG is well-known (see [10], paragraphs 35, 36, 38). The properties NCP and GCC follow from the fact that every group is an inverse property quasigroup. $v(\mathrm{Sim}, \mathscr{G}) = \mathrm{en}$ is well-known; it follows for example from some results of [7]. Hence $v(\mathrm{Sir}, \mathscr{G}) = \mathrm{en}$ as well and $\mathscr{G}$ does not have RSM. It follows from 2.1 that $\mathscr{G}$ does not have CEP, SFG, SBL. It does not have FEP (see [5]). $\upsilon(\mathscr{G}) = 2^{\aleph_0}$ is proved in [13] and [15] and $m(\mathscr{G}) = \aleph_0$ is easy and well-known.

3.3. Theorem. *The variety $\mathscr{A}$ has the properties* SAP, EXT, IDE, CEP, RSM, FEP, SFG, SBL, SCH, NCP, GCC; *it does not have the property* EFG. *We have* $v(\mathrm{Sim}, \mathscr{A}) = \langle \aleph_0, \aleph_0 \rangle$, $v(\mathrm{Sir}, \mathscr{A}) = \langle \aleph_0, \aleph_1 \rangle$ *and* $\upsilon(\mathscr{A}) = m(\mathscr{A}) = \aleph_0$.

Proof. An abelian group is subdirectly irreducible or simple iff it is isomorphic to $C(p^n)$ for some prime p and $0 \leqq n \leqq \infty$ or $0 \leqq n \leqq 1$, respectively; here $C(p^n)$ is the cyclic group of order p^n if $n < \infty$ and $C(p^\infty)$ is the quasicyclic Prüfer p-group. This implies $\nu(\mathrm{Sim}, \mathscr{A}) = \langle \aleph_0, \aleph_0 \rangle$ and $\nu(\mathrm{Sir}, \mathscr{A}) = \langle \aleph_0, \aleph_1 \rangle$. For the rest the reader is referred to an arbitrary text-book on abelian groups.

4. THE VARIETY $\mathscr{D}_1$

In this section we shall establish various properties of the variety $\mathscr{D}_1$, i.e. the variety of quasigroups determined by $x \,.\, yz = y \,.\, xz$. However, it will be convenient to formulate and prove the results not in terms of $\mathscr{D}_1$ but in terms of an equivalent variety, denoted by $\mathscr{K}$.

Let $\mathscr{K}$ denote the variety of algebras $A(+, 0, -, p, p^{-1})$ with one binary, one nullary and three unary operations determined by

$$(x + y) + z = x + (y + z)\,,$$

$$x + y = y + x\,,$$

$$-x + x = 0\,,$$

$$0 + x = x\,,$$

$$p(p^{-1}(x)) = p^{-1}(p(x)) = x\,,$$

$$p(0) = 0\,.$$

Algebras from $\mathscr{K}$ are abelian groups with a permutation p such that $p(0) = 0$.

4.1. Proposition. *The varieties $\mathscr{D}_1$ and $\mathscr{K}$ are equivalent, i.e. there exists a one-to-one correspondence between $\mathscr{D}_1$ and $\mathscr{K}$ preserving underlying sets and homomorphisms. If $A(+, 0, -, p, p^{-1}) \in \mathscr{K}$ then the corresponding quasigroup $Q(\cdot, /, \backslash) \in \mathscr{D}_1$ is defined by $Q = A$ and $xy = p(x) + y$. If $Q(\cdot, /, \backslash) \in \mathscr{D}_1$ then the corresponding algebra $A(+, 0, -, p, p^{-1}) \in \mathscr{K}$ is defined by $0 = x\backslash x$, $x + y = (x / 0)\, y$, $p(x) = x \,.\, 0$.*

Proof. It follows easily from 1.3.

4.2. Proposition. *Every at most countable algebra from $\mathscr{K}$ can be embedded into a cyclic algebra from $\mathscr{K}$; every finite algebra from $\mathscr{K}$ can be embedded into a finite cyclic algebra from $\mathscr{K}$.*

Proof. Let $A(+, 0, -, p, p^{-1}) \in \mathscr{K}$ be at most countable. Denote by $C(+, 0, -)$ the cylic group of the same cardinality as A and by $i \mapsto a_i$ a one-to-one mapping of C onto A. Denote by $D(+, 0, -)$ the cyclic group with two elements 0, 1 and put

$B(+, 0, -) = C(+, 0, -) \times D(+, 0, -)$. Define a permutation q on B as follows: $q(a_i, 0) = \langle p(a_i), 0\rangle$; $q(a_i, 1) = \langle a_{i+1}, 1\rangle$. The algebra $B(+, 0, -, q, q^{-1})$ is cyclic (it is generated by $\langle 0, 1\rangle$), belongs to $\mathscr{K}$ and contains a subalgebra isomorphic to $A(+, 0, -, p, p^{-1})$; it is finite if A is finite.

4.3. Proposition. *The variety $\mathscr{K}$ has enough simple algebras; every finite algebra from $\mathscr{K}$ can be embedded into a finite simple algebra from $\mathscr{K}$.*

Proof. To prove that $\mathscr{K}$ has enough simple algebras, it suffices to show that if $A(+, 0, -, p, p^{-1}) \in \mathscr{K}$ and if a, b, c are three different elements of A, then there exists an algebra $B(+, 0, -, q, q^{-1}) \in \mathscr{K}$ containing $A(+, 0, -, p, p^{-1})$ as a subalgebra and such that $\langle a, c\rangle$ belongs to the congruence generated in B by $\langle a, b\rangle$. Of course, $A(+, 0, -)$ is a proper subgroup of an abelian group $B(+, 0, -)$. Let $d \in B \setminus A$. Evidently, $d + a$, $d + b$, $d + c$ are three different elements of $B \setminus A$. Define a permutation q on B as follows: $p \subseteq q$; $q(d + b) = d + c$; $q(d + c) = d + b$; $q(u) = u$ for all $u \in B \setminus (A \cup \{d + b, d + c\})$. Evidently, $B(+, 0, -, q, q^{-1})$ has the required property.

Now let $A(+, 0, -, p, p^{-1}) \in \mathscr{K}$ be finite. Evidently, there exists an abelian group $B(+, 0, -)$ containing $A(+, 0, -)$ as a subgroup such that $\mathrm{Card}(B \setminus A) > \mathrm{Card}(A) + 1$. Let $b_0, b_1, \ldots, b_n$ be the elements of $B \setminus A$. Define a permutation q of B as follows: $p \subseteq q$; $q(b_0) = b_0$; $q(b_i) = b_{i+1}$ for $i = 1, \ldots, n - 1$; $q(b_n) = b_1$. Suppose that $\sim$ is a congruence of $B(+, -, 0, q, q^{-1})$ different from id_B. Then $b_0 \sim a$ for some $a \neq b_0$. If $a = b_i$ for some $i = 1, \ldots, n$, then $b_0 = q^m(b_0) \sim q^m(b_i)$ for all m, so that $B \setminus A$ is contained in a block of $\sim$ and thus $\sim\; = B \times B$. If $a \in A \setminus \{0\}$, then $0 = a - a \sim b_0 - a = b_i$ for some $i \in \{1, \ldots, n\}$ and similarly as above we see $\sim\; = B \times B$. Finally, let $\{0, b_0\}$ be a block of $\sim$. Then every block of $\sim$ has exactly two elements; a certain block is contained in $\{b_1, \ldots, b_n\}$ and thus by the definition of q on $\{b_1, \ldots, b_n\}$ every b_i ($i = 1, \ldots, n$) is congruent to some b_j with $j \neq i$; now it is easy to see that if $a \in A \setminus \{0\}$ then $\{a\}$ is a block, a contradiction.

4.4. Proposition. *The variety $\mathscr{K}$ has uncountably many minimal subvarieties. Moreover, if $n \geqq 2$, then the variety $\mathscr{K}_n$ of algebras from $\mathscr{K}$ satisfying $p^n(x) = x$ has uncountably many minimal subvarieties.*

Proof. We shall prove that $\mathscr{K}_2$ has uncountably many minimal subvarieties; the proof for $n \geqq 3$ is analogous. Let N be the set of positive integers. For every subset S of N let V_S denote the subvariety of $\mathscr{K}_2$ determined by the following identities:

$$p(7^n \,.\, p(3x)) = 2 \,.\, 7^n \,.\, p(3x) \quad \text{for } n \in S\,,$$

$$p(11^n \,.\, p(3x)) = 2 \,.\, 11^n \,.\, p(3x) \quad \text{for } n \in S\,,$$

$$p(7^m \,.\, p(3x)) = 7^m \,.\, p(3x) \quad \text{for } m \in N \setminus S\,,$$

$$p(11^m \,.\, p(3x)) = 11^m \,.\, p(3x) \quad \text{for } m \in N \setminus S\,,$$

$$
\begin{aligned}
p(7^n\ .\ p(5x)) &= 2\ .\ 7^n\ .\ p(5x) && \text{for} \quad n \in S\,,\\
p(11^n\ .\ p(5x)) &= 2\ .\ 11^n\ .\ p(5x) && \text{for} \quad n \in S\,,\\
p(7^m\ .\ p(5x)) &= 7^m\ .\ p(5x) && \text{for} \quad m \in N \setminus S\,,\\
p(11^m\ .\ p(5x)) &= 11^m\ .\ p(5x) && \text{for} \quad m \in N \setminus S\,.
\end{aligned}
$$

Let us prove first that if S, T are two different subsets of N, then the variety $V_S \cap V_T$ is trivial. Suppose that there is an $n \in T \setminus S$ (the other case is similar). Let $A \in V_S \cap \cap V_T$. We have $p(7^n\ .\ p(3a)) = 2\ .\ 7^n\ .\ p(3a)$ for every $a \in A$ since $A \in V_T$. On the other hand, $p(7^n\ .\ p(3a)) = 7^n\ .\ p(3a)$ since $A \in V_S$. Hence $7^n\ .\ p(3a) = 0$ for every $a \in A$. Similarly $11^n\ .\ p(3a) = 0$ and consequently $p(3a) = 0$, so that $3a = 0$ for every $a \in A$. Similarly $5a = 0$ and thus $a = 0$ for every $a \in A$.

Since every non-trivial variety contains at least one minimal subvariety, the proof will be complete if we prove that the variety V_S is non-trivial for any subset S of N. Let $Z(+, 0, -)$ be the additive group of integers and $A = (3Z \cup 5Z) \setminus \{0\}$. Denote by B the set of prime numbers $p \in Z$ such that $p \geqq 12$ and put $C = \bigcup_{n \in S} 7^n B \cup \bigcup_{n \in S} 11^n B$. The sets A and B are countably infinite and $A \cap B = \emptyset$. Hence there exists a one-to-one mapping f of A onto B. Further we put $D = 2C$ and $E = Z \setminus (A \cup B \cup C \cup D)$. It is easy to see that $A \cap B = A \cap C = B \cap C = C \cap D = A \cap D = B \cap D = \emptyset$ and $0 \in E$. We shall define a mapping p of Z into Z as follows:

$$
\begin{aligned}
&p(a) = f(a) \quad \text{for every} \quad a \in A\,;\\
&p(b) = f^{-1}(b) \quad \text{for every} \quad b \in B\,;\\
&p(c) = 2c \quad \text{and} \quad p(2c) = c \quad \text{for every} \quad c \in C\,;\\
&p(e) = e \quad \text{for every} \quad e \in E\,.
\end{aligned}
$$

As one may check easily, $p^2 = \mathrm{id}_Z$ and $Z(+, 0, -, p, p) \in V_S$.

4.5. Theorem. *The variety* $\mathcal{D}_1$ *has the properties* SAP, EXT, IDE, FEP, EFG, SCH, GCC; *it does not have* CEP, RSM, SFG, SBL, NCP. *We have* $v(\mathrm{Sim}, \mathcal{D}_1) = v(\mathrm{Sir}, \mathcal{D}_1) = \mathrm{en}$ *and* $v(\mathcal{D}_1) = m(\mathcal{D}_1) = 2^{\aleph_0}$.

Proof. Since the variety of abelian groups has SAP, EXT, IDE, FEP, it is easy to see that $\mathcal{K}$ has them as well; but then $\mathcal{D}_1$ has also these properties. EFG follows from 4.2. For SCH see [1]. $v(\mathrm{Sim}, \mathcal{D}_1) = \mathrm{en}$ follows from 4.3 and $m(\mathcal{D}_1) = 2^{\aleph_0}$ from 4.4. By 2.1, $\mathcal{D}_1$ does not have CEP, SFG, SBL. Now it is enough to prove that $\mathcal{D}_1$ has GCC and does not have NCP.

Let $Q(\cdot, /, \backslash) \in \mathcal{D}_1$ and let $Q(+, 0, -, p, p^{-1})$ be the corresponding algebra from $\mathcal{K}$, so that $xy = p(x) + y$ for all $x, y \in Q$. Let r be a congruence of $Q(\cdot)$. If $\langle a, b\rangle \in r$ and $c \in Q$ then $\langle c + a, c + b\rangle = \langle p^{-1}(c)\ .\ a, p^{-1}(c)\ .\ b\rangle \in r$. Thus every congruence of $Q(\cdot)$ is a congruence of $Q(+)$ and, of course, every two congruences of $Q(+)$ commute.

Define a quasigroup $Q(\circ, /, \backslash)$ as follows: Q is the set of rational numbers; $a \circ b = 2a + b$; $a / b = \frac{1}{2}(a - b)$; $a \backslash b = b - 2a$. One may check easily that $Q(\circ, /, \backslash) \in \mathscr{D}_1$. Define a relation r on Q by $\langle a, b\rangle \in r$ iff $a - b$ is an integer. It is easy to see that r is a congruence of $Q(\circ)$. However, $\langle 2, 1\rangle \in r$ and $\langle 2/0, 1/0\rangle \notin r$, so that r is not a congruence of $Q(\circ, /, \backslash)$.

5. THE VARIETIES $\mathscr{E}_1, \mathscr{F}_1$ AND $\mathscr{H}$

It follows from 1.4 that $\mathscr{E}_1$, $\mathscr{F}_1$, $\mathscr{H}$ are varieties of medial quasigroups, i.e. quasigroups satisfying $xy \,.\, zu = xz \,.\, yu$. Varieties of medial quasigroups were studied in [6] (medial quasigroups are called abelian there) and so in proving various properties of the varieties $\mathscr{E}_1$, $\mathscr{F}_1$, $\mathscr{H}$ we shall exploit the results from [6] as well as the terminology introduced there. The reader is supposed to be acquainted with [6].

Let a ring R with unit and two elements $\alpha, \beta \in R$ be given. We shall say that α, β are i-generators of R if they are invertible and R is generated as a ring by α, β, α^{-1}, β^{-1}. A quasigroup $Q(., /, \backslash)$ is called an (R, α, β)-quasigroup if there exists an R-module $Q(+, rx)$ and an element $h \in Q$ with $ab = \alpha a + \beta b + h$ for all $a, b \in Q$. Given a ring R and its i-generators α, β, the class of all (R, α, β)-quasigroups is a variety; it is denoted by $\mathscr{P}(R, \alpha, \beta)$.

Let us denote by A_1 the free abelian group with one free generator a, by Z the ring of integers and by ZA_1 the corresponding group-ring. Let $\mathscr{M}$ denote the variety of ZA_1-modules.

5.1. Proposition. *ZA_1 is a commutative noetherian domain which is i-generated by a^2, a. We have $\mathscr{E}_1 = \mathscr{P}(ZA_1, a^2, a)$ and the varieties $\mathscr{E}_1^*$ and $\mathscr{M}^*$ are equivalent.*

Proof. See 1.4 and Proposition 5.5 of [6].

5.2. Theorem. *The variety $\mathscr{E}_1$ has the properties* SAP, EXT, CEP, RSM, SFG, SBL; *it does not have* IDE, EFG, SCH, NCP. *We have $v(\mathrm{Sim}, \mathscr{E}_1) = \langle \aleph_0, \aleph_0\rangle$ and $v(\mathscr{E}_1) = m(\mathscr{E}_1) = \aleph_0$.*

Proof. Since $\mathscr{E}_1^*$ and $\mathscr{M}^*$ are equivalent, the validity of SAP, CEP, RSM, SFG and SBL follows from 2.3 and the fact that modules have these properties (ZA_1 is noetherian). Extensivity follows from 8.3 of [6]. The negation of SCH follows from 7.5 of [6] (the fact that ZA_1 is not a principal ideal domain is clear). The negations of IDE and EFG are obvious. To prove that $\mathscr{E}_1$ does not have NCP, it is enough to consider the quasigroup $Q(\circ, /, \backslash)$ where Q is the set of rational numbers and $a \circ b = 4a + 2b$, and to define a congruence $\sim$ of $Q(\circ)$ by $x \sim y$ iff $x - y$ is an integer. By 10.3 of [6], $\mathscr{E}_1$ has countably many subvarieties; since $\mathscr{A} \subseteq \mathscr{E}_1$, it has infinitely many minimal subvarieties. The assertion on simple quasigroups follows from 11.4 of [6] and from $\mathscr{A} \subset \mathscr{E}_1$.

Consider the following ring S. Its additive group is that of $Z \times Z$ and the multiplication is defined by $\langle a, b \rangle . \langle c, d \rangle = \langle ac + bd, ad + bc \rangle$. Let $\mathscr{N}$ be the variety of S-modules.

5.3. Proposition. *S is isomorphic to the group-ring $ZC(2)$, where $C(2)$ is the two-element group. S is a commutative noetherian ring and it is not a domain. The element $\langle 1, 0 \rangle$ is its unit and $\langle 0, 1 \rangle$, $\langle 1, 0 \rangle$ are its i-generators. We have $\mathscr{F}_1 \subseteq \mathscr{P}(S, \langle 0, 1 \rangle, \langle 1, 0 \rangle)$ and the varieties $\mathscr{F}_1, \mathscr{N}$ are equivalent.*

Proof. Most of the assertions are easy; see also 15.11 of [6].

5.4. Theorem. *The variety $\mathscr{F}_1$ has the properties* SAP, EXT, IDE, CEP, RSM, SFG, SBL, NCP, GCC; *it does not have* EFG, SCH. *We have $v(\mathrm{Sim}, \mathscr{F}_1) = \langle \aleph_0, \aleph_0 \rangle$ and $v(\mathscr{F}_1) = m(\mathscr{F}_1) = \aleph_0$.*

Proof. Most of the properties can be proved analogously as in 5.2. We shall prove only NCP. Let $Q(., /, \backslash) \in \mathscr{F}_1$ and let r be a congruence of $Q(.)$. By 1.5 there exists an abelian group $Q(+)$ and its automorphism f such that $f^2 = \mathrm{id}_Q$ and $ab = f(a) + b$ for all $a, b \in Q$. Let $a, b, c \in Q$ and $\langle ac, bc \rangle \in r$. Put $d = -f(c)$. We have $\langle ac . d, bc . d \rangle \in r$, i.e. $\langle f(f(a) + c) + d, f(f(b) + c) + d \rangle \in r$, i.e. $\langle a + f(c) + d, b + f(c) + d \rangle \in r$, i.e. $\langle a, b \rangle \in r$. Now let $\langle ca, cb \rangle \in r$. Put $e = -c$. We have $\langle e . ca, e . cb \rangle \in r$, i.e. $\langle f(e) + f(c) + a, f(e) + f(c) + b \rangle \in r$, i.e. $\langle a, b \rangle \in r$.

Finally, consider the following ring T. Its additive group is that of $Z \times Z \times Z$ and the multiplication is defined by $\langle a, b, c \rangle . \langle d, e, f \rangle = \langle ad + bf + ce, ae + bd + cf, af + cd + be \rangle$. Let $\mathscr{T}$ be the variety of T-modules.

5.5. Proposition. *T is isomorphic to $ZC(3)$, where $C(3)$ is the three-element group. T is a commutative noetherian ring and it is not a domain. The element $\langle 1, 0, 0 \rangle$ is its unit and $\langle 0, 1, 0 \rangle$, $\langle 0, 0, 1 \rangle$ are its i-generators. We have $\mathscr{H} = \mathscr{P}(T, \langle 0, 1, 0 \rangle, \langle 0, 0, 1 \rangle)$ and the varieties $\mathscr{H}^*$, $\mathscr{T}^*$ are equivalent.*

Proof. See 1.6 and Proposition 5.5 of [6].

5.6. Theorem. *The variety $\mathscr{H}$ has the properties* SAP, EXT, CEP, RSM, SFG, SBL, NCP, GCC; *it does not have* IDE, EFG, SCH. *We have $v(\mathrm{Sim}, \mathscr{H}) = \langle \aleph_0, \aleph_0 \rangle$ and $v(\mathscr{H}) = m(\mathscr{H}) = \aleph_0$.*

Proof. Again, we shall prove only NCP. Let $Q(., /, \backslash) \in \mathscr{H}$ and let r be a congruence of $Q(.)$. By 1.6 there exists an abelian group $Q(+)$, its automorphism f and an element $g \in Q$ such that $f^3 = \mathrm{id}_Q$ and $ab = f^2(a) + f(b) + g$ for all $a, b \in Q$. Let $a, b, c \in Q$ and $\langle ac, bc \rangle \in r$. Put $d = -(c + f^2(g) + g)$. We have

$\langle d \,.\, ac, d \,.\, bc \rangle \in r$, i.e. $\langle f^2(d) + f(f^2(a) + f(c) + g) + g,\ f^2(d) + f(f^2(b) + f(c) + g) + g \rangle \in r$, i.e. $\langle a, b \rangle \in r$. Let $\langle ca, cb \rangle \in r$. Put $e = -(c + f(g) + f^2(g))$. We have $\langle ca \,.\, e, cb \,.\, e \rangle \in r$, i.e. $\langle f^2(f^2(c) + f(a) + g) + f(e) + g,\ f^2(f^2(c) + f(b) + g) + f(e) + g \rangle \in r$, i.e. $\langle a, b \rangle \in r$.

6. SUMMARY

	$\mathscr{R}$	$\mathscr{C}$	$\mathscr{G}$	$\mathscr{A}$	$\mathscr{D}_1$	$\mathscr{D}_2$	$\mathscr{E}_1$	$\mathscr{E}_2$	$\mathscr{F}_1$	$\mathscr{F}_2$	$\mathscr{H}$
SAP	+	+	+	+	+	+	+	+	+	+	+
EXT	+	+	+	+	+	+	+	+	+	+	+
IDE	—	—	+	+	+	+	—	—	+	+	—
CEP	—	—	—	+	—	—	+	+	+	+	+
RSM	—	—	—	+	—	—	+	+	+	+	+
FEP	+	+	—	+	+	+	?	?	?	?	?
SFG	—	—	—	+	—	—	+	+	+	+	+
EFG	+	+	+	—	+	+	—	—	—	—	—
SBL	—	—	—	+	—	—	+	+	+	+	+
SCH	+	+	+	+	+	+	—	—	—	—	—
NCP	—	—	+	+	—	—	—	—	+	+	+
GCC	—	—	+	+	+	+	?	?	+	+	+
$\nu(\mathrm{Sim}, V)$	en	en	en	$\langle \aleph_0, \aleph_0 \rangle$	en	en	$\langle \aleph_0, \aleph_0 \rangle$	$\langle \aleph_0, \aleph_0 \rangle$	$\langle \aleph_0, \aleph_0 \rangle$	$\langle \aleph_0, \aleph_0 \rangle$	$\langle \aleph_0, \aleph_0 \rangle$
$\nu(\mathrm{Sir}, V)$	en	en	en	$\langle \aleph_0, \aleph_1 \rangle$	en	en	?	?	?	?	?
$v(V)$	$2^{\aleph_0}$	$2^{\aleph_0}$	$2^{\aleph_0}$	$\aleph_0$	$2^{\aleph_0}$	$2^{\aleph_0}$	$\aleph_0$	$\aleph_0$	$\aleph_0$	$\aleph_0$	$\aleph_0$
$m(V)$	$2^{\aleph_0}$	$2^{\aleph_0}$	$\aleph_0$	$\aleph_0$	$2^{\aleph_0}$	$2^{\aleph_0}$	$\aleph_0$	$\aleph_0$	$\aleph_0$	$\aleph_0$	$\aleph_0$

References

[1] *T. M. Baranovič:* Free decompositions in intersections of primitive classes of algebras. (Russian), Matem. Sb. *67* (1965), 135—153.

[2] *A. D. Bolbot:* On equationally complete varieties of totally symmetric quasigroups. (Russian), Algebra i logika *6*/2 (1967), 13—19.

[3] *A. D. Bolbot:* On varieties of quasigroups. (Russian), Sibirsk. Mat. Ž. *13* (1972), 252—271.

[4] *R. H. Bruck:* A survey of binary systems, Springer Verlag, Berlin 1958.

[5] *T. Evans:* Embeddability and the word problem, J. London Math. Soc. *28* (1953), 76—80.

[6] *J. Ježek, T. Kepka:* Varieties of abelian quasigroups, Czech. Math. J. *27* (1977), 473—503.

[7] *A. Karrass, D. Solitar:* Some remarks on the infinite symmetric groups, Math. Z. *66* (1956), 64—69.

[8] *T. Kepka:* Regular mapping of groupoids, Acta Univ. Carolinae *12*/1 (1971), 25—37.

[9] *T. Kepka:* The totally simple quasigroups, Comment. Math. Univ. Carolinae *13* (1972), 577—582.

[10] *A. G. Kuroš:* Theory of groups. (Russian), Nauka, Moskva 1967.

[11] *J. Lambek:* Lectures on rings and modules, Blaisdell Publ. Comp. London 1966.

[12] *P. Němec, T. Kepka:* *T*-quasigroups I., Acta Univ. Carolinae *12*/1 (1971), 39—49.
[13] *A. Ju. Olšanskij:* On the problem of finite basis property in groups. (Russian), Izv. AN SSSR *34* (1970), 376—384.
[14] *H. A. Thurston:* Noncommuting quasigroup congruences, Proc. Amer. Math. Soc. *3* (1952), 363—366.
[15] *M. R. Vaughan-Lee:* Uncountably many varieties of groups, Bull. London Math. Soc. *2* (1970), 280—286.

Author's address: 186 00, Praha 8 - Karlín, Sokolovská 83, ČSSR (Matematicko-fyzikální fakulta UK).