Jaroslav Ježek; Tomáš Kepka

Modular groupoids

Czechoslovak Mathematical Journal, Vol. 34 (1984), No. 3, 477–487

Persistent URL: `http://dml.cz/dmlcz/101972`

Czechoslovak Mathematical Journal, 34 (109) 1984, Praha

MODULAR GROUPOIDS

JAROSLAV JEŽEK and TOMÁŠ KEPKA, Praha

(Received November 17, 1983)

1. INTRODUCTION

By a left modular groupoid we mean a groupoid satisfying the identity $x \, . \, yz = z \, . \, yx$. Right modular groupoids are defined dually by $xy \, . \, z = zy \, . \, x$. A groupoid is said to be bi-modular if it is both left and right modular.

The aim of this paper is to study left modular and bi-modular groupoids. The main results are the description of all simple left modular groupoids (Theorem 3.1) and the description of the equational theory of bi-modular groupoids (Theorem 4.6).

1.1. Example. Let $S(+)$ be a commutative semigroup and f its endomorphism. Define a new binary operation on S by $ab = f^2(a) + f(b)$. We obtain a left modular groupoid.

1.2. Example. Let $S(+)$ be a commutative semigroup and f, g its two endomorphisms such that $f = g^2$ and $g = f^2$. Define a new binary operation on S by $ab = f(a) + g(b)$. We obtain a bi-modular groupoid.

1.3. Example. Let $S(+)$ be a commutative semigroup. Define a binary operation on S^3 by $(a, b, c)(d, e, f) = (c + e, a + f, b + d)$. We obtain a bi-modular groupoid. (This follows from 1.2, since we can define two endomorphisms f, g of $S^3(+)$ by $f(a, b, c) = (c, a, b)$ and $g(a, b, c) = (b, c, a)$.) We shall see later that the variety of bi-modular groupoids is generated by bi-modular groupoids obtained in this way.

It turns out that every left modular groupoid is medial, i.e. satisfies the identity $xy \, . \, zu = xz \, . \, yu$ (see 2.1). Thus the theory of medial groupoids, as developed in [2], will be of use in the present paper.

The notation introduced in Section 1.3 of [2] will be adopted. Recall that every term t can be expressed in the form $t = \sum_{i=1}^{n} e_i x_i$ where x_i are variables and e_i are elements of the free monoid over $\{\alpha, \beta\}$; for every i, e_i is called an *occurrence* of x_i in t. If e is an occurrence of a variable in t, then $P_\alpha(e)$ denotes the number of α's and $P_\beta(e)$ denotes the number of the β's in e; the ordered pair $(P_\alpha(e), P_\beta(e))$ is called the *weight* of e.

2. LEFT MODULAR GROUPOIDS AND MEDIALITY

2.1. Proposition. *Every left modular groupoid is medial.*

Proof. $xy \,.\, zu = u(z \,.\, xy) = u(y \,.\, xz) = xz \,.\, yu$.

Following [2], we call a *groupoid entropic* if it is a homomorphic image of a medial cancellation groupoid. Entropic groupoids form a variety. It is proved in [2] that an identity (t, u) is satisfied in the variety of entropic groupoids iff the following is true for any variable x and any pair k, l of non-negative integers: the number of occurrences of x of weight (k, l) in t equals the number of occurrences of x of weight (k, l) in u.

2.2. Proposition. *The variety of left modular groupoids is not contained in the variety of entropic groupoids.*

Proof. The identity

$$(x(yz \,.\, u))((pq \,.\, r)\, s) = (x(yq \,.\, u))((pz \,.\, r)\, s)$$

is satisfied in all entropic groupoids. On the other hand, it is not satisfied in all left modular groupoids. This can be shown mechanically by finding all terms t such that the identity $(x(yz \,.\, u))((pq \,.\, r)\, s) = t$ is a consequence of the left modular law; there are just 24 such terms t and the term $(x(yq \,.\, u))((pz \,.\, r)\, s)$ is not on the list.

3. SIMPLE LEFT MODULAR GROUPOIDS

Let p be a prime number and n a positive integer. Consider the finite field $GF(p^n)$ with p^n elements. A pair (a, b) of elements of this field is called admissible if $a \neq 0$, the field is generated by a and either $b = 0$ or $b = 1 = a + a^2$. For every admissible pair (a, b) denote by $U[p^n, a, b]$ the groupoid with the underlying set $GF(p^n)$ and with the binary operation $\circ$ defined by $x \circ y = a^2x + ay + b$.

For every integer $n \geqq 2$ define a groupoid $V[n]$ with the underlying set $\{0, 1, \ldots, n\}$ and with binary operation $\circ$ as follows: put $0 \circ i = i \circ 0 = 0$ for all $i \in \{0, \ldots, n\}$; put $f(1) = 2, f(2) = 3, \ldots, f(n-1) = n, f(n) = 1$; if $i, j \in \{1, \ldots, n\}$ and $f(i) = j$, put $i \circ j = f(j)$; put $i \circ j = 0$ in all the other cases. Further, denote by $V[1]$ the groupoid with the underlying set $\{0, 1\}$ and with zero multiplication.

3.1. Theorem. *The only simple left modular groupoids are, up to isomorphism, the following ones:*
(1) $U[p^n, a, b]$ *where p is a prime number, $n \geqq 1$ and (a, b) is an admissible pair;*
(2) $V[n]$ *where $n \geqq 1$;*
(3) *the two-element semilattice.*
These groupoids are pairwise non-isomorphic, with the following exception: $U[p^n, a, b] \simeq U[q^m, c, d]$ iff $p = q$, $n = m$, $b = d$ and $c = h(a)$ for some automorphism h of the field $GF(p^n)$.

The proof of this theorem will be divided into several lemmas.

3.2. Lemma. *The groupoids $U[p^n, a, b]$ are, up to isomorphism, the only simple left modular cancellative groupoids. We have $U[p^n, a, b] \simeq U[q^m, c, d]$ iff $p^n = q^m$, $b = d$ and $c = h(a)$ for some automorphism h of $GF(p^n)$.*

Proof follows from 2.1 and from Propositions 5.5.4 and 7.2.1 of [2].

3.3. Lemma. *The groupoids $V[n]$ $(n \geqq 1)$ are, up to isomorphism, the only simple left modular zeropotent groupoids.*

Proof follows from Proposition 7.5.1 of [2].

3.4. Lemma. *Let $H(\circ, f_1, f_2)$ be a simple algebra with one binary and two unary operations such that $H(\circ)$ is a commutative idempotent medial groupoid and f_1, f_2 are two automorphisms of $H(\circ)$. Then either $H(\circ)$ is cancellative or $H(\circ)$ is a semilattice.*

Proof follows from Proposition 11.4 of [4].

3.5. Lemma. *If 3.1 is not true then there exists a simple left modular groupoid G with the following properties:*

(1) *G is infinite;*
(2) *G is not cancellative;*
(3) *G is not zeropotent;*
(4) *the mapping $f(a) = aa$ is an automorphism of G;*
(5) *if $t(x)$ is a term containing a single variable x and if the mapping $a \mapsto t(a)$ is injective then this mapping is an automorphism of G;*
(6) *G satisfies either the identity $xx \,.\, yz = yy \,.\, xz$ or the identity $xy \,.\, zz = xz \,.\, yy$.*

Proof follows from Theorems 7.9.3 and 1.1.1 of [2] and from the following fact which can be easily proved. If $t(x)$ is a term containing a single variable x, then in any medial groupoid the mapping $a \mapsto t(a)$ is an endomorphism; moreover, any two endomorphisms of this form commute.

3.6. Lemma. *Let G be as in 3.5. Define two binary relations p_G, q_G on G by $(a, b) \in p_G$ iff $ax = bx$ for all $x \in G$, and $(a, b) \in q_G$ iff $xa = xb$ for all $x \in G$. Then $p_G = q_G = \mathrm{id}_G$.*

Proof. Since G is simple and infinite, $GG = G$. This together with the mediality of G implies that p_G and q_G are congruences. If $p_G = G \times G$ then G is a right unar and so G is finite, a contradiction. Hence $p_G = \mathrm{id}_G$. We can prove $q_G = \mathrm{id}_G$ similarly.

3.7. Lemma. *Let G be as in 3.5. The mapping $g(a) = a \,.\, aa$ is an automorphism of G.*

Proof. If this is not true then, as follows from 3.5(5), g is not injective. Since $\mathrm{Ker}(g)$ is a congruence different from id_G, we get that there exists an idempotent o of G with $g(a) = o$ for all $a \in G$. We have $ao = a(a \,.\, aa) = aa \,.\, aa = f^2(a)$, $o \,.\, oa = a \,.\, oo = ao$, $R_0 = f^2 = L_0^2$ and we see that both R_0 and L_0 are automorphisms of G. Now, define a new binary operation $+$ on G by $a + b = R_0^{-1}(a) L_0^{-1}(b)$. It is easy to check that $G(+)$ is a medial groupoid and o is its neutral element. Consequently, $G(+)$ is a commutative semigroup. However, $a + L_0 R_0^{-1}(aa) = R_0^{-1}(a) R_0^{-1}(aa) = R_0^{-1}(a \,.\, aa) = R_0^{-1}(o) = o$, and we have proved that $G(+)$ is an abelian group. In particular, G is a quasigroup, a contradiction.

3.8. Lemma. *Let G be as in* 3.5. *Then G does not satisfy $xx \,.\, yz = yy \,.\, xz$.*

Proof. Suppose that G satisfies $xx \,.\, yz = yy \,.\, xz$. Then $c(a \,.\, bb) = bb \,.\, ac = aa \,.\, bc = c(b \,.\, aa)$ for all $a, b, c \in G$; by 3.6 we have $q_G = \mathrm{id}_G$ and so $a \,.\, bb = b \,.\, aa$ for all $a, b \in G$. Put $a \circ b = g^{-1}(a) g^{-1}(bb)$ for all $a, b \in G$. Then $G(\circ)$ is a medial groupoid, $a \circ b = g^{-1}(a \,.\, bb) = g^{-1}(b \,.\, aa) = b \circ a$, $a \circ a = g^{-1}(a \,.\, aa) = a$, $G(\circ)$ is a commutative idempotent medial groupoid, $ab = g(a) \circ f^{-1} g(b)$ for all $a, b \in G$ and $g, f^{-1}g$ are two commuting automorphisms of $G(\circ)$. Moreover, the algebra $G(\circ, g, f^{-1}g)$ is clearly simple. Evidently, $G(\circ)$ is not cancellative and so it follows from 3.4 that $G(\circ)$ is a semilattice. However, in [1] all simple semilattices with two commuting endomorphisms are found and from the description it follows that the groupoid G is either finite or zeropotent or not left modular, a contradiction.

3.9. Lemma. *Let G be as in* 3.5. *Then G does not satisfy $xy \,.\, zz = xz \,.\, yy$.*

Proof. Suppose that G satisfies $xy \,.\, zz = xz \,.\, yy$. Let $a, b \in G$. Then $a \,.\, bb = cc$ and $b \,.\, aa = dd$ for some $c, d \in G$ and we have $(aa)(e \,.\, bb) = (ae)(a \,.\, bb) = ae \,.\, cc = ac \,.\, ee$ and $(aa)(e \,.\, bb) = (bb)(e \,.\, aa) = (be)(b \,.\, aa) = be \,.\, dd = bd \,.\, ee$ for every $e \in G$. Hence $(ac, bd) \in p_G$ and so $ac = bd$ by 3.6. Now, $(aa)(b \,.\, bb) = (bb)(b \,.\, aa) = bb \,.\, dd = bd \,.\, bd = ac \,.\, ac = aa \,.\, cc = (aa)(a \,.\, bb) = (bb) \,.\, (a \,.\, aa)$.

Put $h(a) = (aa)(a \,.\, aa)$ for all $a \in G$, so that h is an endomorphism of G commuting with f and g. Suppose that h is injective. Then h is an automorphism of G by 3.5(5). Put $a \circ b = h^{-1} f(a) \,.\, h^{-1} g(b)$. Then $G(\circ)$ is a commutative idempotent medial groupoid, $ab = hf^{-1}(a) \circ hg^{-1}(b)$ and the algebra $G(\circ, hf^{-1}, hg^{-1})$ is simple. We can derive a contradiction similarly as in the proof of 3.8.

Hence h is not injective, so that there exists an idempotent o with $h(a) = o$ for all $a \in G$. Let us prove that o is a zero of G. There are three cases:

Case 1: L_0 is not injective. Then o is a left zero of G. Moreover, $ao = a \,.\, oo = o \,.\, oa = o$, so that o is a zero.

Case 2: R_0 is not injective. Then o is a right zero and $o = ao = a \,.\, oo = o \,.\, oa$. Hence L_0 is not injective and, again, o is a zero.

Case 3: L_0, R_0 are injective. Then by Proposition 1.1.1 of [2] there is a simple groupoid H containing G as a subgroupoid and satisfying the same identities as G, such that L_0 and R_0 are automorphisms of H. Put $a + b = R_0^{-1}(a) \,.\, L_0^{-1}(b)$. Then $H(+)$ is a medial groupoid and o is its neutral element, so that it is a commutative semigroup. Let $a \in H$. There are elements $b, c \in H$ with $R_0^{-1}(a \,.\, aa) = bb$ and

$c = o(R_0^{-1}(a) \,.\, R_0^{-1}(a)\, b)$. We have $o = h(R_0^{-1}(a)) = R_0^{-1}(aa) \,.\, bb = R_0^{-1}(a)\, b \,.\, .\, R_0^{-1}(aa) = R_0^{-1}(a)\,(R_0^{-1}(a) \,.\, R_0^{-1}(a)\, b) = R_0^{-1}(a) \,.\, L_0^{-1}(c) = a + c$. We see that $H(+)$ is an abelian group and so G is cancellative, a contradiction.

This proves that o is a zero of G. By Proposition 3.4.1 of [2] there exists a commutative semigroup $S(+)$ and its two commuting endomorphisms p, q such that o is a neutral element of $S(+)$, $p(o) = q(o) = o$, $G \subseteq S$, $ab = p(a) + q(b)$ for all $a, b \in G$ and such that the algebra $S(+, p, q)$ is generated by G. Let r be a congruence of $S(+, p, q)$ which is maximal with respect to $r \cap (G \times G) = \mathrm{id}_G$. If s is a congruence of $S(+, p, q)$ such that $s \supset r$ then, by the maximal property of r, $s \cap (G \times G) \neq \mathrm{id}_G$, so that $G \times G \subseteq s$ (since G is simple); since $o \in G$ and $S(+, p, q)$ is generated by G, we get $s = S \times S$. This shows that r is a maximal congruence of $S(+, p, q)$. Now it is clear that an algebra $S_1(+, p_1, q_1)$ isomorphic to $S(+, p, q)/r$ has the following properties: $S_1(+, o)$ is a commutative monoid, p_1, q_1 are two commuting endomorphisms of $S_1(+, o)$, the algebra $S_1(+, p_1, q_1)$ is simple, $G \subseteq S_1$ and $ab = p_1(a) + q_1(b)$ for all $a, b \in G$. According to Theorem 2.1 of [3], $S_1(+)$ is a semilattice with the least element o. Now, from the description of simple semilattices with two commuting endomorphisms (see [1]) we see that G is either finite or zeropotent or not left modular, a contradiction.

The contradiction induced by 3.8, 3.9 and 3.5(6) proves Theorem 3.1.

3.10. Corollary. *For every cardinal number n denote by $a(n)$ the number of isomorphism classes of simple left modular groupoids with n elements.*

(1) *If n is infinite then* $a(n) = 0$.

(2) *If n is a positive integer which is not a prime power then* $a(n) = 1$.

(3) $a(2) = 3$, $a(3) = 3$, $a(5) = 6$.

(4) *If p is a prime number, $p \geqq 7$ and $i^2 + i \equiv 1 \pmod p$ for an integer i then* $a(p) = p + 2$.

(5) *If p is a prime number, $p \geqq 7$ and there is no i with $i^2 + i \equiv 1 \pmod p$ then* $a(p) = p$.

(6) *If p is a prime number and $i^2 + i \equiv 1 \pmod p$ for an integer i then* $a(p^2) = (\frac{1}{2})(p^2 - p) + 1$.

(7) *If p is a prime number and there is no i with $i^2 + i \equiv 1 \pmod p$ then* $a(p^2) = (\frac{1}{2})(p^2 - p) + 3$.

(8) *If p is a prime number and $n \geqq 3$ then*

$$a(p^n) = 1 + (1/n) \sum_{m|n} \mu(n/m)\, p^m .$$

Proof. The result is an easy consequence of 3.1 and some simple considerations concerning finite fields.

Let us remark that if $p \geqq 7$ is a prime number then it is easy to see that $i^2 + i \equiv 1 \pmod p$ for an integer i iff $j^2 \equiv 5 \pmod p$ for an integer $j \in \{0, \ldots, p - 1\}$.

3.11. Corollary. *There are only countably many minimal varieties of left modular groupoids.*

Given a term t, an integer $n \geqq 0$ and terms $u_1, \ldots, u_n$, we define two terms $L_1(t, u_1, \ldots, u_n)$ and $L_2(t, u_1, \ldots, u_n)$ as follows:

$L_1(t) = L_2(t) = t$;

$L_1(t, u_1, \ldots, u_n) = L_1(t, u_1, \ldots, u_{n-1})\, u_n$ if $n \geqq 1$ is odd;

$L_1(t, u_1, \ldots, u_n) = u_n L_1(t, u_1, \ldots, u_{n-1})$ if $n > 1$ is even;

$L_2(t, u_1, \ldots, u_n) = u_n L_2(t, u_1, \ldots, u_{n-1})$ if $n \geqq 1$ is odd;

$L_2(t, u_1, \ldots, u_n) = L_2(t, u_1, \ldots, u_{n-1})\, u_n$ if $n > 1$ is even.

4.1. Lemma. *Let $n, m \geqq 0$ and let p be any permutation of the set $\{1, \ldots, 2n + 2m + 1\}$. The identity*

$$L_1(x, z_1, \ldots, z_{2n+1}) \,.\, L_1(y, z_{2n+m+1}, z_{2n+2m}, \ldots, z_{2n+2}) =$$
$$= L_1(x, z_{p(1)}, \ldots, z_{p(2n+1)}) \,.\, L_1(y, z_{p(2n+2m+1)}, \ldots, z_{p(2n+2)})$$

is satisfied in all bi-modular groupoids.

Proof. Every permutation p is a composition of transpositions of the form $i \leftrightarrow i+1$, and so it is enough to prove the identity for these transpositions only. Let p be a tranposition $i \leftrightarrow i + 1$. If $i \leqq 2n - 1$ and i is odd, then the identity is a consequence of the left modular law. If $i \leqq 2n$ nad i is even, it is a consequence of the right modular law. For $i = 2n + 1$, it is a consequence of the medial law. If $i > 2n + 1$, then similarly the identity is a consequence either of the left or of the right modular law.

4.2. Lemma. *Let $n, m \geqq 0$. Then the following two identities are satisfied in all bi-modular groupoids*:

(1) $L_1(x, z_1, \ldots, z_{2n+1}) \,.\, L_1(y, u_1, .., u_{2m}) = L_1(y, z_1, \ldots, z_{2n+1}) \,.\, L_1(x, u_1, \ldots, u_{2m})$,

(2) $L_2(x, z_1, \ldots, z_{2m}) \,.\, L_2(y, u_1, \ldots, u_{2n+1}) = L_2(y, z_1, \ldots, z_{2m}) \,.\, L_2(x, u_1, \ldots, u_{2n+1})$.

Proof. Denote these two identities by $E_{n,m}$ and $F_{n,m}$. Since $F_{n,m}$ is dual to $E_{n,m}$, it is enough to prove $E_{n,m}$. $E_{0,0}$ is just the right modular law. We shall proceed by induction on $n + m$.

Let $n > 0$ and $m > 0$. Since $E_{n-1,m-1}$ is satisfied by the induction assumption, an application of 4.1 gives

$L_1(x, z_1, \ldots, z_{2n+1}) \,.\, L_1(y, u_1, \ldots, u_{2m}) =$
$= L_1(z_2 \,.\, xz_1, z_3, \ldots, z_{2n+1}) \,.\, L_1(u_2 \,.\, yu, u_3, \ldots, u_{2m}) =$
$= L_1(u_2 \,.\, yu_1, z_3, \ldots, z_{2n+1}) \,.\, L_1(z_2 \,.\, xz_1, u_3, \ldots, u_{2m}) =$
$= L_1(y, z_1, \ldots, z_{2n+1}) \,.\, L_1(x, u_1, \ldots, u_{2m})$.

Let $n = 1$ and $m = 0$. Then $(z_2 \,.\, xz_1)\, z_3 \,.\, y = (z_3 \,.\, xz_1)\, z_2 \,.\, y = yz_2 \,.\, (z_3 \,.\, xz_1) = yz_2 \,.\, (z_1 \,.\, xz_3) = xz_3 \,.\, (z_1 \,.\, yz_2) = xz_3 \,.\, (z_2 \,.\, yz_1) = (z_2 \,.\, yz_1)\, z_3 \,.\, x$.

Let $n \geqq 2$ and $m = 0$. We already know that the identity $E_{n-1,1}$ is satisfied and so

$$L_1(x, z_1, \ldots, z_{2n+1}) . y = yz_{2n+1} . L_1(x, z_1, \ldots, z_{2n}) =$$
$$= yz_{2n+1} . z_{2n}L_1(x, z_1, \ldots, z_{2n-1}) = L_1(x, z_1, \ldots, z_{2n-1}) . (z_{2n} . yz_{2n+1}) =$$
$$= L_1(y, z_1, \ldots, z_{2n-1}) . (z_{2n} . xz_{2n+1}) = xz_{2n+1} . (z_{2n} . L_1(y, z_1, \ldots, z_{2n-1}) =$$
$$= L_1(y, z_1, \ldots, z_{2n+1}) . x.$$

If $n = 0$ and $m > 0$, we already know that $E_{m,0}$ is satisfied, so that

$$xz_1 . L_1(y, u_1, \ldots, u_{2m}) = L_1(y, u_1, \ldots, u_{2m}) z_1 . x =$$
$$= L_1(y, u_1, \ldots, u_{2m}, z_1) . x = L_1(x, u_1, \ldots, u_{2m}, z_1) . y =$$
$$= yz_1 . L_1(x, u_1, \ldots, u_{2m}).$$

4.3. Lemma. *The following identities are satisfied in all bi-modular groupoids for any* $n \geqq 0$:

(1) $yz . L_1(x, z_1, \ldots, z_{2n+1}) = yx . L_1(z, z_1, \ldots, z_{2n+1})$,
(2) $L_1(x, z_1, \ldots, z_{2n}) . yz = L_1(z, z_1, \ldots, z_{2n}) . yx$,
(3) $L_2(x, z_1, \ldots, z_{2n+1}) . yz = L_2(y, z_1, \ldots, z_{2n+1}) . xz$,
(4) $yz . L_2(x, z_1, \ldots, z_{2n}) = xz . L_2(y, z_1, \ldots, z_{2n})$.

Proof. The last two identities are dual to the first two and so it is enough to prove (1) and (2). (1) follows from 4.2, since

$$yz . L_1(x, z_1, \ldots, z_{2n+1}) = L_1(x, z_1, \ldots, z_{2n+1}) z . y =$$
$$= L_1(z, z_1, \ldots, z_{2n+1}) x . y = yx . L_1(z, z_1, \ldots, z_{2n+1}).$$

The identity (2) is just the left modular law in the case $n = 0$; if $n > 0$, it follows from (1):

$$L_1(x, z_1, \ldots, z_{2n}) . yz = (z_{2n} . L_1(x, z_1, \ldots, z_{2n-1}))(yz) =$$
$$= (yz . L_1(x, z_1, \ldots, z_{2n-1})) z_{2n} = (yx . L_1(z, z_1, \ldots, z_{2n-1})) z_{2n} =$$
$$= L_1(z, z_1, \ldots, z_{2n}) . yx.$$

We denote by T the equational theory of bi-modular groupoids, i.e. the set of pairs (t, u) such that the identity $t = u$ is satisfied in all bi-modular groupoids.

4.4. Lemma. *Let t be a term, x a variable and e an occurrence of x in t.*

(1) *If* $P_\alpha(e) - P_\beta(e) \equiv 0 \pmod 3$ *then either* $(t, ux . v) \in T$ *for some terms* u, v *or* $(t, L_1(x, z_1, \ldots, z_{2n})) \in T$ *or* $(t, L_2(x, z_1, \ldots, z_{2n})) \in T$ *for some variables* $z_1, \ldots, z_{2n}$ $(n \geqq 0)$.
(2) *If* $P_\alpha(e) - P_\beta(e) \equiv 1 \pmod 3$ *then either* $(t, xu) \in T$ *for some term* u *or* $(t, L_1(x, z_1, \ldots, z_{2n+1})) \in T$ *for some variables* $z_1, \ldots, z_{2n+1}$ $(n \geqq 0)$.
(3) *If* $P_\alpha(e) - P_\beta(e) \equiv 2 \pmod 3$ *then either* $(t, ux) \in T$ *for some term* u *or* $(t, L_2(x, z_1, \ldots, z_{2n+1})) \in T$ *for some variables* $z_1, \ldots, z_{2n+1}$ $(n \geqq 0)$.

Proof. If $t = x$ then (1) takes place with $n = 0$. We shall proceed by induction on the length of t.

First, let $P_\alpha(e) - P_\beta(e) \equiv 0 \pmod 3$ and $e = \alpha f$ for some f. Then $P_\alpha(f) - P_\beta(f) \equiv \equiv 2 \pmod 3$. By induction, there are two possibilities. If $(t_1, ux) \in T$ then $(t, ux \,.\, t_2) \in \in T$. If $(t_1, L_2(x, z_1, \ldots, z_{2n+1})) \in T$ then $(t, L_2(x, z_1, \ldots, z_{2n+1}, t_2)) \in T$ and we are through if t_2 is a variable. So, let $t_2 = t_{21}t_{22}$. We have $(t, L_2(x, z_1, \ldots, z_{2n+1}) \,.\, t_{21}t_{22}) \in T$ and so $(t, L_2(t_{21}, z_1, \ldots, z_{2n+1}) \,.\, xt_{22}) \in T$ by 4.3(3); by the medial law we get $(t, z_{2n+1}x \,.\, v) \in T$ for some v.

Let $P_\alpha(e) - P_\beta(e) \equiv 0$ and $e = \beta f$. Then $P_\alpha(f) - P_\beta(f) \equiv 1$ and, by induction, there are two posibilities. If $(t_2, L_1(x, z_1, \ldots, z_{2n+1})) \in T$, we can proceed similarly as in the previous case. So, let $(t_2, xu) \in T$. Then $(t, t_1 \,.\, xu) \in T$. If t_1 is not a variable, $t_1 = t_{11}t_{12}$, then $(t, t_{11}x \,.\, t_{12}u) \in T$. If u is not a variable, $u = u_1u_2$, then $(t, u_1x \,.\, u_2t_1) \in T$. If t_1 and u are both variables, then $(t, L_1(x, u, t_1)) \in T$.

Let $P_\alpha(e) - P_\beta(e) \equiv 1$ and $e = \beta f$. Then $P_\alpha(f) - P_\beta(f) \equiv 2$ and, by induction, there are two possibilities. If $(t_2, ux) \in T$ then $(t, t_1 \,.\, ux) \in T$ and so $(t, x \,.\, ut_1) \in T$. If $(t_2, L_2(x, z_1, \ldots, z_{2n+1})) \in T$ then $(t, t_1 \,.\, L_2(x, z_1, \ldots, z_{2n+1})) \in T$ and so $(t, x \,.\, L_2(t_1, z_1, \ldots, z_{2n+1})) \in T$ by 4.2.

Let $P_\alpha(e) - P_\beta(e) \equiv 1$ and $e = \alpha f$. Then $P_\alpha(f) - P_\beta(f) \equiv 0$. By induction, there are three possibilities. If $(t_1, ux \,.\, v) \in T$ then $(t, x(u \,.\, t_2v)) \in T$. If $(t_1, L_2(x, z_1, \ldots \ldots, z_{2n})) \in T$ then $(t, L_2(x, z_1, \ldots, z_{2n}) \,.\, t_2) \in T$, $(t, t_2z_{2n} \,.\, L_2(x, z_1, \ldots, z_{2n-1})) \in T$ and we can proceed as in the case $e = \beta f$. If $(t_1, L_1(x, z_1, \ldots, z_{2n})) \in T$ then $(t, L_1(x, z_1, \ldots, z_{2n}, t_2)) \in T$ and it is enough to consider the case when t_2 is not a variable, $t_2 = t_{21}t_{22}$. But then $(t, L_1(t_{22}, z_1, \ldots, z_{2n}) \,.\, t_{21}x) \in T$ by 4.3(2), so that $(t, x \,.\, t_{21}L_1(t_{22}, z_1, \ldots, z_{2n})) \in T$.

In the case $P_\alpha(e) - P_\beta(e) \equiv 2$ the proof is similar.

Let a term t, a variable x and a number $i \in \{0, 1, 2\}$ be given We denote by $Q_i(x, t)$ the number of occurrences e of x in t such that $P_\alpha(e) - P_\beta(e) \equiv i \pmod 3$.

4.5. Lemma. *Let t, u be two terms and x a variable. Moreover, let h be an endomorphism of the groupoid of terms. Then*

$$Q_0(x, tu) = Q_2(x, t) + Q_1(x, u),$$
$$Q_1(x, tu) = Q_0(x, t) + Q_2(x, u),$$
$$Q_2(x, tu) = Q_1(x, t) + Q_0(x, u),$$
$$Q_0(x, h(t)) = \sum_y (Q_0(y, t)\, Q_0(x, h(y)) + Q_1(y, t)\, Q_2(x, h(y)) + Q_2(y, t)\, Q_1(x, h(y))),$$
$$Q_1(x, h(t)) = \sum_y (Q_0(y, t)\, Q_1(x, h(y)) + Q_1(y, t)\, Q_0(x, h(y)) + Q_2(y, t)\, Q_2(x, h(y))),$$
$$Q_2(x, h(t)) = \sum_y (Q_0(y, t)\, Q_2(x, h(y)) + Q_1(y, t)\, Q_1(x, h(y)) + Q_2(y, t)\, Q_0(x, h(y))),$$

where y ranges over all variables.

Proof is easy.

4.6. Theorem. *Let t, u be two terms. The identity $t = u$ is satisfied in all bi-*

modular groupoids iff $Q_i(x, t) = Q_i(x, u)$ *for all variables* x *and all* $i \in \{0, 1, 2\}$.

Proof. Denote by T (as above) the equational theory of bi-modular groupoids and by D the set of pairs (t, u) such that $Q_i(x, t) = Q_i(x, u)$ for all variables x and all $i \in \{0, 1, 2\}$. We must prove $T = D$. It follows directly from 4.5 that D is a fully invariant congruence of the algebra of terms. Moreover, the pairs $(x \, . \, yz, z \, . \, yx)$ and $(xy \, . \, z, zy \, . \, x)$ evidently belong to D and so $T \subseteq D$. It remains to prove that if $(t, u) \in$ $\in D$ then $(t, u) \in T$. This will be proved by induction on the sum of the lengths of t and u. If one of the terms t, u is a variable then $t = u$ and so $(t, u) \in T$ is clear. So, let t, u be not variables.

First, suppose that $(t, xa) \in T$ and $(u, xb) \in T$ for some variable x and some terms a, b. Then evidently $(a, b) \in D$ and so $(a, b) \in T$ by the induction assumption, so that $(t, u) \in T$. If $(t, ax) \in T$ and $(u, bx) \in T$, the proof is analogous.

Evidently, there exists an occurrence e of some variable x in t such that either $P_\alpha(e) - P_\beta(e) \equiv 1 \pmod 3$ or $P_\alpha(e) - P_\beta(e) \equiv 2 \pmod 3$; it is enough to consider the first case. Since $(t, u) \in D$, there is an occurrence f of x in u with $P_\alpha(f) - P_\beta(f) \equiv$ $\equiv 1 \pmod 3$. By 4.4, either $(t, xa) \in T$ et $(u, xb) \in T$ for some terms a, b (and we are through) or there are variables $z_1, \ldots, z_{2n+1}$ such that either $(t, L_1(x, z_1, \ldots, z_{2n+1})) \in$ $\in T$ or $(u, L_1(x, z_1, \ldots, z_{2n+1})) \in T$. It is enough to consider the case $(t, L_1(x, z_1, \ldots$ $\ldots, z_{2n+1})) \in T$. Then $P_\alpha(g) - P_\beta(g) \equiv 2 \pmod 3$ for any occurrence g of any variable in t different from e. Since $(t, u) \in D$, $P_\alpha(g) - P_\beta(g) \equiv 2 \pmod 3$ for any occurrence g of any variable in u different from f. Now it easily follows from 4.4 that there exists a variable y and terms a, b such that $(t, ay) \in T$ and $(t, by) \in T$.

5. FREE BI-MODULAR GROUPOIDS AND THE NUMBER OF VARIETIES

Let X be a non-empty set. We denote by $C_X(+, 0)$ the free commutative monoid over X. For every term t in variables from X we define a triple $H(t) = (H_0(t), H_1(t),$ $H_2(t))$ of elements of C_X as follows. Express t in the form $t = \sum_{i=1}^{n} e_i x_i$ and for every $j \in \{0, 1, 2\}$ put $H_j(t) = \sum\{x_i; P_\alpha(e_i) - P_\beta(e_i) \equiv j \pmod 3\}$.

5.1. Theorem. *Let X be a non-empty set. Denote by F the set of triples $(a, b, c) \in$ $\in C_X^3$ satisfying the following two conditions:*
(1) *if $b = c = 0$ then $a \in X$;*
(2) *either the length of a is odd and the lengths of b, c are both even or the length of a is even and the lengths of b, c are both odd.*
Define a binary operation on F by $(a, b, c)(d, e, f) = (c + e, \; a + f, \; b + d)$. Then F is a free bi-modular groupoid over the set $\{(x, 0, 0); x \in X\}$.

Proof. Denote by A the groupoid of terms over X and by G the groupoid with the underlying set C_X^3 and with the binary operation $(a, b, c)(d, e, f) = (c + e, a + f,$ $b + d)$. It is easy to verify that F is a subgroupoid of G containing the elements $(x, 0, 0)$ $(x \in X)$ and that H is a homomorphism of A into G such that $H(x) = (x, 0, 0)$

for all $x \in X$. Consequently, H is a homorphism of A into F. Evidently, $H(t) = H(u)$ iff $Q_i(x, t) = Q_i(x, u)$ for all $x \in X$ and all $i \in \{0, 1, 2\}$ and so it follows from Theorem 4.6 that $H(A)$ is a free bi-modular groupoid over $H(x)$. It remains to prove $H(A) = F$ This follows from the following five observations.

Observation 1: *If $(a, b, c) \in H(A)$ then $(a + x,\ b + y,\ c + z) \in H(A)$ for any $x, y, z \in X$. Indeed, if $(a, b, c) = H(t)$ then $(a + x,\ b + y,\ c + z) = H(u)$ where $u = y(x\ .\ zt)$.*

Observation 2: *If $(a, b, c) \in F$ and $c = 0$ then $(a, b, c) \in H(A)$. Indeed, let $a = \sum_{i=1}^{n} x_i$ and $b = \sum_{i=1}^{m} y_i$. Then m is even, n is odd and (if $m \neq 0$) we have $(a, b, c) = H(t)$ where $t = L_1(L_1(y_1, x_1, \ldots, x_n), y_2, \ldots, y_m)$.*

Observation 3: *If $(a, b, c) \in F$ and $b = 0$ then $(a, b, c) \in H(A)$. This is similar to the second observation.*

Observation 4: *If $(a, b, c) \in F$ and $a = 0$ then $(a, b, c) \in H(A)$. Indeed, let $b = \sum_{i=1}^{n} x_i$ and $c = \sum_{i=1}^{m} y_i$. Then n and m are both odd and we have $(a, b, c) = H(t)$ where $t = L_1(x_1, y_1, \ldots, y_m), x_2, \ldots, x_n)$.*

Observation 5: *If $(a, b, c) \in F$ and $b, c \in X$ then $(a, b, c) \in H(A)$. Indeed, let $a = \sum_{i=1}^{n} x_i$, so that n is even. We have $(a, b, c) = H(t)$ where $t = bL_1(c, x_1, \ldots, x_n)$.*

5.2. Theorem. *The variety of bi-modular groupoids has uncountably many subvarieties.*

Proof. Let us fix a variable x. For any even number $n \geqq 2$ fix two terms t_n, u_n such that $H(t_n) = (nx + 4x, x, x)$ and $H(u_n) = (nx, 3x, 3x)$. For any subset M of $\{2, 4, 6, \ldots\}$ denote by V_M the variety of bi-modular groupoids satisfying the identity (t_n, u_n) for all $n \in M$. In order to prove that the varieties V_M are pairwise different, it is enough to show that (t_n, u_n) is not implied by the set $I_n = \{(t_m, u_m);\ m \neq n\} \cup \cup \{(x\ .\ yz, z\ .\ yx), (xy\ .\ z, zy\ .\ x)\}$. Suppose, on the contrary, that there exists a proof $a_0, \ldots, a_k$ from t_n to u_n, such that (a_{i-1}, a_i) is an immedaite consequence of an identity from I_n for any $i \in \{1, \ldots, k\}$. It is enough to prove by induction on i that $H(a_i) = (nx + 4x, x, x)$. For $i = 0$ this is clear. Let $H(a_i) = (nx + 4x, x, x)$, where $i < k$. If (a_i, a_{i+1}) is an immediate consequence of either the left or the right modular law, it is clear that $H(a_{i+1}) = (nx + 4x, x, x)$. Suppose that (a_i, a_{i+1}) is an immediate consequence of (t_m, u_m) for some $m \neq n$. Then there exists a substitution f such that either $f(t_m)$ or $f(u_m)$ is a subterm of a_i. Now, $f(u_m)$ cannot be subterm of a_i, since $H(f(u_m)) = (p, q, r)$ where p, q, r are of length $\geqq 2$. For the same reason, if $f(t_m)$ is a subterm of a_i then $f(x) = x$, so that $f(t_m) = t_m$. Now, $H(t_m) = (mx + 4x, x, x)$ and it is easy to see that if w is any term such that t_m is a proper subterm of w and if $H(w) = (a, b, c)$ then at least two of the elements a, b, c have lengths $\geqq 2$. Hence $t_m = a_i$ and so $m = n$, a contradiction.

References

[1] *J. Ježek:* Simple semilattices with two commuting automorphisms. Algebra Universalis *15*, 1982, 162—175.

[2] *J. Ježek* and *T. Kepka:* Medial groupoids. Rozpravy ČSAV, Řada Mat. a Přír. Věd. *93*/1, 1983. Academia, Praha.

[3] *J. Ježek* and *T. Kepka:* Simple semimodules over commutative semirings. (To appear)

[4] *T. Kepka:* Distributive groupoids and preradicals II. CMUC *24*, 1983, 199—209.

Authors' address: 186 00 Praha 8, Sokolovská 83, ČSSR (MFF UK).