Varieties of idempotent commutative groupoids

by

J. Dudek (Wrocław)

Abstract. In this paper we present several results about varieties of idempotent and commutative groupoids. In particular, we characterize the varieties of such groupoids defined by identities called strongly regular identities.

1. Introduction. The main purpose of this paper is to investigate strongly regular and nonregular identities in idempotent commutative groupoids. We prove that every idempotent commutative groupoid satisfying a strongly regular (nontrivial) identity is medial (Theorem 4). In Theorem 5 we give a characterization of strongly regular identities (for $V(\cdot)$) which are nontrivial. We also prove that every medial idempotent commutative groupoid in which a nonregular identity holds is a quasigroup (Theorem 6). Idempotent commutative groupoids satisfying some strongly regular identities and some nonregular identities are characterized in Theorem 7. We describe medial groupoids as direct sums of reducts of abelian groups (Theorems 1–3) and we establish the necessary and sufficient conditions for an idempotent groupoid to be a semilattice (Theorem 8). Theorems 4–10 and some related result will, as we hope, prove useful in finding all the atoms of the lattice of varieties of idempotent commutative groupoids.

2. Preliminaries. We adopt here the definitions and notation given by Grätzer [6] and Marczewski [8]. Two identical algebras, i.e., algebras having the same sets of polynomials, will be called *polynomially equivalent*.

An identity $f = g$ where f and g are terms in an algebra will be called *regular* if on both sides of it the same free variables occur (see [10]). A regular identity is called *strongly regular* if each of its free variables occurs only once.

Let E be a set of identities with respect to a fixed type τ and some fundamental symbols. Then by E^* we denote the variety of all algebras of type τ satisfying all identities of E. An identity $f = g$ is called *nontrivial with respect to* E^* if the class $(E \cup \{f = g\})^*$ is properly contained in E and is different from the class $\{x = y\}^*$.

Let $f = f(x_1, \ldots, x_n)$ be a function on A. We say that f *admits a* *permutation* $\sigma \in S_n$ *of its variables if* $f = f^\sigma$, i.e., $f(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n})$ for all $x_1, \ldots, x_n \in A$, where $f^\sigma(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n})$. By $G(f)$ we denote the group of all admissible permutations of f (see [7]).

Let E be a set of identities. Then an admissible permutation σ of a given polynomial $f = f(x_1, \ldots, x_n)$ is said to be *trivial* (*with respect to* E) if the identity $f(x_1, \ldots, x_n) = f(x_{\sigma 1}, \ldots, x_{\sigma n})$ can be obtained from E, i.e., if $E^* = (E \cup \{f = f^\sigma\})^*$.

Let $(G, \cdot)$ be a groupoid. We write xy instead of $x \cdot y$ and xy^n $(n \geqslant 1)$ for the polynomial $(\ldots(xy)\ldots y)y$ where x appears once and y appears n times. We also write $x_1 \ldots x_n$ instead of $(\ldots((x_1 x_2)x_3 \ldots x_{n-1})x_n)$. If the groupoid is written additively, we use the notation $x + ny$ and $x_1 + \ldots + x_n$, respectively. The class of all idempotent and commutative groupoids $(G, \cdot)$ is denoted by $V(\cdot)$. By $V_n(\cdot)$, for a fixed $n \geqslant 1$, we denote the subvariety of $V(\cdot)$ of all groupoids $(G, \cdot)$, which satisfies $xy^n = x$.

A polynomial $f = f(x_1, \ldots, x_n)$ over $V(\cdot)$ (or over $(G, \cdot) \in V(\cdot)$) is said to be a *good one* if f has no repetitions of its variables.

A variable x_i $(i = 1, \ldots, n)$ is bound up with a variable x_j $(j = 1, \ldots, n)$ in a good polynomial $f = f(x_1, \ldots, x_n)$ if the term $x_i x_j$ appears in f.

If we have a strongly regular identity $f = g$ in the groupoid $(G, \cdot) \in V(\cdot)$ with variables x_i and x_j bound up together in the polynomials f and g, then by a couple reduction of the variables x_i and x_j in $f = g$ we mean the substitution of x_i for $x_i x_j$, and the resulting identity $f' = g'$ will be called the *result of the reduction*. Since $\cdot$ is idempotent, the identities $f = g$ and $f' = g'$ are equivalent.

A groupoid $(G, \cdot)$ is said to be *distributive* if $(xy)z = (xz)(yz)$ and $x(yz) = (xy)(xz)$ for all $x, y, z \in G$. A groupoid $(G, \cdot)$ is medial if it satisfies the medial law, i.e., if $(xy)(uv) = (xu)(yv)$ for all $x, y, u, v \in G$ (for the above definition see [1]). The class of all idempotent commutative and medial groupoids $(G, \cdot)$ will be denoted by $M(\cdot)$. Further, we put $M_n(\cdot) = M(\cdot) \cap V_n(\cdot)$ and we denote by $M_n^*(\cdot)$ the subvariety of all groupoids from $M(\cdot)$ which satisfy $xy = xy^{n+1}$. It turns out that, from our point of view, the most important strongly regular identities in $V(\cdot)$ are the medial law and the following identity:

(n) $$x_1 x_2 \ldots x_{n-1} x_n = x_n x_2 \ldots x_{n-1} x_1 \quad \text{for some } n \geqslant 3.$$

For $n \geqslant 3$, we denote by $K_n^*(\cdot)$ the subvariety of $V(\cdot)$ of all groupoids which satisfy the identity (n) and by $K_n(\cdot)$ we denote the subvariety of $K_n^*(\cdot)$ which satisfies $xy^{n-2} = x$ $(n \geqslant 3)$.

3. Theorems and comments. Here we present all the theorems with some comments. The proofs of the theorems are given in the next section.

Let n be a natural number and let $(G, +)$ be an abelian group of exponent $d | 2^n - 1$. Denote by $G(d, n)$ the groupoid $\left(G, \frac{d+1}{2}(x+y)\right)$. Observe that $G(d, n) = (G, 2^{n-1}(x+y))$. Indeed, we have $2^{n-1}(x+y) = \frac{d+1}{2}(x+y)$ for all $x, y \in G$ since

$$2^{n-1}(x+y) - \frac{d+1}{2}(x+y) = \frac{k-1}{2} d(x+y) = 0, \quad \text{where } dk = 2^n - 1.$$

In [3] a characterization theorem for groupoids from $M_n(\cdot)$ is given. Let us recall that theorem for the convenience of the reader and also Theorem 3 from [2] (here Theorem 2).

THEOREM 1 ([3], Characterization Theorem). *A groupoid $(G, \cdot)$ belongs to $M_n(\cdot)$ iff there exists an abelian group G of exponent $d | 2^n - 1$ such that $(G, \cdot) = G(d, n)$.*

THEOREM 2 ([2], Theorem 3). *A groupoid $(G, \cdot)$ belongs to $K_n(\cdot)$ iff it is the sum of a direct system of groupoids from $K_n(\cdot)$ (the sum of a direct system of algebras is understood here in the sense of* [10]).

THEOREM 3. *For every n, $M_n(\cdot) = K_{n+2}(\cdot)$ and $M_n^*(\cdot) = K_{n+2}^*(\cdot)$.*

As a corollary we obtain a characterization theorem for groupoids from $M_n^*(\cdot)$.

COROLLARY (Characterization Theorem). *A groupoid $(G, \cdot)$ belongs to the variety $M_n^*(\cdot)$ iff it is the sum of a direct system of groupoids from $M_n(\cdot)$, i.e., of groupoids of the form $G(d, n)$.*

THEOREM 4. *If $(G, \cdot) \in V(\cdot)$ satisfies a nontrivial strongly regular identity, then it is medial, i.e., $(G, \cdot) \in M(\cdot)$.*

THEOREM 5. *A strongly regular identity $f = g$ is nontrivial in the variety $V(\cdot)$ if and only if after several steps of couple reductions of $f = g$ we obtain an identity $f' = g'$ such that there exist two variables x_i and x_j bound up with each other in f' and not bound up with each other in g'.*

THEOREM 6. *If $(G, \cdot) \in M(\cdot)$ satisfies a nonregular identity, then $(G, \cdot)$ is a medial quasigroup.*

THEOREM 7. *If $(G, \cdot) \in V(\cdot)$ satisfies some nontrivial strongly regular identities and some nonregular identities, then there exist an abelian group $(G, +)$ and an automorphism φ of $(G, +)$ such that $xy = \varphi(x) + \varphi(y)$ and $2\varphi(x) = x$ for all $x, y \in G$.*

Theorems 4, 6 and 7 are useful in investigating complete groupoids from the variety $V(\cdot)$.

THEOREM 8. (A characterization of semilattices). *For every idempotent groupoid $(G, \cdot)$ the following conditions are equivalent:*

(i) $(G, \cdot)$ *is a semilattice.*

(ii) $(G, \cdot)$ *is commutative and distributive, and* $xy = xy^2$ *for all* $x, y \in G$.

(iii) $(G, \cdot)$ *is commutative and the polynomial* $s(x, y, z) = (xz)(yz)$ *admits a nontrivial permutation of its variables.*

(iv) $(G, \cdot)$ *is commutative and distributive, and* $xy^2 = yx^2$ *for all* $x, y \in G$.

(v) $(G, \cdot)$ *is commutative and medial, and* $xy^2 = xy^3$ *for all* $x, y \in G$.

(vi) $(G, \cdot)$ *satisfies the identity*

$$x_1 x_2 \ldots x_{n-1} x_n = x_2 x_3 \ldots x_n x_1 \quad \textit{for some } n \geqslant 3.$$

(vii) *the same as in* (vi) *for some left iteration of the polynomial* xy, *i.e.,*

$$x_1\big(x_2\big(\ldots(x_{n-1}x_n)\ldots\big)\big) = x_2\big(x_3\big(\ldots(x_n x_1)\ldots\big)\big)$$

for some $n \geqslant 3$.

(viii) $(G, \cdot)$ *is commutative and some simple iteration* $s_n(x_1, \ldots, x_n) = x_1 \ldots x_n$ *of* xy *where* $n \geqslant 3$ *admits a transposition* $(k, k+1)$ *of its variables where* $2 \leqslant k \leqslant n-1$, *i.e., the following identity holds in* $(G, \cdot)$:

$$x_1 \ldots x_{k-1} x_k x_{k+1} \ldots x_{n-1} x_n = x_1 \ldots x_{k-1} x_{k+1} x_k \ldots x_{n-1} x_n.$$

Theorem 8 is useful in estimating the number of essentially n-ary polynomials over an idempotent commutative groupoid (see [5]).

THEOREM 9. *A groupoid* $(G, \cdot)$ *is a quasigroup if at least one of the following conditions holds*:

(i) $(G, \cdot) \in V_n(\cdot)$ *for some* $n \geqslant 1$.

(ii) $(G, \cdot) \in V(\cdot)$ *and the polynomial* xy^n *ist not essentially binary.*

(iii) $(G, \cdot) \in V(\cdot)$ *and the polynomial* $(xy^2)x$ *is not essentially binary.*

(iv) $(G, \cdot)$ *satisfies the identities* $x = xy^m$ *and* $x = \underbrace{y\big(y\big(\ldots(yx)\ldots\big)\big)}_{n \text{ times } y}$, *for some* m *and* n.

Denote by $Q_{m,n}(\cdot)$ the variety of all groupoids satisfying the above two identities.

THEOREM 10. *If* $(G, \cdot) \in Q_{2,n}(\cdot)$ *for some* $n \geqslant 2$, *then there exists a binary commutative polynomial* $+$ *over* $(G, \cdot)$ *such that the groupoids* $(G, \cdot)$ *and* $(G, +)$ *are polynomially equivalent and* $(G, +) \in V_n(+)$ *in case* $(G, \cdot)$ *is idempotent.*

This theorem shows that the investigation of some noncommutative groupoids can be reduced to the commutative case. Such a reduction proves useful for example in finding the number of all essentially n-ary polynomials over a groupoid and in deciding whether a given groupoid is equationally complete.

4. Lemmas and proofs of the theorems. Recall that the proofs of Theorems 1 and 2 can be found in [3] and [2], respectively.

Proof of Theorem 3. Using Theorem 2 and Lemma 1 of [2], we infer that if $(G, \cdot) \in K_{n+2}(\cdot)$, then there exists an abelian group $(G, +)$ of exponent d such that $d | 2^n - 1$ and $(G, \cdot) = G(d, n)$. Since, by Lemma 1 of [3], $G(d, n) \in M_n(\cdot)$, we have $(G, \cdot) \in M_n(\cdot)$. The inclusion $M_n(\cdot) \subseteq K_{n+2}(\cdot)$ follows by the Characterization Theorem for groupoids from the variety

$M_n(\cdot)$ (see [3]) and the method used in the proof of Lemma 1 of [2]. Let us now prove $M_n^*(\cdot) = K_{n+2}^*(\cdot)$ for all n. Let $(G, \cdot) \in K_{n+2}^*(\cdot)$. Then, by Theorem 3 of [2], the groupoid $(G, \cdot)$ is the sum of a direct system of groupoids (for the definition of the sum of a direct system of algebras see [10]) from the class $K_{n+2}(\cdot)$ and therefore using the Characterization Theorem for groupoids from $M_n(\cdot)$ (see [3]) and the fact $M_n(\cdot) = K_{n+2}(\cdot)$ we infer that G is the sum of groupoids which are medial. Since the medial law is a regular identity and the sum of a direct system of algebras preserves regular identities (see [10]), we infer that $(G, \cdot)$ is medial, i.e., $(G, \cdot) \in M(\cdot)$. We also have

$$xy^{n+1} = (\ldots(xy)\ldots y)y = (\ldots(yy)\ldots y)x = yx = xy$$

and thus $(G, \cdot) \in M_n^*(\cdot)$. Suppose now that $(G, \cdot) \in M_n^*(\cdot)$. We have to prove that the identity $(n+2)$ holds in $(G, \cdot)$. We have

$$\begin{aligned}
x_1 x_2 \ldots x_n x_{n+1} x_{n+2} &= \big((x_1 x_2 \ldots x_n) x_{n+2}\big)(x_{n+1} x_{n+2}) \\
&= \Big(\big((x_1 x_2 \ldots x_{n-1}) x_{n+2}\big)(x_n x_{n+2})\Big)(x_{n+1} x_{n+2}) = \ldots \\
\ldots &= \Big(\ldots\Big(\big((x_1 x_{n+2})(x_2 x_{n+2})\big)(x_3 x_{n+2})\Big) \ldots (x_n x_{n+2})\Big)(x_{n+1} x_{n+2}) \\
&= \Big(\ldots\Big(\big((x_1 x_{n+2}) x_2\big)\big((x_1 x_{n+2}) x_{n+2}\big)\Big)(x_3 x_{n+2}) \ldots (x_n x_{n+2})\Big)(x_{n+1} x_{n+2}) \\
&= \Big(\ldots\Big(\big((x_1 x_{n+2}) x_2\big)(x_1 x_{n+2}^2)\Big)(x_3 x_{n+2}) \ldots (x_n x_{n+2})\Big)(x_{n+1} x_{n+2}) \\
&= \Big(\ldots\Big(\big((x_1 x_{n+2}) x_2\big) x_3\Big)(x_1 x_{n+2}^3) \ldots (x_n x_{n+2})\Big)(x_{n+1} x_{n+2}) = \ldots \\
\ldots &= \Big(\ldots\Big(\Big(\Big(\big((x_1 x_{n+2}) x_2\big) x_3\Big) \ldots x_{n-1}\Big) x_n\Big)(x_1 x_{n+2}^n)\Big)(x_{n+1} x_{n+2}) \\
&= (x_1 x_{n+2} x_2 x_3 \ldots x_n x_{n+1})(x_1 x_{n+2}^{n+1}) \\
&= \Big(\ldots\big((x_1 x_{n+2}) x_2 \ldots x_n\big) x_{n+1}\Big)(x_1 x_{n+2}) \\
&= x_{n+2} x_2 \ldots x_n x_{n+1} x_1
\end{aligned}$$

(the variables x_1 and x_{n+2} can be interchanged), which proves that $(G, \cdot)$ satisfies the identity $(n+2)$. Hence $M_n^*(\cdot) = K_{n+2}^*(\cdot)$. The theorem is proved.

Before proving Theorem 4 we need some lemmas.

LEMMA 1. *If* $g = g(x_1, \ldots, x_n)$ *is a good polynomial over* $(G, \cdot) \in V(\cdot)$ *and* g *admits a transposition* (i, j) *where* x_i *is bound with some variable* x_k *and* x_j *is not bound with any variable, then* $(G, \cdot)$ *is medial.*

Proof. Let $(G, \cdot) \in V(\cdot)$. Assume that n is the smallest number for which there exists a polynomial g satisfying the assumption of the lemma. Of course, we may assume that the polynomial has no other bound-up variables except x_i and x_k (and $n \geqslant 3$) since in the opposite case by identifying the bound-up variables other than x_i and x_k we get a contradiction with the minimality of n. So we infer that g is of the form $x_1 \ldots x_n$, i.e., $g(x_1, \ldots, x_n) = x_{\sigma 1} \ldots x_{\sigma n}$ for some $\sigma \in S_n$. Hence we infer that $x_1 \ldots x_n$ $(n \geqslant 3)$ admits a nontrivial transposition. Using Theorem 1 of [2] we deduce that $(G, \cdot)$ satisfies the identity (n) for some $n \geqslant 3$, i.e. $(G, \cdot)$ is in $K_n^*(\cdot)$. An application of Theorem 3 gives the mediality of $(G, \cdot)$.

LEMMA 2. *If $g = g(x_1, \ldots, x_n)$ is a good polynomial over $(G, \cdot) \in V(G, \cdot)$ and g admits a transposition (i, j), where none of variables x_j and x_j is bound up, then $(G, \cdot)$ is medial.*

Proof. As in the proof above, identifying all bound-up variables in g in such a way that the resulting polynomial g^* is again a good one, we infer that the groupoid $(G, \cdot)$ again satisfies the identity (m) for some $m \geq 3$. The proof then runs as in Lemma 1.

LEMMA 3. *If $g = g(x_1, \ldots, x_n)$ is a good polynomial over $(G, \cdot) \in V(\cdot)$ and g admits a transposition (i, j), where x_i and x_j are not bound up with each other but are both bound up with some variables, then $(G, \cdot)$ is medial.*

Proof. Let $g = g(x_1, \ldots, x_n)$ be the good polynomial over $(G, \cdot) \in V(\cdot)$ and let x_a be bound up with x_i and x_b with x_j. Without loss of generality one can assume that n is the smallest number for which g satisfies the assumption of our lemma. Thus we infer that the variables x_a, x_i, x_b, x_j are the only ones which are bound up in the polynomial g since in the opposite case we may identify the remaining bound-up pairs of variables. By the commutativity of $\cdot$ we infer that the polynomial g admits all permutations $\sigma \in S_n$ with a fixed $k \notin \{a, b, i, j\}$, i.e. permutes variables x_a, x_i, x_b, x_j. Using the commutativity of $\cdot$ and the minimality of n, we also infer that g starts from the term $x_a \cdot x_i$ or from the term $x_b \cdot x_j$ and that there are no other terms of that form in the polynomial g. Suppose that g starts from $x_a x_i$. Now to complete the proof we have to consider two possibilities for the polynomial g:

(g_1) $g(x_1, \ldots, x_n) = h_1(x_1, \ldots)x_s$ where h_1 is an $(n-1)$-ary good polynomial containing variables x_a, x_i, x_b, x_j and starting from the expression $x_a x_i$.

(g_2) $g(x_1, \ldots, x_n) = h_2(x_1, \ldots)(x_b x_j)$ where h_2 is an $(n-2)$-ary good polynomial starting from $x_a x_i$.

Let (g_1) hold in $(G, \cdot)$. Since g admits all permutations changing variables x_a, x_i, x_b, x_j with the variable x_s fixed, we infer that $g = h_1 x_s = h_1^{\sigma_1} x_s$ for any permutation $\sigma_1 \in S_{n-1}$ which changes the above-mentioned variables and does not change others. Using the idempotency of xy and the last identity, we get $h_1 = h_1 h_1 = h_1^{\sigma_1} h_1 = h_1 h_1^{\sigma_1} = h_1^{\sigma_1} h_1^{\sigma_1} = h_1^{\sigma_1}$, which gives a contradiction ($h_1 = h_1^{\sigma_1}$) with the minimality of n.

Let (g_2). If $n = 4$, then, of course, $(G, \cdot)$ is medial. Therefore, we may further assume that $n \geq 5$ and h_2 is at least ternary starting from $x_a x_i$. We may also assume that h_2 contains at least one variable which is not bound up with any other variable. Setting $x = x_a = x_i$ and $y = x_b = x_j$ in the polynomial g, we get the $(n-2)$-ary good polynomial g^* which admits a transposition of variables x and y, with x bound up and y not bound up. An application of Lemma 1 completes the proof of this lemma.

LEMMA 4. *If $g(x_1, \ldots, x_n)$ is a good polynomial over $(G, \cdot) \in V(\cdot)$ admitting a transposition of variables x_i and x_j which are not bound up with each other, then $(G, \cdot)$ is medial,*

Proof. It follows from Lemmas 1, 2, 3.

Now let $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ be a nontrivial strongly regular identity in $(G, \cdot) \in V(\cdot)$. We can further assume without loss of generality that f starts from $x_1 x_2$ in the identity $f = g$ after a certain number of parentheses.

LEMMA 5. *If $f = g$ is a nontrivial strongly regular identity in $(G, \cdot) \in V(\cdot)$, then the identity is equivalent to a strongly regular identity $f' = g'$, where g' starts from $x_1 x_2$ and x_1 and x_2 are not bound up with each other in g'.*

Proof. Let x_i and x_j be bound up in the polynomial f in the identity $f = g$. If x_i and x_j are also bound up in g, then putting $x_i = x_j$ we get a new nontrivial strongly regular identity equivalent to the identity $f = g$. Continuing this process, we infer that $f = g$ is equivalent to some nontrivial strongly regular identity ($f_1 = g_1$) in which on one side (say f_1) there is a bound-up pair of variables and on the other side this pair of variables is not bound up. Renumbering the variables in the identity $f_1 = g_1$, we get the required assertion.

Proof of Theorem 4. Let $(G, \cdot) \in V(\cdot)$ and let $f = g$ be a nontrivial strongly regular identity satisfied in $(G, \cdot)$. Applying Lemma 5, we may assume that f starts from $x_1 x_2$ and x_1 and x_2 are not bound up with each other in g. Using the commutativity of $\cdot$, we infer that g admits a transposition of variables x_1 and x_2. To end the proof of the theorem we apply Lemma 4.

To prove the next theorem we need the following

LEMMA 6. *There exist nonmedial groupoids in the variety $V(\cdot)$.*

Proof. Let N be the set of all natural numbers (0 is excluded from N) and let $a \in N$. Consider the groupoids $N_a = (N, \cdot_a)$ where $\cdot_a$ is idempotent and $x \cdot_a y = a + \max(x, y)$ for $x \neq y$ $(x, y \in N)$. It is easy to check that N_a is nonmedial (for all a) and $N_a \in V(\cdot)$. One can also see that the groupoids satisfy the identity considered in Theorem 4 of [4], i.e., $(x \cdot_a y) \cdot_a y = (y \cdot_a x) \cdot_a x$.

Proof of Theorem 5. Let $G(\aleph_0)$ denote a free groupoid in the variety $V(\cdot)$ with countable free generators and let $f = g$ be a strongly regular identity in $V(\cdot)$. If the identity $f = g$ is nontrivial in $V(\cdot)$, i.e., is nontrivial in $G(\aleph_0)$, then, using Lemma 5 and the definition of a couple reduction, we get the part "if". To prove the converse we infer from the assumption that $f' = g'$ is satisfied in $G(\aleph_0)$. And now, applying Lemma 4 to the good polynomial g', we deduce that $G(\aleph_0)$ is medial and therefore the variety $V(\cdot)$ consists only of medial groupoids. This contradicts Lemma 6. The proof of the theorem is completed.

In the sequel we shall use the following description of the set $A^{(n)}(\mathfrak{A})$ of all n-ary polynomial over an algebra $\mathfrak{A} = (A, F)$ (see [8]):

$$A^{(n)} = A^{(n)}(\mathfrak{A}) = \bigcup_{k=0}^{\infty} A_k^{(n)}(\mathfrak{A}),$$

where

$$A_0^{(n)} = A_0^{(n)}(\mathfrak{A}) = \{e_1^{(n)}, \dots, e_n^{(n)}\}$$

and

$$A_{k+1}^{(n)} = A_{k+1}^{(n)}(\mathfrak{A}) = A_k^{(n)}(\mathfrak{A}) \cup \{f(f_1, \dots, f_m)\colon f_i \in A_k^{(n)},\ f \in F \text{ and } i = 1, \dots, m\}$$

(Marczewski's formula).

To prove Theorem 6 we need some more lemmas.

LEMMA 7. *If $(G, \cdot) \in M(\cdot)$ and $ax_1 = ax_2$ for some $a, x_1, x_2 \in G$, then for every nontrivial $f \in A^{(2)}(G, \cdot)$ we have $f(a, x_1) = f(a, x_2)$ (and $f(x_1, a) = f(x_2, a)$).*

Proof. By assumption, our assertion holds for every nontrivial $f \in A_1^{(2)}(G, \cdot)$. Suppose that is holds for every nontrivial $f \in A_k^{(2)}(G, \cdot)$. Using Lemma 1 of [4], we see that if $g \in A_{k+1}^{(2)}(G, \cdot)$, then $g = g_1 x$ or $g = g_1 y$ where $g_1 \in A_k^{(2)}(G, \cdot)$ and $g_1(a, x_1) = g_1(a, x_2)$, $g_1(x_1, a) = g_1(x_2, a)$ and g_1, g are nontrivial. We have to prove that $g(a, x_1) = g(a, x_2)$ and $g(x_1, a) = g(x_2, a)$. We shall check only the first of the above equations. If $g = g_1(x, y)y$, then, in view of the fact that $T_u(v) = uv$ is an endomorphism of $(G, \cdot) \in M(\cdot)$,

$$\begin{aligned} g(a, x_1) &= g_1(a, x_1)x_1 = g_1(a, x_2)x_1 = g_1(ax_1, x_2x_1) = g_1(ax_2, x_1x_2) \\ &= g_1(a, x_1)x_2 = g_1(a, x_2)x_2 = g(a, x_2). \end{aligned}$$

If $g(x, y) = g_1(x, y)x$, then

$$g(a, x_1) = g_1(a, x_1)a = g_1(a, x_2)a = g(a, x_2).$$

This shows that g satisfies the assertion of the lemma, which, in view of Marczewski's formula, completes the proof.

LEMMA 8. *If $(G, \cdot) \in M(\cdot)$ and there exists a nontrivial binary polynomial f over $(G, \cdot)$ such that $f(x, y) = x$ for $x, y \in G$, then $(G, \cdot)$ is a quasigroup.*

Proof. (1) G is cancellative. Indeed, assume that $ax_1 = ax_2$ for some $a, x_1, x_2 \in G$. From Lemma 7 we infer that if f is a nontrivial binary polynomial over $(G, \cdot)$, then $f(a, x_1) = f(a, x_2)$ and $f(x_1, a) = f(x_2, a)$. Since $f(x, y) = x$, we have $x_1 = f(x_1, a) = f(x_2, a) = x_2$, which proves that G is cancellative.

(2) For every $a, b \in G$ the equation $au = b$ has a solution. Indeed, by Lemma 2 of [4] we infer that $f(x, y) = x^{\alpha_1}y^{\beta_1} \dots y^{\beta_{n-1}}x^{\alpha_n}y^{\beta_n}$ for some nonnegative integers α_i, β_j $(i, j = 1, \dots, n)$. Hence $b = f(b, a) = b^{\alpha_1}a^{\beta_1} \dots a^{\beta_{n-1}}b^{\alpha_n}a^{\beta_n}$. If $\beta_n > 0$, then we put $u = b^{\alpha_1}a^{\beta_1} \dots a^{\beta_{n-1}}b^{\alpha_n}a^{\beta_n - 1}$. Let $\beta_n = 0$. Without loss of generality we may assume that the remaining integers α_i, β_j are positive. Using the cancellation law and the idempotency of $(G, \cdot)$, we infer that $b = b^{\alpha_1}a^{\beta_1} \dots b^{\alpha_{n-1}}a^{\beta_{n-1}}$. It is clear that in this case $u = b^{\alpha_1}a^{\beta_1} \dots b^{\alpha_{n-1}}\ a^{\beta_{n-1}-1}$, which completes the proof of the lemma.

Proof of Theorem 6. Assume that $(G, \cdot)$ belongs to $M(\cdot)$ and satisfies a nonregular identity

$$f(x_1, \dots, x_n) = g(y_1, \dots, y_m).$$

If this identity is equivalent to the identity $u = v$, then of course $(G, \cdot)$ is a one-element quasigroup. Therefore we can assume that at least one of the polynomials f and g is not trivial (and at least binary), say f. Without loss of generality one can assume that x_1 does not appear as a variable in $g(y_1, \dots, y_m)$ because the identity $f = g$ is nonregular. Putting in this identity $x_1 = y$ and x for the remaining variables, we get a new identity $h(x, y) = x$ for some nontrivial $h \in A^{(2)}(G, \cdot)$. An application of Lemma 8 completes the proof.

Proof of Theorem 7. The proof follows from Theorems 4 and 6 and from Theorem 2.10 of [1, pp. 33].

Proof of Theorem 8. Let $(G, \cdot)$ be an idempotent groupoid. It is easy to see that condition (i) implies all the other conditions of the theorem. We shall prove the converse implications.

(ii) $\Rightarrow$ (i). In this case we have to prove that xy is associative. Indeed, we have

$$\begin{aligned} (xy)z &= (xz)(yz) = \big(x(yz)\big)\big(z(yz)\big) = \big(x(yz)\big)\big((yz)z\big) \\ &= \big(x(yz)\big)(yz) = x(yz). \end{aligned}$$

(iii) $\Rightarrow$ (i). Let $(G, \cdot)$ be commutative and suppose the polynomial $s(x, y, z) = (xz)(yz)$ admits a nontrivial permutation of its variables. Then $s(x, y, z)$ is a symmetric polynomial, whence we have $(xz)(yz) = (xz)(xy) = (xy)(zy)$. Setting in this identity $z = y$, we get $xy = (xy)(xy) = (xy)(yy) = (xy)y = xy^2$. Putting xz for x in the identity $(xz)(yz) = (xz)(xy)$ and using $xy = xy^2$, we get

$$(xz)(yz) = \big((xz)z\big)(yz) = \big((xz)z\big)\big((xz)y\big) = (xz)\big((xz)y\big) = \big(y(xz)\big)(xz) = y(xz) = x(yz)$$

since $s(x, y, z)$ admits a transposition of variables x, y.

(iv) $\Rightarrow$ (i). Suppose $(G, \cdot)$ is commutative and distributive, and $xy^2 = yx^2$. We have

$$\begin{aligned} xy^2 &= (xy^2)(xy^2) = (xy^2)(yx^2) = \big((xy)y\big)\big((yx)x\big) \\ &= \big((xy)y\big)\big((xy)x\big) = (xy)(yx) = (xy)(xy) = xy. \end{aligned}$$

Hence, applying (ii), we get (i).

(v) $\Rightarrow$ (i). Let $(G, \cdot) \in M(\cdot)$ and $xy^2 = xy^3$. Then we prove that $(G, \cdot)$ is a semilattice. We have

$$\begin{aligned} xy &= (xy^2)(yx^2) = (xy^3)(yx^2) \\ &= \Big(\big((xy)y\big)y\Big)\big((yx)x\big) = \Big(\big((xy)y\big)(yx)\Big)(yx) = \Big(\big(y(xy)\big)(xy)\Big)(xy) \\ &= y(xy)^3 = y(xy)^2 = \big(y(xy)\big)(xy) = \big(x(xy)\big)(yy) = \big((yx)x\big)y. \end{aligned}$$

And now

$$(xy)x = \big(((yx)x)y\big)x = \big(((yx)x)x\big)(yx) = (yx)^3(xy) = (yx^2)(xy)$$
$$= ((yx)x)(xy) = ((yx)y)(xx) = ((xy)y)x = xy,$$

whence $(G, \cdot)$ satisfies condition (ii) and therefore it is a semilattice.

(vi) $\Rightarrow$ (i). Assume now that $(G, \cdot)$ satisfies

$$x_1x_2 \ldots x_{n-1}x_n = x_2x_3 \ldots x_{n-1}x_1 \quad \text{for some } n \geqslant 3.$$

Observe that

$$xy = (\ldots(xx)\ldots x)y = x^{n-1}y = x^{n-2}yx = \ldots = yx^{n-1}$$

and

$$xy^2 = x^{n-2}y^2 = yx^{n-2}$$

and

$$xy^3 = (xy^2)y = (yx^{n-2})y = (x^{n-2}y)y = (yy)x^{n-2} = yx^{n-2} = xy^2.$$

Hence we have $xy^k = xy^{k+1}$ for $k = 2, 3, \ldots$, and $yx = xy^{n-1} = xy^{n-2} = yx^2$. So we have $xy = xy^k$ for all k and $xy = xy^{n-1} = (\ldots(xy)\ldots y)y = (\ldots(yy)\ldots y)x = yx$. Consider the polynomial $(xy)z$; we have $(xy)z = (x^{n-2}y)z = (yz)x^{n-2} = (yz)x = x(yz)$, which proves that $(G, \cdot)$ is a semilattice.

Similarly, we prove (vii) $\Rightarrow$ (i).

(viii) $\Rightarrow$ (i). Assume that $(G, \cdot)$ is commutative and

$$(+) \qquad x_1 \ldots x_{k-1}x_kx_{k+1} \ldots x_{n-1}x_n = x_1 \ldots x_{k-1}x_{k+1}x_k \ldots x_{n-1}x_n$$

for some $n \geqslant 3$ and for some k, where $2 \leqslant k \leqslant n-1$. Without loss of generality one can assume that n is the smallest number such that the identity $(+)$ holds in $(G, \cdot)$. If $n = 3$, then it is clear that the groupoid is a semilattice. Assume now that $n \geqslant 4$. If $k \geqslant 3$, then, putting $x_1 = x_2$ in $(+)$, we get a contradiction with the minimality of n. So let $k = 2$. Then in the identity $(+)$ we put $x_n = x_1x_2 \ldots x_{n-1}$. Using the commutativity and idempotency of xy, we have

$$x_1x_2 \ldots x_{n-2}x_{n-1} = (x_1x_3x_2 \ldots x_{n-2}x_{n-1})(x_1x_2 \ldots x_{n-2}x_{n-1})$$
$$= (x_1x_2 \ldots x_{n-2}x_{n-1})(x_1x_3x_2 \ldots x_{n-2}x_{n-1})$$
$$= (x_1x_3x_2 \ldots x_{n-2}x_{n-1})(x_1x_3x_2 \ldots x_{n-2}x_{n-1})$$
$$= x_1x_3x_2 \ldots x_{n-2}x_{n-1} = x_1x_2x_3 \ldots x_{n-2}x_{n-1}.$$

The last identity contradicts the minimality of n.

The proof of the theorem is completed.

We should mention here that the implication (vi) $\Rightarrow$ (i) has been proved by Padmanabhan for $n = 3$ in [9].

Proof of Theorem 9. To prove (i) see (3) of Theorem 2 of [4]. Condition (ii) follows from Theorem 1 and (3) of Theorem 2 of [4].

(iii). Let $(G, \cdot) \in V(\cdot)$ and suppose that the polynomial $(xy^2)x$ is not essentially binary. Since $\cdot$ is idempotent, we have to consider two cases: (1) $(xy^2)x = x$ and (2) $(xy^2)x = y$. If (1), then

$$xy^2 = ((xy^2)x^2)(xy^2) = \big(((xy^2)x)x\big)(xy^2)$$
$$= (xx)(xy^2) = (xy^2)x = x,$$

whence $(G, \cdot) \in V_2(\cdot)$ and by (i), $(G, \cdot)$ is a quasigroup. Assume now that (2) holds. Then

$$x = ((xy^2)x^2)(xy^2) = \big(((xy^2)x)x\big)(xy^2) = (yx)(xy^2)$$
$$= \big(y(xy)\big)(xy) = y(xy)^2,$$

whence

$$x = (xy^2)\big(x(xy^2)\big)^2 = (xy^2)\big((xy^2)x\big)^2 = (xy^2)y^2 = xy^4.$$

So $(G, \cdot) \in V_4(\cdot)$ and therefore again, by (i), $(G, \cdot)$ is a quasigroup.

(iv). Assume that $(G, \cdot) \in Q_{m,n}(\cdot)$ for some m and n. This means that $(G, \cdot)$ satisfies $xy^m = x$ and $y^nx = y\big(y(\ldots(yx))\ldots\big) = x$. Using the same method as in the proof of (3) of Theorem 2 of [4], one can show that $(G, \cdot)$ is a quasigroup.

Proof of Theorem 10. Let $(G, \cdot) \in Q_{2,n}(\cdot)$ for a certain $n \geqslant 2$. Then $(G, \cdot)$ satisfies $y(yx) = x = xy^n$. Let $x + y = xy^{n-1}$. We have

$$x = (xy^{n-1})y \quad \text{and} \quad y = (xy^{n-1})\big((xy^{n-1})y\big) = (xy^{n-1})x,$$

whence

$$x + y = xy^{n-1} = (xy^{n-1})x^n = \big((xy^{n-1})x\big)x^{n-1} = yx^{n-1} = y + x.$$

Further, we have

$$x + 2y = (x+y) + y = (xy^{n-1})y^{n-1} = (xy^n)y^{n-2} = xy^{n-2}.$$

In general, $x + ky = xy^{n-k}$. Hence $xy = x + (n-1)y$ and $x + ny = (xy)y^{n-1} = xy^n = x$. So, $A(G, \cdot) \subseteq A(G, +)$. Since $x + y = xy^{n-1}$ and $xy = x + (n-1)y$, we see that $(G, \cdot)$ and $(G, +)$ are polynomially equivalent and in addition $(G, +) \in V_n(+)$ if $(G, \cdot)$ is idempotent. The proof of the theorem is completed.

References

[1] W. Belousow, *Introduction in the theory of quasigroups and loops*, Moscow 1967 (in Russian).

[2] J. Dudek, *A characterization of some idempotent abelian groupoids*, Colloq. Math. 30 (1974), pp. 204–209.

[3] J. Dudek, *Medial groupoids and Mersenne numbers*, Fund. Math. 114 (1981), pp. 235–256.

[4] — *On binary polynomials in idempotent commutative groupoids*, Fund. Math. 120 (1983), pp. 165–169.

[5] —, *Polynomials in idempotent commutative groupoids*, Dissertationes Math. (to appear).

[6] G. Grätzer, *Universal Algebra*, Springer-Verlag, 1979.

[7] — and J. Płonka, *On the number of polynomials of an idempotent algebra* I, Pacific J. Math. 32 (1970), pp. 697–709.

[8] E. Marczewski, *Independence and homomorphism in abstract algebras*, Fund. Math. 50 (1961), pp. 45–61.

[9] R. Padmanabhan, *On axioms for semilattices*, Canad. Math. Bull. 9 (1966), pp. 357–358.

[10] J. Płonka, *On equational classes of abstract algebras defined by regular equations*, Fund. Math. 64 (1969), pp. 241–247.

Accepté par la Rédaction le 18.5.1981

On elementary cuts in recursively saturated models of Peano Arithmetic

by

Henryk Kotlarski (Warszawa)

Abstract. If M is a model of Peano Arithmetic, let $Y = \{N \subsetneq_e M\colon N \prec M\}$; we study this family under the assumption that M is countable and recursively saturated.

§ 1. Introduction and notation. Let PA denote Peano Arithmetic in any of its usual formalizations. For $M \models \mathrm{PA}$ we set $Y^M = \{N \subsetneq_e M\colon N \prec M\}$; when no confusion arises we omit the superscript M. Clearly the properties of this family depend on M; we shall study this family under the assumption that M is countable and recursively saturated. In § 2 we show that M has many cuts which have some combinatorial properties introduced by Kirby and Paris (see [1]), in § 3 we show many non-isomorphic elements of Y and in § 4 we study the connection between elementary cuts of M and automorphisms of M.

We use standard terminology and notation. We assume that the reader knows the notion of recursive saturation (see Schlipf [9] and Smorynski [10] for a survey of recursively saturated models of PA) and knows the notion of a satisfaction class studied in some depth by Krajewski [6] and in several more recent papers; also some knowledge of initial segments (= cuts) in models of PA (see e.g. Kirby [3]) is required (however, we shall define the combinatorial properties of cuts in the body of the paper). The present paper has grown out from our earlier paper [4], where Theorem 1.1 below was proved. The results of [4] and the present paper were annouced in abstract [5].

Before we state the main result of [4], we need some more notation:

$$Y_1 = \{N \in Y\colon N \text{ is not recursively saturated}\}.$$

For $a \in M$ we denote $M(a) = \{x \in M\colon$ for some parameter-free term $t(v)\ M \models x < t(a)\}$.

The following notion is taken from [1]. Two families A, B of cuts of $M \models \mathrm{PA}$ are symbiotic iff, for all $a, b \in M$

$$(\exists N \in A\ a < N < b) \equiv (\exists N \in B\ a < N < b).$$