COMMUTING POLINOMIALS IN THE MEDIAL QUASIGROUPS

Vladimir IZBAŞ

Institute of Mathematics and Computer Science, Academy of Sciences of Moldova,
str. Academiei 5, MD-2028 Chisinau, Moldova,
vizb@math.md

Abstract: Some properties of medial quasigroups are studied. It is proved that all parastrophes of the medial quasigroups are medial and any two polynomial are commuting.

A universal algebra (brifly algebra) is a cuple (Q,Σ) where Q is a set and Σ is a collection of finitary operations on Q. Collection Σ is called the signature of universal algebra (Q,Σ). Each finitary operation $f\in\Sigma$ is a single valued function which assigns to every n-tuple $a_1,a_2,\ldots,a_n$ of elements of Q a unique element (value) of Q denoted by $f(a_1,a_2,\ldots,a_n)$. Natural number n is called the arity of operation n.

A polynomial (word) in a signature Σ and variables $x,y,z,u,v,\ldots$ is defined inductively:

1. the variables $x,y,z,u,v,\ldots$ are polynomials;
2. if $p_1,p_2,\ldots,p_n$ are polynomials and $f\in\Sigma$ is an operation symbol of arity n then $f(p_1,p_2,\ldots,p_n)$ is a polynomial;
3. polynomials are obtained only by steps 1 and 2.

The length of polynomial $f(p_1,p_2,\ldots,p_n)$ is denoted by $l(f(p_1,p_2,\ldots,p_n))$ and is defined by $l(f(p_1,p_2,\ldots,p_n))=l(p_1)+l(p_2)+\ldots+l(p_n)$, where the length of a variable is taken as 1. Strictly speaking the length of a polynomial $p(x,y,z,\ldots)$ is the number of occurrences of variables in it. The collection of all polynomials in a signature Σ and variables from the countable set X we shall denote by $P(X,\Sigma)$.

Each polynomial $f(x_1,x_2,\ldots,x_n)$ in the variables $x_1,x_2,\ldots,x_n$ can be regarded as a $n-$ary function ($n-$ary operation) defined on the set of elements of a given algebra, denoted also by f and termed as polynomial function (polynomial operation). The result (value) of the polynomial function (polynomial operation, polynomial) f applied to the elements $a_1,a_2,\ldots,a_n$ of an algebra (Q,Σ) is the element which is obtained by substituting the elements $a_1,a_2,\ldots,a_n$ instead of corresponding variables $x_1,x_2,\ldots,x_n$ in the polynomial $f(x_1,x_2,\ldots,x_n)$ and performing within the given algebra the operations specified in the record of the polynomial.

Let be (Q,Σ) an algebra and $G\subseteq Q$. The subalgebra $<G>$ of (Q,Σ) generated by G is the intersection of all subalgebra of (Q,Σ) containing the subset $G\subseteq Q$. It is well known that the subalgebra $<G>$ of (Q,Σ) generated by G is the collection of all values of polynomials from $P(X,\Sigma)$, when the polynomial variables receive values in G, that is

$$<G>=\{w(g_1,\ldots,g_n)\mid w(x_1,\ldots,x_n)\in P(X,\Sigma),$$
$$,g_i\in G, i\in\overline{1,n}, n\geq 1\}$$

A groupoid is a pair $(Q,\cdot)$, where Q is a set and "$\cdot$" a binary operation on Q a function from $Q\times Q$ to Q. We usually write the image of the operation on the pair (a,b) as $a\cdot b$ or ab and shall it called the product ab. A groupoid $(Q,\cdot)$ is called a quasigroup if and only if the equations

$$a\cdot x=b,\quad y\cdot a=b \qquad (1)$$

are unique solutions in Q for any $a,b\in Q$ [2], that is the mappings $L_a:Q\to Q,\ L(x)=ax$, $R_a:Q\to Q,\ R(x)=xa$ are permutations of Q for any $a\in Q$.

The equations (1) define two new binary operations, left division \ and right division /,

respectively, such that $a \setminus b = x$, $b / a = y$. So, for every $x, y, z \in Q$,

$$x \cdot y = z \Leftrightarrow x \setminus z = y \Leftrightarrow z / y = x. \quad (2)$$

In a quasigroup $(Q, \cdot)$ left and right division operations are often called as inverse operations of "$\cdot$". Both of the inverse operations of $(Q, \cdot)$ are also quasigroups and they have division operations.

The right division operation of $\setminus$ we shall denoted by ∇, so

$$x \nabla y = z \Leftrightarrow z \setminus y = x \Leftrightarrow z \cdot x = y.$$

The left division operation of $/$ we shall denoted by Δ, so

$$x \Delta y = z \Leftrightarrow x / z = y \Leftrightarrow y \cdot z = x.$$

By "$*$" is denoted the dual of "$\cdot$", i. e.

$$x * y = z \Leftrightarrow y \cdot x = z$$

for all $x, y, z \in Q$.

These five operations $\setminus, /, *, \nabla, \Delta$ are quasigroup operations, and are said to be parastrophes (or conjugates) of "$\cdot$".

Analoguously with (2) we obtain

$$x \cdot y = z \Leftrightarrow y \nabla z = x \Leftrightarrow z \Delta x = y \quad (3)$$

for every $x, y, z \in Q$.

Also it is easy to check that the following equalities

$$\begin{array}{ll} x \cdot (x \setminus y) = y, & x \setminus (x \cdot y) = y, \\ (y \cdot x) / x = y, & (y / x) \cdot x = y, \\ y / (x \setminus y) = x, & (y / x) \setminus y = x. \end{array} \quad (4)$$

hold for every elements $x, y \in Q$.

Conversely, if an algebra $(Q, \cdot, \setminus, /)$ with three binary operations $(\cdot)$, $(\setminus)$ and $(/)$, satisfies the identities

$$\begin{array}{lll} y \cdot (y \setminus x) = x, & y \setminus (y \cdot x) = x, & (x \cdot y) / y = x, \\ & (x / y) \cdot y = x & \end{array},$$

then $(Q, \cdot)$ is a quasigroup.

The algebra $(Q, \cdot, \setminus, /)$ with binary operations $(\cdot)$, $(\setminus)$ and $(/)$, satisfying the identities (4) is called a primitiv quasigroup or equational quasigroup (equasigroup). The systems of quasigroups and equational quasigroups are equivalent, but the system of equational quasigroups is a variety while the system of quasigroups is not one. An other advantage of the equational quasigroups is connected with the property of generating subquasigroups.

So, if $(Q, \cdot)$ is a quasigroup and $G \subseteq Q$, then

$$< G >= \{w(g_1, \ldots, g_n) \mid w(x_1, \ldots, x_n) \in$$

$$\in P(X, \{\cdot, \setminus, /\}),\ g_i \in G, i \in \overline{1, n}, n \geq 1\}$$

where $< G >$ is a suquasigroup generated by G.

If a quasigroup $(Q, \cdot)$ is finite, then the following statement is true.

Theorem 1. *Let be $(Q, \cdot)$ a finite quasigroup and $G \subseteq Q$. Then*

$$< G >= \{w(g_1, \ldots, g_n) \mid w(x_1, \ldots, x_n) \in$$

$$\in P(X, \{\cdot\}),\ g_i \in G, i \in \overline{1, n}, n \geq 1\}$$

i. e. $< G >$ consists of all possible products with a finite number of factors of G and the various ways of combining the factors.

Proof. We denote

$$H = \{w(g_1, \ldots, g_n) \mid w(x_1, \ldots, x_n) \in$$

$$\in P(X, \{\cdot\}),\ g_i \in G, i \in \overline{1, n}, n \geq 1\}$$

It is easy to see that $H \cdot H \subseteq H$ and $G \subseteq H$. So, $(H, \cdot)$ is a finite subgroupoid of quasigroup $(Q, \cdot)$ and then $(H, \cdot)$ is a subquasigroup of $(Q, \cdot)$. On the other hand it is clear that $H \subseteq < G >$. Therefore $< G >= H$.

The theorem is not valid if $(Q, \cdot)$ is an infinite quasigroup.

A quasigroup $(Q, \cdot)$ is said to be a medial quasigroup if for every $a, b, c \in Q$ the equality

$$(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d)$$

holds [3,4].

Lemma 2. *In a quasigroup* $(Q,\cdot)$ *the following identities are equivalent:*

(1) $xy\cdot uv = xu\cdot yv$;
(2) $(x/y)/(u/v) = (x/u)/(y/v)$;
(3) $(x\backslash y)\backslash(u\backslash v) = (x\backslash u)\backslash(y\backslash v)$;
(4) $(x*y)*(u*v) = (x*u)*(y*v)$;
(5) $xy\backslash uv = (x\backslash u)\cdot(y\backslash v)$;
(6) $xy/uv = (x/u)\cdot(y/v)$;
(7) $(x/y)\backslash(u/v) = (x\backslash u)/(y\backslash v)$,

where $(Q,\backslash)$, $(Q,/)$ *and* $(Q,*)$ *are the parastrofs of a quasigroup* $(Q,\cdot)$.

Proof. (2) $\Rightarrow$ (6). Assume $(x/y)/(u/v) = (x/u)/(y/v)$ for all $x,y,u,v\in Q$. With x replaced by xy and u replaced by uv, this becomes $(xy/y)/(uv/v) = (xy/uv)/(y/v)$. From this, using the identity $yx/x = y$, we obtain $x/u = (xy/uv)/(y/v)$ and, using the identity $(y/x)x = y$, we obtain $(x/u)\cdot(y/v) = xy/uv$ which is the identity (6).

(6) $\Rightarrow$ (1). Suppose, now, that the identity $xy/uv = (x/u)\cdot(y/v)$ is fulfilled in the algebra $(Q,\cdot,\backslash,/)$. Then, using the identity $(y/x)x = y$, we obtain $xy = ((x/u)\cdot(y/v))\cdot uv$. With xu in place of x and yv in place of y this becomes $xu\cdot yv = ((xu/u)\cdot(yv/v))\cdot uv$ and, using the identity $yx/x = y$, we obtain $xu\cdot yv = xy\cdot uv$ which is the identity (1).

(1) $\Rightarrow$ (5). Assume $xy\cdot uv = xu\cdot yv$ for all $x,y,u,v\in Q$. With u replaced by $x\backslash u$ and v replaced by $y\backslash v$, this becomes

$$xy\cdot((x\backslash u)\cdot(y\backslash v)) = (x\cdot(x\backslash u)\cdot(y\cdot(y\backslash v)).$$

From this, using the identity $x\cdot(x\backslash y) = y$, we obtain $xy\cdot((x\backslash u)\cdot(y\backslash v)) = uv$ and, using the identity $x\backslash(x\cdot y) = y$, we obtain $(x\backslash u)\cdot(y\backslash v) = xy\backslash uv$ which is the identity (5).

(5) $\Rightarrow$ (3). Suppose, that the identity $xy\backslash uv = (x\backslash u)\cdot(y\backslash v)$ holds in the algebra $(Q,\cdot,\backslash,/)$. Then, using the identity $x\backslash(x\cdot y) = y$, we obtain $(x\backslash u)\backslash(xy\backslash uv) = (y\backslash v)$. With $x\backslash y$ in place of y and $u\backslash v$ in place of v this becomes $(x\backslash u)\backslash((x\cdot(x\backslash y))\backslash(u\cdot(u\backslash v))) = (x\backslash y)\backslash(u\backslash v)$ and, using the identity $x\cdot(x\backslash y) = y$, we obtain $(x\backslash u)\backslash(y\backslash v) = (x\backslash y)\backslash(u\backslash v)$ which is the idenity (3).

(3) $\Rightarrow$ (7). Let be $(x\backslash y)\backslash(u\backslash v) = (x\backslash u)\backslash(y\backslash v)$ for all $x,y,u,v\in Q$. With x replaced by u/x and y replaced by v/y, this becomes $((u/x)\backslash(v/y))\backslash(u\backslash v) = ((u/x)\backslash u)\backslash((v/y)\backslash v)$ From this, using the identity $(y/x)\backslash y = x$, we obtain $((u/x)\backslash(v/y))\backslash(u\backslash v) = x\backslash y$ and, using the identity $x\cdot(x\backslash y) = y$, we obtain

$$u\backslash v = ((u/x)\backslash(v/y))\cdot(x\backslash y).$$

From this, using the identity $yx/x = y$, we obtain $(u\backslash v)/(x\backslash y) = (u/x)\backslash(v/y)$ which is (7).

(7) $\Rightarrow$ (2). Suppose, that the identity $(x/y)\backslash(u/v) = (x\backslash u)/(y\backslash v)$ holds in the algebra $(Q,\cdot,\backslash,/)$. With x replaced by u/x and y replaced by v/y, this becomes $((u/x)/(v/y))\backslash(u\backslash v) = ((u/x)\backslash u)/((v/y)\backslash v)$. From this, using the identity $(y/x)\backslash y = x$, we obtain $((u/x)/(v/y))\backslash(u\backslash v) = x/y$ and, by the identity $x\cdot(x\backslash y) = y$, we obtain $u/v = ((u/x)/(v/y))\cdot(x/y)$. From this, by the identity $yx/x = y$, we obtain $(u/v)/(x/y) = (u/x)/(v/y)$ which is (2).

(1) $\Leftrightarrow$ (3). Let $x,y,u,v\in Q$ be arbitrary elements. Then

$$(x*y)*(u*v) = (u*v)\cdot(x*y) = (v\cdot u)\cdot(y\cdot x)$$
$$(x*u)*(y*v) = (y*v)\cdot(x*u) = (v\cdot y)\cdot(u\cdot x)$$

So, (1) $\Leftrightarrow$ (3), and the lemma is prooved.

Colorary 3. *If* $(Q,\cdot)$ *is a medial quasigroup, then all its parastrofes, are medial quasigroups.*

The following statement generalizes some rezults from [4], formulated for the finite medial quasigroup in the signature $(\cdot)$.

Theorem 4. *Let* $(Q,\cdot)$ *be a medial quasigroup,* $P(x,y,\ldots,z)$ *and* $R(u,v,\ldots,w)$ *be polynomial in the signature* $\Sigma=\{\cdot,\backslash,/\}$. *Then*

$$P(R(a,b,\ldots,c),R(d,e,\ldots,f),\ldots,R(p,q,\ldots,r))=$$
$$=R(P(a,d,\ldots,p),P(b,e,\ldots,q),\ldots,P(c,f,\ldots,r))$$

for all $a,b,\ldots,c,d,e,\ldots,f,\ldots,p,q,\ldots,r\in Q$.

To prove this we applied mathematical induction on the length of the polynomials.

Colorary 5. *Let* $(Q,\cdot)$ *is a medial quasigroup,* $P(x)$ *and* $R(u,v,\ldots,w)$ *be polynomials in the signature* $\Sigma=\{\cdot,\backslash,/\}$. *Then*

$$P(R(a,b,\ldots,c))=R(P(a),P(b),\ldots,P(c))$$

for all $a,b,\ldots,c\in Q$, *that is the function* $P:Q\to Q, a\to P(a), \forall a\in Q$ *is an endomorphism of* $(Q,\{\cdot,\backslash,/\})$.

Example 6. *For polynomials* $P(x,y,z)=(x/y)\backslash z$ *and* $R(u,v,w)=u\cdot(v/w)$ *we have*

$$P(R(a,b,c),R(d,e,f),R(p,q,r))=$$

$$=((a\cdot(b/c))/(d\cdot(e/f)))\backslash(p\cdot(q/r))=$$

$$=[((a/d)\cdot((b/c)/(e/f))]\backslash(p\cdot(q/r))=$$

$$=((a/d)\backslash p)\cdot[((b/c)/(e/f))\backslash(q/r)]=$$

$$=((a/d)\backslash p)\cdot[((b/e)/(c/f))\backslash(q/r)]=$$

$$=((a/d)\backslash p)\cdot[((b/e)\backslash q)/((e/f)\backslash r)]=$$

$$=R(P(a,d,p),P(b,e,q),P(c,f,r))$$

References

1. I. Mal'tsev. *On the general theory of algebraic systems.* (Russian), Matem. sbornik, 1954, 35(1), 3-20.
2. V. D. Belousov. *Foundations of the theory of quasigroups and loops* .(Russian), Izdat. "Nauka", Moscow, 1967, 223 pp.
3. D.C.Murdoch. *Quasigroups which satisfy certain generalized associative law*, Amer. J. Math. **61** (1939), 509-522.
4. D.C.Murdoch. *Structure of abelian quasigeroups*, Trans. Amer. Math. Soc. **49** (1941), 392-409.