Remarks to the first publications
of V. D. Belousov

Wieslaw A. Dudek and Victor A. Shcherbacov

Abstract

We give a short survey and comments to the Belousov's results published in the articles which have not been reviewed neither in Mathematical Reviews nor in Zentralblatt für Mathematik and are not well-known for the Western mathematicians.

A part of the first Belousov's results is contained in the papers which were published in small local Russian (Moldavian) journals. Since the most part of those journals were not reviewed neither in Mathematical Reviews nor in Zentralblatt für Mathematik, the results are unknown in general.

We give a short survey of these papers below. We present them in a chronological order and add some comments because several years ago some of these results were generalized by Belousov himself or by his pupils.

We also describe these Belousov's papers which were reviewed (in German) only in Zentralblatt für Mathematik. Some of these papers are reviewed in Referativnyi Zhurnal of Math. (in Russian) by L. M. Gluskin, E. S. Lyapin, B. M. Schein, A. I. Shirshov and others.

We save Belousov's style and terminology.

1. Regular groups of permutations in quasigroups [1]

Let \((M, A)\) be a quasigroup. The set of all permutations \(\lambda\) of the set \(M\) satisfying the identity \(\lambda A(x, y) = A(\lambda x, y)\) forms a group which is denoted by \(L_A\) and is called a group of left regular permutations of \((M, A)\).

2000 Mathematics Subject Classification: 20N05

Keywords: Operation, complete operation, quasigroup, orthogonality, mediality, left \(F\)-quasigroup, left distributive quasigroup, functional equation.
Similarly, the set of all permutations \( \rho \) of \( M \) satisfying the identity \( \rho A(x, y) = A(x, \rho y) \) forms a group \( R_A \) of right regular permutations of \((M, A)\). Also the set of all permutations \( \varphi \) of \( M \) for which there exists such permutation \( \varphi^* \) of \( M \) that \( A(\varphi x, y) = A(x, \varphi^* y) \) is valid for all \( x, y \in M \) forms a group. This group is denoted by \( C_A \) and is called a group of middle regular permutations of \((M, A)\).

A triple \((L_A, C_A^*, R_A^*)\), where \( R_A^* \) and \( C_A^* \) are groups anti-isomorphic to \( C_A \) and \( R_A \) respectively, is called a type of a quasigroup \((M, A)\). A type \((L', C', R')\) is a subtype of a type \((L, C, R)\) if groups \( L', C', R' \) are isomorphic to some subgroups of groups \( L, C, R \) respectively.

**Theorem 1.** If a quasigroup \((M, B)\) is isotopic to a loop \((M, A)\), then the type of \((M, B)\) is a subtype of \((M, A)\).

Results of this article are repeated in [11] and in the book [18].

2. On the structure of distributive quasigroups [2]

It is an abstract of Belousov’s lecture presented at the All-Union Colloquium on General Algebra organized by Moscow State University in February 1958. Later these results were proved in [16].

A quasigroup \((M, \cdot)\) in which \( x \cdot y = y \cdot x \) and \( (x \cdot x) \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z) \) hold for all \( x, y \in M \) is called a commutative Moufang loop (CML). Please note that Belousov knew the fact that a quasigroup satisfying these two identities is a loop.

The following famous Belousov’s theorem is announced in this note:

**Theorem 2.** Any distributive quasigroup is isotopic to a CML.

A permutation \( \varphi \) of a distributive quasigroup \((M, \circ)\) is called regular if there exist such permutation \( \varphi^* \) of the set \( M \) that

\[
\varphi x \circ y = x \circ \varphi^* y
\]

holds for all \( x, y \in M \).

The set of all such permutations forms a group denoted by \( C_0 \). The set of all elements of the form \( \varphi(1) \), where 1 is the identity of a CML \((M, \cdot)\) isotopic to \((M, \circ)\) and \( \varphi \in C_0 \), is denoted by \( C_0(1) \). A distributive quasigroup \((M, \circ)\) for which \( C_0(1) = M \) is called transitive.

**Theorem 3.** \( C_0(1) \) is a normal transitive subquasigroup of a distributive quasigroup \((M, \circ)\) and \((M, \circ)/C_0(1)\) is a distributive TS-quasigroup.
**Theorem 4.** Any three elements of a distributive quasigroup $(M, \circ)$ generate a transitive distributive quasigroup and so do any four elements $a, b, c, d$ which satisfy the medial law $(a \circ b) \circ (c \circ d) = (a \circ c) \circ (b \circ d)$.

**Theorem 5.** Any CML of odd order is isotopic to a commutative distributive quasigroup.

### 3. Associative systems of quasigroups [3]

It is an abstract of the second Belousov’s lecture presented at the All-Union Colloquium on General Algebra organized by Moscow State University in February 1958. These results were proved later in [17].

Let $\Omega_M$ be the set of all binary quasigroup operations defined on a finite or infinite set $M$.

A system of operations $\Sigma \subset \Omega_M$ is called associative from the left side, if for any two operations $A, B \in \Sigma$ there exist such operations $A', B' \in \Sigma$ that the following identity

$$A(B(x, y), z) = A'(x, B'(y, z))$$

(1)

is satisfied. Analogously, a system of operations associative from the right side is defined. A system which is associative from the both sides is called associative.

R. Schaufler proved in [34] that $\Omega_M$ is an associative system only in case $|M| \leq 3$. He also constructed an associative system $\Sigma$ on $M$ containing four elements and posed a problem of a construction of all such systems.

The answer is given by the following Belousov’s theorem now called **Theorem about four quasigroups:**

**Theorem 6.** Any four quasigroup operations satisfying the identity (1) are isotopic to the same group $(M, \cdot)$. Moreover, all these operations have the form $C(a, b) = \varphi a \cdot t \cdot \psi b$, where $\varphi, \psi$ are automorphisms of $(M, \cdot)$ and $t$ is a fixed element of $M$.

The proof is given in [17]. Some modifications of this proof are presented in the book [21] and [13].

This theorem gives the possibility of the construction of left (right) associative systems of quasigroup operations on any finite or infinite set. Belousov observed that there exist left but non-right associative systems of quasigroup operations.

A quasigroup \((G, \cdot)\) with the identity \((ab)c = \varphi a(\psi b \cdot \chi c)\), where \(\varphi, \psi, \chi\) are fixed permutations of the set \(G\), is called a \(D\)-quasigroup.

It is proved that a quasigroup \((Q, \circ)\) with the operation of the form \(a \circ b = (\pi a) \cdot q \cdot (\rho b)\), where \(\pi, \rho\) are fixed automorphisms of a group \((Q, \cdot)\) and \(q\) is a fixed element of \(Q\), is a \(D\)-quasigroup.

Any \(D\)-quasigroup can be obtained in this way.

5. A semigroup of binary operations ... [5]

It is an abstract of a lecture given at the Second Soviet Colloquium on General Algebra organized by Moscow State University in April 1959. These results were included later to the article [7].

Two operations \(A\) and \(B\) defined on the same set \(M\) are called compatible if the system of equations \(A(x, y) = a, B(x, y) = b\) is compatible, i.e., has a unique solution for any \(a, b \in M\). (Now such operations are called orthogonal.) Operations \(A\) and \(B\) are called uniform, if there exists a pair of compatible operations \(C, D\) such that

\[ A(a, b) = B(C(a, b), D(a, b))\]

holds for all \(a, b, c \in M\).

V. D. Belousov wrote that an isotopy and an isomorphism of binary operations can be considered as a partial case of the uniformity of binary operations.


It is an abstract of a lecture at the Second Soviet Colloquium on General Algebra (Moscow State University, April 1959).

Let \(\Phi_M\) be the set of all quasigroup operations defined on a set \(M\). A system \(\Sigma \subseteq \Phi_M\) is called medial if for any three operations \(A, B, C \in \Sigma\) there exist operations \(A', B', C'\) such that

\[ A(B(a, b), C(c, d)) = A'(B'(a, c), C'(b, d))\]

for all \(a, b, c \in M\).

It is announced that any operation \(F\) belonging to a medial system \(\Sigma\) can be written in the form \(F(a, b) = \varphi a \cdot t \cdot \psi b\), where \((M, \cdot)\) is a commutative group, \(\varphi, \psi \in Aut(M, \cdot)\) and \(t\) is a fixed element of \(M\).
7. On the properties of binary operations [7]

Let $\Omega_M$ be the set of all binary operations defined on a set $M$. An operation $A \in \Omega_M$ is called an invertible from the right side if for any $a, b \in M$ there exists such uniquely determined $x \in M$ that $A(a, x) = b$. Analogously an operation invertible from the left side is defined. Operations $A, B \in \Omega_M$ are said to be of one-type if there exists a permutation $\varphi$ of the set $M \times M$ such that $B = A\varphi$, i.e., $B(a, b) = A(a', b')$, where $(a', b') = \varphi(a, b)$ for all $a, b \in M$. Operations which are one-type with the projection $E(a, b) = b$ are called complete. Operations invertible from the left (right) side are complete. But there are examples of complete operations which are not invertible neither from the left nor from the right.

For any complete operation $A \in \Omega_M$ there is in $\Omega_M$ at least one operation $B$ compatible with $A$. If $A$ is not complete, then there are no operations compatible with $A$. Obviously, the operations compatible with a complete operation are also complete. All such operations can be written in the form $K(B, A)$, where $B$ is an operation compatible with $A$, $K$ is an invertible from the left side operation, and $K(B, A)(a, b) = K(B(a, b), A(a, b))$ for all $(a, b) \in M \times M$. For different $K$ we obtain different operations $K(B, A)$.

Each permutation $\varphi$ of the set $M \times M$ is uniquely determined by a pair of compatible complete operations $A, B \in \Omega_M$. Namely, $\varphi(a, b) = (A(a, b), B(a, b))$ for all $(a, b) \in M \times M$.

On the set $\Omega_M$ we can consider two operations $\circ$ and $\bullet$ defined in the following way:

$$(A \circ B)(a, b) = A(B(a, b), b), \quad (A \bullet B)(a, b) = A(a, B(a, b)).$$

Since these operations are associative, the algebra $(\Omega_M, \circ, \bullet)$ is called a semigroup of operations. A subset $\Sigma$ of $\Omega_M$ is called a mixed basis of $(\Omega_M, \circ, \bullet)$ if each operation from $\Omega_M$ can be expressed by $\circ$, $\bullet$ and some operations belonging to $\Sigma$.

It is proved, that in the case when $M$ is finite and has more than four elements (for convenience $M$ is represented as a ring of integers modulo $n$), then $(\Omega_M, \circ, \bullet)$ has a basis containing only two operations $S$ and $K$, where $S$ is an addition in the ring $M$, and $K$ is defined by the formula $K(0, 0) = 1$ and $K(a, b) = 0$ in other cases. This basis is minimal.

Now, the operations $\circ$ and $\bullet$ are called the Mann's compositions. Algebras of the form $(\Omega_M, \circ, \bullet)$ are called $(2, 2)$-semigroups of operations. Different sets of $n$-ary operations (or partial $n$-place functions) closed with respect to some generalizations of the above compositions and having some other properties were studied by K. Denecke, W. A. Dudek, H. Länger,
8. On one class of quasigroups [8]

Let \((M, A)\) be a quasigroup. For any fixed element \(a \in M\) the equality \(A(A(a, b), c) = A(a, A_a(b, c))\) defines on \(M\) a new quasigroup operation \(A_a(b, c)\). If all quasigroups \((M, A_a)\) are isomorphic to \((M, A)\), i.e., if for every \((M, A_a)\) there exists a permutation \(\alpha (\alpha \text{ depends on } a)\) such that \(A_a(b, c) = \alpha^{-1}A(\alpha b, \alpha c)\), then a quasigroup \((M, A)\) is called a left \(G\)-quasigroup. For a given \((M, A)\) the set of all such permutations forms a group denoted by \(\Phi_A\) (Theorem 2 in [8]). Moreover, if \((M, A)\) is a left \(G\)-quasigroup, then also every \((M, A_a)\) is a left \(G\)-quasigroup.

For any fixed \(a, b \in M\) the equation \(A(A(a, b), c) = A(a, A(b, x))\) defines on \(M\) such permutation \(S_{a,b}\) that \(S_{a,b}c = x\). A quasigroup \((M, A)\) in which each permutation \(S_{a,b}\) depends only on \(a\) is called a left \(F\)-quasigroup. In this case \(S_{a,b}\) is denoted by \(S_a\). So, a left \(F\)-quasigroup can be defined as a quasigroup satisfying the identity \(A(A(a, b), c) = A(a, A(b, S_a c))\). Earlier such quasigroups were studied by D. C. Murdoch [33], but the name "\(F\)-quasigroup" probably was firstly used by V. D. Belousov.

Every left \(F\)-quasigroup with a left identity is a left \(G\)-quasigroup (Theorem [8]). From this it follows that any left \(F\)-quasigroup is isotopic to a left \(G\)-quasigroup.

A quasigroup is called left simple if \(A_a = A_b\) implies \(a = b\).

Any left distributive quasigroup is isotopic to some left simple \(F\)-quasigroup with the left identity (Theorem 3 [8]).

An element \(e_a\) of a quasigroup \((M, A)\) is called a right local identity for \(a \in M\) if \(A(a, e_a) = a\). A left local identity is defined analogously.

Using these identities V. D. Belousov re-proved the following theorem firstly proved by D. C. Murdoch [33].

**Theorem 7.** A left \(F\)-quasigroup \((M, A)\) can be homomorphically mapped onto a \(F\)-quasigroup of all right local identities of \((M, A)\).

The set

\[
A^l = \{ z \in M \mid A(A(z, a), b) = A(z, A(a, b)) \text{ for all } a, b \in M \}
\]

is called a left associator of a quasigroup \((M, A)\). For left \(F\)-quasigroups it is a normal (associative) subquasigroup. In this case the factor-quasigroup
$M/A^1$ is isomorphic to a subquasigroup of all right local identities of $(M, A)$ (Theorem 5).

Let $\Gamma_A$ be a group of all automorphisms of a left $F$-quasigroup $(M, A)$ and let $\Sigma_A$ be a group generated by all permutations $S_a$ of $M$.

**Theorem 8.** (Theorem 7) If a left $F$-quasigroup $(M, A)$ has a left identity, then $\Sigma_A$ is a normal subgroup of $\Phi_A$, $\Gamma_A \cap \Sigma_A$ is a normal subgroup of $\Gamma_A$ and $\Phi_A = \Gamma_A \Sigma_A$.

In the end of this article V. D. Belousov proved that a left $F$-quasigroup with a left identity for which the set of all permutations $S_a$ is closed with respect to the multiplication of permutations is isotopic to a group.

9. **Globally transitive quasigroups** [9]

Let $\Omega_M$ be the set of all invertible operations defined on $M$. It is clear that $\Omega_M$ contains all quasigroup operations defined on $M$.

A subset $\Sigma$ of $\Omega_M$ is called a **globally weakly transitive system of quasigroups** (briefly: $\mathcal{T}$-system), if for any $A, B, C \in \Sigma_M$ there exists an operation $D \in \Omega_M$ such that

$$A(B(b, a), C(c, a)) = D(b, c)$$

for all $a, b, c \in M$. In the case when $D \in \Sigma$ we say that $\Sigma$ is a **globally transitive system of quasigroups** (briefly: $\mathcal{T}$-system).

A permutation $\alpha$ of $M$ is called a **quasi-automorphism** of a group $(M, \cdot)$, if $\alpha(ab) = \alpha a \cdot (\alpha 1)^{-1} \cdot ab$ for all $a, b \in M$, where $1$ is the identity of $(M, \cdot)$.

It is proved that if in a group $(M, \cdot)$ the identity $\alpha(ab) = \beta a \cdot \gamma b$, where $\alpha, \beta, \gamma$ are permutations of $M$, is satisfied, then permutations $\alpha, \beta, \gamma$ are quasi-automorphisms of $(M, \cdot)$. Moreover, if $\Sigma \subset \Omega_M$ is a $\mathcal{T}$-system, then on $M$ can be defined a group $(M, \cdot)$ such that any operation $A \in \Sigma$ can be presented in the form $A(a, b) = q \sigma(ab^{-1})$, where $q$ is a fixed element of $M$ and $\sigma$ is an automorphism of $(M, \cdot)$.

If $\Sigma \subset \Omega_M$ is a $\mathcal{T}$-system, then on $M$ it can be defined a group $(M, \cdot)$ with the center $C$ such that any operation $A \in \Sigma$ can be presented in the form $A(a, b) = ab^{-1}t$, where $t$ is an element of a fixed coset (the same for all operations) of $C$ by some subgroup $Z_0$ of $C$.

10. **Closed systems of mutually orthogonal quasigroups** [10]

It is an abstract of Belousov’s lecture at the IV-th Soviet Meeting on General Algebra (Kiev 1962).
Let’s remind that quasigroups \((M, A_i)\) and \((M, A_j)\) are orthogonal, if the system of equations \(A_i(x, y) = a, A_j(x, y) = b\) has a unique solution for all \(a, b \in M\).

Let \(\Sigma = \{E, F, A_1, A_2, \ldots, A_{s-2}\}\) be a system of binary operations defined on a finite set \(M\), where \(E(a, b) = b, F(a, b) = a\) for all \(a, b \in M\), and \(A_1, \ldots, A_{s-2}\) are mutually orthogonal quasigroup operations. A system \(\Sigma\) is closed if it is closed with respect to the following composition of operations \(A_i A_j(a, b) = A_i(a, A_j(a, b))\).

V. D. Belousov announced that he found the necessary and sufficient conditions under which a system \(\Sigma\) is closed. He also announced that if in a closed system \(\Sigma\), where \(s \geq 4\), \(m = |M|\), we have \(A_i(a, a) = a\) for all operations \(A_i \in \Sigma\), then \(k = (m - 1)/(s - 1)\) is a natural number and \(k \geq s\) or \(k = 1\). Construction of quasigroups of a closed system \(\Sigma\) with \(k = 1\) is given.

Later V. D. Belousov investigated the orthogonality of operations together with some important problems in combinatorics and algebraic nets. See, for example, the series of articles: [12, 19, 20, 23, 24].


Let \((G, A)\) be an \(n\)-ary quasigroups, i.e., an algebra \((G, A)\), where \(A\) is an \(n\)-ary operation defined on \(G\) such that for all \(x_0, x_1, \ldots, x_n \in G\) and all \(i \in \{1, 2, \ldots, n\}\) there exists a uniquely determined \(z_i \in G\) satisfying the equation

\[
A(x_1, \ldots, x_{i-1}, z_i, x_{i+1}, \ldots, x_n) = x_0.
\]

In the abbreviated form this equation can be written as

\[
A(x_i^{-1}, z_i, x_{i+1}) = x_0,
\]

where \(x_i^j\) means the sequence \(x_i, x_{i+1}, \ldots, x_j\). (For \(j < i\) \(x_i^j\) means the empty symbol.)

The solutions of the equation of so-called generalized associativity

\[
A(x_i^{-1}, B(x_i^{p-1}), x_{i+p}) = C(x_j^{-1}, D(x_j^{q-1}), x_{j+q}),
\]

where \(A, B, C, D\) are quasigroup operations defined on the same set \(G\), are described. The solutions of (3) in the case when the variables on the right side are permutation of variables on the left side are also given. Other proofs of these results one can find in the book [21].

The special case of (3), i.e., the equation

\[
A(B(x_i^p), x_{i+p+1}) = C(x_i^{-1}, D(x_j^q))
\]
An important role in the theory of \( n \)-ary systems play \( n \)-ary algebras \((G, A)\) in which the identity (3) (with \( A = B = C = D \)) is satisfied for all or only for some \( 1 \leq i < j \leq n \) and \( p = q = n, \ l = 2n - 1 \). Such algebras were studied, for example, by W. A. Dudek [26], F. Sokhatsky [35], Ja. Užan [37] and others. On the other hand, many authors studied different types of \( n \)-ary algebras in which (2) has a unique solution for all or only for some \( i \in \{1, \ldots, n\} \) (see [36] and [37]).

12. On orthogonal \( n \)-ary operations [12]

The concept of the set of \( n \) orthogonal \( n \)-ary operations is a generalization of the concept of a pair of binary orthogonal operations. This article and Ph.D. thesis of T. Yakubov [38] (V. D. Belousov was a supervisor) are probably one of the first works in which the orthogonality of \( n \)-ary operations is studied.

Denote by \( \Omega_n \) the set of all \( n \)-ary operations defined on a fixed set \( Q \). On \( \Omega_n \) the so-called Menger superposition of operations is defined:

\[
C(x^n_1) = A(B_1(x^n_1), B_2(x^n_1), \ldots, B_n(x^n_1)).
\]

On \( \Omega_n \) also binary compositions \((A \times B) = A(E_1^{i-1}, B, E_{i+1}^n)\), \( i = 1, 2, \ldots, n \), where \( E_i(x^n_1) = x_i \) are \( i \)-th projectors, are defined.

An \( n \)-tuple \( \langle A_1, \ldots, A_n \rangle = \langle A^n_1 \rangle \) of \( n \)-ary operations \( A_1, \ldots, A_n \in \Omega_n \) is orthogonal, if the system of equations \( \{A_i(x^n_1) = a_i\} \) has a unique solution for all \( a_1, \ldots, a_n \in Q \).

An operation \( A \in \Omega_n \) is \( i \)-invertible \((i\text{-solvable in the other terminology})\) if the equation \( A(a_1^{i-1}, x, a_{i+1}^n) = b \) has a unique solution \( x \in Q \) for all \( a_1, \ldots, a_n, b \in Q \). Such operation is denoted by \( A^i \).

If \( \sigma \) is a permutation of \( Q \), then a \( \sigma \)-parastrophe \( \sigma A \) of a quasigroup operation \( A \in \Sigma \) is defined in the following way:

\[
\sigma A(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma n}) = x_{\sigma(n+1)} \iff A(x_1, x_2, \ldots, x_n) = x_{n+1}.
\]

If \( \sigma(n+1) = n + 1 \), then such parastrophe is called main.

An \( n \)-tuple \( S_1 = \langle A_1^{(1)}, A_2^{(1)}, \ldots, A_n^{(1)} \rangle \) of different operations from \( \Omega_n \) is called admissible, if there exist permutations \((i_1, i_2, \ldots, i_n)\) and \((j_1, j_2, \ldots, j_n)\) of the set \( \{1, 2, \ldots, n\} \) such that in \( S_1 \) the operation \( A_i^{(1)} \) is \( j_i \)-invertible and in \( S_{r+1} = \langle A_1^{(r+1)}, A_2^{(r+1)}, \ldots, A_n^{(r+1)} \rangle \), where \( A_i^{(r+1)} = A_i^r \times (i^r A_i^r) \), the operation \( A_i^{(r+1)} \) is \( j_{r+1} \)-invertible.
The main results are formulated in the following two theorems.

**Theorem 9.** An admissible $n$-tuple is orthogonal.

**Theorem 10.** If all operations of an $n$-tuple $\langle A^n_i \rangle$ satisfy the condition $A_i = \sigma C(E_i, A^n_{i+1})$, where $\sigma C$ is the main parastrophe of a quasigroup operation $C$, then $\langle A^n_i \rangle$ is orthogonal.

A system $\Sigma = \{A^1_i, E^n_j\} \subset \Omega_n$, where all $A_i$ are quasigroup operations and $E_j$ are projectors, is called a $S$-system, if it is closed with respect to the Menger superposition of operations.

It is proved that for finite $Q$ and $n > 2$ such systems do not exist.

In other papers V.D. Belousov studied the property of the orthogonality of binary and $n$-ary operations and systems of operations from the algebraic and geometric point of view. His researches were continued by his pupils, among them we can mention A. S. Bektenov, G. B. Belyavskaya, A. M. Cheban, V.I. Dement’eva, I. A. Golovko, I. V. Lyakh, S. Muratkhudzhaev, V. A. Scherbakov, F. N. Sokhatskiy, P. N. Syrbu, T. Yakubov, and many others. See, for example, [14, 25, 31, 32].

**References**


Received September 20, 2005