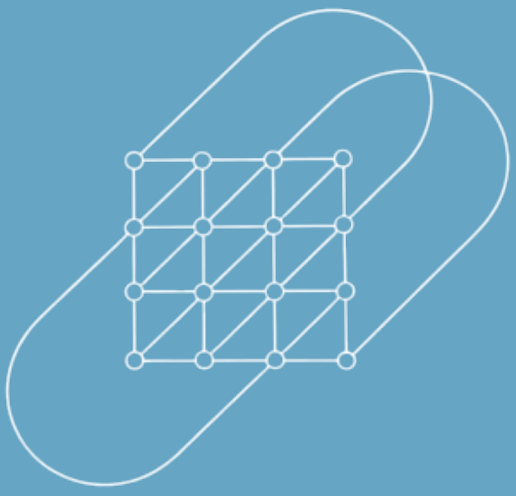
Valentin BELOUSOV

FOUNDATIONS OF THE THEORY OF QUASIGROUPS AND LOOPS



$\cdot$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$$N = < S, \mathcal{L} >$$
$$\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$$
$$(\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3) \to (Q, A)$$
$$B(\alpha x, \beta y) = \gamma A(x, y)$$

Chișinău 2025

ISBN 978-9975-62-981-2.

ISBN 978-9975-62-982-9 (PDF)

Valentin BELOUSOV

Foundations of the theory of quasigroups and loops

The English translation of the Russian language original was conducted by Jonathan D.H. Smith and Fedir Sokhatsky

Editura USM

Chișinău 2025

512.548 ISBN 978-9975-62-981-2.

B 43 ISBN 978-9975-62-982-9 (PDF)

DESCRIEREA CIP A CAMEREI NAŢIONALE A CĂRŢII DIN REPUBLICA MOLDOVA

Belousov, Valentin.

Foundations of the theory of quasigroups and loops / Valentin Belousov ; the English translation of the Russian language by Jonathan D. H. Smith and Fedir Sokhatsky. – Chişinău : Editura USM, 2025. – 222 p.

Bibliogr.: p. 217-222 (91 tit.). – 150 ex.

ISBN 978-9975-62-981-2.

ISBN 978-9975-62-982-9 (PDF).

512.548

B 43

Contents

Introduction **3**

Chapter I. Main concepts and definitions **5**
Quasigroups and loops 5
Regular permutations of quasigroups and nuclei of loops 8
Isotopy 12
Mutually inverse quasigroups and loops 16

Chapter II. Groups of regular permutations. Autotopies of quasigroups **21**
Groups of left and right regular permutations 21
Middle regular permutations 23
Autotopies of quasigroups. Quasi-automorphisms 24
Type of a quasigroup 28
Transitive quasigroups. Medial quasigroups 31

Chapter III. Derivative operations. F-quasigroups **35**
Postulates of Sushkevich and Murdoch 35
Elementary properties of derivative operations 37
Mixed derivatives 41
Pseudo-automorphisms 43
F-quasigroups 47

Chapter IV. Homomorphism. Normal subquasigroups **53**
Homomorphic mappings of quasigroups 53
Normal subquasigroups 56
Inner permutations in quasigroups 59
Homotopy 66

Chapter V. Quasigroups and loops with the inverse property (IP-quasigroups) **69**
Definitions and elementary properties 69
Crossed product of quasigroups. One example of an IP-quasigroup 71
Isotopes of IP-quasigroups. Moufang quasigroups 73
Autotopies of IP-quasigroups and IP-loops 79

Weak IP-loops 85

Chapter VI. Moufang Loops **88**
The main properties of Moufang loops 88
Inner permutations of a Moufang loop 91
Moufang's Theorem 94
Commutative Moufang loops 98
Examples of Moufang loops 102
Bol loops 104

Chapter VII. TS-quasigroups. Prolongation of quasigroups **108**
Definitions and examples 108
Autotopy of TS-quasigroups 110
Isotopes of TS-quasigroups 112
Permissible quasigroups 115
Prolongations of quasigroups 118

Chapter VIII. Distributive quasigroups **131**
Some elementary properties of distributive quasigroups 131
Connection with commutative Moufang loops 132
Middle nuclei of distributive quasigroups 138
Connection with Steiner quasigroups and medial quasigroups 144
Examples of non-transitive distributive quasigroups 151

Chapter IX. Left-distributive quasigroups **154**
Left-distributive quasigroups which are isotopic to groups 154
Moufang loop cores 157
Certain results on F-quasigroups 162
Left distributive quasigroups and F-quasigroups 166

Chapter X. The question of G-loops **174**
Moufang G-loops. 174
Loops with nuclei of index two. 177
An example of G-loop that is not a WIP-loop 183
Universal properties of loops 185

Chapter XI. Quasigroups and nets **192**
Algebraic nets 192
Closure conditions 195
Moufang-Bol axioms and loop cores 204
Bol loop cores 208

Problems **215**

Bibliography **216**

Introduction

In various areas of mathematics, for example, the theory of projective planes, non-associative rings, in a number of problems of combinatorial analysis, the theory of functional equations, etc., it becomes necessary to study one natural generalization of the concept of a group, namely, a quasigroup.

An impetus to the development of the theory of quasigroups was given by the work of R. Moufang (1935) on non-Desarguesian projective planes, where the connection of such planes with quasigroups, or more precisely loops (that is, quasigroups with a neutral element), now bearing her name, was clarified. Over the past decades, the theory of quasigroups and loops has received considerable development in the works of various mathematicians, and the main attention was focused on loops. R. Bruck is a leading expert in this field, and he has summarized research on loop theory in his monograph "A Survey of Binary Systems", Springer Verlag, 1958.

Unlike the book of Bruck, the current book focuses on quasigroups. In this sense, the present work can be considered, to some extent, as a complement to the book of Bruck. However, here we also consider the most well-known classes of loops: loops with the inverse property (IP-loops), Moufang loops, Bol loops, etc.

The author has tried to make the book accessible to a wide range of readers, so all the results are presented in an elementary way. To understand the book, it is sufficient to know the basic elements of group theory that are part of a university course of higher algebra.

Not wishing to increase the size of the book, the author does not consider such aspects of the theory of quasigroups as free quasigroups, ordered loops, systems of quasigroups, etc. A number of concepts are mentioned in the book, but not developed further, although the author has indicated literature where these concepts are treated in detail. On the other hand, some results are considered rather deeply, for example, the Moufang Theorems, etc.

The book is based on lectures from a special course given by the author at Chişinău State University in 1963–1965, and at Moscow State University in the spring of 1965.

Chişinău, 1965. *V. Belousov*

Translators' note

The English translation of the Russian language original was initially undertaken and typeset in LaTeX by a team of students under the guidance of Fedir Sokhatsky, and examined by Vira Obshanska, at Vinnytsia Pedagogical University. Mathematical and linguistic editing

was then conducted by Jonathan D.H. Smith at Iowa State University (using a personal copy of the original signed and donated by Belousov in 1987). The publication project was coordinated by Parascovia Syrbu at Moldova State University.

The editing process aimed to maintain the spirit and layout of Belousov's original as much as possible, while introducing minor clarifications necessary to make the book readily accessible to a broad modern Anglophone readership. Theorem 3.4 provides a representative example where rather more extensive editing was deemed necessary. The original version of the proof included a number of excursions, such as the important definition of a groupoid congruence required for the first section of Chapter IV. In the translation, these excursions have been taken out of the actual proof, and located in one preliminary and two additional subsequent remarks. Furthermore, since much of the gist of Theorem 3.4 involves demonstrating the equality between two differently defined equivalence relations, both written as $\sim$ in the original, the notation $\simeq$ is used for the second in the translation.

Almost 60 years have passed since Sade called for a translation of the initial Russian language version in his review for *Mathematical Reviews* [MR#218483]. In accordance with the translators' philosophy of staying true to Belousov's original content, there are no changes, notes, or additional comments in the translation to reflect the subsequent developments and terminological variations within the theory of quasigroups that have arisen after the original publication. Nevertheless, many of these developments have been referenced, in close relation to Belousov's book, by V. Shcherbacov, *Elements of Quasigroup Theory and Applications*, CRC Press, Boca Raton, FL, 2017.

Chapter I. Main concepts and definitions

1°. Quasigroups and loops

One of the most basic concepts of general algebra is that of an *algebraic operation*, or simply *operation*, usually defined as follows [47].

Let a non-empty set Q be given, finite or infinite. We will denote elements of the set Q by small Latin letters: $a, b, c, \ldots, x, y, z, \ldots$. By the n-th power of the set Q we understand the set Q^n consisting of all possible ordered sequences $(a_1, a_2, \ldots, a_n)$ of elements from Q. Then an *n-ary operation* A defined on the set Q is a mapping of the set Q^n into the set Q. If the sequence $(a_1, a_2, \ldots, a_n)$ is sent to the element b (also belonging to Q), then we write $A(a_1, a_2, \ldots, a_n) = b$. The number n is called the *arity* of the operation A. If $n = 2$, then the operation A is called *binary*: $A(a_1, a_2) = b$. If $n = 1$, then the operation A is called *unary*: $A(a_1) = b$. We can also consider operations of infinite and of zero arity (nullary operations); for more see [47] page 109. A set Q with a set Ω of operations, where the operations from Ω can be of any arity, is called a *universal algebra* or simply an *algebra*, denoted by $Q(\Omega)$.

We are interested only in binary operations, so in future we will omit the word "binary". Operations defined on a set Q will be denoted by capital Latin letters $A, B, C, \ldots$ Sometimes we write the operations as an ordinary multiplication. Thus, we will not write $A(a, b) = c$, but rather $ab = c$. If necessary, we may use other signs for the operation: $\circ$, $*$, $\bullet$, Δ etc., for example $a \circ b = c$, $a * b = c$ etc.

A set Q being considered together with a binary operation A is called a *groupoid*, and is denoted by $Q(A)$. If the operation is indicated by a sign, for example $(\circ)$ or $(\cdot)$, then we will also write $Q(\circ)$ or $Q(\cdot)$. Consequently, on the set Q there are as many groupoids as there exist different operations. Two operations A and B coincide if $A(a, b) = B(a, b)$ for each $a, b \in Q$.

If Q is a finite groupoid, then $Q(A)$ can be given by means of a table such as

A	a	b	c	d
a	c	c	b	a
b	d	d	a	b
c	c	b	a	c
d	a	b	a	b

where the element $A(a, b)$ is located at the intersection of the row labeled by the element a and the column labeled by the element b, in this case $A(a, b) = c$. Such a table is called the

Cayley table of the groupoid $Q(A)$.

It can happen that in the Cayley table of the groupoid $Q(A)$, all the elements in each row and in each column are different, as in the following example.[1]

A	a	b	c	d
a	b	a	d	c
b	c	b	a	d
c	a	d	c	b
d	d	c	b	a

If this property holds for $Q(A)$, we say that $Q(A)$ is a quasigroup. Thus, we can give the following

Definition 1. A groupoid $Q(A)$ (that is, a set Q with an operation A) is called a *quasigroup* if for every $a, b \in Q$, the equations

$$A(a,\ x) = b,\ A(y,\ a) = b \tag{1.1}$$

always have unique solutions x, y in Q.

This definition is equivalent to the following: a groupoid $Q(A)$ is a quasigroup if each pair of the elements from the equality $A(a, b) = c$ uniquely defines the third. One can also give the following definition. An operation A is said to be *right invertible* if the equation $A(a, x) = B$ is uniquely solvable for all a, b, and is said to be *left invertible* if $A(y, a) = b$ is uniquely solvable for all $a, b,$. Finally, the operation A is said to be *invertible* if it is both left and *right invertible*. Thus, by "the quasigroup $Q(A)$" we understand the set Q with the invertible operation A.

There is another definition which is also often used. To arrive at this definition, note that in fact, the equations (1.1) define two new operations. The first of the equations (1.1) shows that to each ordered pair $a, b \in Q$, an element x of Q is uniquely assigned. Thus, a new operation is defined on Q. We denote it by B: $B(a, b) = x$. Similarly, the second of the equations (1.1) again determines an operation. We denote it by C, and we assume that $C(b, a) = y$. Thus, three operations are defined on Q, i.e., we have an algebra $Q(\Omega)$, where $\Omega = \{A, B, C\}$. In this algebra, the identities following from (1.1) and the definition of the operations B and C must be satisfied:

$$A\ [a,\ B\ (a,\ b)] = b,\ A\ [C\ (b,\ a),\ a] = b. \tag{1.2}$$

The question naturally arises: if in the algebra $Q(\Omega) = Q(A, B, C)$ we have the identities (1.2), then can $Q(A)$ be a quasigroup? It is easy to see that $Q(A)$ is not necessarily a quasigroup. More precisely, in $Q(A)$ the equations (1.2) are solvable, but, generally speaking, not uniquely. Therefore, we give the following

Definition 2. A groupoid $Q(A)$ is a *quasigroup* if there exist two other operations B and C on the same set Q such that in the algebra $Q(A, B, C)$ the identities[2]

$$\left.\begin{array}{ll} A\,[x,\ B(x,\ y)] = y, & B\,[x,\ A(x, y)] = y, \\ A\,[C\ (y,\ x),\ x] = y, & C\,[A(y,\ x),\ x] = y. \end{array}\right\} \tag{1.3}$$

hold.

Let us show the equivalence of Definitions 1 and 2. We have already seen that equations (1.1) are solvable, using the first row of identities (1.3). For example, $B(a,b)$ is the solution of the equation $A(a,x) = b$. To show uniqueness of the solution, suppose $A(a,c) = A(a,d) = b$. Then

$$B\ [a,\ A\ (a,\ c)] = B\ [a,\ A\ (a,\ d)]\ .$$

Hence, on the basis of (1.3), it follows that $c = d$. In the same way, we obtain the unique solvability of the second equation. Consequently, Definition 1 follows from Definition 2. To show that Definition 2 follows from Definition 1, it is necessary to prove that the second row of identities in (1.3) hold. For this purpose, suppose that $B\ [a,\ A\ (a,\ b)] = c$, so $A\ \{a,\ B\ [a,\ A\ (a,\ b)]\} = A(a,c)$. From here, on the basis of (1.2), we have $A(a,b) = A(a,c)$. As the equation $A\ (a,\ x) = d$ must have a unique solution, we conclude that $b = c$, i.e., $B\ [a,\ A\ (a,\ b)] = b$.

Definition 3. We call the operation B from Definition 2 the *right inverse operation* of A, and denote it by A^{-1}. We call the operation C the *left inverse operation* of A, and denote it by ${}^{-1}\mathrm{A}$.

Thus,

$$\left.\begin{array}{ll} A\,[x,\ A^{-1}(x,\ y)] = y, & A^{-1}\,[x,\ A(x,y)] = y, \\ A\,[{}^{-1}\mathrm{A}\ (y,\ x),\ x] = y, & {}^{-1}\mathrm{A}\,[A(y,\ x),\ x] = y. \end{array}\right\} \tag{1.4}$$

Consequently, the solution of the equation $A(a,x) = b$ is $x = A^{-1}(a,b)$, and the solution of $A(y,a) = b$ is $y = {}^{-1}\ \mathrm{A}(b,a)$.

Remark 1. The definition of the operations A^{-1} and ${}^{-1}\mathrm{A}$ implies that the equalities $A(a,b) = c$, $A^{-1}(a,c) = b$ and ${}^{-1}\mathrm{A}(c,b) = a$ are equivalent.

Remark 2. If the basic operation in a quasigroup is denoted by usual multiplication $(\cdot)$, then instead of $(\cdot)^{-1}$ and ${}^{-1}(\cdot)$ we will often write $(\backslash)$ and $(/)$ respectively.

Remark 3. If $Q(A)$ is a *quasigroup*, then $Q(A^{-1})$ and $Q({}^{-1}\mathrm{A})$ are also quasigroups. In fact, we show that the equation

$$A^{-1}(a,\ x) = b \tag{1.5}$$

has a unique solution. If c is some solution of this equation, then the equality $A^{-1}(a,c) = b$ implies $A(a,b) = c$, and (1.3) implies that $A(a,b)$ is a solution of the equation (1.5). Thus, the equation (1.5) is solvable uniquely.

Let c be a solution of the equation

$$A^{-1}(y,\ a) = b, \tag{1.6}$$

that is, $A^{-1}(c,a) = b$. Then $A(c,b) = a$, so $c = {}^{-1}\ \mathrm{A}(a,b)$. Let us verify that ${}^{-1}\mathrm{A}(a,b)$ is a solution of the equation (1.6). Let

$$A^{-1}({}^{-1}\mathrm{A}(a,b),a) = b'.$$

This equality is equivalent to the equality $A(^{-1}\mathrm{A}(a,b),b') = a$. But, by virtue of (1.3), we also have $A(^{-1}\mathrm{A}(a,b),b) = a$. Comparing the last two equations, we find that $b' = b$. Therefore, $Q(A^{-1})$ is a quasigroup. Similarly, one can prove that $Q(^{-1}\mathrm{A})$ is also a quasigroup.

Let $Q(\cdot)$ be a quasigroup. If a subset $Q' \subseteq Q$ is a quasigroup with respect to the same operation $(\cdot)$, then $Q'(\cdot)$ is called a *subquasigroup* of the quasigroup $Q(\cdot)$.

Another important concept on which we will focus is the concept of a loop. Consider a quasigroup $Q(\cdot)$. Suppose there is an element e in Q such that $ae = ea = a$ for every $a \in Q$. Then e is called a *neutral element* of the quasigroup $Q(\cdot)$.

Definition 4. A quasigroup $Q(\cdot)$ with a neutral element is called a *loop*[3].

The most studied class of loops are groups, construed as associative quasigroups. Thus, a quasigroup is called a *group* if in $Q(\cdot)$ the identity of associativity holds: $xy \cdot z = x \cdot yz$[*] (see [46], [85]). It is easy to show (see, for example, [85]) that the associativity of the quasigroup $Q(\cdot)$ implies the existence of a neutral element in $Q(\cdot)$.

An example of a non-associative loop is

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

$Q(\cdot)$ is a loop, but not a group, since $Q(\cdot)$ is not associative. For example, $(2\cdot 2)\cdot 5 = 1\cdot 5 = 5$, and $2 \cdot (2 \cdot 5) = 2 \cdot 4 = 3$, that is, $(2 \cdot 2) \cdot 5 \neq 2 \cdot (2 \cdot 5)$.

Suppose that $Q(\cdot)$ is a quasigroup, but not a loop. Then, nevertheless, for each element a there exists a *right local neutral element* e_a, i.e., $ae_a = a$; this follows from the fact that the equation $ax = a$ must have a solution. The *left local neutral element* $f_a : f_a a = a$ is defined similarly. If all the right neutral elements coincide, $(e_a = e)$, then e is called a *right neutral element*. A *left neutral element* f is defined similarly. There are quasigroups with a right neutral element (they are called *right loops*), but without a left neutral element, and conversely. If $Q(\cdot)$ has right and left neutral elements, then they coincide, so then $Q(\cdot)$ is a loop.

The concept of a *subloop* is introduced in a natural way: $Q'(\cdot)$ is a subloop of a loop $Q(\cdot)$ if $Q'(\cdot)$ is a loop and $Q' \subseteq Q$.

2°. Regular permutations of quasigroups and nuclei of loops

Let $Q(\cdot)$ be a quasigroup. The mapping $x \to ax$ is called *a left translation by means of an element* a and is denoted by $L_a : L_a x = ax$. Obviously, L_a is a one-to-one mapping

[*] Often we will write $(xy)z$ as $xy \cdot z$. So, $x(yz \cdot x)$ means $x[(yz)x]$, etc.

of the set Q onto itself, i.e., L_a is a permutation* of the set Q. This follows from the definition of a quasigroup. *The right translation* R_a by an element a is determined by the equality $R_a x = xa$ and, therefore, is also a permutation. The set of all the translations of a quasigroup $Q(\cdot)$ generates a group G, which is called the *group associated with* $Q(\cdot)$ [1]. If $Q(\cdot)$ is a group, then there are obvious equalities, each of which is equivalent to the law of associativity:

$$\left.\begin{aligned} L_a(x\,y) &= L_a\,x \cdot y, \\ R_a(x\,y) &= x \cdot R_a y. \end{aligned}\right\} \tag{1.7}$$

The equations (1.7) are true for all $a, x, y \in Q$. These equations imply the following.

Definition 5. A permutation λ of a set Q is called a *left regular permutation of a quasigroup* $Q(\cdot)$ if

$$\lambda(x\,y) = \lambda x \cdot y \tag{1.8}$$

for all $x, y \in Q$. A *right regular permutation* ρ is defined similarly:

$$\rho(x\,y) = x \cdot \rho y.$$

Thus, in a group, any left (right) translation is a left (right) regular permutation.

Left and right regular permutations always exist for any quasigroup; the unit permutation ε (with $\varepsilon x = x$)* is always regular on the left and on the right. It is easy to see that the set $\mathscr{L}$ (or more specifically, $\mathscr{L}_{(\cdot)}$) of all the left regular permutations of a quasigroup $Q(\cdot)$ is a group. More precisely, $\mathscr{L}$ is a subgroup of the group G. Indeed, let $\lambda_1, \lambda_2 \in \mathscr{L}$. Then

$$(\lambda_1\lambda_2)(xy) = \lambda_1[\lambda_2(xy)] = \lambda_1(\lambda_2 x \cdot y) = \lambda_1(\lambda_2 x) \cdot y = (\lambda_1\lambda_2)x \cdot y,$$

i.e., $\lambda_1\lambda_2 \in \mathscr{L}$. Let us show that $\lambda \in \mathscr{L}$ follows from $\lambda^{-1} \in \mathscr{L}$. Indeed, $xy = \lambda^{-1}(\lambda x \cdot y)$ follows from (1.8). After replacing x by $\lambda^{-1}x$, we obtain $\lambda^{-1}x \cdot y = \lambda^{-1}(xy)$, i.e., $\lambda^{-1} \in \mathscr{L}$.

It remains to show that $\mathscr{L} \subseteq G$. For this, note that the equation (1.8) can be rewritten in the form $\lambda L_x y = L_{\lambda x} y$, whence $\lambda L_x = L_{\lambda x}$ follows. Therefore $\lambda = L_{\lambda x} L_x^1 \in G$. It is proved similarly that the set $\mathscr{R}$ of all right regular permutations of a quasigroup $Q(\cdot)$ forms a subgroup of the group G.

Let us find left regular permutations for the case where $Q(\cdot)$ is a loop. Let $\lambda \in \mathscr{L}$ and let $\lambda e = a$, where e is the neutral element of the loop $Q(\cdot)$. Then

$$\lambda x = \lambda(ex) = \lambda e \cdot x = ax,$$

i.e., $\lambda = L_a$. On the other hand, we note that the element $a = \lambda e$ has the following property:

$$ax \cdot y = a \cdot xy \tag{1.9}$$

for all x and y. Indeed, $ax \cdot\ y = \lambda x \cdot y = \lambda(xy) = a \cdot xy$.

*A one-to-one mapping of a set Q onto itself is called a *permutation* of the set Q.

*Often we will denote the unit permutation by 1, i.e., $1x = x$.

If an element a satisfies the equality (1.9), then it is said to be *left associative*. The collection of all left associative elements of a loop $Q(\cdot)$ is called the *left nucleus of* $Q(\cdot)$ and is denoted by N_l.

Similarly, the *right nucleus* N_r is defined as the set of all right associative elements, i.e., elements b such that

$$xy \cdot b = x \cdot yb \tag{1.10}$$

for all x and $y \in Q$. If $\rho \in \mathscr{R}$, then, as above, one can show that $\rho = R_b$, where $b \in N_r$.

The neutral element of a loop always belongs to the left and right nuclei. Finally, we can define *the middle nucleus* N_m as the collection of all the *mid-associative* elements c with

$$xc \cdot y = x \cdot cy. \tag{1.11}$$

The definitions of the left, right and middle nucleus are formulated for quasigroups: in the equalities $(1.9) - (1.11)$, the neutral element does not participate directly. However, the following statements hold [39]:

a) *A quasigroup* $Q(\cdot)$ *has a left (right) nucleus if and only if it has a left (right) neutral element;*

b) *A quasigroup* $Q(\cdot)$ *has a middle nucleus if and only if it is a loop.*

In fact, if $Q(\cdot)$ has a left neutral element f, then f is left associative. Now suppose that $Q(\cdot)$ has a left nucleus N_l, and let $a \in N_l$. Let as show that the right local neutral element e_a of the element a is the left neutral element of the quasigroup $Q(\cdot)$. Let $e_a x = x'$. Then $ax' = a \cdot e_a x = ae_a \cdot x = ax$, whence $x' = x$. Consequently $e_a x = x$. To prove b), note that the neutral element of a loop always belongs to all three nuclei. Now suppose $Q(\cdot)$ has a middle nucleus N_m, and let $a \in N_m$, f_a and e_a, respectively, be the left and the right local neutral elements of a. If x is an arbitrary element from Q, then elements y and z such that $x = ay = za$ exist. We have

$$f_a x = f_a(ay) = (f_a a)y = ay = x,$$

$$xe_a = (za)e_a = z(ae_a) = za = x.$$

Hence it follows that f_a and e_a are respectively the left and right neutral elements of the quasigroup $Q(\cdot)$. Therefore they coincide, i.e., $Q(\cdot)$ is a loop.

In the case when $Q(\cdot)$ is a group, then $N_l = N_m = N_r = Q$, i.e., all three nuclei are subgroups of $Q(\cdot)$ and even coincide with Q. In the general case, we have

Theorem 1.1. *Each nucleus of a quasigroup* $Q(\cdot)$ *is an associative subquasigroup* (i.e., a group).

Proof. a) Let $Q(\cdot)$ have left nucleus N_l. Then, as above, there is a left neutral element e in $Q(\cdot)$. Obviously, $e \in N_l$. Now let us show that $a, b \in N_l$ implies $ab \in N_l$:

$$(ab)(xy) = a(b \cdot xy) = a(bx \cdot y) = (a \cdot bx)y = (ab \cdot x)y.$$

Thus, N_l is closed under the operation of multiplication in $Q(\cdot)$. Further, we have

$$ae \cdot x = a \cdot ex = ax,$$

hence $ae = a$, i.e., e is a neutral element in N_l.

Now we note the following. If $Q(\cdot)$ is a loop with neutral element e, then each element $x \in Q$ has inverse elements which are defined by the equalities

$$xx^{-1} = e, \quad {}^{-1}\mathrm{x}x = e.$$

The element x^{-1} is called the *right inverse* for x, and ${}^{-1}\mathrm{x}$ is the *left inverse* for x.

Let us show that if $a \in N_l$, then $a^{-1} \in N$. In fact, there must exist an element y' such that the equality

$$a^{-1} \cdot xy = a^{-1}x \cdot y' \tag{1.12}$$

holds. We multiply from the left by a:

$$a(a^{-1} \cdot xy) = a(a^{-1}x \cdot y'),$$

whence, in view of the fact that $a \in N_l$,

$$aa^{-1} \cdot xy = (a \cdot a^{-1}x)y',$$

$$e \cdot xy = (aa^{-1} \cdot x)y',$$

$$xy = xy'.$$

Thus, $y = y'$ and from (1.12) it follows that $a^{-1} \in N_l$. Now recall that a group can be defined as a groupoid in which the law of associativity holds, there exists a right neutral element $xe = x$ and a right inverse element x^{-1}, $xx^{-1} = e$ for arbitrary $x \in Q$ (see, for example, [46]). Thus, from all the above it follows that N_l is a group under the operation $(\cdot)$ in a quasigroup $Q(\cdot)$. Similarly, it is proved that N_r is a group under the operation $(\cdot)$ in a quasigroup $Q(\cdot)$.

b) Let $a, b \in N_m$, then also $ab \in N_m$, since

$$(x \cdot ab)y = (xa \cdot b)y = xa \cdot by = x(a \cdot by) = x(ab \cdot y).$$

Earlier, we saw that the quasigroup $Q(\cdot)$ must be a loop with a neutral element e. If $a \in N_m$, then ${}^{-1}\mathrm{a} = a^{-1}$, since ${}^{-1}\mathrm{a}(aa^{-1}) = ({}^{-1}\mathrm{a}a)a^{-1} = a^{-1}$ or ${}^{-1}\mathrm{a} = a^{-1}$ follows from the equality $({}^{-1}\mathrm{a}a)a^{-1} = a^{-1}$ and from $a \in N_m$. Moreover $a^{-1} \in N_m$, so N_m is a group (an associative subloop.) To see this, we reason as above: there must exist an element y' such that

$$xa^{-1} \cdot y = x \cdot a^{-1}y'.$$

We replace x with za (when x takes all the values of the whole set Q, then z takes all the values of Q):

$$(za \cdot a^{-1})y = za \cdot a^{-1}y', zy = za \cdot a^{-1}y' = z(a \cdot a^{-1}y'),$$

whence $y = a \cdot a^{-1}y'$. Multiplying on the left by a^{-1}, we have

$$a^{-1}y = a^{-1}(a \cdot a^{-1}y') = a^{-1}a \cdot a^{-1}y' = a^{-1}y', y = y'.$$

Thus, $xa^{-1} \cdot y = x \cdot a^{-1}y$ which is what we had to prove.

Often, the concept of the *nucleus* of a loop $Q(\cdot)$ is also considered: the intersection* of the three nuclei N_l, N_m, N_r of $Q(\cdot)$.

3°. Isotopy

Another important notion of the theory of quasigroups and loops is the notion of an isotopy which generalizes the group-theoretical notion of an isomorphism.

Consider two operations A, B, defined on the same set Q.

Definition 6. The operation B is said to be *isotopic* to the operation A, or an *isotope* of A, if there exists a triple of permutations α, β, γ of the set Q such that

$$B(x, y) = \gamma^{-1}A(\alpha x, \beta y)$$

for arbitrary $x, y \in Q$.

The ordered triple $T = (\alpha, \beta, \gamma)$ is called an *isotopy*. The permutations α, β, γ are respectively the *left, right,* and *principal components* of the isotopy T. The fact that B and A are isotopic will sometimes be written as $B = A^T$ or $B = A^{\alpha,\beta,\gamma}$**. If all three permutations coincide, $\alpha = \beta = \gamma$, then the isotopy becomes an *isomorphism*

$$B(x, y) = \alpha^{-1}A(\alpha x, \alpha y).$$

In this case, we write $(\alpha, \alpha, \alpha) = \alpha$ and, consequently,

$$B = A^{(\alpha,\alpha,\alpha)} = A^{\alpha}.$$

An isotopy of the form $T = (\alpha, \beta, 1)$, i.e., if the principal component is equal to 1, is called *principal*.

Example. Let $Q(\cdot)$ be the quasigroup defined by the following Cayley table:

	1	2	3	4	5
1	3	1	4	2	5
2	5	2	3	1	4
3	1	4	2	5	3
4	4	5	1	3	2
5	2	3	5	4	1

*That is, the set of common elements of the nuclei N_l, N_m, N_r.

**If the operations B and A are written with symbols, for example in the form $(\circ)$ and $(\cdot)$, then we will write $(\circ) = (\cdot)^T$.

In this table, we move the rows, then the columns, and finally permute the elements within the table itself:

	1	2	3	4	5
1	3	1	4	2	5
2	5	2	3	1	4
3	1	4	2	5	3
4	4	5	1	3	2
5	2	3	5	4	1

$\rightarrow$

	1	2	3	4	5
1	5	2	3	1	4
2	1	4	2	5	3
3	4	5	1	3	2
4	3	1	4	2	5
5	2	3	5	4	1

$\rightarrow$

	1	2	3	4	5
1	2	3	5	1	4
2	4	2	1	5	3
3	5	1	4	3	2
4	1	4	3	2	5
5	3	5	2	4	1

$\rightarrow$

	1	2	3	4	5
1	1	2	5	3	4
2	4	1	3	5	2
3	5	3	4	2	1
4	3	4	2	1	5
5	2	5	1	4	3

We can move the rows by applying $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$, and the columns by applying $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$. Inside the table, we apply the permutation $\gamma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$, i.e., everywhere where there was 1, we put 3, where there was 2, we put 1, etc. Thus, we have obtained another quasigroup in $Q(\circ)$ by means of the isotopy $T = (\alpha, \beta, \gamma)$, or in more detail we have $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$. We find, for example, $3 \circ 4$:

$$3 \circ 4 = \gamma^{-1}(\alpha 3 \cdot \beta 4) = \gamma^{-1}(4 \cdot 4) = \gamma^{-1} 3 = 2.$$

From this example, we see that an *isotope $Q(\circ)$ of a quasigroup $Q(\cdot)$ is also a quasigroup.* This fact also follows from the definition of an isotopy. First we prove the uniqueness of the solution. Suppose, the equation $a \circ x = b$ has two solutions c_1 and $c_2 : a \circ c_1 = b$, $a \circ c_2 = b$. But then $\gamma^{-1}(\alpha a \cdot \beta c_1) = b$ and $\gamma^{-1}(\alpha a \times \beta c_2) = b$, whence $\alpha a \cdot \beta c_1 = \gamma b$ and $\alpha a \cdot \beta c_2 = \gamma b$. Since $Q(\cdot)$ is a quasigroup, we conclude that $\beta c_1 = \beta c_2$, whence $c_1 = c_2$. We prove the existence of a solution of the equation $a \circ x = b$ in the following way. There must be an element c in $Q(\cdot)$ such that $\alpha a \cdot c = \gamma b$. Then $\beta^{-1} c$ is the desired solution. In fact,

$$a \circ \beta^{-1} c = \gamma^{-1}[\alpha a \cdot \beta(\beta^{-1} c)] = \gamma^{-1}(\alpha a \cdot c) = \gamma^{-1}(\gamma b) = b.$$

Similarly it is proved that the equation $y \circ a = b$ is uniquely solvable.

We introduce the *product of isotopies* $T = (\alpha, \beta, \gamma)$ and $T_1 = (\alpha_1, \beta_1, \gamma_1)$, namely, we put $TT_1 = (\alpha\alpha_1, \beta\beta_1, \gamma\gamma_1)$. It is easy to see that all the isotopies defined on a set Q form a group under this multiplication. The neutral element of this group is $(1, 1, 1) = 1$, where 1 is the unit permutation of the set Q. The inverse isotopy for $T = (\alpha, \beta, \gamma)$ is obviously $T^{-1} = (\alpha^{-1}, \beta^{-1}, \gamma^{-1})$.

For arbitrary operations A and B, the following relations hold:

$$a) \text{ if } B = A^T, \text{ then } A = B^{T^{-1}}; \tag{1.13}$$

$$b)\ (A^T)^{T_1} = A^{TT_1}. \tag{1.14}$$

Indeed, if $T = (\alpha, \beta, \gamma)$, then $B(x, y) = \gamma^{-1}A(\alpha x, \beta y)$, whence after replacing x and y by $\alpha^{-1}x$ and $\beta^{-1}y$ respectively we obtain $B(\alpha^{-1}x, \beta^{-1}y) = \gamma^{-1}A(x, y), \gamma B(\alpha^{-1}x, \beta^{-1}y) = A(x, y)$, i.e., $A = B^{T^{-1}}$.

For the proof of b), we introduce the notation $B = A^T$ and calculate $C = B^{T_1}$. We have $C(x, y) = \gamma_1^{-1}B(\alpha_1 x, \beta_1 y)$, but $B(x, y) = \gamma^{-1}A(\alpha x, \beta y)$, and consequently

$$C(x, y) = \gamma_1^{-1}[\gamma^{-1}A(\alpha(\alpha_1 x), \beta(\beta_1 y))] = \gamma_1^{-1}\gamma^{-1}A(\alpha\alpha_1 x, \beta\beta_1 y),$$

i.e.,

$$C = A^{\alpha\alpha_1, \beta\beta_1, \gamma\gamma_1} = A^{TT_1}.$$

But $C = B^{T_1} = (A^T)^{T_1}$. Thus, the relationship b) has been proved.

Taking into account that $A^1 = A$, we conclude that isotopies define an equivalence relation on the set of all the operations and, in particular, on the set of all the quasigroups. Therefore, for example, we can say: A and B are *isotopic*.

Using the relationship b), one can easily prove the following:

Theorem 1.2. *If an operation B is isotopic to an operation A, then B is isomorphic to some principal isotope A.*

Proof. Let $B = A^T = A^{(\alpha,\beta,\gamma)}$. But $(\alpha, \beta, \gamma) = (\alpha\gamma^{-1}, \beta\gamma^{-1}, 1)\gamma = S_\gamma$, where as we know, $\gamma = (\gamma, \gamma, \gamma)$. Therefore, $B = A^{S_\gamma} = [A^S]^\gamma$. If we put $A^S = C$, then C is a principal isotope of the operation A, and B is isomorphic to C, since $B = C^\gamma$.

This theorem enables us to prove a number of properties of quasigroups with the help of principal isotopes, and not isotopes. The power of quasigroup isotopy comes from the following simple theorem:

Theorem 1.3. *Each quasigroup is isotopic to a loop.*

Indeed, let a, b be two fixed arbitrary elements of a quasigroup $Q(\cdot)$, and let $e = ba$. Consider the isotopy $R_a^{-1}, L_b^{-1}, 1)$, where 1 is a unit permutation of a set Q:

$$x \circ y = R_a^{-1}x \cdot L_b^{-1}y. \tag{1.15}$$

$Q(\circ)$ is a quasigroup, as we have just seen. In addition, $Q(\circ)$ has a neutral element e, so $Q(\circ)$ is a loop. In fact, from $e = ba$ it follows that $e = L_b a$, whence

$$x \circ e = R_a^{-1}x \cdot L_b^{-1}e = R_a^{-1}x \cdot L_b^{-1}(L_b a) = R_a^{-1}x \cdot a = R_a(R_a^{-1}x) = x,$$

and similarly $e \circ x = x$. Thus, the quasigroup $Q(\cdot)$ is principally isotopic to a loop $Q(\circ)$.

Example. We take the quasigroup $Q(A)$ given on page 6. We move the rows and columns so that the first row and the first column are a, b, c, d:

A	a	b	c	d
a	b	a	d	c
b	c	b	a	d
c	a	d	c	b
d	d	c	b	a

$\rightarrow$

	a	b	c	d
a	a	d	c	b
b	b	a	d	c
c	c	b	a	d
d	d	c	b	a

$\rightarrow$

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Thus, we obtain a principal isotope $Q(\circ)$ of the quasigroup $Q(A)$. Obviously, $Q(\circ)$ is a loop with neutral element a (and also a group). We have the isotopy: $T = (\alpha, \beta, 1)$, $(\circ) = A^T$, where $\alpha = \begin{pmatrix} a & b & c & d \\ c & a & b & d \end{pmatrix}$, $\alpha = \begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}$, i.e., $x \circ y = A(\alpha x, \beta y)$. It is easy to see, however, that α and β also belong to the group G. Indeed, we have the following.

Lemma 1.1. *If a loop $Q(\circ)$ is principally isotopic to a quasigroup $Q(A)$, then the isotopy must have the form*

$$T = (R_a^{-1}, L_b^{-1}, 1).$$

Indeed, let $T = (\alpha, \beta, 1)$, and let e be the neutral element of the loop $Q(\circ)$. Then $x = x \circ e = A(\alpha x, \beta e) = R_{\beta e}\alpha x$, so $R_{\beta e}\alpha = 1$ or $\alpha = R_{\beta e}^{-1}$. Similarly, we have $\beta = L_{\alpha e}^{-1}$, so $T = (R_{\beta e}^{-1}, L_{\alpha e}^{-1}, 1)$. For the example considered above, remembering that the neutral element of the loop $Q(\circ)$ is a, we have $\beta a = a, \alpha a = c$. Consequently, $T = (R_a^{-1}, L_c^{-1}, 1)$.

We introduce the notation

$$A(R_a^{-1}, L_b^{-1}, 1) = A_{a,b}.$$

Then from Lemma 1.1 and Theorem 1.3 we obtain the following:

Lemma 1.2. *If a loop B is isotopic to a quasigroup A, then the isotopy has the form*[*]

$$B = (A_{a,b})^\gamma,$$

or in the abbreviated notation

$$B = A_{a,b}^\gamma. \tag{1.16}$$

The converse assertion is also obvious: *any isotope of the form* (1.16) *of a quasigroup A is a loop.* The neutral element of the loop $Q(A_{a,b})$ is $A(b, a)$.

If $Q(A)$ is a loop with neutral element 1, then $Q(A^\gamma)$ is a loop with neutral element $\gamma^{-1}1$. Thus, the neutral element of the loop $Q(A_{a,b}^\gamma)$ is $\gamma^{-1}A(b, a)$.

For groups, the concept of isotopy does not play a significant role, as shown by the following theorem:

[*]Often, instead of a "quasigroup", we will say a "quasigroup A", that is, the operation A itself will be called a quasigroup. However, we will say "an element x belongs to the quasigroup $Q(A)$" instead of "an element x belongs to the quasigroup A".

Theorem 1.4. (Albert [1]). *If two groups are isotopic, then they are isomorphic.*

This theorem follows from a more general proposition, which is now commonly called the *Albert Theorem: If a loop $Q(\circ)$ is isotopic to a group $Q(\cdot)$, then it is a group isomorphic to the group $Q(\cdot)$.* We will prove this proposition. For this we use the remark made after the proof of Theorem 1.2: it suffices to prove the theorem for a principal isotope. Therefore, suppose that a loop $Q(\circ)$ is principally isotopic to a group $Q(\cdot)$. Then, by the proof of Lemma 1.1, the isotopy must have the form $(R_a^{-1}, L_b^{-1}, 1)$:

$$x \circ y = R_a^{-1}x \cdot L_b^{-1}y.$$

But in the group $R_a^{-1} = R_{a^{-1}}$, for every a. Indeed,

$$R_a^{-1}x \cdot a = R_a(R_a^{-1}x) = x,$$

whence $R_a^{-1}x = xa^{-1} = R_{a^{-1}}x$. Similarly, we obtain $L_b^{-1} = L_{b^{-1}}$. Thus

$$x \circ y = R_{a^{-1}}x \cdot L_{b^{-1}}y = xa^{-1} \cdot b^{-1}y = x(ba)^{-1}y = xcy.$$

Because

$$R_c(x \circ y) = (x \circ y)c = (xcy)c = xc \cdot yc = R_c x \cdot R_c y,$$

we may conclude that $(\circ) = (\cdot)^{R_c}$. Consequently, $Q(\circ)$ is a group that is isomorphic to the group $Q(\cdot)$.

4°. Mutually inverse quasigroups and loops

Isotopy gives the possibility of obtaining new quasigroups from a quasigroup A. Another way of obtaining new quasigroups is the following.

Two inverse operations are associated with each quasigroup A: a left inverse operation ${}^{-1}\mathrm{A}$, which is defined by the equation $A(y, a) = b$, namely $y = {}^{-1}\mathrm{A}(b, a)$, and a right inverse operation A^{-1}, which is defined by the equation $A(a, x) = b$, namely $x = A^{-1}(a, b)$. It was shown above that A^{-1} and ${}^{-1}\mathrm{A}$ are also quasigroups. Therefore, each has its inverse operations. Thus, A^{-1} has two inverse operations ${}^{-1}(A^{-1})$ and $(A^{-1})^{-1}$. However, $(A^{-1})^{-1} = A$. Indeed, according to the definition of $(A^{-1})^{-1}$, we must have $A^{-1}(x, (A^{-1})^{-1}(x, y)) = y$. Simultaneously, by (1.4), we find

$$A^{-1}(x, A(x, y)) = y,$$

whence

$$(A^{-1})^{-1}(x, y) = A(x, y).$$

Consequently, we get one new operation from A^{-1} : ${}^{-1}(A^{-1})$. Generally speaking, we can get five inverse operations: $A^{-1}, {}^{-1}A, {}^{-1}(A^{-1}), ({}^{-1}A)^{-1}, [{}^{-1}(A^{-1})]^{-1}$.

Following Stein [74][4] , we denote the permutation $\sigma(a, b, c) = (\sigma a, \sigma b, \sigma c)$ of three elements a, b, c by σ. Then $A(a, b) = c$ is equivalent to the equality ${}^{\sigma}A(\sigma a, \sigma b) = \sigma c$. For example, if $\sigma(a, b, c) = (b, c, a)$, then ${}^{\sigma}A = {}^{-1}(A^{-1})$, since ${}^{-1}(A^{-1})(b, c) = a \Leftrightarrow A(a, b) = c$.[4] If we

consider all possible permutations of the three elements a, b, c, then we obtain the five inverse operations listed above, along with operation A. Note that $[^{-1}(A^{-1})]^{-1} =^{-1} [(^{-1}A)^{-1}] = A^*$, where A^* is the operation which is obtained as $A^*(x, y) = A(y, x)$ from the operation A. Indeed, we have

$$[^{-1}(A^{-1})]^{-1}(a, b) = c \Leftrightarrow {}^{-1}(A^{-1})(a, c) = b$$
$$\Leftrightarrow A^{-1}(b, c) = a \Leftrightarrow A(b, a) = c,$$

i.e., $[^{-1}(A^{-1})]^{-1} = A^*$. Similarly, it is shown that $^{-1}[(^{-1}A)^{-1}] = A^*$.

Thus, a system $\sum_A{}^5$ of six quasigroups $\sum_A = \{A^{-1}, A, A^{-1,-1}(A^{-1}), (^{-1}A)^{-1}, A^*\}$ is associated with each quasigroup A. We call it the *system of inverse quasigroups* for A. It is easy to see that if B is one of the quasigroups of a system $\sum_A$, then $\sum_B = \sum_A$. For example, if $B =^{-1} (A^{-1})$, then $B^{-1} = A^{*,-1} B = A^{-1}$, etc. More precisely, the following assertions hold:

1) Let σ be a permutation from $\mathfrak{S}_3$, the symmetric group of degree 3. Then $B =^{\sigma} A$ implies $A =^{\sigma^{-1}} B$;

2) Further, suppose $\tau \in \mathfrak{S}_3$. Then

$$^{\tau}(^{\sigma}\mathrm{A}) =^{\tau\sigma} \mathrm{A}. \tag{1.17}$$

Let us prove, for example, the second assertion. By definition, the following equivalences hold:

$$A(a, b) = c \Leftrightarrow {}^{\sigma}\mathrm{A}(\sigma a, \sigma b) = \sigma c \Leftrightarrow {}^{\tau}(^{\sigma}\mathrm{A})(\tau(\sigma a), \tau(\sigma b)) = \tau(\sigma c),$$

that is, $A(a, b) = c$ is equivalent to the equality $^{\tau}(^{\sigma}\mathrm{A})(\tau\sigma a, \tau\sigma b) = \tau\sigma c$. On the other hand, we have $A(a, b) = c \Leftrightarrow {}^{\tau\sigma}A(\tau\sigma a, \tau\sigma b) = \tau\sigma c$. Consequently $^{\tau}(^{\sigma}\mathrm{A})(\tau\sigma a, \tau\sigma b) =^{\tau\sigma} A(\tau\sigma a, \tau\sigma b)$, from which we obtain (1.17).

If A is a loop, then $\sum_A$ does not consist just of loops. Indeed, if $A(x, y) = xy$ is a group, then $A^{-1}(x, y) = x^{-1}y$ and A^{-1} have no right neutral element in the general case. Therefore, it is expedient to consider the isotopes of inverse operations for A which are also loops. We will do this in the following way. If A is a loop with neutral element 1, then we consider the substitution I defined by the equality $A(x, Ix) = 1$, that is, Ix is the right inverse element of x.

We introduce the following two operations:

$$A^{\rho}(x, y) = A^{-1}(I^{-1}x, y), \quad A^{\lambda}(x, y) =^{-1} \mathrm{A}(x, Iy). \tag{1.18}$$

We show that A^{ρ} and A^{λ} are *loops with the same neutral element* 1. It follows from the definition of I that $I1 = 1$. *If A is a loop, then A^{-1} has a left neutral element.*

Indeed, let $A^{-1}(1, x) = x'$, so $A(1, x') = x$, whence $x' = x$. Therefore, $A^{\rho}(1, x) = A^{-1}(I^{-1}1, x) = A^{-1}(1, x) = x$. Now let $A^{\rho}(x, 1) = x'$. By virtue of the definition of the operation A^{ρ}, we conclude that $A(I^{-1}x, x') = 1$. But from $A(x, Ix) = 1$ it follows that $A(I^{-1}x, x) = 1$, where $x' = x$. Thus, two further loops A^{ρ} and A^{λ}, called the *left and right inverse loops for A* respectively, can be associated with each loop. Their consideration is suggested by inverse operations for a group or, more generally, for an IP-loop (see Chapter V).

The definitions for A^ρ and A^λ can be rewritten as:

$$A^\rho = (A^{-1})^{PA}, A^\lambda = ({}^{-1}A)^{SA},$$

where $P_A = (I_A^{-1}, 1, 1), S_A = (1, I_A, 1)$, and $I_A = I$ is defined by the equality $A(x, I_{A^x}) = 1$. It is easy to show that $I_{A^\rho} = I_{A^\lambda} = I^{-1}$. Indeed, it follows from $A^\rho(x, I_{A^\rho}x) = 1$ that $A^{-1}(I^{-1}x, I_{A^\rho}^{-1}x) = 1$, whence $A(I^{-1}x, 1) = I_{A^\rho}x$, i.e., $I_{A^\rho} = I^{-1}$. The equality $I_{A^\lambda} = I^{-1}$ is proved similarly. Consequently, from here we have the relationship

$$P_{A^\rho} = P_{A^\lambda} = P_A^{-1}, \;\; S_{A^\rho} = S_{A^\lambda} = S_A^{-1}.$$

As for inverse quasigroups, we can consider inverse loops for the loops A^ρ and A^λ, etc., defining $(A^\rho)^\rho = A^{\rho^2}, (A^\rho)^\lambda = A^{\rho\lambda}$, etc.

For quasigroups we have seen that there are only six inverse quasigroups (including the quasigroup itself). In order to study an analogous problem for inverse loops, we should first verify the equations:

$$\left.\begin{array}{c} A^{\rho^2} = A, \;\; A^{\lambda^2} = A, \\ A^{\rho\lambda} = [{}^{-1}(A^{-1})]^{(1, I^{-1}, I^{-1})}, \;\; A^{\lambda\rho} = [{}^{-1}(A^{-1})]^{(I,1,I)}, \\ A^{\rho\lambda\rho} = (A^*)^{(I^{-1})}, \;\; A^{\lambda\rho\lambda} = (A^*)^I \end{array}\right\} \tag{1.19}$$

and

$$A^{\rho\alpha} = A^{\alpha\rho}, \;\; A^{\lambda\alpha} = A^{\alpha\lambda},$$

where α is an arbitrary permutation of the underlying set Q.

Let us prove, for example, the equality $A^{\rho\lambda\rho} = (A^*)^{I^{-1}}$. Let

$$A^{\rho\lambda\rho}(x, y) = z. \tag{1.20}$$

Then, applying the definitions of A^ρ and $A^{\rho\lambda}$ several times, we obtain

$$(A^{\rho\lambda})^\rho(x, y) = z, \;\; (A^{\rho\lambda})^{-1}(I_{A^{\rho\lambda}}^{-1}x, \;\; y) = z, A^{\rho\lambda}(I_{A^{\rho\lambda}}^{-1}x, z) = y,$$

$${}^{-1}(A^\rho)(I_{A^{\rho\lambda}}^{-1}x, I_{A^\rho}z) = y, A^\rho(y, I_{A^\rho}z) = I_{A^{\rho\lambda}}^{-1}x,$$

and finally

$$A^{-1}(I_A^{-1}y, I_{A^\rho}z) = I_{A^{\rho\lambda}}^{-1}x,$$

whence

$$A(I_A^{-1}y, I_{A^{\rho\lambda}}^{-1}x) = I_{A^\rho}z. \tag{1.21}$$

However,

$$I_A = I, \;\; I_{A^\rho} = I^{-1}, \;\; I_{A^{\rho\lambda}} = I_{(A^\rho)^\lambda} = I_{A^\rho}^{-1} = I_A = I.$$

Therefore, from (1.21), we have

$$A(I^{-1}x, I^{-1}y) = I^{-1}z, \;\; A^*(I^{-1}x, I^{-1}y) = I^{-1}z,$$

whence

$$z = (A^*)^{I^{-1}}(x, y). \tag{1.22}$$

Comparing (1.2) and (1.22), we obtain the equality $A^{\rho\lambda\rho} = (A^*)^{I^{-1}}$. Thus, from the given loop A we can get the loops

$$A, A^{\rho},\ A^{\lambda},\ A^{\rho\lambda},\ A^{\lambda\rho},\ A^{\lambda\rho\lambda},\ A^{\rho\lambda\rho},\ A^{\lambda\rho\lambda\rho}, \cdots \tag{1.23}$$

But *up to isomorphism, there exist only six of them*, since $A^{\rho\lambda\rho}$ and $A^{\lambda\rho\lambda}$ are isomorphic in view of the equality $A^{\lambda\rho\lambda} = (A^{\rho\lambda\rho})^{I^2}$, and, applying the equalities (1.19), we reduce all the loops from (1.23) to the first six.

For example,

$$A^{\lambda\rho\lambda\rho} = (A^{\lambda\rho\lambda})^{\rho} = [(A^{\rho\lambda\rho})^{I^2}]^{\rho} = [(A^{\rho\lambda\rho})^{\rho}]^{I^2} = [(A^{\rho\lambda})^{\rho^2}]^{I^2} = (A^{\rho\lambda})^{I^2}.$$

Consider the connection that exists between inverse operations and isotopy. Let ${}^{\sigma}A$ be an arbitrary inverse quasigroup, and let $T = (\alpha, \beta, \gamma)$. For a permutation σ, we can write

$$T = (\alpha, \beta, \gamma) \leftrightarrow \sigma T = \sigma(\alpha, \beta, \gamma) = (\sigma\alpha, \sigma\beta, \sigma\gamma).$$

Lemma 1.3. ${}^{\sigma}(A^T) = ({}^{\sigma}A)^{\sigma T}$.

Let

$${}^{\sigma}(A^T)(x, y) = z. \tag{1.24}$$

By virtue of the definition of ${}^{\sigma}A$, the equality (1.24) is equivalent to the equality

$$A^T(x', y') = z', \tag{1.25}$$

where $\sigma(x',\ y',\ z') = (x, y, z)$. But (1.25) implies

$$A(\alpha x',\ \beta y') = \gamma z',$$

which is equivalent to the equality

$${}^{\sigma}A(\alpha' x,\ \beta' y) = \gamma' z, \tag{1.26}$$

where $(\alpha',\ \beta',\ \gamma') = \sigma(\alpha,\ \beta,\ \gamma) = \sigma T$. Consequently, it follows from (1.26) that

$$({}^{\sigma}A)^{\sigma T}(x, y) = z. \tag{1.27}$$

Comparing (1.24) with (1.27), the lemma is verified.

Corollary 1. We have $(A^T)^{-1} = (A^{-1})^{T^{\gamma}}$ and ${}^{-1}(A^T) = ({}^{-1}A)^{T^l}$, where $T^{\gamma} = (\alpha, \beta, \gamma)^{\gamma} = (\alpha, \gamma, \beta)$ and $T^l = (\gamma, \beta, \alpha)$.

Corollary 2. *If B and A are isotopic, then so are ${}^{\sigma}B$ and ${}^{\sigma}A$.*

Indeed, from $B = A^T$ it follows that ${}^{\sigma}B = {}^{\sigma}(A^T) = ({}^{\sigma}A)^{\sigma T}$.

Notes

[1]Such tables are known as *Latin squares*, particularly in combinatorial analysis (see Hall [85, 86]).

[2]Definition 2 asserts that $Q(A)$ is a quasigroup if the identities (1.3) hold in the algebra $Q(A, B, C)$. All the algebras $Q(A, B, C)$ satisfying the identities (1.3) form a so-called *primitive class* (see A.G. Kurosh [47, *i*. 155]). Thus $Q(A, B, C)$ is sometimes called a *primitive quasigroup*.

[3]The term "quasigroup" was introduced by Moufang [54], and the term "loop" was introduced by Albert [1, 2]

[4]The transformation $A \to {}^{\sigma}A$ is called *a parastrophy* (Sade [66], Artzy [8]). Stein [74] and Culik [88] study the change of identities under quasigroup parastrophy — see also Chapter VIII (invariance of distributivity under a parastrophy). All isotopies and parastrophies of a quasigroup generate a certain group — the *group of isostrophies*. This group is studied by Sade [70], Artzy [7, 8], and also by the author [18]. Artzy [6] gives an alternative presentation of the concepts of inverse loops, and studies their nuclei. In [18], groups of regular permutations of inverse quasigroups are studied.

[5]Stein [74] calls the operations from $\sum_A$ *conjugates*. Sade [66, 69] introduces a special term for each of the operations from $\sum_A$ (except A).

Chapter II. Groups of regular permutations. Autotopies of quasigroups

1°. Groups of left and right regular permutations

We have already seen that left and right regular permutations are closely related to the notion of the nucleus, having proved the following two propositions:

1) The left (right) regular permutations of a quasigroup $Q(\cdot)$ form a group $\mathscr{L}(\mathscr{R})$.

2) If $Q(\cdot)$ has a left (right) identity e, then for any $\lambda \in \mathscr{L}$ ($\rho \in \mathscr{R}$), we have $\lambda e \in N_l$ ($\rho e \in N_r$), and hence

$$N_l = \{\lambda e \mid \lambda \in \mathscr{L}\} = \mathscr{L}e \ (N_r = \mathscr{R}e).$$

Moreover, we have the following

Theorem 2.1. *The group of left regular permutations of a quasigroup $Q(\cdot)$ with left identity is isomorphic to the left nucleus N_l.*

Indeed, we have just observed that $N_l = \mathscr{L}_e = \{\lambda e \mid \lambda \in \mathscr{L}\}$. Let us consider the correspondence $\lambda \to \lambda e$. It is a mapping of $\mathscr{L}$ onto N_l: if $a \in N_l$, then for $\lambda = L_a$ we have $\lambda \to \lambda e = L_a e = a$. Furthermore, the correspondence is one-to-one, since $\lambda e = \mu e$ implies $\lambda = \mu$. Indeed, if x is an element of Q, then $\lambda x = \lambda(ex) = \lambda e \cdot x = \mu e \cdot x = \mu(ex) = \mu x$, that is $\lambda = \mu$. Consider $\lambda, \mu \in \mathscr{L}$. Then $\lambda\mu \to (\lambda\mu)e = \lambda(\mu e) = \lambda(e \cdot \mu e)$, whence $\lambda\mu \to \lambda e \cdot \mu e$, meaning that $\mathscr{L}$ and N_l are isomorphic.

Remark. $\mathscr{R} \cong N_r$ is proved similarly, if N_r exists. It is noteworthy that the correspondence $\rho \to \rho e$, where $\rho \in R$ and e is the right identity of the quasigroup $Q(\cdot)$, leads to an anti-isomorphism of the groups $\mathscr{R}$ and N_r: $\rho_1 \to \rho_1 e$ and $\rho_2 \to \rho_2 e$ (for $\rho_1, \rho_2 \in \mathscr{R}$) imply $\rho_1\rho_2 \to \rho_2 e \cdot \rho_1 e$. However, if two groups are anti-isomorphic, then they are isomorphic, so $\mathscr{R} \cong N_r$.

The proof of Theorem 2.1 also implies the following property for left (and right) regular permutations: *if $\lambda, \mu \in \mathscr{L}$ and $\lambda a = \mu a$ for any element a, then $\lambda = \mu$.*

In the quasigroup $Q(\cdot)$, the group $\mathscr{L}$ of left regular permutations defines an equivalence. Namely, we will consider that b and a are equivalent, and write $b \sim a \ (\mathscr{L})$, if there exists a left regular permutation $\lambda \in \mathscr{L}$ such that $b = \lambda a$. Each equivalence class, therefore, has the form $K = \mathscr{L}k = \{\lambda k \mid \lambda \in \mathscr{L}\}$, where k is an arbitrary element of K.

Definition 1. The equivalence class $K = \mathscr{L}k$, where k is an arbitrary element of the quasigroup $Q(\cdot)$ and $\mathscr{L}$ is the group of left regular permutations, is called the *left nucleus (relative to k)* of the quasigroup $Q(\cdot)$. We will denote the left nucleus (relative to the element k) by $N_l(k)$.

Similarly, we define the *right nucleus (relative to the element k)* of the quasigroup $Q(\cdot)$.

In the case when $Q(\cdot)$ has a left identity e, one of the equivalence classes is the left nucleus N_l : $N_l = \mathscr{L}e$ $(e \in N_l)$, and, as we have already seen, N_l is a subquasigroup.

Generally speaking, one of the equivalence classes of a quasigroup $Q(A)$ can be a subquasigroup, even when $Q(A)$ has no neutral element. We have

Theorem 2.2. *Let K be a relative left nucleus of the quasigroup $Q(\cdot)$. If K is a subquasigroup, then it is isotopic to the group $\mathscr{L}$ of all left regular permutations.*

Indeed, a relative left nucleus K must have the form $\mathscr{L}k$, where k is some fixed element of the set K, and if K is a quasigroup, then the composition $\lambda k \cdot \mu k$, where $\lambda, \mu \in \mathscr{L}$, must also belong to K. Consequently, there exists a left regular permutation γ depending on λ and μ (for a fixed k), such that $\lambda k \cdot \mu k = \gamma k$. Thus, on the set $\mathscr{L}$ we introduce a new operation, denoted by $(\circ)$, with $\gamma = \lambda \circ \mu$ if $\lambda k \cdot \mu k = (\lambda \circ \mu)k$. From the definition of this operation it follows that $\mathscr{L}(\circ)$ is a quasigroup which is isomorphic to a subquasigroup $K(\cdot)$; the isomorphism is realized by the correspondence $k \to \lambda k$. Let $\alpha \in \mathscr{L}$. Then

$$\alpha(\lambda \circ \mu) = \alpha\lambda \circ \mu. \tag{2.1}$$

Indeed, $\alpha(\lambda \circ \mu)k = \alpha\left[(\lambda \circ \mu)k\right] = \alpha(\lambda k \circ \mu k) = \alpha(\lambda k)\mu k = (\alpha\lambda \circ \mu)k$. On the basis of the properties of the left regular permutations from above, we conclude that equality (2.1) holds.

If ε is the unit permutation (the neutral element of the group $\mathscr{L}$), then $\varepsilon \circ \lambda = \lambda'$. The correspondence $\lambda \to \lambda'$ is a one-to-one mapping of the set $\mathscr{L}$ onto itself, since in the quasigroup $\mathscr{L}(\circ)$. the equation $\varepsilon \circ \xi = \lambda$ always has a unique solution. If we put $\lambda = \varepsilon$ in (2.1) we get

$$\alpha\varepsilon \circ \mu = \alpha(\varepsilon \circ \mu),$$

whence

$$\alpha \circ \mu = \alpha\mu'.$$

This equality means that $\mathscr{L}(\circ)$ and $\mathscr{L}(\cdot)$ are principally isotopic, and since $\mathscr{L}(\circ)$ and $K(\cdot)$ are isomorphic, the theorem is proved.

It is easy to see that Theorem 2.1 is a particular case of Theorem 2.2, with $K = N_l$ and $k = e$. Then $\mu' = \mu$ since $\mu' e = (\varepsilon \circ \mu)e = e \cdot \mu e = \mu e$, and, consequently, $\alpha \circ \mu = \alpha\mu$.

If K is a relative left nucleus, then $Kl = \{kl \mid k \in K\}$, where l is an arbitrary fixed element of Q, is also a relative left nucleus. If we fix k in K and take $k_1 \sim k$ $(\mathscr{L})$, then also $k_1 l \sim kl$ $(\mathscr{L})$. Indeed, there must be a permutation $\lambda \in \mathscr{L}$ such that $k_1 = \lambda(k)$, and then $k_1 l = \lambda k \cdot l = \lambda(kl)$, i.e. $k_1 l \sim kl$ $(\mathscr{L})$. Conversely, let $p \sim kl$ $(\mathscr{L})$. Consider the equation $p = xl$. There exists $\mu \in \mathscr{L}$ such that $p = \mu(kl)$. Consequently, $p = \mu k \cdot l = xl$, whence $x = \mu k$, i.e. $x \in K$. There is a one-to-one correspondence $k \to kl$ between elements of the classes K and Kl. This, in the case when Q is finite, implies the following.

Theorem 2.3. *Let $Q(\cdot)$ be a finite quasigroup. Then the order of its group $\mathscr{L}$ of left regular permutations is a divisor of the order of the quasigroup.*

The theorem follows from the equality $K = \mathscr{L}k$, i.e., the order of its group $\mathscr{L}$ coincides with the number of elements of any relative left nucleus.

Note that all the above statements for the group of left regular permutations similarly hold for the group of right regular permutations.

2°. Middle regular permutations

The groups of left and right regular permutations are closely related respectively to the concepts of the left and right nuclei. For a quasigroup, these groups play the same role as the left and right nucleus for a loop. Now we introduce a group of permutations which will play the same role for a quasigroup as the middle nucleus for a loop.

Definition 2. A permutation φ of a set Q is called a *middle regular permutation* of a quasigroup $Q(\cdot)$ if there exists a permutation φ^* such that

$$\varphi x \cdot y = x \cdot \varphi^* y \tag{2.2}$$

for all $x, y \in Q$.

The unit permutation is a middle regular permutation, which is why middle regular permutations always exist. It is easy to see that they form a group, which we denote by Φ. Indeed, if $\varphi, \psi \in \Phi$, then

$$\varphi\psi x \cdot y = \psi x \cdot \varphi^* y = x \cdot \psi^*\varphi^* y. \tag{2.3}$$

According to the definition of middle regular permutations, we conclude that $\varphi\psi \in \Phi$. From the obvious equality $\varphi^{-1}x \cdot y = x \cdot (\varphi^*)^{-1}y$ we see that $\varphi^{-1} \in \Phi$ as well.

Like the groups $\mathscr{R}$ and $\mathscr{L}$, the group Φ of middle regular permutations of a quasigroup $Q(\cdot)$ is also a subgroup of the associated group G of the quasigroup $Q(\cdot)$. Indeed, the equality (2.2) can be rewritten by using translations in the form $R_y\varphi x = R_{\varphi^* y}x$, i.e., $R_y\varphi = R_{\varphi^* y}$, whence $\varphi = R_y^{-1}R_{\varphi^* y}$. Consequently, $\varphi \in G$ and $\Phi \subseteq G$.

The permutation φ^* is said to be *adjoint* to the permutation φ. As follows from (2.3), the set of permutations adjoint to middle regular permutations forms a group, which we denote by Φ^*, and in view of the equality (2.3), the group Φ^* is anti-isomorphic to the group Φ. Consequently Φ^* is isomorphic to the group Φ (see Remark 1).

Suppose that $Q(\cdot)$ is a loop with neutral element e. We put $x = e$ in the equality (2.2):

$$\varphi^* y = \varphi e \cdot y.$$

Consequently,

$$\varphi x \cdot y = x(\varphi e \cdot y).$$

Now taking $y = e$, we have

$$\varphi x = x \cdot \varphi e.$$

Thus, $(x \cdot \varphi e)y = x(\varphi e \cdot y)$. This equality shows that φe belongs to the middle nucleus N_m. Therefore, $\varphi = R_a$, where $a = \varphi e \in N_m$. The converse is obvious: if $\varphi = R_a$ for $a \in N_m$, then $\varphi \in \Phi$. Indeed, $\varphi x \cdot y = xa \cdot y = x \cdot ay = x \cdot \varphi^* y$, so $\varphi^* = L_a$. Just as for the groups $\mathscr{L}$ and $\mathscr{R}$, we have the following.

Theorem 2.4. *The group Φ of middle regular permutations of a loop $Q(\cdot)$ is isomorphic to the middle nucleus N_m. Therefore, the group Φ^* of permutations adjoint to the middle regular permutations is also isomorphic to the middle nucleus N_m.*

The proof of Theorem 2.4 is analogous to the proof of Theorem 2.1. Relatively to the group Φ one can also consider equivalence classes $K = \Phi k$, where k is some fixed element from K, and two elements b and a are equivalent modulo Φ if there exists a middle regular permutation φ such that $b = \varphi a$. The equivalence class modulo Φ containing an element k is called the *middle nucleus relative to k.*

The middle nuclei are equipollent, since the one-to-one correspondence $\varphi k_1 \leftrightarrow \varphi k_2$ can be established between the elements of the relative nuclei $K_1 = \Phi k_1$ and $K_2 = \Phi k_2$. The one-to-one correspondence comes from the following proposition: If for some a we have $\varphi a = \psi a$, where $\varphi, \psi \in \Phi$, then $\varphi = \psi$. Indeed, let $\varphi a \cdot x = \psi a \cdot x$ for all x. Then $a \cdot \varphi^* x = a \cdot \psi^* x$, whence $\varphi^* x = \psi^* x$, i.e., $\varphi^* = \psi^*$. But from here, by applying the definition of a middle regular permutation, we conclude that $\varphi = \psi$. Thus, we can formulate the following theorem:

Theorem 2.5. *Let $Q(\cdot)$ be a finite quasigroup. Then the order of the group Φ of middle regular permutations is a divisor of the order of the quasigroup* [1].

Incidentally, from Theorem 2.3 and Theorem 2.5 it follows that the orders of the nuclei of a finite loop are divisors of the order of the loop [39]. [2]

3°. Autotopies of quasigroups. Quasi-automorphisms

In quasigroup theory, the concept of autotopy also plays an important role.

Definition 3. An ordered triple $T = (\alpha, \beta, \gamma)$ of permutations of a set Q is called an *autotopy* [3] of a quasigroup $Q(\cdot)$ if

$$\gamma^{-1}(\alpha x \cdot \beta y) = x \cdot y$$

for all $x, y \in Q$.

Consequently, autotopies are particular cases of isotopies (see page 13). It is enough to put $B = A$. If $T = (\alpha, \beta, \gamma)$ is an autotopy of a quasigroup $Q(A)$, then we can write

$$A^T = A.$$

In particular, an autotopy of the form $(\alpha, \alpha, \alpha) = \alpha$ is an automorphism.

Using equations (1.13) and (1.14), it is clear that the autotopies of a quasigroup $Q(A)$ form a group under composition. We denote this group by $\mathfrak{A}_A$.

It is easy to see that the sets of all corresponding components of the autotopies of a quasigroup $Q(\cdot)$ also form groups. For example, let γ_1 and γ_2 be the principal components of some autotopies T_1 and T_2, i.e., $T_1 = (\alpha_1, \beta_1, \gamma_1)$ and $T_2 = (\alpha_2, \beta_2, \gamma_2)$. Then $T_1T_2 = (\alpha_1\alpha_2, \beta_1\beta_2, \gamma_1\gamma_2) \in \mathfrak{A}_A$, and consequently, $\gamma_1\gamma_2$ is also a principal component of an autotopy.

We note here that if T is an autotopy, then any two components uniquely determine the third. For example, let $T = (\alpha, \beta, \gamma)$, $T' = (\alpha, \beta', \gamma)$ and $T, T' \in \mathfrak{A}_A$. Then $\beta = \beta'$. Indeed, $T', T^{-1} \in \mathfrak{A}_A$ and $T', T^{-1} = (1, \beta'\beta^{-1}, 1)$, i.e., $A(x, \beta'\beta^{-1}y) = A(x, y)$, whence $\beta'\beta^{-1} = 1$ and $\beta' = \beta$.

If a permutation φ is one of the components of an autotopy T, then we call it *autotopic*. *All the regular permutations of a quasigroup $Q(\cdot)$ are autotopic* since $U_\lambda = (\lambda, 1, \lambda)$, $V_\rho = (1, \rho, \rho)$, $W_\varphi = (\varphi, \varphi^{*-1}, 1)$ are autotopies for $Q(\cdot)$[*]. We now prove some lemmas.

Lemma 2.1. *If quasigroups $Q(B)$ and $Q(A)$ are isotopic, then their autotopy groups are isomorphic.*

A more precise formulation of Lemma 2.1 is the following:

$$\mathfrak{A}_{A^T} = T^{-1}\mathfrak{A}_A T.$$

Indeed, let

$$B = A^T \tag{2.4}$$

and let $S \in \mathfrak{A}_B$, so $B^S = B$. Then $(A^T)^S = A^T$, whence $A^{TST^{-1}} = A$, which means that

$$T\mathfrak{A}_B T^{-1} \subseteq \mathfrak{A}_A. \tag{2.5}$$

But (2.4) implies $A = B^{T^{-1}}$ and, applying the relation (2.5) to this equation, we obtain $T^{-1}\mathfrak{A}_A T \subseteq \mathfrak{A}_B$, whence

$$\mathfrak{A}_A \subseteq T\mathfrak{A}_B T^{-1}. \tag{2.6}$$

Comparing the inclusions (2.5) and (2.6), we obtain the equality $\mathfrak{A}_A = T\mathfrak{A}_B T^{-1}$.

Lemma 2.2. *Let $S_1 = (1, \beta, \gamma)$, $S_2 = (\lambda, 1, \mu)$, $S_3 = (\pi, \rho, 1)$. Then:*

a) If S_3 is an autotopy of a quasigroup $Q(\cdot)$, then π is a middle regular permutation and ρ^{-1} is adjoint to it.

b) If $Q(\cdot)$ is a loop and S_1, S_2 are autotopies of the loop, then $\beta = \gamma$ and $\lambda = \mu$. Consequently, β is a right regular permutation, and λ is a left regular permutation.

Indeed, let $(\cdot)^{S_3} = (\cdot)$, i.e., $\pi x \cdot \rho y = xy$. Then $\pi x \cdot y = x \cdot \rho^{-1}y$, whence, in view of the definition of a middle regular permutation, the proposition *a*) is valid.

Now let $Q(\cdot)$ be a loop and let $(\cdot)^{S_1} = (\cdot)$ or $\gamma^{-1}(x \cdot \beta y) = xy$. We put $x = 1$ (where 1 is the neutral element of the loop). Then $\gamma^{-1}\beta y = y$, i.e., $\gamma = \beta$. Consequently, $S_1 = (1, \beta, \beta)$, whence it follows that β is a right regular permutation.

We introduce the following concept.

[*]Here $\lambda \in \mathscr{L}$, $\rho \in \mathscr{R}$, $\varphi \in \Phi$.

Definition 4. A principal component of an autotopy T of a quasigroup $Q(\cdot)$ is called a *quasi-automorphism* of the quasigroup $Q(\cdot)$. In other words, a permutation γ of a set Q is called a quasi-automorphism of the quasigroup $Q(\cdot)$ if there exist two permutations α and β of the set Q such that

$$\gamma(xy) = \alpha x \cdot \beta y, \tag{2.6'}$$

i.e., $T = (\alpha, \beta, \gamma)$ is an autotopy of the quasigroup $Q(\cdot)$.

Since the corresponding components of the autotopies form groups, then Definition 4 implies the following.

Lemma 2.3. *The quasi-automorphisms of a quasigroup $Q(\cdot)$ form a group.*

Obviously, the group of automorphisms is a subgroup of the group of quasi-automorphisms.

Let $T = (\alpha, \beta, \gamma)$ be an autotopy of a loop $Q(\cdot)$. Then γ is a quasi-automorphism of the loop $Q(\cdot)$. In other words,

$$\gamma(xy) = \alpha x \cdot \beta y.$$

Set $x = 1$. Then

$$\gamma y = \alpha 1 \cdot \beta y = l \cdot \beta y,$$

i.e., $\gamma = L_l \beta$, whence

$$\beta = L_l^{-1} \gamma (l = \alpha 1). \tag{2.7}$$

Similarly, we have

$$\alpha = R_k^{-1} \gamma (k = \beta 1), \tag{2.8}$$

i.e,

$$T = (R_k^{-1}, L_l^{-1}, 1)\gamma. \tag{2.9}$$

Thus, *any autotopy T of a loop $Q(\cdot)$ must have the form* (2.9), where k and l are certain elements of the set Q. We obtain the following.

Lemma 2.4. *All the components of an autotopy $T = (\alpha, \beta, \gamma)$ of a loop $Q(\cdot)$ are quasi-automorphisms, if R_k and L_l, for $k = \beta 1$ and $l = \alpha 1$, are quasi-automorphisms of the loop.*

Lemma 2.4 follows from Lemma 2.3 and the equations (2.7) (2., 8).

Corollary. *If $Q(\cdot)$ is a group, then the components of any autotopy are quasi-automorphisms of the group.*

Indeed, in this case R_k and L_l are always quasi-automorphisms:

$$R_k(x \cdot y) = x \cdot R_k y,\ L_l(x \cdot y) = L_l x \cdot y,$$

i.e., $(1, R_k, R_k)$, $(L_l, 1, L_l)$ are autotopies of the group $Q(\cdot)$. In other words, in this case R_k and L_l are respectively right and left regular permutations of the group $Q(\cdot)$.

When $Q(\cdot)$ is a group, quasi-automorphisms have a simple construction.

Lemma 2.5. *Each quasi-automorphism γ of a group $Q(\cdot)$ has the form*

$$\gamma = R_s\gamma_0, \tag{2.10}$$

where γ_0 is an automorphism of the group $Q(\cdot)$ and s is some element from Q. Conversely, the permutation γ defined by (2.10) *is a quasi-automorphism of the group $Q(\cdot)$.*

Indeed, let γ be a quasi-automorphism of the group $Q(\cdot)$. i.e., there exists an autotopy of the form (α, β, γ). By virtue of equations (2.7), (2.8), we have $\alpha = R_k^{-1}\gamma$ and $\beta = L_l^{-1}\gamma$. But in a group, $R_a^{-1} = R_{a^{-1}}$ and $L_a^{-1} = L_{a^{-1}}$ hold for each element a. Consequently, the equality (2.6′) takes the form

$$\gamma(xy) = (\gamma x \cdot k^{-1})(l^{-1}\gamma y)$$

or

$$\gamma(xy) = \gamma x(\gamma 1)^{-1}\gamma y, \tag{2.11}$$

since

$$k^{-1}l^{-1} = (lk)^{-1} = (\alpha 1 \cdot \beta 1)^{-1} = (\gamma 1)^{-1}.$$

Let

$$\gamma x(\gamma 1)^{-1} = \gamma_0 x. \tag{2.12}$$

Multiplying both sides of the equality (2.11) by $(\gamma 1)^{-1}$ on the right, we obtain

$$\gamma_0(xy) = \gamma_0(x) \cdot \gamma_0(y),$$

i.e., γ_0 is an automorphism of the group $Q(\cdot)$. The equality (2.12) implies the equality (2.10). The converse assertion is obvious: an arbitrary translation and an arbitrary automorphism in a group are quasi-automorphisms, so their product $R_s\gamma_0$ must be a quasi-automorphism.

Remark. A quasi-automorphism γ can be represented in the form

$$\gamma = L_s\gamma_0',$$

where γ_0' is some automorphism. Indeed, (2.10) implies

$$\gamma x = R_s\gamma_0 x = \gamma_0 x \cdot s = s(s^{-1}\gamma_0 x \cdot s) = s \cdot \theta_s\gamma_0 x = s \cdot \gamma_0' x = L_s\gamma_0' x,$$

where $\gamma_0' = \theta_s\gamma_0$ and θ_s is the inner automorphism

$$\theta_s x = s^{-1}xs.$$

Corollary. *A quasi-automorphism γ of a group $Q(\cdot)$ is an automorphism if and only if* $\gamma 1 = 1$. Indeed, $\gamma 1 = R_s\gamma_0 1 = R_s 1 = s$, i.e., $s = 1$, and, consequently, $\gamma = \gamma_0$.

Theorem 2.6. *An arbitrary autotopy T of a group $Q(\cdot)$ has the form*

$$T = (L_c, R_d, L_c R_d)\theta,$$

where θ is an automorphism of the group $Q(\cdot)$, while c and d are fixed elements from Q.

Indeed, we note that in a group Q the equality

$$R_k L_l = L_l R_k \tag{2.13}$$

is true for all k and $l \in Q$, since the equality (2.13) is equivalent to the law of associativity.

Let $T = (\alpha, \beta, \gamma)$ be an autotopy of a group $Q(\cdot)$. Then T has the form (2.9):

$$T = (R_k^{-1}, L_l^{-1}, 1)\gamma,$$

whence by virtue of (2.13), we obtain

$$T = (L_l, R_k, L_l R_k) R_k^{-1} L_l^{-1} \gamma.$$

The permutations L_l, R_k, γ are quasi-automorphisms of the group $Q(\cdot)$, so $\theta = R_k^{-1} L_l^{-1} \gamma$ is also a quasi-automorphism of the group $Q(\cdot)$.

But $\theta 1 = 1$:

$$R_k^{-1} L_l^{-1} \gamma 1 = R_k^{-1} L_l^{-1} (\alpha 1 \cdot \beta 1) = R_k^{-1} L_l^{-1} (lk) = 1,$$

so by virtue of the corollary to Lemma (2.5), θ is an automorphism of the group $Q(\cdot)$.

4°. Type of a quasigroup

We give the following

Definition 5. The ordered triple $(\mathscr{L}, \Phi, \mathscr{R})$ of left, middle, and right regular permutation groups of a quasigroup $Q(\cdot)$ (or isomorphic groups) is called the *type of the quasigroup*. A type (F, G, H) is called a *subtype* of a type (F', G', H'), if F, G, H are (isomorphic to) subgroups of F', G', H' respectively [14].

On the basis of Theorem 2.1, Remark 1 and Theorem 2.4, it follows that for a loop $Q(\cdot)$, the triple (N_l, N_m, N_r) of nuclei is a type. In particular, if $Q(\cdot)$ is a group, then the type is (Q, Q, Q). The following natural question arises: how does the type of a quasigroup change under isotopy? A partial answer to this question for quasigroups is given by the following.

Theorem 2.7. *The type of a quasigroup $Q(A)$ is a subtype of the type of any loop to which it is isotopic.*

Proof. Suppose that the quasigroup $Q(A)$ is isotopic to a loop $Q(\cdot)$: $A = (\cdot)^T$, where $T = (\alpha, \beta, \gamma)$.

1. Let us determine $\mathscr{L}_A$. For this we find autotopies of the quasigroup $Q(A)$ that have the form $U_\lambda = (\lambda, 1, \lambda)$. According to Lemma 2.1, $\mathfrak{A}_{(\cdot)} = T\mathfrak{A}_A T^{-1}$, so $TU_\lambda T^{-1} \in \mathfrak{A}_{(\cdot)}$. Thus

$$TU_\lambda T^{-1} = (\alpha, \beta, \gamma)(\lambda, 1, \lambda)(\alpha, \beta, \gamma)^{-1} =$$

$$= (\alpha, \beta, \gamma)(\lambda, 1, \lambda)(\alpha^{-1}, \beta^{-1}, \gamma^{-1}) = (\alpha\lambda\alpha^{-1}, 1, \gamma\lambda\gamma^{-1}).$$

Applying Lemma 2.2, we find

$$\alpha\lambda\alpha^{-1} = \gamma\lambda\gamma^{-1} \tag{2.14}$$

and

$$\gamma\lambda\gamma^{-1} \in \mathscr{L}. \tag{2.15}$$

Now (2.14) implies $(\gamma^{-1}\alpha)\lambda = \lambda(\gamma^{-1}\alpha)$, i.e., λ belongs to the centralizer* $\mathfrak{N}_{\gamma^{-1}a}$ of the permutation $\gamma^{-1}a$ in the symmetric group $\mathfrak{S}_Q$. Besides, the relation (2.15) implies $\lambda \in \gamma^{-1}\mathscr{L}\gamma$. Thus,

$$\mathscr{L}_A \subseteq \gamma^{-1}\mathscr{L}\gamma \cap \mathfrak{N}_{\gamma^{-1}\alpha}. \tag{2.16}$$

Conversely, let $\lambda \in \gamma^{-1}\mathscr{L}\gamma \cap \mathfrak{N}_{\gamma^{-1}\alpha}$. Then $\lambda = \gamma^{-1}\lambda'\gamma$, where $\lambda' \in \mathscr{L}$. We show that $\lambda \in \mathscr{L}_A$:

$$\lambda A(x, y) = \lambda\gamma^{-1}(\alpha x \cdot \beta y) = \gamma^{-1}\lambda'\gamma\gamma^{-1}(\alpha x \cdot \beta y) = \gamma^{-1}\lambda'(\alpha x \cdot \beta y)$$
$$= \gamma^{-1}(\lambda'\alpha x \cdot \beta y) = \gamma^{-1}(\gamma\lambda\gamma^{-1}\alpha x \cdot \beta y) = \gamma^{-1}(\gamma\lambda(\gamma^{-1}\alpha)x \cdot \beta y)$$
$$= \gamma^{-1}(\gamma\gamma^{-1}\alpha\lambda x \cdot \beta y) = \gamma^{-1}(\alpha\lambda x \cdot \beta y) = A(\lambda x, y).$$

Consequently,

$$\gamma^{-1}\mathscr{L}\gamma \cap \mathfrak{N}_{\gamma^{-1}\alpha} \subseteq \mathscr{L}_A. \tag{2.17}$$

Comparing the relationships (2.16) and (2.17), we obtain the equality

$$\mathscr{L}_A = \gamma^{-1}\mathscr{L}\gamma \cap \mathfrak{N}_{\gamma^{-1}\alpha}. \tag{2.18}$$

Similarly we have

$$\mathscr{R}_A = \gamma^{-1}\mathscr{R}\gamma \cap \mathfrak{N}_{\gamma^{-1}\beta}. \tag{2.19}$$

Thus, $\mathscr{L}_A$ is a subgroup of the group $\gamma^{-1}\mathscr{L}\gamma$, i.e., $\mathscr{L}_A$ is isomorphic to some subgroup of the group $\mathscr{L}$. Similarly, (2.19) implies that $\mathscr{R}_A$ is isomorphic to a subgroup of the group $\mathscr{R}$.

Remark. If $Q(A)$ is principally isotopic to a loop, then the formulas (2.18) and (2.19) are simplified: let $A = (\circ)^T$ with $T = (\alpha, \beta, 1)$. Then

$$\mathscr{L}_A = \mathscr{L} \cap \mathfrak{N}_\alpha, \quad \mathscr{R}_A = \mathscr{R} \cap \mathfrak{N}_\beta.$$

2. Now let us prove the following proposition: *If quasigroups $Q(A)$ and $Q(B)$ are isotopic, then Φ_A and Φ_B are isomorphic.*

Let $A = B^T = B^{(\alpha,\beta,\gamma)}$ and $\varphi \in \Phi_A$. Then there exists a permutation $\varphi^* \in \Phi_A^*$ such that

$$A(\varphi a, b) = A(a, \varphi^* b).$$

Proceeding to the operation B, we obtain

$$\gamma^{-1}B(\alpha\varphi a,\ \beta b) = \gamma^{-1}B(\alpha a,\ \beta\varphi^* b),$$

*The set of all elements x commuting with a (so $xa = ax$) is called the centralizer $\mathfrak{N}_a$ of the element a of a group $Q(\cdot)$. The centralizer $\mathfrak{N}_a$ is a subgroup of the group $Q(\cdot)$.

so replacing a by $\alpha^{-1}a$ and b by $\beta^{-1}b$ gives

$$B(\alpha\varphi\alpha^{-1}a,\, b) = B(a,\, \beta\varphi^*\beta^{-1}b).$$

Consequently, $\alpha\varphi\alpha^{-1} \in \Phi_B$, whence $\varphi \in \alpha^{-1}\Phi_B\alpha$, and therefore

$$\Phi_A \subseteq \alpha^{-1}\Phi_B\alpha. \tag{2.20}$$

But if $A = B^T$, then $B = A^{T^{-1}}$, and applying the relationship (2.20) to this equality, we obtain

$$\Phi_B \subseteq \alpha\Phi_A\alpha^{-1},$$

whence

$$\alpha^{-1}\Phi_B\alpha \subseteq \Phi_A. \tag{2.21}$$

Comparing the relationships (2.20) and (2.21), we find

$$\Phi_A = \alpha^{-1}\Phi_B\alpha. \tag{2.22}$$

In the case of our theorem, when $B = (\cdot)$, we have

$$\Phi_A = \alpha^{-1}\Phi\alpha.$$

Relationships (2.20), (2.21) and (2.22) prove the theorem. □

An immediate corollary of Theorem 2.7 is

Theorem 2.8. *Isotopic loops have the same type.*

Indeed, let $Q(A)$ and $Q(\cdot)$ be loops, and let $A = (\cdot)^T = (\cdot)^{(\alpha,\beta,\gamma)}$. Equation (2.22) immediately gives $\Phi_A = \alpha^{-1}\Phi\alpha$. From equation (2.16) we have

$$\mathscr{L}_A \subseteq \gamma^{-1}\mathscr{L}\gamma. \tag{2.23}$$

Since $(\cdot) = A^{T^{-1}}$, substitution in (2.23) yields $\mathscr{L} \subseteq \gamma^{-1}\mathscr{L}_A\gamma$, whence $\gamma^{-1}\mathscr{L}\gamma \subseteq \mathscr{L}_A$. Thus

$$\mathscr{L}_A = \gamma^{-1}\mathscr{L}\gamma.$$

Similarly, we obtain

$$\mathscr{R}_A = \gamma^{-1}\mathscr{R}\gamma.$$

Corollary. *The respective nuclei of isotopic loops are isomorphic.*

Albert's Theorem is another corollary of Theorem 2.7. If a loop $Q(A)$ is isotopic to a group $Q(\cdot)$, then its type coincides with the type of the group $Q(\cdot)$, i.e., with (Q, Q, Q). Thus, for example, the left nucleus of the loop $Q(A)$ coincides with Q, i.e., A is an associative operation.

5°. Transitive quasigroups. Medial quasigroups

If the left nucleus relative to some element k coincides with the whole quasigroup $Q(\cdot)$, then the group of left regular permutations is transitive on the set Q. It is thus useful to introduce the following concept:

Definition 6. A quasigroup $Q(\cdot)$ is called *$\mathscr{L}$-transitive* if the group $\mathscr{L}$ of all left regular permutations acts transitively on the set Q.

$\mathscr{R}$- and Φ-transitivity are defined similarly. Immediate examples of transitive (i.e., $\mathscr{L}$-, $\mathscr{R}$- or Φ-transitive) quasigroups are provided by groups. (Other examples exist). On the other hand, if a loop $Q(\cdot)$ is $\mathscr{L}$-transitive ($\mathscr{R}$-transitive, Φ-transitive), then it is a group. Indeed, in this case, for example, $N_l = \mathscr{L}1 = \{\lambda 1 \mid \lambda \in \mathscr{L}\} = Q$ by virtue of the transitivity of $\mathscr{L}$. Transitive quasigroups are very closely related to groups.

Theorem 2.9. *Any loop $Q(\cdot)$ isotopic to a transitive quasigroup $Q(A)$ is a group.*

Proof. For $\mathscr{L}$- and $\mathscr{R}$-transitivity, the assertion follows from Theorem 2.2. Indeed, if a quasigroup $Q(A)$ is $\mathscr{L}$-transitive, then $Q = \mathscr{L}k$ for some element k of Q. In this case Q is a relative left nucleus. Then, by Theorem 2.2, $Q(A)$ must be isotopic to the group $\mathscr{L}_A$ of all left regular permutations.

Now suppose $Q(A)$ is Φ-transitive, i.e., Φ_A acts transitively on Q. Further, let $Q(\cdot)$ be an arbitrary loop isotopic $Q(A)$, say $A = (\cdot)^T$, where $T = (\alpha, \beta, \gamma)$. In view of the equation (2.22) we have $\Phi_A = \alpha^{-1}\Phi\alpha$, where Φ is the group of middle regular permutations for the loop $Q(\cdot)$. Consequently, $\Phi = \alpha\Phi_A\alpha^{-1}$. Since Φ_A is transitive on Q, then Φ is also transitive on Q. Consequently, $Q(\cdot)$ is a Φ-transitive loop. But then $Q(\cdot)$ is a group, since in this case $N_m = Q$. □

Conversely, if a quasigroup $Q(A)$ is isotopic to a group $Q(\cdot)$, then it is Φ-transitive. This statement follows from equation (2.23). We note that for $\mathscr{L}$- and $\mathscr{R}$-transitivity the converse statement does not hold in general: a quasigroup isotopic to a group need not be $\mathscr{L}$- or $\mathscr{R}$-transitive (see Chapter VIII, 3°).

Thus, there exist transitive quasigroups which are not groups. The most important transitive quasigroups are medial quasigroups.

Definition 7. A quasigroup $Q(\cdot)$ is called *medial* [4] if the identity

$$(xy)(uv) = (xu)(yv) \tag{2.24}$$

is satisfied.

Example. Let Q be the field of all rational numbers. We define the operation $A(x, y) = ax + by + c$ for constants a, b, c with $a, b \neq 0$ It is easily verified that $Q(A)$ is a medial quasigroup.

Lemma 2.6. A medial quasigroup is Φ-transitive.

Indeed, using translations, the identity (2.24) can be rewritten as

$$R_y x \cdot L_u v = R_u x \cdot L_y v,$$

whence

$$R_y R_u^{-1} x \cdot v = x \cdot L_y L_u^{-1} v.$$

Thus, the permutation $\alpha = R_y R_u^{-1}$ is a middle regular permutation for $Q(\cdot)$, with adjoint $L_y L_u^{-1}$. If a and b are given elements, then there exists a middle regular permutation β such that $\beta a = b$. As β we can put $R_c R_d^{-1}$, where d is some fixed element, and c is a solution of the equation $R_d^{-1} a \cdot x = b$.

The previous lemma and Theorem 2.8 make it possible to derive the following, *Toyoda's Theorem* [79] [5]:

Theorem 2.10. *Let $Q(A)$ be a medial quasigroup. Then there exists an abelian group $Q(+)$ such that the operation A has the form*

$$A(x, y) = \varphi x + \psi y + c,$$

where φ, ψ are automorphisms of the group $Q(+)$ with $\varphi\psi = \psi\varphi$, and c is some fixed element of Q.

Proof. Since the medial quasigroup $Q(A)$ is Φ-transitive, then by Theorem 2.10 an arbitrary loop $Q(+)$ isotopic to $Q(A)$ is a group. Let us consider the principal isotope $(+) = A_{(}a, b)$, so

$$x + y = A(R_a^{-1} x, L_b^{-1} y). \tag{2.25}$$

Thus, $Q(+)$ is a group with the neutral element $A(b, a)$. We denote $A(b, a)$ by 0. Then (2.25) implies

$$A(x, y) = R_a x + L_b y. \tag{2.26}$$

Rewriting (2.24) with the operation $(+)$ gives

$$R_a(R_a x + L_b y) + L_b(R_a u + L_b v) = R_a(R_a x + L_b u) + L_b(R_a y + L_b v),$$

whence

$$R_a(x + y) + L_b(u + v) = R_a(x + L_b R_a^{-1} u) + L_b(R_a L_b^{-1} y + v).$$

Let $u = 0$ and $v = L_b^{-1} 0$. Then

$$R_a(x + y) = \alpha x + \beta y,$$

where

$$\alpha x = R_a(x + L_b R_b^{-1} 0) \quad \beta y = L_b(R_a L_b^{-1} y + L_b^{-1} 0).$$

Consequently, R_a is a quasi-automorphism of the group $Q(+)$. Similarly, L_b is a quasi-automorphism of the group $Q(+)$. By virtue of Lemma 2.5, R_a and L_b have the form

$$R_a x = \varphi x + k, \quad L_b x = l + \psi x, \tag{2.27}$$

where φ, ψ are automorphisms of the group $Q(+)$.

Consequently, from (2.26) and (2.27) we obtain

$$A(x,y) = \varphi x + c + \psi y, \tag{2.28}$$

where $c = k + l$. We again rewrite (2.24) with the operation $(+)$, this time using equation (2.28):

$$\varphi(\varphi x + c + \psi y) + c + \psi(\varphi u + c + \psi v) = \varphi(\varphi x + c + \psi u) + c$$

$$+\psi(\varphi y + c + \psi v),$$

whence

$$\varphi^2 x + \varphi c + \varphi\psi y + c + \psi\varphi u + \psi c + \psi^2 c = \varphi^2 x + \varphi c + \varphi\psi u$$

$$+c + \psi\varphi y + \varphi c + \psi^2 v,$$

or after simplification

$$\varphi\psi y + c + \psi\varphi u = \varphi\psi u + c + \psi\varphi y. \tag{2.29}$$

If $u = 0$, then from (2.29) we obtain

$$\varphi\psi y + c = c + \psi\varphi y, \tag{2.30}$$

whence replacing y and u with $\varphi^{-1}\psi^{-1}y$ and $\varphi^{-1}\psi^{-1}u$ respectively, we obtain

$$y + u = u + y,$$

i.e., $Q(+)$ is an Abelian group. The equality (2.30) implies $\varphi\psi y = \psi\varphi y$. This completes the proof of the theorem. □

Notes

[1]Other properties of groups of regular permutations are considered in [12, 14, 18]. In the latter article, types of loops are studied. It is shown that there exist loops with a predefined type, and, in particular, loops with type $(1, 1, 1)$. Regular permutations of quasigroups are also studied by Mattenet [50].

[2]Other properties of loop nuclei are considered in the works of Garrison [39], Bruck [31], etc.

[3]Along with the concept of autotopy, one may consider the concept of anti-autotopy. An ordered triple $T = (\alpha, \beta, \gamma)$ is called an *anti-autotopy* of a quasigroup $Q(\cdot)$ if $\gamma(xy) = \alpha y \cdot \beta x$. Autotopies and anti-autotopies were studied by various authors. We note here the later works of Sade [69, 73].

[4]In the quasigroup literature, there is no consensus on the name for quasigroups with the identity (2.24). They are called *Abelian* by Bruck [24], Griffin [43], Murdoch [52]. Etherington [91] and Sade [64, 67] call the identity (2.24) *entropy*. In functional equation theory, the identity (2.24) is customarily called *bisymmetry* (see Aczél [9], and also [11]). Following Stein [74], we adhere to the term "medial" quasigroup.

[5]Bruck [24] and Murdoch [52] also give proofs of the theorem.

Chapter III. Derivative operations. F-quasigroups

1°. Postulates of Sushkevich and Murdoch

The identity of associativity should be considered, perhaps, the most important and frequently used identity in algebra. An operation A on a set Q is associative if

$$A\left[A\left(x,y\right),z\right]=A\left[x,A\left(y,z\right)\right]$$

for all $x,y,z\in Q$. An associative groupoid $Q(A)$ is called *a semigroup*. Studying quasigroups and loops, it is natural to ask the question: How close are they to groups, i. e., to what extent does the law of associativity hold in them. This is how the concept of the nucleus considered in Chapter I arose. Thus, in the theory of quasigroups, identities which are more or less related to the law of associativity are often considered. Murdoch [51] suggested the following approach to the study of quasigroups and loops.

Let $Q(A)$ be a quasigroup. Consider the equation $A\left[A\left(a,b\right),c\right]=A\left[a,A\left(b,x\right)\right]$ in $Q(A)$. The equation has a unique solution, depending on a,b,c. Therefore, we can write $x=S_{a,b}c$, where $S_{a,b}$ is a permutation of the set Q. It can be even expressed with translations as $S_{a,b}=L_b^{-1}L_a^{-1}L_{A(a,b)}$, but currently this is not important for us. The closer $S_{a,b}$ is to the unit permutation, the closer the quasigroup $Q(A)$ is to being a group. The equality

$$A\left[A\left(a,b\right),c\right]=A\left[a,A\left(b,S_{a,b}c\right)\right], \tag{3.1}$$

having the form of the law of associativity, holds in each quasigroup, but of course it is still far from true associativity.

If $S_{a,b}$ depends on a and b, then indeed we get nothing new. However, we may consider certain particular cases.

(1). $S_{a,b}$ depends only on b: $S_{a,b}=S_b$.

Here, we can write the expression $A(b,S_bc)$ as $B(b,c)$, and (3.1) takes the form

$$A\left[A(a,b),c\right]=A\left[a,B(b,c)\right]. \tag{3.2}$$

That is nothing other than Sushkevich's Postulate A [78]. Sushkevich's First Theorem is as follows.

Theorem 3.1. *If Postulate* A *holds in a quasigroup $Q(A)$, then $Q(B)$ is a group, and A is an isotope of B of the form $B^{(\varphi,1,\varphi)}$.*

Indeed, it is easy to see that the operation B is invertible, by equation (3.2). It is necessary to prove that B is associative. Using Postulate A several times, we have:

$$A\{a, B[B(b,c),d]\} = A\{A[a, B(b,c)], d\} = A\{A[A(a,b),c], d\}$$

$$= A[A(a,b), B(c,d)] = A\{a, B[b, B(c,d)]\},$$

so

$$B[B(b,c),d] = B[b, B(c,d)].$$

Let $\varphi^{-1} = L_a$. Then from (3.2) we obtain $A(\varphi^{-1}b, c) = \varphi^{-1}B(b,c)$, whence $A(b,c) = \varphi^{-1}B(\varphi b, c)$, i.e., $A = B^{(\varphi,1,\varphi)}$. Conversely, if $Q(B)$ is a group and φ is an arbitrary permutation of Q, then Postulate A is satisfied in the quasigroup $Q(A)$, with $A = B^{(\varphi,1,\varphi)}$. It is easy to check this fact by a simple verification of (3.2).

(2). $S_{a,b}$ depends only on a: $S_{a,b} = S_a$.

Here the equality (3.1) takes the form

$$A[A(a,b),c] = A[a, A(b, S_a c)]. \tag{3.3}$$

Unlike the first case, construction of a quasigroup satisfying the identity (3.3) is much more complicated. For convenience, we call these quasigroups F-quasigroups[1]. We will see that there are F-quasigroups which are not isotopic to groups. They were studied in [51, 15].

(3). $S_{a,b}$ does not depend on a and b,i.e., $S_{a,b} = S$.

Here

$$A[A(a,b),c] = A[a, A(b, Sc)]. \tag{3.4}$$

This is Postulate B of Sushkevich [78]. Consider an isotope B of the operation A:

$$B = A^{(1,S,1)}. \tag{3.5}$$

Equation (3.4) turns into (3.2), and according to Sushkevich's First Theorem $Q(B)$ is a group. Moreover, we have

Theorem 3.2. *If Sushkevich's Postulate* B *holds in a quasigroup $Q(A)$, then $Q(A)$ is isotopic to a group $Q(B)$. Furthermore, $A = B^{(1,\theta,1)}$, where θ is an automorphism of the group $Q(B)$.*

Indeed, by Sushkevich's First Theorem it follows that A has the form $A = B^{(\varphi,1,\varphi)}$. On the other hand, from (3.5) we have $A = B^{(1,S^{-1},1)}$. Thus $B^{(\varphi,1,\varphi)} = B^{(1,S^{-1},1)}$, whence $B^{(\varphi,1,\varphi)(1,S^{-1},1)^{-1}} = B$ or $B^{(\varphi,S,\varphi)} = B$. Therefore, $T = (\varphi, S, \varphi)$ is an autotopy of the group $Q(B)$. Then, in virtue of Theorem 2.6 there exist two elements $c, d \in Q$ and an automorphism θ of the group $Q(B)$ such that

$$T = (L_c, R_d, L_c R_d)\theta = (L_c\theta, R_d\theta, L_c R_d\theta).$$

Consequently, $\varphi = L_c\theta = L_cR_d\theta$, which implies that $R_d = 1$, $d = 1$ and $S = R_d\theta = \theta$, i.e., S is an automorphism of the group $Q(B)$. Note here that S is also an automorphism of the quasigroup $Q(A)$, since

$$A^S = [B^{(1,S^{-1},1)}]^S = B^{(1,S^{-1},1)S} = B^{(S,1,S)} = B^{S(1,S^{-1},1)} = B^{(1,S^{-1},1)} = A.$$

We have identified a new class of quasigroups. A quasigroup is called $Q(A)$ *special* if $S_{a,b}$ is an automorphism. Many well-known loops are special.

Thus, according to the equation $A[A(a,b),c] = A(a.A(b,x)]$, we have arrived at two new classes of quasigroups: F-quasigroups and special quasigroups. But the equation (3.1) that holds in an arbitrary quasigroup can also be considered from the aspect presented in item (1). The expression $A(b, S_{a,b}c)$ can be regarded as the result of applying an operation that depends on a to the elements b and c. If we denote this operation by A_a, then we have $A(b, S_{a,b}c) = A_a(b,c)$ and

$$A\left[A(a,b),c\right] = A\left[a, A_a(b,c)\right]. \tag{3.6}$$

We arrived at this equality by considering the equation $A[A(a,b),c] = A(a,x)$. The solution of the equation for a fixed element a depends on b and c, i.e., the equation defines a binary operation that depends on a which we denote by A_a. We call the operation A_a a *right derivative operation*[2] of the operation A evaluated at the element a. Similarly, the equation $A[b, A(c,a)] = A(y,a)$ defines a *left derivative operation* ${}_aA$

$$A\left[b, A(c,a)\right] = A\left[{}_aA(b,c), a\right].$$

More generally, we can associate right and left derivative operations with each invertible operation.

2°. Elementary properties of derivative operations

Let us consider some simple properties of derivative operations. We combine them into one general theorem. Derivatives of the form ${}_b(A_a)$, as appearing in part 4) of the theorem, will be called *mixed*.

Theorem 3.3. *Suppose that $Q(A)$ is a quasigroup. Consider the right derivative operation A_a evaluated at an element a. Then*:

1) *A_a is an invertible operation, i.e., $Q(A_a)$ is a quasigroup. The quasigroup $Q(A_a)$ has a left neutral element e_a, which is also the right local neutral element for a;*

2) Right derivatives of right derivatives are right derivatives:

$$(A_a)_b = A_{A(a,b)}; \tag{3.7}$$

3) *If $A_a = A$, then a is a left associative element;*

4) *For all elements a, b of Q, the mixed derivative $Q({}_b(A_a))$ is a loop with neutral element e_a;*

5) *The quasigroups $Q(A_a)$ and $Q({}_bA)$ are isotopic to the quasigroup $Q(A)$.*

For left derivative operations, similar properties hold.

Proof. 1. Let us prove that the equation $A_a(x,b)=c$ has a unique solution for all b,c. For this, we consider the equation $A[A(a,x),b]=A(a,c)$. The solution of the equation exists. Since $A[A(a,x_0),b]=A[a,A_a(x_0,b)]=A(a,c)$, we find $A_a(x_0,b)=c$. Thus, the equation $A_a(x,b)=c$ has the solution x_0. Uniqueness of the solution is obvious. The equation $A_a(b,y)=c$ is solved similarly.

Further, let e_a be a right local neutral element for a, so $A(a,e_a)=a$. Substituting e_a for b in (3.6), we have

$$A[A(a,e_a),c]=A[a,A_a(e_a,c)],$$

so

$$A(a,c)=A[a,A_a(e_a,c)],$$

and

$$c=A_a(e_a,c),$$

i.e., e_a is the left neutral element of the quasigroup $Q(A_a)$.

2. To determine $(A_a)_b$, it is necessary to take the right derivative of the operation A_a at b, using the definition

$$A_a[A_a(b,c),d]=A_a[b,(A_a)_b(c,d)].$$

We have

$$A\{a,A_a[A_a(b,c),d]\}=A\{a,A_a[b,(A_a)b(c,d)]\},$$

so

$$A\{A[a,A_a(b,c)],d\}=A\{A(a,b),(A_a)_b(c,d)\},$$

$$A\{A[A(a,b),c],d\}=A\{A(a,b),(A_a)_b(c,d)\},$$

and

$$A\left\{A(a,b),A_{A(a,b)}(c,d)\right\}=A\{A(a,b),(A_a)_b(c,d)\},$$

whence

$$(A_a)_b=A_{A(a,b)}.$$

Thus, a right derivative of a right derivative is again a right derivative.

3. Suppose $A_a=A$. This means $A[A(a,x),y]=A[a,A_a(x,y)]=A[a,A(x,y)]$, i.e., $a\in N_l$. The converse is obvious.

4. Let us prove the following statement:*If $Q(A)$ has a right neutral element, then $Q(A_a)$ is a loop.* Indeed, suppose $A(a,e)=a$. Then, substituting $c=e$ in (3.6), we find $A[A(a,b),e]=A[a,A_a(b,e)]$, whence $A(a,b)=A[a,A_a(b,e)]$ and $b=A_a(b,e)$, i.e., $Q(A_a)$ has e as a right neutral element. But by part 1), $Q(A_a)$ has a left neutral element e_a, so $e_a=e$ and $Q(A_a)$ is a loop. Similarly, we can show that if $Q(A)$ has a left neutral element, then $Q({}_bA)$ is a loop. These statements verify part 4) of the theorem.

5. Using translations, the equality (3.6) can be rewritten as

$$A(L_ab,c)=L_aA_a(b,c),$$

whence

$$A_a=A^{(L_a,1,L_a)}. \tag{3.8}$$

Similarly, we find

$$ {}_bA = A^{(1,R_b,R_b)}. \tag{3.9} $$

This completes the proof of Theorem 3.3. □

Two elements a and b will be called *equivalent*, written $a \simeq b$, if $A_a = A_b$. Evidently, $\simeq$ is an equivalence relation. Thus, the set Q is partitioned into disjoint equivalence classes: $Q = K_a \cup K_b \cup \ldots$, where K_a consists of all the elements which are equivalent to the element a. If the entire set Q is itself an equivalence class, then $A_a = A_b$ for arbitrary a and b. Thus, A_a does not depend on a, and we can set $A_a = B$. Then, the equality (3.6) reduces to (3.2), i.e., Sushkevich's Postulate A holds in $Q(A)$. This case was already considered above.

Note that if $Q(A)$ has a left nucleus N_l, then N_l is an equivalence class.

Now let us formulate some statements about this equivalence in a quasigroup $Q(A)$. We combine them into the following theorem.

Theorem 3.4. *Let $Q(A)$ be a quasigroup. Suppose $a \simeq b$, in the sense that $A_a = A_b$. Then:*

1) *The relation $a \simeq b$ implies $A(a,x) \simeq A(b,x)$ for all $x \in Q$;*

2) *If $a \simeq b$, then $e_a = e_b$;*

3) *The classes K_a are equipollent. If Q is finite, then the size of each equivalence class is a divisor of the order of Q;*

4) *If λ is a left regular permutation of $Q(A)$, then $\lambda a \simeq a$ for all a.*

5) *If $a \simeq b$, then there is a left regular permutation λ of $Q(A)$ such that $\lambda a = b$.*

Proof. 1. Let $a \simeq b$, i.e., $A_a = A_b$. Then $A_{A(a,x)} = (A_a)_x = (A_b)_x = A_{A(b,x)}$, i.e., $A(a,x) \simeq A(b,x)$.

2. In general, the quasigroups $Q(A_a)$ and $Q(A_b)$ have respective left neutral elements e_a and e_b. If $A_a = A_b$, then the left neutral elements of the equal quasigroups $Q(A_a)$ and $Q(A_b)$ must coincide, i.e., $e_a = e_b$.

3. Let F and H be two equivalence classes. Suppose $a \in F$ and $b \in H$. Then there exists an element p such that $b = A(a,p)$. Let $F' = \{A(x,p) \mid x \simeq a\}$. Let us show that $F' \subseteq H$. Suppose $x \simeq a$, so $A(x,p) \in F'$. Then $A_{A(x,p)} = (A_x)_p = (A_a)_p = A_{A(a,p)} = A_b$, i.e., $A(x,p) \simeq b$, whence $A(x,p) \in H$. Therefore, F is equipollent to some part of H. Similarly, it is shown that H is equipollent to some part of F. Hence it follows that the sets F and H have the same cardinality. The second part of statement 3 is immediate.

4. From the definition of a left regular permutation λ we have

$$ L_{\lambda a} = \lambda L_a. $$

Now we use the equality (3.8):

$$ A_{\lambda a} = A^{(L_{\lambda a},1,L_{\lambda a})} = A^{(\lambda L_a,1,\lambda L_a)} = A^{(\lambda,1,\lambda)(L_a,1,L_a)}. $$

Since $\lambda \in \mathscr{L}$, we have $A^{(\lambda,1,\lambda)} = A$, so $A_{\lambda a} = A^{(L_a,1,L_a)} = A_a$, i. e., $\lambda a \simeq a$.

5. Suppose $a \simeq b$. We apply the relationship II(2.17) to $A_a = A^{(L_a,1,L_a)}$:

$$\gamma^{-1}\mathscr{L}\gamma \cap \mathfrak{N}_{\gamma^{-1}\alpha} \subseteq \mathscr{L}_A.$$

This relation was proved without the assumption that $(\cdot)$ is a loop, so we can apply it in our case:

$$L_a^{-1}\mathscr{L}_A L_a \cap \mathfrak{N}_{L_a^{-1}L_a} \subseteq \mathscr{L}_{A_a},$$

whence

$$L_a^{-1}\mathscr{L}_A L_a \subseteq \mathscr{L}_{A_a}$$

or

$$\mathscr{L}_A \subseteq L_a\mathscr{L}_{A_a}L_a^{-1}. \tag{3.10}$$

As there exists a left neutral element in $Q(A_a)$, an arbitrary left regular permutation of this quasigroup has the form $\lambda_a x = A_a(z_a, x)$, where z_a belongs to the left nucleus of the quasigroup $Q(A_a)$*. Thus, according to (3.10), each left regular permutation λ of the quasigroup $Q(A)$ has the form $\lambda = L_a\lambda_a L_a^{-1}$. Consequently,

$$\lambda x = L_a\lambda_a L_a^{-1}x = A[a, A_a(z_a, L_a^{-1}x)],$$

i.e.,

$$\lambda x = A[A(a, z_a), L_a^{-1}x].$$

The element $c = A(a, z_a)$ is equivalent to the element a, i.e., $c \simeq a$. Indeed, we have

$$A_c = A_{A(a,z_a)} = \big(A_a\big)_{z_a} = A_a,$$

since z_a is an element of the left nucleus of the quasigroup $Q(A_a)$. Therefore,

$$\lambda x = A(c, L_a^{-1}x)$$

or

$$\lambda = L_c L_a^{-1}.$$

Let us find a left regular permutation λ of the quasigroup $Q(A)$ such that $\lambda a = b$. We consider

$$\lambda a = L_b L_a^{-1}a = L_b e_a,$$

since $L_a e_a = A(a, e_a) = a$, i.e. $e_a = L_a^{-1}a$. But $b \simeq a$, i.e., $e_b = e_a$ by part 2), so indeed $\lambda a = L_b e_a = L_b e_b = b$. □

As a corollary, we have the following result: *An arbitrary left regular permutation of a quasigroup $Q(A)$ has the form $L_b L_a^{-1}$, where $b \simeq a$.*

*See Chapter II, 1°.

Remark 1. Consider a groupoid $Q(\cdot)$. An equivalence relation $\simeq$ on Q is a *congruence* on $Q(\cdot)$ if $a \simeq b$ implies $ac \simeq bc$ and $ca \simeq cb$ for arbitrary $c \in Q$.

By part 1) of the theorem, the relation $a \simeq b$ given by $A_a = A_b$ is a congruence if the additional condition $A(x,a) \simeq A(x,b)$ holds for all x in $Q(A)$. But as the following example shows, this condition is not necessarily satisfied in an arbitrary quasigroup. Let $Q(\cdot)$ be the symmetric group of degree three, say $Q = \{1, a, a^2, b, ab, a^2b\}$, $a^3 = 1$, $b^2 = 1$, $ba = a^2b$. Consider the quasigroup $Q(A)$, where $A(x,y) = bxby$. Then $a^2b \simeq a$, but $A(a, a^2b)$ and $A(a,a)$ are not equivalent.

If $Q(A)$ is commutative, then the equivalence relation defined by the equality $A_a = A_b$ is indeed a congruence, according to part 1) of the theorem.

Remark 2. The converse statement to part 2) of the theorem is not valid. Indeed, in a loop $Q(\cdot)$, the equality $e_a = e_b$ holds for all elements a and b, but $a \sim b$ does not follow if, for example, $N_l \neq Q$.

Remark 3. Parts 4) and 5) of the theorem assert that the equivalence $a \simeq b$ defined by the equality $A_a = A_b$ coincides with the equivalence $a \sim b$ ($\mathscr{L}$) that was defined in Chapter II, 1°. Each of the classes K_a is a relative left nucleus: $K_a = \mathscr{L}a$. Theorem 2.3 is a corollary of Theorem 3.4 — see part 3) of Theorem 3.4.

An analogous theorem holds if instead of the right derivative operations we consider the left derivative operations.

3°. Mixed derivatives

Let us establish a connection between the loops which are the principal isotopes of a quasigroup and the mixed derivatives of the quasigroup.

Lemma 1.1 asserts that an arbitrary loop B which is principally isotopic to a quasigroup A has the form $A_{a,b}$, where according to (1.16), $A_{a,b}$ denotes the isotope $A^{(R_a^{-1}, L_b^{-1}, 1)}$. If e is the neutral element of the loop $Q(B)$, then the equality $e = A(b,a)$ holds (see Chapter I, 3°).

The expression $A_{a,b}(x,y)$ can also be rewritten * as:

$$A_{a,b}(x,y) = A[{}^{-1}A(x,a), A^{-1}(b,y)]. \tag{3.11}$$

According to the definition of the translations L_b, R_a, it is easy to show that

$$R_a^{-1}x = {}^{-1}A(x,a), \quad L_b^{-1}y = A^{-1}(b,y).$$

Let us prove the following relationship for the loops $A_{a,b}$:

$$(A_{a,b})_{c,d} = A_{A^{-1}(b,c), {}^{-1}A(d,a)}.$$

*See the definition of left and right inverse operations ${}^{-1}A$ and A^{-1} in Chapter I, 1°.

According to the definition we have

$$(A_{a,b})_{c,d}(x,y) = A_{a,b}[{}^{-1}A_{a,b}(x,c)A^{-1}_{a,b}(d,y)].$$

Write $t = {}^{-1}A_{a,b}(x,c)$. Then we have

$$A_{a,b}(t,c) = x, A[{}^{-1}A(t,a), A^{-1}(b,c)] = x,$$

with

$${}^{-1}A(t,a) = {}^{-1}A[x, A^{-1}(b,c)].$$

If we denote $A^{-1}_{a,b}(d,y)$ by ω, then in analogous fashion we obtain

$$A^{-1}(b,\omega) = A^{-1}[{}^{-1}A(d,a), y].$$

Now it is easy to find $(A_{a,b})_{c,d}$:

$$(A_{a,b})_{c,d}(x,y) = A_{a,b}(t,\omega) = A[{}^{-1}A(t,a), A^{-1}(b,\omega)]$$

$$= A\left\{{}^{-1}A[x, A^{-1}(b,c)], A^{-1}[{}^{-1}A(d,a), y]\right\} = A_{A^{-1}(b,c),\,{}^{-1}A(d,a)}(x,y).$$

As we have seen before (see Theorem 3.3), a left derivative of a left derivative is also a left derivative, and a right derivative of a right derivative is also a right derivative. That is why further new quasigroups are only obtained by considering mixed derivatives. They can be of two types: a right derivative of a left derivative $({}_bA)_a$ and a left derivative of a right derivative ${}_b(A_a)$. For loops, these derivatives are isomorphic.

Theorem 3.5. *If A is a loop, then the mixed derivatives $({}_bA)_a$ and ${}_b(A_a)$ are isomorphic.*

Proof. 1. *The following relationships hold:*

$$A_a = A^{L_a}_{e,a}, \quad {}_aA = A^{R_a}_{a,e}, \tag{3.12}$$

where e is the neutral element of the loop A. Indeed,

$$A^{L_a}_{e,a} = (A^{(R_e^{-1},L_a^{-1},1)})^{L_a} = A^{(1,L_a^{-1},1)L_a} = A^{(L_a,1,L_a)} = A_a$$

in view of the equality (3.8). The second equality (3.12) is proved similarly.

2. *The mixed derivative $({}_bA)_a$ is isomorphic to the loop $A_{b,a}$.*

Let $A_a = B$. Since A is a loop, then B is also a loop, indeed with the same neutral element (this statement follows from $e_a = e$ and from part 1) of Theorem 3.3). Then

$$C = {}_b(A_a) = {}_bB = B^{R_b^{\cdot}}_{b,e},$$

where $R_b^{\cdot}x = A_a(x,b)$. Furthermore,

$$C = (A_a)^{R_b^{\cdot}}_{b,e} = (A^{L_a}_{e,a})^{R_b^{\cdot}}_{b,e}. \tag{3.13}$$

It is easy to see that for an arbitrary permutation θ of a set Q the equation

$$(A^\theta)_{u,v} = A^\theta_{\theta u,\theta v} \tag{3.14}$$

is true. Indeed, by virtue of equation (3.11), we find

$$(A^\theta)_{u,v}(x,y) = A^\theta[{}^{-1}(A^\theta)(x,u), (A^\theta)^{-1}(v,y)].$$

But $(A^\theta)^{-1} = (A^{-1})^\theta$ and ${}^{-1}(A^\theta) = ({}^{-1}A)^\theta$, so

$$\begin{aligned}(A^\theta)_{u,v}(x,y) &= A^\theta[({}^{-1}A)^\theta(x,u), (A^{-1})^\theta(v,y)]\\ &= \theta^{-1}A[\theta\theta^{-1}({}^{-1}A)(\theta x,\theta u), \theta\theta^{-1}(A^{-1})(\theta v,\theta y)]\\ &= \theta^{-1}A[{}^{-1}A(\theta x,\theta u), A^{-1}(\theta v,\theta y)] = \theta^{-1}A_{\theta u,\theta v}(\theta x,\theta y) = (A_{\theta u,\theta v})^\theta(x,y),\end{aligned}$$

which implies the equality (3.14) (denoting the operation $(A_{u,v})^\theta$ by $A^\theta_{u,v}$). We transform the equality (3.13) using the relationship (3.14):

$$C = (A_{e,a})^{L_aR_b^{\cdot}}_{L_ab,L_ae} = (A_{e,a})^{L_aR_b^{\cdot}}_{A(a,b),a} = A^{L_aR_b^{\cdot}}_{A^{-1}[a,A(a,b)],{}^{-1}A(a,e)}.$$

Therefore,

$$L_aR_b^{\cdot}x = L_aA_a(x,b) = A[a,A_a(x,b)] = A[A(a,x),b] = R_bL_ax$$

and

$$A^{-1}[a,A(a,b)] = b, {}^{-1}A(a,e) = a.$$

Thus

$${}_b(A_a) = A^{R_bL_a}_{b,a}. \tag{3.15}$$

Similarly, we prove that

$$({}_bA)_a = A^{L_aR_b}_{b,a}. \tag{3.16}$$

The validity of Theorem 3.5 follows from the equations (3.15) and (3.16). □

One can form derivatives of higher orders, for example, ${}_d\{[{}_b(A_a)]_c\}$, but being loops, they are all isotopic to the loop A. But an arbitrary loop B, isotopic to a quasigroup $Q(C)$, takes the form $C^\gamma_{u,v}$ with elements $u, v \in Q$ and γ a permutation of Q (compare Lemma 1.2). Thus, an arbitrary derivative of higher order has the form $A^\gamma_{u,v}$ and, consequently, it is isomorphic, for example, to the mixed derivative ${}_u(A_v)$.

In the process, we have proved the following assertion.

Theorem 3.6. *Suppose that a loop B is isotopic to a loop A. Then it is isomorphic to a mixed derivative of A.*

4°. Pseudo-automorphisms

Along with the left and right regular permutations that are closely related to the concept of derived operations, the other important autotopic* permutations are the pseudo-automorphisms of a quasigroup [31].

*See the definition of autotopic permutations in Chapter II, 3°.

Definition 1. A permutation φ of a set Q is called a *right pseudo-automorphism* of a quasigroup $Q(A)$ if there exists an element $c \in Q$ such that

$$A_c = A^{\varphi^{-1}}. \tag{3.17}$$

Here, the element c is called a *companion* of the right pseudo-automorphism φ.

A left pseudo-automorphism is defined similarly. If φ is simultaneously both a left and a right pseudo-automorphism, then it is called a *pseudo-automorphism.*

According to the definition (3.17) of the right pseudo-automorphism φ, the operations A and A_c are isomorphic. However, the right derivative A_c has a left neutral element, by part 1) of Theorem 3.3. Consequently, A also has a left neutral element. Thus, the existence of a right pseudo-automorphism of $Q(A)$ implies an existence of a left neutral element. Furthermore, the existence of a pseudo-automorphism of $Q(A)$ implies the existence of a neutral element, i. e., $Q(A)$ is a loop.

From the previous remarks, it follows that an automorphism of a quasigroup $Q(A)$ with a left neutral element is a special case of a right pseudo-automorphism. Indeed, in this instance we have $A_f = A = A^\theta$ for an arbitrary automorphism θ.

Using the definition of a right derivative of an operation, we can rewrite the definition of a right pseudo-automorphism as

$$A^{\varphi^{-1}} = A^{(L_c, 1, L_c)},$$

whence

$$A^{(L_c,1,L_c)\varphi} = A^{(L_c\varphi,\varphi,L_c\varphi)} = A, \tag{3.18}$$

i.e.,

$$A[A(c, \varphi x), \varphi y] = A[c, \varphi A(x, y)]. \tag{3.19}$$

If φ is a left pseudo-automorphism, i.e.,

$${}_cA = A^{\varphi^{-1}},$$

then we have

$$A[\varphi x, A(\varphi y, c)] = A[\varphi A(x, y), c]. \tag{3.20}$$

The previous equation is equivalent to the definition of a left pseudo-automorphism (see Bruck [31, p.113]).

Remark 1. Equation (3.18) shows that a right pseudo-automorphism φ is an autotopic permutation.

Remark 2. Equation (3.18) implies that if $(L_a\varphi, \varphi, L_a\varphi)$ is an autotopy of the quasigroup $Q(A)$, then φ is a right pseudo-automorphism of $Q(A)$ with companion a. Similarly, if $(\varphi, R_b\varphi, R_b\varphi)$ is an autotopy, then φ is a left pseudo-automorphism with companion b.

Lemma 3.1. *Let $Q(A)$ be a quasigroup with a left neutral element f. If φ is a right pseudo-automorphism with companion c, then*

$$\varphi^{-1}e_c = f,$$

where e_c is a right local neutral element for c.

Indeed,

$$A(\varphi^{-1}e_c, x) = \varphi^{-1}\varphi A(\varphi^{-1}e_c, \varphi^{-1}\varphi x) = \varphi^{-1}A^{\varphi^{-1}}(e_c, \varphi x)$$
$$= \varphi^{-1}A_c(e_c, \varphi x) = \varphi^{-1}(\varphi x) = x,$$

i.e.,

$$\varphi^{-1}e_c = f.$$

The hypothesis of the following theorem implies that the quasigroup $Q(A)$ has a left unit element, say f.

Theorem 3.7. *The right pseudo-automorphisms of a quasigroup $Q(A)$ form a group Π_A.*

Proof. Consider $\varphi, \psi \in \Pi_A$, with respective companions a and b. We will show that the product $\psi\varphi$ also lies in Π_A. Using the relationship (3.7), we have

$$A_{A(b,\psi a)} = (A_b)_{\psi a} = (A^{\psi-1})_{\psi a}. \tag{3.21}$$

Using the convention $A_a^\theta := (A_a)^\theta$, we have

$$(A^\theta)_a = A^\theta_{\theta a}, \tag{3.22}$$

where θ is an arbitrary permutation of the set Q. Then equation (3.21) implies

$$A_{A(b,\psi a)} = A^{\psi^{-1}}_{\psi^{-1}(\psi a)} = A^{\psi^{-1}}_a = (A_a)^{\psi^{-1}} = (A^{\varphi^{-1}})^{\psi^{-1}} = A^{(\varphi\psi)^{-1}}, \tag{3.23}$$

so that $\psi\varphi \in \Pi_A$.

Let us consider the equation $A(a, x) = f$ with the left unit element f of $Q(A)$. Using the equations (3.7) and (3.22) again, we obtain

$$A = A_f = A_{A(a,x)} = (A_a)_x = (A^{\varphi^{-1}})_x = A^{\varphi^{-1}}_{\varphi^{-1}x},$$

whence

$$A_{\varphi^{-1}x} = A^\varphi = A^{(\varphi^{-1})^{-1}},$$

i.e., $\varphi^{-1} \in \Pi_A$. Thus, Π_A is a group. □

As we noted before, the group Γ_A of automorphisms of a loop $Q(A)$ (a quasigroup having a left and right neutral element) is a subgroup of the group Π_A.

The definition of a right pseudo-automorphism implies that several companions may correspond to one right pseudo-automorphism. In fact, if a right pseudo-automorphism φ has an element c as its companion, i.e., $A^{\varphi^{-1}} = A_c$, then $A^{\varphi^{-1}} = A_{\lambda c}$, where λ is an arbitrary left regular permutation of the quasigroup $Q(A)$. Indeed, by part 4) of Theorem

3.4 and the following Remark 3, we have $\lambda c \sim c$ $(\mathscr{L})$, i.e., $A_{\lambda c} = A_c = A^{\varphi^{-1}}$. Thus, the set of companions c of a right pseudo-automorphism is a left nucleus (relative to c) of a quasigroup $Q(A)$.

On the other hand, one companion may accompany several right pseudo-automorphisms. Indeed, let φ be a right pseudo-automorphism of a quasigroup $Q(A)$ (with a left neutral element f), and let θ be an automorphism of the quasigroup. As we have seen above, θ is also a right pseudo-automorphism with a companion f. Thus, according to Theorem 3.7, $\varphi\theta$ is also a pseudo-automorphism. Then

$$A^{(\varphi\theta)^{-1}} = A^{\theta^{-1}\varphi^{-1}} = (A^{\theta^{-1}})^{\varphi^{-1}} = (A_f)^{\varphi^{-1}} = A^{\varphi^{-1}} = A_c,$$

i.e., $\varphi\theta$ also has the element c as its companion.

Summarizing, we have the following assertion: There exists a correspondence between the set of left cosets of the subgroup Γ_A of the group Π_A and a set of left nuclei of $Q(A)$.

If Q is finite, we can conclude: the index of the subgroup Γ_A in Π_A is not greater than the index of the group $\mathscr{L}$ of left regular permutations of a quasigroup $Q(A)$*.

It is interesting to consider when the correspondence mentioned above extends to all the left nuclei of the quasigroup $Q(A)$. In other words, when an arbitrary element of Q is a companion of a pseudo-automorphism. It can be true, for example, in a group $Q(\cdot)$, since then $(\cdot)_x = (\cdot)^\varphi$ for $x \in Q$ and $\varphi \in \Gamma_{(\cdot)}$. We are led to the following definition.

Definition 2. A quasigroup $Q(A)$ is called a *right G-quasigroup* if each element is a companion of a right pseudo-automorphism, or if. equivalently, all the right derivatives A_x are isomorphic to A. A left G-quasigroup is defined similarly.

Finally, we have the following.

Definition 3. A quasigroup $Q(A)$ which is simultaneously both a right and a left G-quasigroup, thus if all right and left derivatives of the operation A are isomorphic to A, is called *a G-quasigroup*.

The respective definitions of a right or left G-quasigroup $Q(A)$ imply that it always has a left or right neutral element. Consequently, a G-quasigroup always has a neutral element, and is therefore a loop. Thus, henceforth we speak of *G-loops*.

The following theorem gives one important characterization of G-loops.

Theorem 3.8. *A loop is a G-loop if and only if each loop isotopic to it is actually isomorphic to it.*

Indeed, suppose a loop $Q(B)$ is isotopic to a G-loop $Q(A)$. Then, by virtue of Theorem 3.6, the loop $Q(B)$ is isomorphic to a mixed derivative of $Q(A)$, say

$$B = [_b(A_a)]^\varphi.$$

*Here, the index of the group $\mathscr{L}$ of left regular permutations of a quasigroup $Q(A)$ is understood as the quotient $|Q|/|\mathscr{L}|$.

Thus $A_a = A^\alpha$ with $\alpha = (L_a, 1, L_a)$ according to equation (3.8), so

$$B = [{}_b(A^\alpha)]^\varphi = [({}_{ab}A)^\alpha]^\varphi = {}_{ab}A^{\alpha\varphi}.$$

Here we use the equality

$${}_b(A^\alpha) = ({}_{\alpha b}A)^\alpha,$$

which is similar to the equality (3.22) and as easily proved. But ${}_{\alpha b}A$ is also isomorphic to A: ${}_{\alpha b}A = A^\gamma$, therefore

$$B = (A^\gamma)^{\alpha\varphi} = A^{\gamma\alpha\varphi},$$

i.e., B is isomorphic to A.

Conversely, suppose that each loop isotopic to a loop A is isomorphic to it. In particular, A_a and ${}_bA$ are also loops (with the same neutral element) which are isotopic to the loop A (see (3.8) and (3.9)): $A_a = A^{(L_a,1,L_a)}$ and ${}_bA = A^{(1,R_b,R_b)}$. Therefore, A is a G-loop.

We return to G-loops in Chapter X.

5°. F-quasigroups

The notion of an F-quasigroup was introduced in §1°. Now we refine the concept.

Definition 4. A quasigroup $Q(A)$ is called a *left F-quasigroup* if for all $x, y, z \in Q$, the equality

$$A[A(x, y), z] = A[x, A(y, S_x z)], \tag{3.24}$$

holds, where S_x is an arbitrary permutation of a set Q depending on x.

A *right F-quasigroup* is defined similarly.

Example. *A medial quasigroup $Q(A)$ is a left F-quasigroup.*

Indeed, according to Toyoda's Theorem, $Q(A)$ is isotopic to an abelian group $Q(+)$, where the isotopy has the form (2.30):

$$A(x, y) = \varphi x + \psi y + c.$$

It is easy to verify that $Q(A)$ is a left F-quasigroup, with

$$S_x y = \psi^{-2}(\varphi^2 - \varphi)x + \psi^{-1}y + \psi^{-2}(\varphi - \psi)c.$$

Subsequently, we will only consider left F-quasigroups, so we omit the word "left". In this section, we consider some simple properties of F-quasigroups which we will need later. We return to the study of F-quasigroups in Chapter IV.

Suppose that $Q(A)$ is an F-quasigroup.

Lemma 3.2. *For arbitrary $x, y \in Q$, the following relationship holds:*

$$A_{A(x,y)} = A_y^{S_x}. \tag{3.25}$$

Proof. According to the definition of derivative operations, we have

$$A_x[A_x(y,z),t] = A_x[y,(A_x)_y(z,t)],$$

or, in virtue of the equality (3.7),

$$A_x[A_x(y,z),t] = A_x[y,A_{A(x,y)}(z,t)]. \tag{3.26}$$

From the basic equality (3.24) for F-quasigroups, and the definition of a right derivative operation, we obtain the relationship

$$A_x(y,z) = A(y,S_xz). \tag{3.27}$$

Thus, from (3.26) we find

$$A[A(y,S_xz),S_xt] = A[y,S_xA_{A(x,y)}(z,t)],$$

$$A[y,A_y(S_xz,S_xt)] = A[y,S_xA_{A(x,y)}(z,t)], \text{ and}$$

$$S_x^{-1}A_y(S_xz,S_xt) = A_{A(x,y)}(z,t),$$

i.e.,

$$A_{A(x,y)} = A_y^{S_x}.$$

Lemma 3.3. *A right derivative of an F-operation is also an F-operation.*

Proof. Consider the equation

$$(A_x)_y(p,q) = A_x(p,t). \tag{3.28}$$

According to the equality (3.27), it is enough to show that the element t does not depend only on p. Using (3.27), turn the equation (3.28) into:

$$A_{A(x,y)}(p,q) = A(p,S_xt) \text{ or } A(p,S_{A(x,y)}q) = A(p,S_xt).$$

Then

$$S_{A(x,y)}q = S_xt, \text{ or } t = S_x^{-1}S_{A(x,y)}q.$$

Remark. A_x is an F-operation with a left neutral element. It is easy to show that if the F-quasigroup $Q(A)$ has a two-sided neutral element e, i.e., $Q(A)$ is an F-loop, then it is a group.

In fact, substituting $y = e$ into (3.3), we get

$$A[A(x, e), z] = A[x, A(e, S_x z)],$$

or

$$A(x, z) = A(x, S_x z),$$

whence

$$S_x z = z,$$

i.e., $S_x = 1$. Consequently, the equality (3.24) becomes the associative law

$$A[A(x, y), z] = A[x, A(y, z)],$$

whence it follows that $Q(A)$ is a group.

Theorem 3.9. *Every F-quasigroup with a left neutral element f is also a right G-quasigroup.*

Proof. Consider the permutation R defined by the equality

$$Rx = A(x, f).$$

Then it follows from (3.23) that

$$A_{Rx} = A_{A(x,f)} = A_f^{S_x} = A^{S_x}, \tag{3.29}$$

whence

$$A_x = A^{S_{R^{-1}x}}.$$

This equality shows that $Q(A)$ is a G-quasigroup. □

Corollary. *Every F-quasigroup is isotopic to a right G-quasigroup.*

We now consider some properties of the permutations S_x. We have seen that for arbitrary x and y,

$$A_{A(x,y)} = A_y^{S_x},$$

or, more explicitly,

$$A_{A(x,y)}(p, q) = S_x^{-1} A_y(S_x p, S_x q), \tag{3.30}$$

where x, y, p, q are arbitrary elements of Q.

Transforming equation (3.30) using (3.27),

$$A(p, S_{A(x,y)} q) = S_x^{-1} A(S_x p, S_y S_x q),$$

or

$$A(S_x p, S_y S_x S_{A(x,y)}^{-1} q) = S_x A(p, q).$$

Thus, $T_1 = (S_x, S_y S_x S_{A(x,y)}^{-1}, S_x)$ is an autotopy of an F-operation for arbitrary $x, y \in Q$. In particular, for $y = e_x$ it follows that $T_2 = (S_x, S_{e_x}, S_x)$ is also an autotopy of the operation A. Consequently, $T_2 T_1^{-1}$ (see Chapter II, 3°) is also an autotopy of the quasigroup $Q(A)$. We find

$$T_2 T_1^{-1} = (S_x, S_{e_x}, S_x)(S_x, S_y S_x S_{A(x,y)}^{-1}, S_x)^{-1}$$
$$= (1, S_{e_x} S_{A(x,y)} S_x^{-1} S_y^{-1}, 1).$$

By virtue of the remark made in Chapter II, 3°, we conclude that $S_{e_x} S_{A(x,y)} S_x^{-1} S_y^{-1} = 1$, whence

$$S_{A(x,y)} = S_{e_x}^{-1} S_y S_x. \tag{3.31}$$

An explicit form for a permutation S_x may be given. For this, we put $y = e_x$ in (3.24):

$$A(x, z) = A[A(x, e_x), z] = A[x, A(e_x, S_x z)],$$

so

$$z = A(e_x, S_x z),$$

and

$$S_x z = A^{-1}(e_x, z). \tag{3.32}$$

Lemma 3.4. *In an F-quasigroup $Q(A)$, the following relationships are equivalent:*

$$x \sim y \quad (\mathscr{L}); \tag{3.33}$$

$$e_x = e_y; \tag{3.34}$$

$$S_x = S_y. \tag{3.35}$$

Proof. The equvalence of the first two relationships follows generally from Theorem 3.4 and the following Remark 3. Further, the equality (3.32) implies that the relationship (3.35) follows from (3.34). Finally, we show that relation (3.35) implies (3.33). Indeed, we have

$$A_x(p, q) = A(p, S_x q) = A(p, S_y q) = A_y(p, q),$$

i.e., $x \sim y$ $(\mathscr{L})$. □

Corollaries. Consider a finite F-quasigroup $Q(A)$.

1. The number of right neutral elements is a divisor of the order of Q.

2. The number of distinct permutations S_x corresponding to elements from Q is also a divisor of an order Q.

Lemma 3.5. *If $Q(A)$ is an F-quasigroup with a left neutral element f, and if $S_x = \theta S_y$, where θ is an automorphism of $Q(A)$, then $\theta = 1$ and $x \sim y$ $(\mathscr{L})$.*

Proof. Set $x_0 = Rx$ and $y_0 = Ry$, where $Rx = A(x, f)$. Then by virtue of equation (3.29), we have

$$A_{x_0} = A_{Rx} = A^{S_x} \text{ and } A_{y_0} = A_{Ry} = A^{S_y}.$$

Let $S_x = \theta S_y$, where θ is an automorphism of the quasigroup $Q(A)$, i. e., $A^\theta = A$. Then

$$A_{x_0} = A^{S_x} = A^{\theta S_y} = (A^\theta)^{S_y} = A^{S_y} = A_{y_0},$$

whence $x_0 \sim y_0$ $(\mathscr{L})$ or $A(x, f) \sim A(y, f)$. By part 5 of Theorem 3.4, there exists a left regular permutation λ such that

$$A(y, f) = \lambda A(x, f),$$

whence $A(y, f) = A(\lambda x, f)$. Consequently, $y = \lambda x$ and $y \sim x$ $(\mathscr{L})$. □

Notes

[1](Left) F-quasigroups were first considered by Murdoch in [51], where the identity (3.3) is called "the law of associativity A_1". In this work a theory of normal subquasigroups of F-quasigroups was developed.

[2]The concept of derivative operations was introduced in [12, 14]. Here, one may find other results related to derivative operations.

Chapter IV. Homomorphism. Normal subquasigroups

1°. Homomorphic mappings of quasigroups

Previously we considered quasigroups on the same fixed set Q. Of course, we can also consider quasigroups on different sets. Let two quasigroups $Q(\cdot)$ and $Q'(\circ)$ be given. A function $\varphi\colon Q \to Q'$ is a *homomorphic mapping* or *homomorphism* from the quasigroup $Q(\cdot)$ to the quasigroup $Q'(\circ)$ if the equation

$$\varphi(xy) = \varphi x \circ \varphi y$$

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

The set $\varphi Q = \{\varphi x \mid x \in Q\}$ is called the (*homomorphic*) *image* of the quasigroup $Q(\cdot)$ under φ. If the homomorphic image of the quasigroup $Q(\cdot)$ coincides with Q', then φ is a homomorphism from the quasigroup $Q(\cdot)$ *onto* the quasigroup $Q'(\circ)$.

If $Q'(\circ)$ is not itself a quasigroup (in the sense of Chapter I, Definition 2), but only a groupoid, then the homomorphic image of $Q(\cdot)$ need not be a quasigroup.[1] Nevertheless, in this case, the homomorphic image $\varphi Q(\circ)$ of the quasigroup $Q(\circ)$ has the following property: for every $a', b' \in \varphi Q$ there exist x' and y' such that $a \circ' x' = b'$ and $y' \circ a' = b'$, i.e., the solvability of the equations holds, but the uniqueness does not.

A groupoid $Q(*)$ in which solutions of the equations $a * x = b$, $y * a = b$ exist, but are not necessarily unique, may be called a *groupoid with division*. However, we are interested in the case where $\varphi Q(\circ)$ is a quasigroup, i.e., we restrict to considering homomorphisms φ from a quasigroup $Q(\cdot)$ to a quasigroup $Q'(\circ)$.

It is easy to prove the following properties of a homomorphic mapping from a quasigroup $Q(\cdot)$ onto a quasigroup $Q'(\circ)$:

1) If $Q(\cdot)$ is a loop with a neutral element e, then $Q'(\circ)$ is a loop with a neutral element $e' = \varphi e$;

2) Even if $Q'(\circ)$ is a loop, then $Q(\cdot)$ need not be a loop, as the following example shows:

$\cdot$	1	2	3	4
1	2	1	3	4
2	1	2	4	3
3	4	3	1	2
4	3	4	2	1

$\circ$	$1'$	$2'$
$1'$	$1'$	$2'$
$2'$	$2'$	$1'$

Here $Q = \{1, 2, 3, 4\}$, $Q(\cdot)$ is a quasigroup, $Q' = \{1', 2'\}$, $Q'(\circ)$ is a loop, and even a group. It is easy to see that the mapping $\varphi 1 = \varphi 2 = 1'$, $\varphi 3 = \varphi 4 = 2'$ is a homomorphism from the quasigroup $Q(\cdot)$ to the loop $Q'(\circ)$.

The concept of congruence defined on a groupoid in Chapter III (Remark 1 to Theorem 3.4) is closely connected with the concept of homomorphism. To clarify this connection, let us consider a homomorphism $Q(\cdot) \to Q'(\circ)$, where $Q'(\circ)$ is a groupoid, but not necessarily a quasigroup. Then we can define a congruence θ on the groupoid $Q(\cdot)$, setting $a\theta b$ if and only if $\varphi a = \varphi b$. Obviously, this relation is an equivalence. Furthermore, we have

$$\varphi(ac) = \varphi a \circ \varphi c, \quad \varphi(bc) = \varphi b \circ \varphi c.$$

If $a\theta b$, then $\varphi a = \varphi b$. Consequently,

$$\varphi(ac) = \varphi a \circ \varphi c = \varphi b \circ \varphi c = \varphi(bc),$$

i.e. $ac\theta bc$. Similarly, we obtain $ca\theta cb$.

Now suppose that φ is a homomorphism from a quasigroup $Q(\cdot)$ to a quasigroup $Q'(\circ)$. Then the following properties for the congruence θ hold:

RI) $ac\theta bc$ implies $a\theta b$ [*Invariance under right multiplication*];

LI) $ca\theta cb$ implies $a\theta b$ [*Invariance under left multiplication*].

Indeed, suppose $ac\theta bc$. Then $\varphi(ac) = \varphi(bc)$, whence $\varphi a \circ \varphi c = \varphi b \circ \varphi c$. But $Q'(\circ)$ is a quasigroup, so $\varphi a = \varphi b$ or $a\theta b$. We can prove 2) similarly. If the first and the second conditions for a (groupoid) congruence θ on $Q(\circ)$ hold, it is called a *normal congruence*. Thus, *to every homomorphism from a quasigroup $Q(\cdot)$ to some quasigroup, there corresponds a normal congruence on $Q(\cdot)$.*

In a group, every congruence is normal. Indeed, let θ be a congruence on a group $Q(\cdot)$. If $ac\theta ad$, then $a^{-1}(ac)\theta a^{-1}(ad)$ or $c\theta d$. In the same way, $ca\theta da$ implies $c\theta d$, so θ is a normal congruence.

For a second example, consider a *totally symmetric* (TS)-quasigroup $Q(\cdot)$ [24], where an equality $ab = c$ implies the equalities $xy = z$, where x, y, z is an arbitrary permutation of the elements a, b, c. In other words, $ab = c$ implies $ba = c$, $bc = a$ etc. It is easy to see that $Q(\cdot)$ is a TS-quasigroup if it satisfies the identities

$$ab = ba, \quad a(ab) = b \tag{4.1}$$

(see chapter VII). As in the group case, use of the second equality in (4.1) yields that any congruence is normal.

The concepts of homomorphism and congruence apply to any algebra $Q(\Omega)$ [47]. Here we recall these definitions, assuming that all the operations from Ω are binary, as agreed above.

1. An algebra $Q(\Omega)$ is mapped homomorphically on an algebra $Q'(\Omega')$ if between the operations of the sets Ω and Ω' there exists a 1-1 correspondence* $A \leftrightarrow A'$ (with $A \in \Omega$ and $A' \in \Omega'$) and a function $\varphi\colon Q \to Q'$ such that

$$\varphi A(x, y) = A'(\varphi x, \varphi y)$$

*In this case the algebras $Q(\Omega)$ and $Q'(\Omega')$ are said to have the *same type*.

for all $A \in \Omega$ and $x, y \in Q$.

2. An equivalence relation θ on the set Q is called a(n *algebra*) *congruence* on the algebra $Q(\Omega)$ if $a\theta b$ implies $A(a,c)\theta A(b,c)$ and $A(c,a)\theta A(c,b)$ for $A \in \Omega$ and $c \in Q$.

In Chapter I, Definition 2, we construed a quasigroup $Q(A)$ as an algebra $Q(A, A^{-1}, {}^{-1}A)$, where $A, A^{-1}, {}^{-1}A$ satisfy the identities $(1.3)^{**}$. Consider a homomorphism from the algebra $Q(A, A^{-1}, {}^{-1}A)$ to an algebra $Q'(A', B', C')$ of the same type. It is easy to see that the identities (1.3) also hold in a homomorphic image of the algebra $\varphi Q(A, B, C)$. Consequently, $\varphi Q(A)$ is a quasigroup.

Let us show that *any (groupoid) congruence θ on a (primitive) quasigroup $Q(A, A^{-1}, {}^{-1}A)$ is a normal (or algebra) congruence on $Q(A)$, and conversely.*

Indeed, let θ be a groupoid congruence on a primitive quasigroup $Q(A, A^{-1}, {}^{-1}A)$, where the identities (1.3) hold, and let the relation $A(a,c)\theta A(b,c)$ hold in $Q(A)$. Then ${}^{-1}A[A(a,c),c]\ \theta\ {}^{-1}A[A(b,c),c]$, as θ is an algebra congruence on $Q(A, A^{-1}, {}^{-1}A)$. Consequently, in view of (1.4) $a\theta b$. Similarly, one can deduce $a\theta b$ from $A(c,a)\theta A(c,b)$.

Conversely, let θ be a normal congruence in $Q(A)$ and let $a\theta b$. Let us show that $A^{-1}(c,a)\theta A^{-1}(c,b)$. According to the identities (1.4) we have $a = A[c, A^{-1}(c,a)]$ and $b = A[c, A^{-1}(c,b)]$. Consequently, $A[c, A^{-1}(c,a)]\ \theta\ A[c, A^{-1}(c,b)]$, whence in view of the normality of θ we have $A^{-1}(c,a)\ \theta\ A^{-1}(c,b)$. Similarly, the remaining requisites for the normality of the congruence θ in $Q(A, A^{-1}, {}^{-1}A)$ are shown.

At the beginning of the current section we showed that to each homomorphic mapping φ from a quasigroup $Q(\cdot)$ to a quasigroup $Q'(\circ)$, there corresponds a normal congruence. Now we prove the converse statement: *Each normal congruence θ on a quasigroup $Q(\cdot)$ determines a homomorphism φ from the quasigroup $Q(\cdot)$ to some quasigroup.*

Let θ be a normal congruence on a quasigroup $Q(\cdot)$. For an element a of Q, set $K_a = \{b \in Q \mid a\theta b\}$, the *congruence class* of a. An arbitrary element of K_a will be called a *representative* of the class K_a. It is easy to verify the validity of the following propositions which come from the definition of a congruence:

1) *If $b \in K_a$, then $K_a = K_b$, and conversely*;

2) *Two congruence classes K_a and K_b either coincide, or do not have any element in common.* Furthermore, note the following property:

3) *aK_b[*], where K_b is a congruence class, is also a congruence class, namely $aK_b = K_{ab}$.*

Indeed, if $x \in aK_b$, then $x = ab_1$, where $b_1 \in K_b$. Consequently $b_1\theta b$. Therefore, $x\theta ab$, whence $x \in aK_b$. Thus $aK_b \subseteq K_{ab}$.

Conversely, if $y \in K_{ab}$, then $y\theta ab$. Let $y = az$. Then $az\theta ab$, whence $z\theta b$ and $y = az \in aK_b$. Therefore $K_{ab} \subseteq aK_b$. Thus, $K_{ab} = aK_b$. Similarly it is proved that $K_b a = K_{ba}$ for arbitrary $a,\ b \in Q$.

On the set $\overline{Q}$ of all the classes of the congruence K_a, we introduce the following operation:

$$K_a \circ K_b = K_{ab}.$$

Let us show that the operation does not depend on the representatives of the classes K_a

[**] Such an algebra is sometimes called a *primitive quasigroup* (see Note 2 to Chapter I).

[*] aM consists of all the elements ax, where $x \in M \subseteq Q$.

and K_b, i.e., if $K_a = K_c$ and $K_b = K_d$, then $K_{ab} = K_{cd}$. Indeed, if $K_a = K_c$, then $c \in K_a$ and $c\theta a$; in the same way we get $d\theta\bar{b}$. From here, we conclude that $cd\theta a\bar{b}$ or $K_{cd} = K_{ab}$.

We now show that $\overline{Q}(\circ)$ is a quasigroup. We consider the equation $\bar{a} \circ \bar{x} = \bar{b}$, where $\bar{a} = K_a$, $\bar{b} = K_b$. In the quasigroup $Q(\cdot)$ the equation $ax = \bar{b}$ has a solution, say x_0. Consequently $ax_0 = \bar{b}$, whence $\bar{a} \circ \bar{x}_0 = K_a \circ K_{x_0} = K_{ax_0} = K_b = \bar{b}$. Assume that there exists another solution $\bar{b}_0$ for the equation $\bar{a} \circ \bar{x} = \bar{b}$. Then $\bar{a}_0 \circ \bar{y}_0 = \bar{b}$ should hold, i.e., $K_{ay_0} = K_b$. In view of the invariance of the congruence under right multiplication, we conclude that $b \in K_{ay_0}$, i.e., $\bar{b}\theta ay_0$. But $\bar{b} = ax_0$, whence $ax_0\theta ay0$. Consequently $x_0\theta y0$ and $x_0 = y_0$. Thus, in $\overline{Q}(\circ)$ the equation $ax = \bar{b}$ is solvable (indeed, uniquely) for all $\bar{a}, \bar{b} \in \bar{Q}$. In the same way it is proved that the equation $\bar{y} \circ \bar{a} = \bar{b}$ has a unique solution.

Now, it is easy to confirm that the correspondence $\varphi\colon a \to \bar{a}$ is a homomorphism from $Q(\cdot)$ to $\overline{Q}(\circ)$:

$$\varphi(a\bar{b}) = \varphi\, a \circ \varphi\bar{b}.$$

Indeed,

$$\alpha(ab) = a\bar{b} = K_{ab} = K_a \circ K_b = \bar{a} \circ \bar{b} = \varphi\, a \circ \varphi b.$$

Such homomorphisms are called *natural* [47].

The quasigroup $Q(\circ)$ is described as the *quotient*[*] of the quasigroup $Q(\cdot)$ by the congruence θ, and is denoted by $Q/\theta(\circ)$, i.e., $\overline{Q} = Q/\theta$, and in $\overline{Q}$ the operation $(\circ)$ is defined. We summarize as follows, with the so-called Homomorphism Theorem.

Theorem 4.1. *If φ is a homomorphism from a quasigroup $Q(\cdot)$ onto a quasigroup $Q'(\cdot)$, then there exists a normal congruence θ on $Q(\cdot)$ such that $Q'(\cdot) \cong (Q/\theta)(\circ)$. Conversely, if θ is a normal congruence on $Q(\cdot)$, then there is a homomorphism $\varphi\colon Q(\cdot) \to (Q/\theta)(\circ)$ sending an element of Q to its congruence class.*

2°. Normal subquasigroups

Consider a normal congruence θ on a quasigroup $Q(\cdot)$. If $Q(\cdot)$ is a group, then the set of elements congruent to the neutral element is a normal subgroup of the group $Q(\cdot)$. In a quasigroup, an analogue of the concept of a normal subgroup is a normal subquasigroup.

Definition 1. A subquasigroup $H(\cdot)$ of a quasigroup $Q(\cdot)$ is *normal* if it is one of the congruence classes of a normal congruence θ on $Q(\cdot)$ In other words, H must have the form $H = K_h$, where h is an element of H.

Lemma 4.1. *A necessary and a sufficient condition for the congruence class K_h of a congruence θ to be a subquasigroup is that $h^2\theta h$.*

First, suppose $H = Kh$ is a subquasigroup, so $a, b \in H$ implies $ab \in H$. Then since $a\theta h$ and $b\theta h$, we have $ab\theta hh$. But $ab\theta hh = h^2$, so $h^2\theta h$.

[*] Translators' note: In the original, a *factor*.

Conversely, suppose $h^2\theta h$. Let us show that $H = K_h$ is a subquasigroup. Closure in $H(\cdot)$ is immediate. Now consider the equation $ax = b$, where $a, b \in H$. We have $b = ax\theta hx$, but $b\theta h\theta h^2$, whence $h^2\theta hx$. In view of the normality of θ, we conclude that $x\theta h$, i.e., $x \in H$. Similarly, the solution y of the equation $ya = b$ belongs to H.

Corollary 1. *Consider a congruence class K_h of θ. Let e_h and f_h be the respective right and left local neutral elements of h. Then K_h is a normal subquasigroup if and only if $h\theta e_h$ and $h\theta f_h$.*

Indeed, $h\theta e_h$ is equivalent to $h^2\theta he_h = h$.

Corollary 2. *If K_h contains an idempotent[*] element, then K_h is a subquasigroup.*

If $a^2 = a$ and $a \in K_h$, then $K_h = K_a$. and we may apply Lemma 4.1.

Corollary 3. *If K_h is a normal subquasigroup, then for arbitrary $a \in K_h$ we have $a^2\theta a$.*

Corollary 4. *If $Q(\cdot)$ is a loop, then the congruence class K_e, where e is the neutral element of the loop, is a normal subloop.*

If H is a subquasigroup, the set aH is called a *left coset* of H. In view of Property 3) of normal congruences, we have $aH = K_{ah}$, where h is an element of H. In view of Property 2) of normal congruences, two left cosets by a subquasigroup H either coincide or have no common elements. One can also define right cosets Ha, but it is easy to show that every right coset is a left coset, and conversely. Indeed, let h be a fixed element from H. The equality $ah = ha'$ defines a one-to-one correspondence $a \leftrightarrow a'$ for all $a \in Q$. Then $aH = Ha'$. Indeed,

$$aH = aK_h = K_{ah} = K_{ha'} = K_h a' = Ha'.$$

Two normal subquasigroups are called *adjacent* if they are classes of the same normal congruence. There exist quasigroups in which all the congruence classes are normal subquasigroups (e.g., distributive quasigroups — see Chapter VIII). In loops there are no adjacent normal subquasigroups: if the class K_h is a subquasigroup, then $h\theta e$. In fact, if K_h is a subquasigroup, then, by the proof of Lemma 4.1, $h^2\theta h$ or $h^2\theta he$. In view of the normality of θ, we obtain $h\theta e$. Thus, $K_h = K_e$.

Remark. Let $Q(\cdot)$ be a loop, and let $H(\cdot)$ be a normal subloop of $Q(\cdot)$, defined by the congruence θ. As we have just seen, $H(\cdot)$ is the unique normal subloop defined by the congruence θ. In this case, the quotient Q/θ is usually written Q/H, and H is called the *kernel* of the natural homomorphism $Q \to Q/H$.

Let θ be a binary relation on a set Q. A permutation σ of Q is said to be *admissible* with respect to θ if the relation $a\theta b$ between elements a, b of Q holds if and only if $\sigma a\theta\sigma b$.

[*] An element a of a quasigroup $Q(\cdot)$ is *idempotent* if $a^2 = a$.

The set P_θ of all permutations of Q admissible with respect to a relation θ on Q forms a group.

Certainly, the unit permutation 1 of Q is admissible, so P_θ is nonempty.

Let $\alpha, \beta \in P_\theta$ and $a, b \in Q$. Then $a\theta b \Leftrightarrow \beta a \theta \beta b \Leftrightarrow \alpha\beta a \theta \alpha\beta b$, so $\alpha\beta \in P_\theta$.

Finally, $\alpha^{-1} a \theta \alpha^{-1} b \Leftrightarrow a = \alpha(\alpha^{-1}a)\theta\alpha(\alpha^{-1}b) = b$, so $\alpha^{-1} \in P_\theta$.

Let G be the group associated with a quasigroup structure $Q(\cdot)$ on Q. Then:

Each permutation in G is admissible with respect to each normal congruence on $Q(\cdot)$.

This follows from the observation that, if $\sigma = L_a$ or $\sigma = R_a$, then the admissibility of σ follows from the congruence property of θ.

Thus, the *normality of a congruence θ is equivalent to the relationship $G \subseteq P_\theta$.*

If θ is a normal congruence on $Q(\cdot)$, then an isotopy $T = (\alpha, \beta, \gamma)$ of $Q(\cdot)$ is said to be *admissible* with respect to θ if each of the permutations α, β, γ is admissible with respect to θ.

Lemma 4.2. *Let θ be a normal congruence on a quasigroup $Q(\cdot)$. If $Q(\circ)$ is isotopic to $Q(\cdot)$, and the isotopy is admissible with respect to θ, then θ is also a normal congruence on $Q(\circ)$.*

Let the isotopy be $T = (\alpha, \beta, \gamma)$. If $a\theta b$, then $\beta a \theta \beta b$ by the admissibility of β. Further, $\alpha c \cdot \beta a \theta \alpha c \cdot \beta b$ by the admissibility of α, and $\gamma^{-1}(\alpha c \cdot \beta a)\theta\gamma^{-1}(\alpha c \cdot \beta b)$ by the admissibility of γ. Thus $c \circ a = \gamma^{-1}(\alpha c \cdot \beta a)\theta\gamma^{-1}(\alpha c \cdot \beta b) = c \circ b$. In similar fashion, the remaining requirements from the definition of a normal congruence are verified.

Remark. Obviously, the lemma applies equally to groupoid congruences.

Corollary 1. *If one of the normal congruence classes H is a subquasigroup (and, consequently, a normal quasigroup) of $Q(\cdot)$, and if H is invariant under the admissible permutations α, β, γ, then H is also a normal subquasigroup of $Q(\circ)$.*

Corollary 2. *Let a and b be elements of a normal subquasigroup H of $Q(A)$. Then H is a normal subloop of $Q(A_{a,b})$.*

Indeed, by the definition, we have

$$A_{a,b} = A^{(R_a^{-1}, L_b^{-1}, 1)},$$

where the isotopy $T = (R_a^{-1}, L_b^{-1}, 1)$ is admissible with respect to any arbitrary congruence θ on $Q(A)$. By Lemma 4.2, θ is also a congruence on $Q(A_{a,b})$. But $Q(A_{a,b})$ is a loop with neutral element $e = A(b, a) \in H$, so by Corollary 4 of Lemma 4.1, H is a normal subloop of $Q(A_{a,b})$.

Theorem 4.2. *Let h be an element of a normal subquasigroup H of a quasigroup $Q(A)$. Then H is a normal subquasigroup of the right derivative quasigroup $Q(A_h)$.*

We have $A_h = A^{(L_h,1,L_h)}$, where the isotopy $L_h, 1, L_h$ is admissible with respect to an arbitrary normal congruence θ of $Q(A)$. By Lemma 4.2, such a congruence θ is also normal on $Q(A_h)$, and, consequently, H is also a congruence class in $Q(A_h)$. Therefore, it suffices to show that H is a subquasigroup of $Q(A_h)$.

The right local neutral element e_h for h is contained in H, since H is a normal subquasigroup of $Q(A)$. Thus, the congruence class H in $Q(A_h)$ contains an idempotent element e_h. In fact, e_h is a left neutral element of the quasigroup $Q(A_h)$ (see part 1 of Theorem 3.3). Corollary 2 of Lemma 4.1 applied to the congruence class H shows that H is a subquasigroup of $Q(A_h)$.

Theorem 4.3. *Suppose that the hypotheses of Lemma 4.2 are satisfied by quasigroups $Q(\circ)$ and $Q(\cdot)$. Then the quotients $Q/\theta(\circ)$ and $Q/\theta(\cdot)$ are isotopic.*

Proof. According to Lemma 4.2, the θ-classes in $Q(\cdot)$ and $Q(\circ)$ coincide. For an element a of Q, define the following potential self-maps of Q/θ:

$$\bar{\alpha}\bar{a} = \overline{\alpha a}, \quad \bar{\beta}\bar{a} = \overline{\beta a}, \quad \bar{\gamma}\bar{a} = \overline{\gamma a}. \tag{4.2}$$

The definitions (4.2) do not depend on the choice of the representative a. Thus, if we take $b \in \bar{a}$, then $\overline{\alpha b} = \overline{\alpha a}$. Indeed, $b \in \bar{a}$ implies $b\theta a$, and hence $\alpha b \theta \alpha a$ by the admissibility of α. Consequently, $\overline{\alpha b} = \overline{\alpha a}$. Again, by the admissibility of α, we find that $\bar{a}$ is a permutation of the set $\bar{Q} = Q/\theta$.

Now, the equations

$$\bar{a} \circ \bar{b} = \overline{a \circ b} = \overline{\alpha^{-1}(\beta a \cdot \gamma b)} = \bar{\alpha^{-1}}\overline{(\beta a \cdot \gamma b)} = \bar{\alpha^{-1}}(\overline{\beta a} \cdot \overline{\gamma b}) =$$

$$= \bar{\alpha^{-1}}(\bar{\beta}\bar{a} \cdot \bar{\gamma}\bar{b}).$$

establish the desired isotopy from $Q/\theta(\circ)$ to $Q/\theta(\cdot)$. □

3°. Inner permutations of quasigroups

We have defined normal subquasigroups as classes of normal congruences. However, one may also define a normal subquasigroups intrinsically. In this, we follow the ideas of Albert and Bruck [2, 31], who considered the analogous question for loops. Thus, we introduce the concept of an inner permutation.

Definition 2. A permutation a in the associated group G of a quasigroup $Q(\cdot)$ is said to *stabilize* or be *inner with respect to* an element h of Q if $ah = h$.

The inner permutations of the element h form a group, written as I_h*.

*If $h = 1$ is the neutral element of a loop $Q(\cdot)$, then the permutation α in this case is said to be *inner*, and the group $I = I_1$ is called the *group of inner permutations of the loop* $Q(\cdot)$ [31].

We identify certain permutations in the group I_h. We consider the right and left derivative operations by h in the quasigroup $Q(\cdot)$. It is convenient to adopt the notation $(\cdot)_h = (\bullet)$, ${}_h(\cdot) = (\circ)$, so we have equations

$$\left.\begin{aligned}(ha)b = h(a \bullet b),\\ a(bh) = (a \circ b)h\end{aligned}\right\} \tag{4.3}$$

which may be rewritten in terms of translations as

$$R_b R_a h = R_{a\bullet b} h,\ L_b L_a h = L_{a\circ b} h.$$

It follows that the permutations

$$\left.\begin{aligned}R_{a,b} = R^{-1}_{a\bullet b} R_b R_a,\\ L_{a,b} = L^{-1}_{a\circ b} L_a L_b\end{aligned}\right\} \tag{4.4}$$

are inner with respect to h.

Let us consider one more permutation from I_h. The equation $ha = xh$ has a unique solution which, for a fixed element h, depends only on a, Therefore we can write

$$ha = \sigma a \cdot h. \tag{4.5}$$

Hence $\sigma = R_h^{-1} L_h$. On the other hand, (4.5) implies $R_a h = L_{\sigma a} h$, whence $L^{-1}_{\sigma a} R_a h = h$: *The permutation*

$$T_a = L^{-1}_{\sigma a} R_a, \tag{4.6}$$

belongs to the group I_h.

The permutations (4.4) and (4.6) play an important role in the theory of quasigroups and loops. In particular, we have the following

Theorem 4.4. *The group* I_h *of inner permutations relative to an element* h *of the quasigroup* $Q(\cdot)$ *is generated by the set* $\{T_a, R_{a,b}, L_{a,b} \mid a, b \in Q\}$[2].

Proof. Let F be the permutation group generated by the set $\{T_a, R_{a,b}, L_{a,b} \mid a, b \in Q\}$. Since the set is a subset of I_h, we have that $F \subseteq I_h$.

To establish the opposite conclusion, first note that each permutation α from I_h, as a permutation from the associated group G, has the form

$$\alpha = S_{a_1}^{\varepsilon_1} S_{a_2}^{\varepsilon_2} \ldots S_{a_n}^{\varepsilon_n}, \tag{4.7}$$

where $S_{a_i} = R_{a_i}$ or L_{a_i} and $\varepsilon_i = \pm 1$ (for $1 \leqslant i \leqslant n$). We call the number n the *length* of the permutation α in the representation (4.7). Without loss of generality, we may assume $S_{a_n} = R_{a_n}$ and $\varepsilon_i = 1$, i.e., $S_{\alpha_n}^{\varepsilon_n} = R_{a_n}$, because otherwise we could add the product $R_x^{-1} R_x$ to a in (4.7).

We now prove $I_h \subseteq F$ by induction on the length n of the permutation α in one of its representations of the form (4.7).

First, suppose $n = 1$. We have$\alpha h = h$. In this case, the permutation $\alpha \in I_h$ must have the form R_x, i.e., $R_x h = h$ or $hx = h$, whence $x = e_h$. But e_h is the left neutral

element of a right derivative of a quasigroup $Q(\bullet)$: $e_h \bullet y = y$ or $x \bullet y = y$. Consequently, $R_{x,y} = R_{x,y}^{-1} R_y R_x = R_y^{-1} R_y R_x = R_x$, i.e., $R_x = R_{x,y} \in F$.

Now suppose that the theorem is true for arbitrary inner permutations $\varphi \in I_h$ whose length in a representation (4.7) is less than n. Let $\alpha \in I_h$ have length n. Let us show that α can be represented in the form

$$\alpha = \alpha' \tau, \tag{4.8}$$

where α' is some inner permutation of length $n-1$, and the permutation τ belongs to F. By the induction hypothesis, we may then conclude that $\alpha' \in F$, whence $\alpha = \alpha'\tau \in F$. Thus, to prove Theorem 4.4, we must prove the relationship (4.8).

There are four possible cases, according to the nature of the penultimate factor $S_{a_{n-1}}^{\varepsilon_{n-1}}$ in (4.7).

Case 1: $\alpha = \alpha'' R_y R_x$. The length of the permutation α'' is $n-2$. From the equality (4.4), it follows that $R_y R_x = R_{x \bullet y} R_{x,y}$. Consequently,

$$\alpha = \alpha'' R_{x \bullet y} R_{x,y} = \alpha' \tau,$$

where $\alpha' = \alpha'' R_{x \cdot y}$ and $\tau = R_{x,y}$. Thus α has the form (4.8).

Case 2: $\alpha = \alpha'' L_y R_x$. Equation (4.6) implies $R_x = L_{\sigma x} T_x$ and equation (4.4) implies $L_u L_v = L_{u \circ v} L_{u,v}$. Thus, we obtain

$$\begin{aligned} \alpha &= \alpha'' L_y L_{\sigma x} T_x = \alpha'' L_{y \circ \sigma x} L_y T_x \\ &= \alpha'' R_{\sigma^{-1}(y \circ \sigma x)} T_{\sigma^{-1}(y \circ \sigma x)}^{-1} L_{y,\, \sigma x} T_x = \alpha' \tau, \end{aligned}$$

where $\alpha' = \alpha'' R_{\sigma^{-1}(y \circ \sigma x)} \in F$ has length $n-1$ and $\tau = T_{\sigma^{-1}(y \circ \sigma x)}^{-1} L_{y,\, \sigma x} T_x \in F$.

Case 3: $\alpha = \alpha'' R_y^{-1} R_x$. We have

$$\alpha = \alpha'' R_y^{-1} R_x = \alpha'' (R_y^{-1} R_x)^{-1} = \alpha'' R_z (R_x^{-1} R_y R_z)^{-1},$$

with z taken to be the solution of the equation $x = z \bullet y$ in the quasigroup $Q(\bullet)$. Then

$$\alpha = \alpha'' R_z (R_{z \bullet y}^{-1} R_y R_z)^{-1} = \alpha'' R_z R_{z,\, y}^{-1} = \alpha' \tau.$$

Here $\alpha' = \alpha'' R_z$ and $\tau = R_{z,y}^{-1}$ lie in F.

Case 4: $\alpha = \alpha'' L_y^{-1} R_x$. We have

$$\alpha = \alpha'' L_y^{-1} L_{\sigma x} T_x = \alpha'' (L_{\sigma x}^{-1} L_y)^{-1} T_x = \alpha'' L_z (L_{\sigma x}^{-1} L_y L_z)^{-1} T_x,$$

with z taken to be the solution of the equation $\sigma x = y \circ z$ in the quasigroup $Q(\circ)$. Then

$$\alpha = \alpha'' L_z (L_{y \circ z}^{-1} L_y L_z)^{-1} T_x = \alpha'' L_z L_{y,x}^{-1} T_x = \alpha'' R_{\sigma^{-1}} T_{\sigma^{-1}}^{-1} L_{y,x}^{-1} T_x = \alpha' \tau.$$

Here $\alpha' = \alpha'' R_{\sigma^{-1} z}$ and $\tau = T_{\sigma^{-1} z}^{-1} L_{y,x}^{-1} T_x$ lie in F.

Thus, the proof of the theorem is completed. □

Remark 1. If $Q(\cdot)$ is a loop, then each subloop H contains the neutral element 1. If we put $I_1 = I$, then I is generated by all the permutations of the forms $T_a = L_a^{-1}R_a$, $R_{a,b} = R_{a,b}^{-1}R_bR_a$, and $L_{a,b} = L_{a,b}^{-1}L_aL_b$, since in this case $(\bullet) = (\circ) = (\cdot)$.

If $Q(\cdot)$ is also a group, then I is generated only by T_a, since $R_{a,b} = L_{a,b} = 1$ according to the equations $R_aR_b = R_{ba}$ and $L_aL_b = L_{ab}$ which are equivalent to the law of associativity in $Q(\cdot)$). But $T_ax = a^{-1}xa$, since in a group $L_a^{-1} = L_{a^{-1}}$. Consequently, if $Q(\cdot)$ is a group, then I is its group of inner automorphisms.

Remark 2. Let I_{h_1} and I_{h_2} be the groups of inner permutations with respect to the elements h_1 and h_2. Then I_{h_1} and I_{h_2} are isomorphic. Indeed, suppose $h_2 = h_1h$, so $h_2 = R_hh_1$. Take $\alpha \in I_{h_2}$. Then $R_h^{-1}\alpha R_h \in I_{h_1}$. In fact, $R_h^{-1}\alpha R_hh_1 = R_h^{-1}\alpha h_2 = R_h^{-1}h_2 = h_1$. Consequently, $R_h^{-1}I_{h_2}R_h \subseteq I_{h_1}$. The reverse inclusion is similar, so $I_h = R_h^{-1}I_{h_2}R_h$, and in particular, I_{h_1} and I_{h_2} are isomorphic.

Let h be an element of a subquasigroup $H(\cdot)$ of a quasigroup $Q(\cdot)$. Suppose that$H$ is invariant under I_h:

$$I_hH \subseteq H, \tag{4.9}$$

i.e., for arbitrary $\alpha \in I_h$ and arbitrary $h_1 \in H$, we have $\alpha h_1 \in H$. The inclusion (4.9) is equivalent to the equality $I_hH = H$, since $\alpha H \subseteq H$ implies $H \subseteq \alpha^{-1}H$, whence $H \subseteq I_hH$.

Remark 3. If a subquasigroup H is invariant under I_h for some $h \in H$, then it is also invariant under I_{h_1} for each $h_1 \in H$. Indeed, according to the previous remark, $I_{h_1} = R_{h_2}^{-1}I_hR_{h_2}$, where $h_1h_2 = h$. Consequently, $I_{h_1}H \subseteq H$, since H is invariant under R_{h_2} and I_h.

Lemma 4.3. *Let H be a subquasigroup invariant under I_h, where h is a fixed element from H. Then for arbitrary $a, b \in Q$ the equalities*

$$\left.\begin{array}{c} \sigma aH = Ha, \\ a(bH) = (a \circ b)H, \\ (Ha)b = H(a \bullet b) \end{array}\right\} \tag{4.10}$$

hold.

Indeed, using (4.6) we have $Ha = R_aH = L_{\sigma a}T_aH = L_{\sigma a}(T_aH) = L_{\sigma a}H$, since $T_a \in I_h$ and, consequently, $T_aH = H$. Thus, the first of the equalities (4.10) is proved. Further,

$$a(bH) = L_aL_bH = L_{a\circ b}L_{a,b}H = L_{a\circ b}H = (a \circ b)H.$$

The third of the equalities (4.10) is proved in similar fashion.

The converse assertion is also true: If the equalities (4.10) hold, then the subquasigroup H is invariant under $T_a, L_{a,b}, R_{a,b}$ and, consequently, is invariant under I_h.

Corollary 1.

$$(xH)y = R_h x(HL_h^{-1}y). \tag{4.11}$$

Indeed, using the equalities (4.10) we have

$$(xH)y = (H\sigma^{-1}x)y = H(\sigma^{-1}x \bullet y) = \sigma(\sigma^{-1}x \bullet y)H.$$

We determine the isotope $(\bullet)^{(\sigma^{-1},1,\sigma^{-1})}$. Given $(\bullet) = (\cdot)_h$ and $(\circ) =_h (\cdot)$, we have $(\bullet) = (\cdot)^{(L_h,1,L_h)}$ (see (3.8) and (3.9)). Thus,

$$\begin{aligned}(\bullet)^{(\sigma^{-1},1,\sigma^{-1})} &= (\cdot)^{(L_h,1,L_h)(\sigma^{-1},1,\sigma^{-1})} = (\cdot)^{(L_h\sigma^{-1},1,L_h\sigma^{-1})} \\ &= (\cdot)^{(1,R_h,R_h)(L_h\sigma^{-1},R_h^{-1},R_h^{-1},L_h\sigma^{-1})} = (\circ)^{(R_h,R_h^{-1},1)}.\end{aligned}$$

This means that $\sigma(\sigma^{-1}x \cdot y) = R_h x \circ R_h^{-1}y$, whence

$$\begin{aligned}(xH)y = (R_h x \circ R_h^{-1}y)H &= R_h x(R_h^{-1}yH) \\ &= R_h x(H\sigma^{-1}R_h^{-1}y) = R_h x(HL_h^{-1}y).\end{aligned}$$

Corollary 2.

$$aH = (a \circ H)H, \quad Ha = H(H \bullet a). \tag{4.12}$$

In fact, $(a\circ H)H$ consists of all the elements of the form $(a\circ h_1)h_2$, where $h_1, h_2 \in H$. But the equality $a(bH) = (a \circ b)H$ implies $(a \circ h_1)h_2 \in a(h_1H)$. Thus, $(a \circ H)H \subseteq aH$. Conversely, let $x \in aH$, say $x = ah_3$ with $h_3 \in H$. Now h_3 can be represented in the form $h_3 = h_4h$. Thus, $x = a(h_4h) = (a \circ h_4)h$ and therefore $x \in (a \circ h_4)H \subseteq (a \circ H)H$. The second of the equalities (4.12) is proved similarly.

Corollary 3.

$$R_h a \cdot H = (aH)H, \quad H \cdot L_h a = H(Ha). \tag{4.13}$$

Derivation of the equalities (4.13) is based on equation (4.10), and is performed in similar fashion to the proof of Corollary 2.

Lemma 4.4. *If a subquasigroup H is invariant under a group of inner permutations I_h, then*

$$aH \cdot bH = (a \odot b)H, \tag{4.14}$$

where $(\odot) = (\cdot)^{R_h}$.

We use the equality (4.11):

$$aH \cdot bH = R_h a[H \cdot L_h^{-1}(bH)] = R_h a[H \cdot L_h^{-1}(H\sigma^{-1}b)].$$

But $L_h^{-1}(Ha) = H \bullet a$. Indeed,

$$L_h(H \bullet a) \subseteq H(H \bullet a) = Ha$$

(by Corollary 2). Conversely, if $x \in Ha$, then $x = h_1a = (hh_2)a = h(h_2 \bullet a) \in L_h(H \bullet a)$. Therefore, $Ha \subseteq L_h(H \bullet a)$, whence $Ha = L_h(H \bullet a)$ and $L_h^{-1}(Ha) = H \bullet a$. We complete the proof of the relationship (4.14) using Corollary 2:

$$\begin{aligned}aH \cdot bH = R_h a[H(H \cdot \sigma^{-1}b)] = R_h a(H\sigma^{-1}b) &= R_h a(bH) \\ &= (R_h a \circ b)H = R_h^{-1}(R_h a \cdot R_h b) = (a \odot b)H.\end{aligned}$$

Lemma 4.5. *Suppose that a subquasigroup H is invariant under I_h, for some $h \in H$. Then two cosets aH and bH are either disjoint, or coincide.*

Indeed, consider $c \in aH \cap bH$. Then there exist elements h_1 and h_2 in H such that $c = ah_1$ and $c = bh_2$. We have

$$c = ah_1 = a(h_1'h) = (a \circ h_1')h \text{ and}$$

$$c = bh_2 = b(h_2'h) = (b \circ h_2')h.$$

Therefore, $a \circ h_1' = b \circ h_2'$. Hence $(a \circ h_1')H = (b \circ h_2')H$, so $a(h_1'H) = b(h_2'H)$, and $aH = bH$.

The significance for quasigroups of the groups of inner permutations follows from the following theorem.

Theorem 4.5. *A subquasigroup H is normal if and only if it is invariant under the group I_h of inner permutations, for any element h of H.*[3]

Proof. **Sufficiency:** Let H be invariant under I_h. We define an equivalence relation $a\theta b$ by $aH = bH$, and show that θ is a normal congruence on $Q(\cdot)$.

1. θ is a groupoid congruence in $Q(\odot)$.

Suppose $a\theta a_1$ and $b\theta b_1$. Then

$$(a \odot b)H = aH \cdot bH = a_1H \cdot b_1H = (a_1 \odot b_1)H,$$

i.e., $(a \odot b)\theta(a_1 \odot b_1)$.

2. The permutation R_h is admissible with respect to θ.

Suppose $a\theta b$. Then by Corollary 3 of Lemma 4.3, we have

$$R_h a \cdot H = (aH)H = (bH)H = R_h b \cdot H,$$

i.e., $R_h a \theta R_h b$.

Conversely, suppose $R_h a \theta R_h b$. Now $R_h a \cdot H = R_h a(H \cdot L_h^{-1}h) = (aH)h$. Similarly, we obtain $R_h b \cdot H = (bH)h$. From $R_h a \cdot H = R_h b \cdot H$ we thus obtain $(aH)h = (bH)h$, whence $aH = bH$ or $a\theta b$. Thus R_h is admissible with respect to θ.

3. θ is a groupoid congruence on $Q(\cdot)$.

This assertion follows from the fact that R_h is an admissible permutation for the congruence θ, and from (the remark to) Lemma 4.2.

4. θ is a normal congruence on $Q(\cdot)$.

Suppose $yx\theta zx$, with $y = L_h y'$ and $z = L_h z'$. We may rewrite $R_h^{-1}(yx)$ as $R_h^{-1}(yx) = R_h^{-1}L_hL_h^{-1} \times (L_h y'x) = \sigma(y' \bullet x)$. Since $yx\theta zx$, we then have $R_h^{-1}(yx)\theta R_h^{-1}(zx)$, whence $R_h^{-1}(yx)H = R_h^{-1}(zx)H$ and $\sigma(y' \bullet x)H = \sigma(z' \bullet x)H$. Hence, by (4.10) we obtain $H(y' \bullet x) = H(z' \bullet x)$. Using (4.10) again, we find $(Hy')x = (Hz')x$, whence $Hy' = Hz'$. Consequently, $\sigma y'H = \sigma z'H$, i.e., $\sigma y'\theta\sigma z'$ or $R_h^{-1}L_h y'\theta R_h^{-1}L_h z'$. Taking into consideration the values for y' and z', we have $R_h^{-1}y\theta R_h^{-1}z$, whence $y\theta z$.

If $xy\theta xz$, then $y\theta z$. This part is easier. Let $y = R_h y'$ and $z = R_h z'$. Then $x \cdot R_h y'\theta x \cdot R_h z'$, so $R_h^{-1}(x \cdot R_h y')\theta R_h^{-1}(x \cdot R_h z')$ and $x \circ y'\theta x \circ z'$. Consequently, $(x \circ y')H = (x \circ z')H$ and $x(y'H) = x(z'H)$, whence $y'H = z'H$, i.e., $y'\theta z'$, $R_h y'\theta R_h z'$ and $y\theta z$.

Thus, we have shown that θ is a normal congruence on $Q(\cdot)$. Since the subquasigroup H is a θ-class, it is a normal subquasigroup.

Necessity: Let H be a class of a normal congruence θ. We show that if $\varphi \in I_h$ and $h' \in H$, then $\varphi h' \in H$. It is sufficient to prove our assertion for the case where φ is one of the generators of the group I_h.

1. Suppose that $\varphi = T_a$, and let $T_a h' = x$. Thus $L_{\sigma a}^{-1} R_a h' = x$, so $\sigma a \cdot x = h' \cdot a$ and $R_h^{-1} L_h a \cdot x = h'a$. Let $a = L_h^{-1} R_h b$. We obtain $bx = h' L_h^{-1} R_h b$. But $h' L_h^{-1} R_h b \theta h L_h^{-1} R_h b = L_h L_h^{-1} R_h b = R_h b$, i.e., $bx \theta R_h b = bh$. Since θ is a normal congruence, we conclude that $x \theta h$, i.e., $x \in H$.

2. Suppose that $\varphi = R_{a,b}$, and let $R_{a,b} h' = x$. Thus $R_{a \bullet b}^{-1} R_b R_a h' = x$, so $R_{a \bullet b} x = R_b R_a h'$ and $(h'a)b = (xa \bullet b)$. Since $(h'a)b \theta (ha)b = h(a \bullet b)$, we have $h(a \bullet b) \theta x (a \bullet b)$, whence $h \theta x$ and $x \in H$. Similarly, it is proved that $L_{a,b} H = H$. □

Normal subquasigroups may also be characterized as follows (compare [25, p.256]).

Theorem 4.6. *A necessary and a sufficient condition for a subquasigroup H to be normal is the following. Let a and b be two arbitrary fixed elements from Q. Then, if in the equality*

$$(ah_1)(bh_2) = (a \odot b) h_3, \tag{4.15}$$

two of the three elements h_1, h_2, h_3 belong to H, then the third one also belongs to H.

Proof. The necessity of condition (4.15) for normality follows immediately from Lemma 4.4. Thus, given the condition, it suffices to show that H satisfies the equations (4.10).

Let us prove the first of the equations (4.10). An arbitrary element from H_a has the form $h_1 a$. We can write h_1 as $f_h h_2$, where f_h is the left local neutral element for h, and set $a = a_0 h$. Then

$$\begin{aligned} h_1 a = (f_h h_2)(a_0 h) = (f_h \odot a) h_3 = R_h^{-1}(R_h f_h \cdot R_h a_0) h_3 \\ = R_h^{-1}(ha) \cdot h_3 = R_h^{-1} L_h a \cdot h_3 = \sigma a \cdot h_3. \end{aligned}$$

Conversely, if h_3 is an arbitrary element from H, then going in the opposite direction we obtain $\sigma a \cdot h_3 = (f_h \odot a_0) h_3$. In view of the hypothesis of the theorem, for given h, h_3 there exists an element h_2 from H such that $(f_h \odot a_0) h_3 = (f_h h_2)(a_0 h)$. Consequently, $\sigma a \cdot h_3 = h_1 a$. Thus, $Ha = \sigma a \cdot H$.

The second of the equations (4.10) is proved similarly. Consider

$$\begin{aligned} a(bh_1) = (a_0 h)(bh_1) = (a_0 \odot b) h_2 \\ = R_h^{-1}(R_h a_0 \cdot R_h b) h_2 = R_h^{-1}(a \cdot R_h b) h_2 = (a \circ b) h_2. \end{aligned}$$

Reading the equations in each direction (h_1 to h_2, and back) yields the required equality of sets.

Finally, we consider the last of the equations (4.10). We have

$$(h_1 a) b = (\sigma a h_1') b = (\sigma a h_1')(b_0 h) = (\sigma a \odot b) h_2 = h_3 \sigma^{-1}(\sigma a \odot b_0).$$

But $\sigma^{-1}(\sigma a \odot b_0) = \sigma^{-1} R_h^{-1}(R_h \sigma a \cdot R_h b_0) = L_h^{-1}(L_h a \cdot b) = a \bullet b$, so $(h_1 a) b = h_3 (a \bullet b)$, and, consequently, $(Ha) b \subseteq H(a \bullet b)$. Similarly, we obtain the reverse inclusion, and from there we have the third of the equations (4.10). □

Corollary. If $Q(\cdot)$ is a loop with neutral element 1 and $h = 1$, then $(\odot) = (\cdot)$, and we have the following assertion: *A subloop H is normal if and only if, in the equation $ah_1 \cdot bh_2 = ab \cdot h_3$, whenever two of the three elements h_1, h_2 and h_3 belong to the subloop H, then the third also belongs to H.*

The theory of normal subquasigroups and homomorphisms of quasigroups can be developed further, but we will not do this here. We merely note the following proposition which follows directly from Theorem 4.5: *Any nonempty intersection of normal subquasigroups is also a normal subquasigroup.*[4]

4°. Homotopy

Isotopy is a natural generalization of isomorphism. The concept of a homotopy of two quasigroups introduced by Albert [1] provides an analogous natural generalization of a homomorphism.

First, we agree on some designations. A *surjection* $\alpha\colon Q \to Q'$ means a mapping of the set Q onto the set Q'. In this case, one can write $\alpha(Q) = Q'$. If $\beta(Q') = Q''$, then the surjections β and α can be multiplied, and the product $\beta\alpha$ yields the equality $\beta\alpha(Q) = Q$", i.e., $\beta\alpha(Q) = \beta[\alpha(Q)]$. Not all surjections can be multiplied, as is clear from the definition. Two surjections $\alpha, \beta\colon P \to Q$ are called *equivalent* if there exist permutations U of P and V of Q such that

$$\alpha = V\beta U\,.$$

Definition 3. A quasigroup $P(B)$ is *homotopic* to a quasigroup $Q(A)$ if there exists a triple $T = (\alpha,\ \beta,\ \gamma)$ of mutually equivalent surjections from P to Q such that

$$\gamma B(x, y) = A(\alpha x, \beta y)$$

for arbitrary $x, y \in P$. In this case, the quasigroup $Q(A)$ is called a *homotopic image* of the quasigroup $P(B)$.

As for isotopy, we will also write $B = A^T = A^{(\alpha,\beta,\gamma)}$ as a shorthand implying that B acts on P and A acts on Q. In particular, if $\alpha = \beta = \gamma$, then we write* $B = A^{(\gamma,\gamma,\gamma)} = A^\gamma$. The triple T is called a *homotopy*, and the surjections α, β, γ are the *components* of T.

The product of homotopies T and S is defined in the same way as the product of isotopies, if, of course, the product of components of T and S makes sense. As for isotopies, the equality $(A^T)^S = A^{TS}$ is true. Furthermore, $B = A^{T^{-1}}$ follows from $B = A^T$ if the components of T are invertible mappings from P to Q.

It is now easy to prove the following theorems.

Theorem 4.7. *A quasigroup $P(B)$ is homotopic to a quasigroup $Q(A)$ if and only if there are respective isotopes $P(B_0)$ of $P(B)$ and $Q(A_0)$ of $Q(A)$ such that $B_0 = A_0^\gamma$ for some γ, (i.e., if $P(B_0)$ is homomorphic to $Q(A_0)$).*

*In this case, the quasigroup $P(B)$ is said to be *homomorphic* to the quasigroup $Q(A)$.

Proof. Let $B = A^T$, where $T = (\alpha, \beta, \gamma)$. By the definition of a homotopy, $\alpha = V_1\gamma U_1$ and $\beta = V_2\gamma U_2$, where U_1, U_2 are permutations of the set P, and V_1, V_2 are permutations of the set Q. Therefore,

$$B = A^{(\alpha,\,\beta,\,\gamma)} = A^{(V_1\gamma U_1,\,V_2\gamma U_2,\,\gamma)} = A^{(V_1,\,V_2,\,1)(\gamma,\,\gamma,\,\gamma)(U_1,\,U_2,\,1)},$$

whence

$$B^{(U_1,\,U_2,\,1)^{-1}} = A^{(V_1,\,V_2,\,1)\gamma}.$$

The required quasigroups are

$$B_0 = B^{(U_1^{-1},\,U_2^{-1},\,1)} \text{ and } A_0 = A^{(V_1,\,V_2,\,1)}.$$

The converse is also easy to see. □

Theorem 4.8. *If a loop $P(B)$ is homotopic to a quasigroup $Q(A)$, then the loop $P(B)$ is homomorphic to a loop isotopic to the quasigroup $Q(A)$.*

Indeed, let $B = A^{(\alpha,\,\beta,\,\gamma)}$ or $\gamma B(x,\,y) = A(\alpha x,\,\beta y)$. Let $x = e$ be the neutral element of the loop $P(B)$. Then $\gamma y = A(\alpha e,\,\beta y) = L^A_{\alpha e}\beta y$, where $L^A_{\alpha e}$ is a left translation in $Q(A)$. Consequently $\beta = (L^A_{\alpha e})^{-1}\gamma$. Similarly, we obtain $\alpha = (R^A_{\beta e})^{-1}\gamma$. Then

$$\gamma B(x,\,y) = A[(R^A_{\beta e})^{-1}\gamma x,\,(L^A_{\alpha e})^{-1}\gamma y] = A_{\beta e,\,\alpha e}(\gamma x,\,\gamma y),$$

i.e.,

$$B = A^{\gamma}_{\beta e,\,\alpha e}$$

(for the definition of $A_{u,\,v}$, see Chapter I).

Corollary. *If a group $P(B)$ is homotopic to a loop $Q(A)$, then $P(B)$ is homomorphic to $Q(A)$. Consequently, $Q(A)$ is a group.*

Indeed, according to Theorem 4.8, the group $P(B)$ is homomorphic to a loop $Q(C)$ which isotopic to a loop $Q(A)$. Thus, $Q(C)$ must also be a group, and since $Q(C)$ is isotopic to a loop $Q(A)$ according to Albert's theorem, we conclude that $Q(A)$ is also a group.

Remark. A non-associative loop $P(B)$ can be homotopic, and even homomorphic, to a group $Q(A)$ (see the example from 1° in this chapter).

Notes

[1]Examples can be found in the articles of Bates and Kiokemeister [38], Cowell [45], Evans [44]; but they are rather challenging. On the other hand, it is very easy to construct an example of a groupoid with division which is not a quasigroup. Let Q be the set of non-negative real numbers, and let $x \circ y = |x - y|$, where $|x|$ is the absolute value of the number $x \in Q$. Then $Q(\circ)$ is the desired example.

[2]Theorem 4.4 was proved for loops by Bruck [31], and in alternative fashion by Osborn. Here Osborn's proof is extended to quasigroups.

[3]From Theorem 4.5 and Lemma 4.5 it follows that if $Q(\cdot)$ is a finite quasigroup, then the order of a normal subquasigroup $H(\cdot)$ is a divisor of the order of the quasigroup (as a weak analogue of the Lagrange Theorem for groups). If $H(\cdot)$ is a subquasigroup which is not normal, then its order does not have to divide the order of the quasigroup. A counterexample is furnished by the non-associative loop $Q(\cdot)$ of order 5, presented with its Cayley table in Chapter I, 1°. Let $H = \{1, a\}$, where a is an arbitrary element of Q with $a \neq 1$. Then $H(\cdot)$ is a subloop of order 2.

Following Bruck [31], we say that a finite loop $Q(\cdot)$ possesses Property (L) (weak Lagrange property) if the order of an arbitrary subloop is a divisor of the order of the loop, and $Q(\cdot)$ has Property (L') if an arbitrary subloop of the loop $Q(\cdot)$ exhibits Property (L). A necessary and a sufficient condition for a finite loop $Q(\cdot)$ to have Property (L') is: There exists a chain $Q = Q_0 \supset Q_1 \supset Q_2 \supset \ldots \supset Q_n = 1$ in $Q(\cdot)$, where each subloop Q_i is a normal subloop in Q_{i-1} (for $1 \leqslant i \leqslant n$), and each Q_{i-1}/Q_i has Property (L').

[4]The theory of normal subquasigroups has been studied by many authors. In addition to Bates and Kiokemeister, we note the works by Albert [1, 2], Baer [36], Garrison [40], Murdoch [53], and also Bruck [31]. Albert studies normal subquasigroups with the help of the associated group G (see Chapter I, 2°). In particular, he proved that a subquasigroup H of a quasigroup $Q(\cdot)$ is normal if and only if $H = \Gamma 1$, where Γ is a normal subgroup of the associated group G.

Chapter V. Quasigroups and loops with the inverse property (IP-quasigroups)

1°. Definitions and elementary properties

Up to this point, we have been analyzing quasigroups and loops in reference to the associativity property that groups possess. However, groups have another important property, the *inverse property*: Each element x is matched by its inverse x^{-1}, such that the equations $xx^{-1} = x^{-1}x = 1$ hold. Using associativity, we then obtain

$$x^{-1}(xy) = y \quad \text{and} \quad (yx)x^{-1} = y. \tag{5.1}$$

The equations (5.1) may be interpreted as a definition of a rather wide class of quasigroups and loops.

Definition 1. A quasigroup $Q(\cdot)$ is said to possess the *right inverse property* if it is equipped with a self-map I_r of the set Q such that

$$(yx)I_r x = y \tag{5.2}$$

for elements x, y of Q. The *left inverse property* is defined similarly. In this case, we have the equation

$$I_l x(xy) = y \tag{5.3}$$

involving a self-map I_l of Q.

The conjunction of the right and left inverse properties is identified as the *inverse property*. Quasigroups with the left (right) inverse property are called *left (right) IP-quasigroups*, and a quasigroups with the inverse property are called an *IP-quasigroups*[1]. A loop with the inverse property is called an *IP-loop* for brevity.

Let $Q(\cdot)$ be a loop with neutral element 1. The equations $ax = 1$ and $ya = 1$ have unique solutions. The element x is called the *right inverse element* for a, and is denoted by a^{-1}, while the element y is called the *left inverse element* for a and is denoted by ${}^{-1}a$. Thus,

$$aa^{-1} = 1 \quad \text{and} \quad {}^{-1}aa = 1.$$

If $Q(\cdot)$ is an IP-loop, then

$$I_r x = x^{-1} \quad \text{and} \quad I_l x = {}^{-1}x. \tag{5.4}$$

For this purpose, it suffices to set $y = 1$ in (5.2) and (5.3). It is convenient to use the index notations of (5.4) for $I_r x$ and $I_l x$ in any IP-quasigroup. In this notation, the equations (5.2) and (5.3) are rewritten as

$$(yx)x^{-1} = y \quad \text{and} \quad {}^{-1}x(xy) = y. \tag{5.5}$$

Now, we will examine a series of simple properties which immediately follow from the definition of an IP-quasigroup.

1. The mapping $I_r : x \to x^{-1}$ is a *permutation of the set Q, with $I_r^2 = 1$.* Indeed, $yx \cdot x^{-1} = y$ implies $(yx \cdot x^{-1})(x^{-1})^{-1} = y(x^{-1})^{-1}$ or $yx = y(x^{-1})^{-1}$, whence $(x^{-1})^{-1} = x$. Similarly, the mapping $I_l \colon x \to {}^{-1}x$ is a permutation of the set Q, with $I_l^2 = 1$.

2. *The solution of the equation $ax = b$ is ${}^{-1}ab$, while the solution of the equation $ya = b$ is ba^{-1}.* Indeed, $a({}^{-1}ab) = {}^{-1}({}^{-1}a)({}^{-1}ab) = b$.

3. *We have the equations*

$$(xy)^{-1} = {}^{-1}y \cdot {}^{-1}x \quad \text{and} \quad {}^{-1}(xy) = y^{-1} \cdot x^{-1}. \tag{5.6}$$

Set $xy = z$, so $y = {}^{-1}xz$, where ${}^{-1}x = yz^{-1}$. Then $z^{-1} = {}^{-1}y^{-1}x$, i.e. $(xy)^{-1} = {}^{-1}y^{-1}x$. The second of the equations (5.6) is proved similarly.

4. *For each a in Q, the equations*

$$L_{I_l a} = L_a^{-1} \quad \text{and} \quad R_{I_r a} = R_a^{-1}$$

hold. They follow from the respective equations (5.2) and (5.3).

5. *In an arbitrary IP-quasigroup the equations*

$$I_r R_a I_l = L_a^{-1}, \qquad I_l L_a I_r = R_a^{-1}, \tag{5.7}$$

$$I_l R_a I_r = L_{I_r a}, \qquad I_r L_a I_l = R_{I_l a} \tag{5.8}$$

hold. Indeed, we have

$$I_r R_a I_l x = ({}^{-1}xa)^{-1} = ({}^{-1}a) \cdot {}^{-1}({}^{-1}x) = {}^{-1}ax = L_{I_l a}x = L_a^{-1}x.$$

The remaining equations from (5.7) and (5.8) are proved similarly.

6. *The right and left inverses of an element x coincide in each IP-loop:*

$${}^{-1}x = x^{-1}. \tag{5.9}$$

For this, it suffices to set $y = x^{-1}$ in the second of the equations (5.5).

7. *The following equalities hold in each IP-loop:*

$$\left.\begin{array}{c} aa^{-1} = a^{-1}a = 1, \\ (ba)a^{-1} = a^{-1}(ab) = b, \\ (a^{-1})^{-1} = a,\ (ab)^{-1} = b^{-1}a^{-1}, \end{array}\right\} \tag{5.10}$$

$$\left.\begin{array}{c} L_a^{-1} = L_{a^{-1}},\ R_a^{-1} = R_{a^{-1}}, \\ IR_aI = L_a^{-1},\ IL_aI = R_a^{-1}, \end{array}\right\} \tag{5.11}$$

where $Ix = x^{-1}$.

8. *Equation* (5.9) *holds in commutative IP-quasigroups.* Indeed, $(ba)a^{-1} = b$, so by the commutativity $a^{-1}(ab) = b$. Comparison of this expression with (5.3) yields ${}^{-1}a = a^{-1}$.

9. *Let e_x, f_x be the respective right and left local units of an element x of an IP-quasigroup. Then:*

$$xx^{-1} = f_x,\ {}^{-1}xx = e_x, \tag{5.12}$$

$$e_x^{-1} = e_x,\ {}^{-1}f_x = f_x. \tag{5.13}$$

For the translations L_x, R_x we have

$$L_x^{-1} = L_{-1_x},\ R_x^{-1} = R_{x^{-1}}. \tag{5.14}$$

The equations (5.12) and (5.14) follow directly from the definition of an IP-quasigroup. For (5.13), we have

$$(xe_x)e_x^{-1} = x.$$

On the other hand, $xe_x = x$, so $xe_x^{-1} = x$, whence $e_x^{-1} = e_x$.

2°. Crossed product of quasigroups. An example of an IP-quasigroup

So far, the only examples of IP-quasigroups that we have noted are groups. Here, we will construct an example of an IP-quasigroup where $I_l \neq I_r$. By (5.9), such a quasigroup cannot be an IP-loop, and certainly not a group. To construct the example, we will use the so-called *crossed product* of quasigroups. It is suggested by the theory of quasigroup extensions.

Let $P(\cdot)$ be a quasigroup defined on a set $P = \{u, v, w, \dots\}$, Suppose that we have a system Σ of quasigroup operations on a given set Q. Consider a mapping $P^2 \to \Sigma$ which assigns the operation $A_{(u,v)}$ to an ordered pair (u, v) from P^2. Consider the set $M = P \times Q$, and an operation

$$(u, a) \circ (v, b) = \big(uv, A_{(u,v)}(a, b)\big) \tag{5.15}$$

on the set M. The groupoid $M(\circ)$ is called the *crossed product*

$$(\circ) =< \cdot, \Sigma >$$

of the quasigroup $P(\cdot)$ and the system $Q(\Sigma)$ of quasigroups.

A crossed product $M(\circ)$ of quasigroups is also a quasigroup. Indeed, consider $x = (u, a)$ and $y = (v, b)$ in M. We will show that there exists a unique element $z = (w, c)$ in M such that $x \circ z = y$. We have

$$(u, a) \circ (w, c) = (v, b)$$

or

$$\big(uw, A_{(u,v)}(a, c)\big) = (v, b),$$

whence

$$uw = v \quad \text{and} \quad A_{(u,w)}(a,c) = b. \tag{5.16}$$

The element w is uniquely defined by the first equation from (5.16), so we have a uniquely defined operation $A_{(u,w)} \in \Sigma$. The second equation from (5.16) then specifies c uniquely. The equation $z \circ x = y$ for z is solved similarly.

The following statement can be proved in similar fashion.

The crossed product $M(\circ)$ is a loop if and only if the following conditions hold:

1) *$P(\cdot)$ is a loop with neutral element* 1;

2) *There exists an element $e \in Q$ such that*

$$A_{(u,1)}(a,e) = A_{(1,u)}(e,a) = a$$

for arbitrary $a \in Q$ and $u, v \in P$.

In this case, the pair $(1,e)$ is the neutral element of the loop $M(\circ)$.

Further it is possible to prove the following statement.

Theorem 5.1. *Let θ be a congruence (a normal congruence) on a quasigroup $P(\cdot)$. Consider the relation $\overline{\theta}$ on M with*

$$(u,a)\overline{\theta}(v,b) \text{ if and only if } u\theta v.$$

Then $\overline{\theta}$ is a congruence (a normal congruence) on $M(\circ)$.

For example, we show, that if θ is a normal congruence on $P(\cdot)$, then $x \circ z\bar{\theta}y \circ z$ implies $x\bar{\theta}y$. Indeed, let $x = (u,a), y = (v,b), z = (w,c)$. Then

$$(u,a) \circ (w,c)\bar{\theta}(v,b) \circ (w,c),$$
$$(uw, A_{u,w}(a,c))\bar{\theta}(uw, A_{u,w}(b,c)),$$

so $uw\overline{\theta}vw$. Consequently, $u\bar{\theta}v$, whence $x\overline{\theta}y$.

Corollary 1. *If $t^2 = t$ in $P(\cdot)$, then $N = \{(t,a) \mid a \in Q\}$ is a normal subquasigroup of $M(\circ)$.*

Indeed, it is easy to verify that N is a subquasigroup in $M(\circ)$. Further, we take the equality relation on $P(\cdot)$ as θ. Then $\overline{\theta}$ is a normal congruence in $M(\circ)$. In view of Lemma 4.1 , N is a normal subquasigroup, because $(t,a) \circ (t,a)\overline{\theta}(t,a)$.

Corollary 2. *If $P(\cdot)$ is a loop with neutral element* 1, *then $N = \{1\} \times Q$ is a normal subquasigroup in $M(\circ)$.*

The crossed product may be used to construct various examples of quasigroups.

1) *The direct product is a special case of the crossed product: if $A_{(u,v)} = (\bullet)$ for each $u, v \in P$, then $M(\circ)$ is the direct product of the quasigroups $P(\cdot)$ and $Q(\bullet)$:*

$$(u,a) \circ (v,b) = (uv, a \bullet b).$$

2) *An example of an IP-quasigroup with $I_r \neq I_l$.* Consider the direct product of a group $P(\cdot)$ and the quasigroup $Q(A)$, where $A(a,b) = \theta a \cdot b$ and θ is an automorphism of order 2 of a group $Q(\cdot)$. We show that $M(\circ)$, with $M = P \times Q$ and $(\circ) =< \cdot, A >$, is an IP-quasigroup with

$$\left.\begin{array}{c} I_r(u,a) = (u^{-1}, \theta a^{-1}), \\ I_l(u,a) = (u^{-1}, a^{-1}). \end{array}\right\} \tag{5.17}$$

Indeed, we have

$$\begin{aligned} I_l(u,a) \circ ((u,a) \circ (v,b)) &= (u^{-1} \cdot uv, \theta a^{-1} \cdot \theta a \cdot b = (v,b) \\ &= [(v,b) \circ (u,a)] \circ I_r(u,a) = (vu, \theta b \cdot a) \circ (u^{-1}, \theta a^{-1}) \\ &= (vu \cdot u^{-1}, \theta(\theta b \cdot a) \cdot \theta a^{-1}) = (v, \theta^2 b \cdot \theta a \theta a^{-1}) = (v, \theta^2 b) = (v,b). \end{aligned}$$

Therefore, $M(\circ)$ is an IP-quasigroup, with $I_r \neq I_l$. The inequality follows from (5.17), since $\theta \neq 1$.

3°. Isotopes of IP-quasigroups. Moufang quasigroups

First of all, we note that the concept of an IP-quasigroup can be defined in terms of the inverse operations from Chapter I, Definition 3: *a quasigroup $Q(A)$ is an IP-quasigroup if and only if there exist two permutations I_r and I_l such that*

$$A^{-1} = A^{(I_l,1,1)} \quad \text{and} \quad {}^{-1}A = A^{(1,I_r,1)}. \tag{5.18}$$

Indeed, according to the definition of an IP-quasigroup $Q(A)$ we have

$$A[A(b,a), I_r a] = b,$$

whence $A(b,a) = {}^{-1}A(b, I_r a)$ and $A = ({}^{-1}A)^{(1,I_r,1)}$. Therefore,

$${}^{-1}A = A^{(1,I_r,1)^{-1}} = A^{(1,I_r^{-1},1)} = A^{(1,I_r,1)}.$$

The first of the equations (5.18) is proved similarly. The equations (5.18) imply the following.

Lemma 5.1. *An IP-quasigroup A and its inverse quasigroups are all isotopic to each other.*

Indeed, let

$$P_l = (I_l, 1, 1) \quad \text{and} \quad P_r = (1, I_r, 1). \tag{5.19}$$

Then the equations (5.18) become

$$A^{-1} = A^{P_l} \quad \text{and} \quad {}^{-1}A = A^{P_r}.$$

Using Corollary 1 of Lemma 1.3, we obtain

$$\begin{aligned} {}^{-1}(A^{-1}) = {}^{-1}(A^{P_l}) = ({}^{-1}A)^{P_l^l} = A^{P_r P_l^l}, \\ {}^{-1}(A)^{-1} = (A^{P_r})^{-1} = (A^{-1})^{P_r^r} = A^{P_l P_r^r}, \\ A^{\bullet} = [{}^{-1}(A^{-1})]^{-1} = (A^{P_r P_l^l})^{-1} = (A^T)^{-1} = (A^{-1})^{T^r} = A^{P_l T^r}. \end{aligned}$$

We recall that $T^r = (\alpha,\beta,\gamma)^r = (\alpha,\gamma,\beta)$ and $T^l = (\alpha,\beta,\gamma)^l = (\gamma,\beta,\alpha)$.

Corollary. *If A is an IP-loop, then all the inverse loops of A coincide.*

The inverse loops for the loop A are defined by the equalities (1.18):

$$A^\rho = (A^{-1})^{P_A} \quad \text{and} \quad A^\lambda = ({}^{-1}A)^{S_A},$$

where $P_A = (I_A^{-1}, 1, 1)$, $S_A = (1, I_A, 1)$ and $A(x, I_A x) = 1$. But by Properties 1 and 5 of IP-loops, we have $I_r = I_l = I_A = I$ and

$$P_A = (I^{-1}, 1, 1) = (I, 1, 1).$$

By (5.19) we obtain $P_A = P_l$ and $P_A^2 = 1$. So,

$$A^\rho = (A^{-1})^{P_A} = A^{P_A^2} = A.$$

We find $A^\lambda = A$ similarly, whence $A^{\rho\lambda} = A$, $A^{\lambda\rho} = A$, etc. The converse is easy to see: *If A is a loop and $A^\rho = A^\lambda = A$, then A is an IP-loop.*

Now, let B be an isotope of an IP-quasigroup A

$$B = A^S.$$

Then by Corollary 1 of Lemma 1.3,

$$B^{-1} = (A^S)^{-1} = (A^{-1})^{S^r} = A^{P_l S^r} = (B^{S^{-1}})^{P_l S^r} = B^{S^{-1} P_l S^r}. \tag{5.20}$$

If B is also an IP-quasigroup, then we must have $B^{-1} = B^{(I_l', 1, 1)} = B^{P_{l'}}$, where I_l' is some permutation. Consequently,

$$B^{S^{-1} P_l S^r} = B^{P_{l'}} = (B^{S^{-1}})^{S P_l'},$$

i. e., $A^{P_l S^r} = A^{S P_l'}$, whence

$$A^{P_l S^r (P_l')^{-1} S^{-1}} = A. \tag{5.21}$$

Let $S = (\lambda, \mu, \nu)$ then

$$\begin{aligned} T_l = P_l S^r (P_l')^{-1} S^{-1} &= (I_l, 1, 1)(\lambda, \mu, \nu)(\lambda^{-1}, \mu^{-1}, \nu^{-1}) = \\ &= (I_l \lambda I_l'^{-1} \lambda^{-1}, \nu\mu^{-1}, \mu\nu^{-1}). \end{aligned}$$

Thus, T_l must be an autotopy of the quasigroup A. Considering ${}^{-1}B$, we similarly obtain that $T_r = (\nu\lambda^{-1}, I_r \mu I_r'^{-1} \mu^{-1}, \lambda\nu^{-1})$ is also an autotopy of the quasigroup A. Thus, we have obtained the following.

Theorem 5.2. *The following property is necessary and sufficient for an isotope of an IP-quasigroup A also to be an IP-quasigroup: There exist two involutions, permutations I_r' and I_l' of order 2, such that $T_l = (I_l \lambda I_l'^{-1} \lambda^{-1}, \nu\mu^{-1}, \mu\nu^{-1})$ and $T_r = (\nu\lambda^{-1}, I_r \mu I_r'^{-1} \mu^{-1}, \lambda\nu^{-1})$ are autotopies of the quasigroup A.*

We have already seen that the condition is necessary. The proof of sufficiency does not present any difficulties: we proceed in the opposite direction from the equation (5.21) to the equation (5.20), using the conditions of the theorem.

Let us apply Theorem‘5, 2 to the case when B is a loop. Thus, we will find conditions under which an isotope B of an IP-quasigroup A is an IP-loop.

It suffices to consider the case where B is a principal isotope of A. Then by Lemma 1.1. the isotopy must have the form:

$$B = A^{(R_c^{-1}, L_d^{-1}, 1)}.$$

By the equations (5.14), we obtain $R_c^{-1} = R_{c^{-1}}$ and $L_d^{-1} = L_{-1_d}$. Thus, the loop B must have the form:

$$B = A^{(R_a, L_b, 1)},$$

where $a = c^{-1}$ and $b =^{-1} d$. If B is an IP-loop, then by Theorem 5.2 there exist two permutations $I_l^{'}$ and $I_r^{'}$ such that

$$T_l = (I_l R_a I_l^{'} R_a^{-1}, L_b^{-1}, L_b) \text{ and } T_r = (R_a^{-1}, L_r L_b I_r^{'} L_b^{-1}, R_a)$$

are autotopies of the quasigroup A. In other words,

$$\left.\begin{array}{l} L_b(xy) = \phi x \cdot L_b^{-1} y \\ R_a(xy) = R_a^{-1} x \cdot \phi y, \end{array}\right\} \tag{5.22}$$

where $\phi = I_l R_a I_l^{'} R_a^{-1}$ and $\psi = I_r L_b I_r^{'} L_b^{-1}$. Since $L_b^{-1} y = L_{-1_b} y =^{-1}$ and $R_a^{-1} x = R_{a^{-1}} x = xa^{-1}$, the equations (5.22) imply

$$\left.\begin{array}{l} b \cdot xy = \phi x \cdot^{-1} by, \\ xy \cdot a = xa^{-1} \cdot \psi y. \end{array}\right\} \tag{5.23}$$

Replacing the element y with by in the first of the equations (5.23),

$$b(x \cdot by) = \phi x \cdot y. \tag{5.24}$$

Let $y = b^{-1}$. Then

$$b(x \cdot bb^{-1}) = \phi x \cdot b^{-1}.$$

Therefore,

$$\phi x = [b(x \cdot bb^{-1})]b = (b \cdot x f_b)b,$$

whence, replacing ϕx with $(b \cdot x f_b)b$ in (5.24), we obtain

$$b(x \cdot by) = \{[b(x \cdot f_b)]b\}\, y. \tag{5.25}$$

Similarly, the second of the equalities (5.23) gives

$$(xa \cdot y)a = x[a(e_a y \cdot ba)]. \tag{5.26}$$

If the equality (5.25) holds for each x and y, the element b is called a *left Moufang element*. If the equality (5.26) holds, the element a is called a *right Moufang element* We obtain the following.

Corollary. *The isotope $B = A^{(R_a, L_b, 1)}$ will be an IP-loop if and only if a and b are respectively right and left Moufang elements of the quasigroup $Q(A)$.*

It may turn out that all the elements of an IP-quasigroup $Q(\cdot)$ are right and left Moufang elements. Such a quasigroup is called a Moufang quasigroup. Thus, we arrive to the following definition:

Definition 2. A quasigroup $Q(\cdot)$ is called a *Moufang quasigroup* if

$$(xy \cdot z)y = x[y(e_y z \cdot y)], \tag{5.27}$$

and

$$y(x \cdot yz) = [(y \cdot xf_y)y]z, \tag{5.28}$$

for $x, y, z \in Q$, recalling ($ye_y = y$ and $f_y y = y$) [2].

Theorem 5.3. *Every Moufang quasigroup $Q(\cdot)$ is an IP-quasigroup.*

Indeed, for every $y \in Q$ there exists a element y' such that $e_y y' \cdot y = e_y$. Let

$$xy \cdot y' = x'.$$

If we show that $x' = x$, it will follow that $Q(\cdot)$ is a right IP-quasigroup. Indeed, using (5.27) we have

$$x'y = (xy \cdot y')y = x[y(e_y(y' \cdot y)] = x(ye_y) = xy,$$

whence $x' = x$. The fact that $Q(\cdot)$ is a right IP-quasigroup is proved similarly.

Each element of a Moufang quasigroup is simultaneously a left and a right Moufang element. Thus, if we use the corollary to Theorem 5.2, we obtain the following statement:

Corollary. *If a loop is an isotope of a Moufang quasigroup, then it is an IP-loop.*

Suppose that a Moufang quasigroup $Q(\cdot)$ is a loop, with $e_y = fy = 1$ as the neutral element. Then, the identities (5.27) and (5.28) become

$$(xy \cdot z)y = x(y \cdot zy), \tag{5.29}$$

and

$$y(x \cdot yz) = (yx \cdot y)z. \tag{5.30}$$

Later (see Chapter VI, ¶1°), it will be proved that the identities (5.29) and (5.30) are equivalent.

Definition 3. A loop $Q(\cdot)$ is a *Moufang loop* if it satisfies one of the identities (5.29) or (5.30). The identities (5.29) and (5.30) are known as *Moufang identities*.

From the definition of a Moufang loop, we immediately have the following.

Theorem 5.4. *If each loop isotopic to a loop $Q(\cdot)$ is an IP-loop, then $Q(\cdot)$ is a Moufang loop.*

Indeed, a Moufang loop is a Moufang quasigroup. We can now give a sharper characterization of Moufang quasigroups.

Theorem 5.5. *Each loop isotopic to a Moufang quasigroup is a Moufang loop.*

Now consider a Moufang quasigroup $Q(\cdot)$. Let $x \circ y = R_a^{-1}x \cdot L_b^{-1}y$. Then $Q(\circ)$ is a loop with neutral element $e = ba$. For brevity we will write $R_a = R$ and $L_b = L$. Then

$$xy = Rx \circ Ly.$$

Rewriting (5.27) in terms of the operation $(\circ)$ produces

$$R[R(Rx \circ Ly) \circ Lz] \circ Lz = Rx \circ LRy \circ L[R(Re_y \circ Lz) \circ Ly].$$

Replacing the respective elements x, y, z here with $R^{-1}x, L^{-1}y, L^{-1}z$ gives

$$R[R(x \circ y) \circ z] \circ y = x \circ LRL^{-1}y \circ L[R(Re_{L^{-1}y} \circ z) \circ y]. \tag{5.31}$$

Set $x = e$, Then (5.31) yields

$$R(Ry \circ z) \circ y = LRL^{-1}y \circ L[R(Re_{L^{-1}y} \circ z) \circ y].$$

Thus, equation (5.31) transforms into

$$R[R(x \circ y) \circ z] \circ y = x \circ [R(Ry \circ z) \circ y]. \tag{5.32}$$

Taking $y = e$ in (5.32) gives

$$R(Rx \circ z) = x \circ R(Re \circ z).$$

Define $\tau z = R(Re \circ z)$. Clearly, τ is a permutation of the set Q. Then

$$R(Rx \circ z) = x \circ \tau z$$

or

$$R(x \circ z) = R^{-1}x \circ \tau z. \tag{5.33}$$

Using (5.33), we can simplify (5.32) as

$$[(x \circ y) \circ \tau z] \circ y = x \circ [(y \circ \tau z) \circ y].$$

Consequently,

$$[(x \circ y) \circ z] \circ y = x \circ [(y \circ z) \circ y] \tag{5.34}$$

represents a reformulation of the Moufang quasigroup identity (5.27) in terms of the loop operation $(\circ)$.

If we use the operation $(\circ)$ in (5.28), then we obtain

$$y \circ [x \circ (y \circ z)] = [y \circ (x \circ y)] \circ z, \tag{5.35}$$

in similar fashion, making use of the relation

$$L(x \circ y) = \theta x \circ L^{-1} y, \tag{5.36}$$

where $\theta x = L(x \circ Le)$, the analogue of $\tau z = R(Re \circ z)$..

A loop $Q(\circ)$ with the identity (5.34) is called a *right Bol loop*, while a loop $Q(\circ)$ with the identity (5.35) is called a *left Bol loop.*

These right and left Bol identites differ slightly from the Moufang identities. It will be shown below that every Moufang loop is both a left and a right Bol loop. However, neither of the left or right Bol identities alone is sufficient to yield a Moufang loop. Nevertheless:

If the identities (5.34) *and* (5.35) *are both satisfied in a loop* $Q(\circ)$*, then it will be a Moufang loop.*

Indeed, according to Theorem 5.3, the loop $Q(\circ)$ will be an IP-loop. Then, using the equality (5.34), we have

$$y \circ (z \circ y) = y \circ [(y^{-1} \circ y) \circ z] \circ y = y \circ y^{-1} \circ [(y \circ z) \circ y],$$

where $y^{-1} \circ y = e$. Thus,

$$y \circ (z \circ y) = (y \circ z) \circ y.$$

This latter equality (known as the *flexible law*) transforms the identity (5.34) into (5.29).

In the opposite direction, we have the following statement.

Let $Q(\cdot)$ *be a Moufang loop, and let* R *be a permutation of* Q *such that*

$$R(x \circ y) = R^{-1} x \circ \tau y \quad \text{and} \quad L(x \circ y) = \theta x \circ L^{-1} y \tag{5.37}$$

for certain permutations τ, θ *of* Q*. Then* $Q(\cdot)$ *is a Moufang quasigroup.* [3]

The proof reduces to the verification of the equations (5.27) and (5.28). The two sides of (5.27) appear as

$$\begin{aligned}(xy \cdot z)y &= R[R(Rx \circ Ly) \circ Lz] \circ Ly \\ &= [(Rx \circ Ly) \circ \tau Lz] \circ Ly = Rx \circ [Ly(\tau Lz \circ Ly)]\end{aligned}$$

and

$$\begin{aligned}x[y(e_y z \cdot y)] &= Rx \circ L\{Ry \circ L[R(Re_y \circ Lz) \circ Ly]\} \\ &= Rx \circ \{\theta Ry \circ [R(Re_y \circ Lz) \circ Ly]\}.\end{aligned}$$

Thus equation (5.27) holds if and only if

$$Ly \circ (\tau Lz \circ Ly) = \theta Ry \circ [(e_y \circ \tau Lz) \circ Ly],$$

or

$$y \circ (z \circ y) = \theta R L^{-1} y \circ [(e_{L_y^{-1}} \circ z) \circ y]. \tag{5.38}$$

In order to prove (5.38) we find e_u, using

$$ue_u = u, \qquad Ru \circ Le_u = u,$$

$$Le_u = (Ru)^{-1} \circ u = IRu \circ u, \qquad e_u = L^{-1}(IRu \circ u).$$

But (5.36) implies

$$L^{-1}(x \circ y) = \theta^{-1}x \circ Ly, \tag{5.39}$$

because if $(\theta, L^{-1}, L) \in \mathfrak{A}_{(0)}$, then $(\theta^{-1}, L, L^{-1}) \in \mathfrak{A}_{(0)}$, where $\mathfrak{A}_{(0)}$ is the autotopy group of the loop $Q(\circ)$. Therefore,

$$e_u = \theta^{-1}IRu \circ Lu,$$

and consequently

$$e_{L^{-1}y} = \theta^{-1}IRL^{-1}y \circ y.$$

Now we will prove the equality

$$\theta^{-1} = I\theta I. \tag{5.40}$$

Indeed, we set $x = y^{-1}$ and $Le = \theta y^{-1} \circ L^{-1}y$ in the second equation of (5.37). Because a Moufang loop is an IP-loop, we obtain

$$\theta y^{-1} = Le \circ (L^{-1}y)^{-1}$$

and

$$(\theta y^{-1})^{-1} = (Le \circ (L^{-1}y)^{-1})^{-1} = L^{-1}y \circ (Le)^{-1}. \tag{5.41}$$

On the other hand, from (5.39) with $y = e$, we find

$$L^{-1}x = \theta^{-1}x \circ Le,$$

whence

$$\theta^{-1}x = L^{-1}x \circ (Le)^{-1}. \tag{5.42}$$

We conclude that $(\theta x^{-1})^{-1} = \theta^{-1}x$, i.e., the equation (5.40) holds by comparison of (5.41) and (5.42). Now we can complete the proof of equation (5.38):

$$\theta RL^{-1}y \circ [(e_{L^{-1}y} \circ z) \circ y] = \theta RL^{-1}y \circ \big\{[(\theta^{-1}IRL^{-1}y \circ y) \circ z] \circ y\big\}$$

$$= \theta RL^{-1}y \circ \big\{I\theta I \cdot IRL^{-1}y \circ [y \circ (z \circ y)]\big\}$$

$$= \theta RL^{-1}y \circ \{I\theta RL^{-1}y \circ [y \circ (z \circ y)]\} = y \circ (z \circ y).$$

Consequently, (5.38) has been proved, along with the equation(5.27). The equation (5.28) can be proved in similar fashion.

4°. Autotopies of IP-quasigroups and IP-loops

We begin with a general statement that applies to any quasigroup $Q(A)$. For $\sigma \in \mathfrak{S}_3$, recall the notion of the corresponding quasigroup ${}^{\sigma}A$ inverse to the quasigroup A (see Chapter I, 4°).

Lemma 5.2. *If T is an autotopy of a quasigroup A, then ${}^{\sigma}T$ is an autotopy of the quasigroup ${}^{\sigma}A$.*

Indeed, let T be an autotopy of a quasigroup A, so

$$A^T = A.$$

Then, using Lemma 1.3, we have

$${}^{\sigma}(A^T) = ({}^{\sigma}A)^{\sigma^T},$$

whence

$$({}^{\sigma}A)^{\sigma^T} = {}^{\sigma}A. \tag{5.43}$$

We apply Lemma 5.2 to an IP-quasigroup A. By Lemma 5.1, the quasigroup ${}^{\sigma}A$ is isotopic to the quasigroup A,

$${}^{\sigma}A = A^S, \tag{5.44}$$

by an autotopy S. Let T be any autotopy of A. The equations (5.43) and (5.44) imply

$$(A^S)^{\sigma T} = A^S,$$

whence

$$A^{S(\sigma T)S^{-1}} = A.$$

In other words, $S(\sigma T)S^{-1}$ is an autotopy of A.

If $A^{\sigma} = A^{-1}$, then $S = P_l = (I_l, 1, 1)$ and $\sigma(\alpha, \beta, \gamma) = (\alpha, \beta, \gamma)$. Consequently,

$$S(\sigma T)S^{-1} = P_l(\sigma T)P_l^{-1} = (I_l, 1, 1)(\alpha, \beta, \gamma)(I_l^{-1}, 1, 1) = (I_l\alpha I_l^{-1}, \gamma, \beta).$$

But $I_l^2 = 1$, so

$$S(\sigma T)S^{-1} = (I_l\alpha I_l^{-1}, \gamma, \beta).$$

Summarizing, we have the following.

Lemma 5.3. *Let $Q(A)$ be an IP-quasigroup. If $T = (\alpha, \beta, \gamma) \in \mathfrak{A}_A$, where $\mathfrak{A}_A$ is the autotopy group of the quasigroup $Q(A)$, then:*

$$(I_l\alpha I_l, \gamma, \beta) \in \mathfrak{A}_A, \ \ (\gamma, I_r\beta I_r, \alpha) \in \mathfrak{A}_A.$$

Corollary 1. *Let $Q(A)$ be an IP-quasigroup. If $T = (\alpha, \beta, \gamma) \in \mathfrak{A}_A$, then:*

$$(\beta, I_r\gamma I_r, I_l\alpha I_l) \in \mathfrak{A}_A \ \ \textit{since} \ \ (I_l\alpha I_l, \gamma, \beta) \in \mathfrak{A}_A;$$

$$(I_l\beta I_l, I_l\alpha I_l, I_r\gamma I_r) \in \mathfrak{A}_A \ \ \textit{since} \ \ (\beta, I_r\gamma I_r, I_l\alpha I_l) \in \mathfrak{A}_A;$$

$$(I_l\gamma I_l, \alpha, I_r\beta I_r) \in \mathfrak{A}_A \ \ \textit{since} \ \ (\gamma, I_r\beta I_r, \alpha) \in \mathfrak{A}_A; \ \ \textit{and}$$

$$(I_r\beta I_r, I_r\alpha I_r, I_l\gamma I_l) \in \mathfrak{A}_A \ \ \textit{since} \ (I_l\gamma I_l, \alpha, I_r\beta I_r) \in \mathfrak{A}_A.$$

Corollary 2. *Let A be an IP-loop and $(\alpha,\beta,\gamma) \in \mathfrak{A}_A$. Then $(I\alpha I,\gamma,\beta)$, $(\gamma,I\beta I,\alpha)$, $(\beta,I\gamma I,I\alpha I)$, $(I\gamma I,\alpha,I\beta I)$, and $(I\beta I,I\alpha I,I\gamma I)$ are also autotopies of A.*

Consider an IP-loop $Q(\cdot)$. If $T=(\alpha,\beta,\gamma)\in\mathfrak{A}_A$ and

$$\alpha 1 = l, \qquad \beta 1 = k,$$

then, as shown in Chapter 2, 3°, we have

$$T=(R_k^{-1},L_l^{-1},1)\gamma$$

and

$$\alpha = R_k^{-1}\gamma,\ \ \beta = L_l^{-1}\gamma. \tag{5.45}$$

The equality $(\cdot)^T=(\cdot)$ implies

$$(\cdot)^{(R_k^{-1}L_l^{-1},1)} = (\cdot)^{\gamma^{-1}},$$

i.e. the isotope $(\cdot)^{(R_k^{-1}L_l^{-1},1)}$ is an IP-loop which is isomorphic to $(\cdot)$. Thus, as shown in the preceding section, $a=k^{-1}=(\beta 1)^{-1}$ is a right, and $b=l^{-1}=(\alpha 1)^{-1}$ is a left Moufang element of the loop $Q(\cdot)$, respectively. In other words, the identities

$$(xa\cdot y)a = x(a\cdot ya), \tag{5.46}$$

and

$$b(x\cdot by) = (bx\cdot b)y. \tag{5.47}$$

hold in the loop $Q(\cdot)$.

As previously noted, the identities (5.29) and (5.30) are equivalent in a loop $Q(\cdot)$. We now confirm the validity of this assertion. To that end, we prove a more general result.

Theorem 5.6. *The set M_l of all left Moufang elements of an IP-loop $Q(\cdot)$ is a subloop of $Q(\cdot)$. The subloop $M_l(\cdot)$ coincides with the subloop $M_r(\cdot)$ of right Moufang elements.*

Let a be a right Moufang element. Then (5.46) implies that $R_a(R_ax\cdot y)=x\cdot L_aR_ay$, so $T_a=(R_a^{-1},L_aR_a,R_a)$ is an autotopy of the loop $Q(\cdot)$. By Corollary 2 of Lemma 5.3, it is seen that $T_a^{'}=(IR_a^{-1}I,R_a,L_aR_a)$ is also an autotopy. Consequently, $(R_a1)^{-1}=a^{-1}$ is also a right Moufang element.

Now consider $a_1,a_2\in M_r$. We show that $a_1a_2\in M_r$. The product

$$T_{a_1}T_{a_2}=(R_{a_1}^{-1}R_{a_2}^{-1},L_{a_1}R_{a_1}L_{a_2}R_{a_2},R_{a_1}R_{a_2}),$$

is an autotopy of $Q(\cdot)$. Then by Corollary 2 of Lemma 5.3, we have $T^{''}=(IR_{a_2}R_{a_2}I,R_{a_1}^{-1}R_{a_2}^{-1},IL_{a_1}R_{a_2}L_{a_2}R_{a_2}I)\in\mathfrak{A}_{(\cdot)}$, so $(R_{a_1}^{-1}R_{a_2}^{-1}1)^{-1}\in M_r$. But $(R_{a_1}^{-1}R_{a_2}^{-1}1)^{-1}=(R_{a_1^{-1}}R_{a_2^{-1}})^{-1}=(a_2^{-1}a_1^{-1})^{-1}=a_1a_2$, so $a_1a_2\in M_r$. In this way, we have shown that M_r is a subloop of the loop $Q(\cdot)$[4].

Now consider $a\in M_r$. Equation (5.46) implies

$$[(xa\cdot y)a]^{-1}=[x(a\cdot ya)]^{-1},$$

whence

$$a^{-1}(y^{-1}\cdot a^{-1}x^{-1}) = (a^{-1}y^{-1}\cdot a^{-1})x^{-1}$$

or

$$a^{-1}(y\cdot a^{-1}x) = (a^{-1}y\cdot a^{-1})x.$$

This means that $a^{-1}\in M_l$. Because a^{-1} can be an arbitrary element from M_r, we have shown that $M_r\subseteq M_l$. Similarly, we can prove that $M_r\subseteq M_l$, so $M_r = M_l$.

Remark. In view of Theorem 5.6, we may set $M_l = M_r = M$.

Corollary 1. *In an IP-loop $Q(\cdot)$ the identities*

$$(xy\cdot z)y = x(y\cdot zy) \tag{5.48}$$

and

$$y(x\cdot yz) = (yx\cdot y)z \tag{5.49}$$

are equivalent.

Indeed, $M_l = Q$ follows from the identity (5.48), from which the equality $M_r = Q$ follows, i.e., the identity (5.49) holds. Similarly, it is proved that (5.48) implies (5.49).

Remark. Consider an IP-loop $Q(\cdot)$. Because the concepts of right and left Moufang elements in IP-loops coincide, then an element $a\in Q$, which satisfies either of the equations (5.46) or equality (5.47) for every $x, y\in Q$, is called a *Moufang element*, and M is the said to be the *Moufang subloop* of the IP-loop $Q(\cdot)$.

Corollary 2. *If $T = (\alpha,\beta,\gamma)$ is an autotopy of an IP-loop $Q(\cdot)$, then $\alpha 1, \beta 1, \gamma 1$ are Moufang elements.*

Indeed, $k^{-1} = (\beta 1)^{-1}$ is a Moufang element, i.e., $k^{-1}\in M$. But then also $k\in M$. Similarly, we obtain $l\in M$. Further, we have $\gamma 1 = \gamma(1\cdot 1) = \alpha 1\cdot\beta 1 = lk$, so $\gamma 1\ \in M$.

We note that if

$$T = (\alpha,\beta,\gamma)$$

is an autotopy of an IP-loop $Q(\cdot)$, then all three components of the autotopy T are quasi-automorphisms of $Q(\cdot)$. This statement directly follows from Lemma 5.3.

Autotopies of an IP-loop can be described using pseudo-automorphisms (see Chapter III, 4°). We note that

$$\varphi 1 = 1 \ \text{ and } \varphi I = I\varphi \tag{5.50}$$

in the IP-loop $Q(\cdot)$, where φ is an arbitrary left (right) pseudo-automorphism. The first of the equalities (5.50) follows from Lemma 3.1. To prove the second, recall the definition (3.20) of a left pseudo-automorphism:

$$\varphi x(\varphi y\cdot c) = \varphi(xy)\cdot c.$$

Let $y = x^{-1}$. Then

$$\varphi x(\varphi x^{-1} \cdot c) = \varphi(xx^{-1}) \cdot c = \varphi 1 \cdot c = c,$$

whence because $Q(\cdot)$ is an IP-loop we obtain $\varphi x^{-1} = (\varphi x)^{-1}$, i.e., the second of the equalities (5.50).

There is no need to distinguish between left and right pseudo-automorphisms in IP-loops. We have

Lemma 5.4. *The respective groups of all right and all left pseudo-automorphisms coincide in an IP-loop $Q(\cdot)$.*

Proof. Let φ be a left pseudo-automorphism with companion a. Then by (3.20), $(\varphi, R_a\varphi, R_a\varphi)$ is an autotopy of $Q(\cdot)$. By Corollary 2 of Lemma 5.3, $S = (IR_a\varphi I, I\varphi I, IR_a\varphi I)$ is also an autotopy of the loop $Q(\cdot)$. Because $\varphi I = I\varphi$ and $I^2 = 1$, the autotopy S takes the form $S = (IR_a\varphi I, \varphi, IR_a\varphi I)$. Further, using the equation (5.11), we find $S = (L_{a^{-1}}\varphi, \varphi, L_{a^{-1}}\varphi)$, so φ is a right pseudo-automorphism with companion a^{-1}. □

Remark. Consider a pseudo-automorphism φ. The element a from $(\varphi, R_a\varphi, R_a\varphi)$ is called a *left companion*, and the element a^{-1} from $(L_{a^{-1}}\varphi, \varphi, L_{a^{-1}}\varphi)$ is called a *right companion*.

Lemma 5.5. *If $T = (\alpha, \beta, \gamma)$ is an autotopy of an IP-loop $Q(\cdot)$, and $\alpha 1 = 1$, then α is a pseudo-automorphism of the loop $Q(\cdot)$ with left companion $\beta 1 = k$.*

Indeed, let $(\cdot)^T = (\cdot)$, where $T = (\alpha, \beta, \gamma)$ Then, as proved in Chapter II, 3°, the autotopy T takes the form

$$T = (R_k^{-1}, L_l^{-1}, 1)\gamma,$$

where $\beta 1 = k$, $\alpha 1 = l$ and

$$\beta = L_l^{-1}\gamma, \ \alpha = R_k^{-1}\gamma. \tag{5.51}$$

But $L_l = L_{\alpha 1} = L_1 = 1$, so $\beta = \gamma$. Consequently, in view of (5.51), we obtain

$$T = (\alpha, \beta, \gamma) = (\alpha, \gamma, \gamma) = (\alpha, R_k\alpha, R_k\alpha),$$

so α is a pseudo-automorphism with a companion k.

Corollary. *The left and right companions of pseudo-automorphisms of IP-loops are Moufang elements* [5].

Indeed, suppose that φ is a pseudo-automorphism of an IP-loop $Q(\cdot)$ with a right companion c, i.e., $T = (L_c\varphi, \varphi, L_c\varphi)$ is an autotopy of the loop $Q(\cdot)$. By Corollary 2 of Theorem 5.6, the element $L_c\varphi 1 = L_c 1 = c$ must be a Moufang element.

Let us begin to identify the structure of IP-loop autotopies.

Let $T = (\alpha, \beta, \gamma)$ be an autotopy of an IP-loop $Q(\cdot)$. Then from Corollary 2 of Lemma 5.3 we have that $T_1 = (I_\alpha I, \gamma, \beta)$ belongs to the group of autotopies $\mathfrak{A}_{(\cdot)}$. Consequently, $T_1 T^{-1} \in \mathfrak{A}_{(\cdot)}$. But

$$T_1 T^{-1} = (I_\alpha I, \gamma, \beta)(\alpha^{-1}, \beta^{-1}, \gamma^{-1}) = (I_\alpha I_{\alpha^{-1}}, \gamma\beta^{-1}, \beta\gamma^{-1}),$$

whence in view of equation(5.45) we have

$$T_1 T^{-1} = (I_\alpha I_{\alpha^{-1}}, L_l, L_l^{-1}).$$

Applying Corollary 2 of Lemma 5.3 to $T_1 T^{-1}$ yields

$$T_2 = (L_l^{-1}, IL_l I, I_\alpha I_{\alpha^{-1}}) \in \mathfrak{A}_{(\cdot)},$$

which by virtue of (5.11) implies

$$T_2 = (L_l^{-1}, R_l^{-1}, I_\alpha I_{\alpha^{-1}}),$$

and hence

$$T_2^{-1} = (L_l, R_l, \alpha I \alpha^{-1} I) = (L_l, R_l, S) \in \mathfrak{A}_{(\cdot)}.$$

Let us determine S. We have

$$S_x = S(x1) = L_l x \cdot R_l 1 = lx \cdot l = R_l L_l x,$$

i.e., $S = R_l L_l$. Moreover, we have

$$S = R_l L_l = L_l R_l,$$

because $R_l L_l x = l \cdot xl = l1 \cdot xl = L_1 1 \cdot R_l x = S(1 \cdot x) = Sx$. Thus,

$$T_2^{-1} = (L_l, R_l, L_l R_l) \in \mathfrak{A}_{(\cdot)}.$$

Finally, we consider the autotopy $T_2 T$:

$$T_2 T = (L_l^{-1}, R_l^{-1}, R_l^{-1} L_l^{-1})(\alpha, \beta, \gamma) = (L_l^{-1}\alpha, R_l^{-1}\beta, R_l^{-1} L_l^{-1}\gamma).$$

The permutation L_l^{-1} leaves 1 invariant:

$$L_l^{-1}\alpha 1 = L_l^{-1} l = 1.$$

By Lemma 5.5, the permutation $\theta = L_l^{-1}\alpha$ is a pseudo-automorphism with companion

$$R_l^{-1}\beta 1 = c,$$

a Moufang element. Therefore, the autotopy $T_2 T$ must have the form

$$T_2 T = (\theta, R_c\theta, R_c\theta).$$

We then have

$$T = T_2^{-1}(\theta, R_c\theta, R_c\theta)$$

or

$$\begin{aligned} T = (\alpha, \beta, \gamma) &= (L_l, R_l, R_l L_l)(\theta, R_c\theta, R_c\theta) \\ T &= (L_l\theta, R_l R_c\theta, L_l R_l R_c\theta). \end{aligned} \tag{5.52}$$

Thus, the following theorem has been proved.

Theorem 5.7. *Each autotopy T of an IP-loop $Q(\cdot)$ takes the form*

$$T = (L_l\theta, R_lR_c\theta, L_lR_lR_c\theta),$$

where θ is a pseudo-automorphism, c is a companion of θ, and l is a Moufang element.

Applied to a group $Q(\cdot)$, we have

$$T = (L_l\theta, R_d\theta, L_lR_d\theta) = (L_l, R_d, L_lR_d)\theta,$$

in Theorem 5.7, where $R_lR_c = R_{lc} = R_d$, and θ is a automorphism.

5°. WIP-loops[6]

In an IP-loop the identities

$$\left.\begin{array}{l} y(xy)^{-1} = x^{-1}, \\ (xy)^{-1}x = y^{-1} \end{array}\right\} \tag{5.53}$$

hold.

In connection with these identities, Baer introduced the following notion [35]:

Definition 4. A loop $Q(\cdot)$ is called a *loop with the weak inverse property* or *WIP-loop* if it satisfies the identity

$$y \cdot I(xy) = Ix, \tag{5.54}$$

where $I_y = y^{-1}$ is an inverse element for y: $yy^{-1} = 1$.

By the equality (5.53), each IP-loop is a WIP-loop. Let us consider some simple properties of WIP-loops:

a) The permutation I^2 is an automorphism of a WIP-loop.

Indeed, $I(y \cdot I(xy)) = I^2x$, so

$$I(xy) \cdot I(y \cdot I(xy)) = I(xy) \cdot I^2x,$$

whence in view of (5.54) we obtain

$$I_y = I(xy) \cdot I^2x. \tag{5.55}$$

From this, the statement easily follows:

$$I^2x \cdot I^2y = I^2x \cdot I(I(xy) \cdot I^2x) = I(I(xy)) = I^2(xy).$$

b)

$$I^{-1}(xy) \cdot x = I^{-1}y. \tag{5.56}$$

We obtain this equality by applying the automorphism I^{-2} to (5.55). Similarly, it is proved that (5.56) implies (5.54).

c) A loop $Q(\cdot)$ is a WIP-loop if and only if $xy \cdot z = 1$ implies $x \cdot yz = 1$.

Indeed, if $xy\cdot z=1$, then $z=I(xy)$, and $x\cdot yz=1$ implies $yz=Ix$. Thus, $y\cdot I(xy)=Ix$. The converse statement is also easily proved.

d)

$$L_y^{-1}=IR_yI^{-1},\quad R_y^{-1}=I^{-1}L_yI. \tag{5.57}$$

Indeed, using translations, the equality (5.54) takes the form

$$L_yIR_yx=Ix,$$

which implies the first of the equalities (5.57).

e) A WIP-loop $Q(\cdot)$ is characterized by the equality

$$[^{-1}(\cdot)]^{-1}=(\cdot)^{(I^{-1},1,I^{-1})}=(\cdot)^S, \tag{5.57}$$

or

$$^{-1}[(\cdot)^{-1}]=(\cdot)^{(1,I,I)}.$$

Note that (5.54) implies $y=^{-1}(\cdot)(Ix,I(xy))$, whence we obtain

$$[^{-1}(\cdot)]^{-1}(Ix,y)=I(xy),$$

i.e., the equality (5.58).

f) If $T=(\alpha,\beta,\gamma)$ is an autotopy of a WIP-loop $Q(\cdot)$, then

$$T_1=(I\,^{-1}\gamma I,\alpha,I^{-1}\beta I)\ \text{ and }\ T_2=(\beta,I\gamma I^{-1},I\alpha I^{-1})$$

are also autotopies.

Using Lemma 5.2 we have that $\sigma T=(\alpha,\beta,\gamma)$ is an autotopy for $[^{-1}(\cdot)]^{-1}=\,^{\sigma}(\cdot)$, whence by (5.58) we find

$$[(\cdot)^S]^{T^{lr}}=(\cdot)^S.$$

Thus,

$$T_1=ST^{lr}S^{-1}=(I^{-1},1,I^{-1})(\gamma,\alpha,\beta)(I,1,I)=(I^{-1}\gamma I,\alpha,I^{-1}\beta I)$$

is an autotopy of the WIP-loop $Q(\cdot)$. Applying the transformation $T\to T_1$ to T_1, we obtain the autotopy T_2.

g) The equations $ax=b$ and $ya=b$ have respective solutions $x=I(I^{-1}b\cdot a)$ and $y=I^{-1}(a\cdot Ib)$.

This follows from the equalities (5.54) and (5.56).

Notes

[1]The concepts of IP-quasigroup and IP-loop were introduced by Bruck [24, 25]. Elementary properties of IP-quasigroups can be found in [24]. One special kind of IP-loop was studied by Ginzburg [41]

[2]One can show that the identities (5.27) and (5.28) in a quasigroup Q (*) are equivalent. Thus, a Moufang quasigroup can be defined as a quasigroup satisfying just one of the identities (5.27) or (5.28).

[3]This statement generalizes a result of Bruck [24, Theorem 3], where $xy = Rx \circ Ly$.

[4]The definition of a subloop requires verification that for given a, b, the equations $ax = b$ and $ya = b$ are solvable. But because $Q(\cdot)$ is an IP-loop, closure under inversion suffices for this purpose.

[5]The converse statement, generally speaking, is not true, i.e., not every Moufang element is a companion (left or right) of some pseudo-automorphism. Indeed, in a Moufang loop $Q(\cdot)$ (see Definition 3), every element is a Moufang element. If they were all left companions of pseudo-automorphisms, then, by virtue of Lemma 5.4., the loop $Q(\cdot)$ would be a G-loop (see Definition 4, Chapter III). In particular, non-associative commutative Moufang loops would be G-loops, contradicting Theorem 10.1.

[6]Loops with the weak inverse property (WIP-loops) were studied in detail by Osborne [57]. In particular, an example of a WIP-loop which is a G-loop (see Chapter III, 4°) is constructed in [57]. This example is reproduced in Chapter X, where other properties of WIP-loops are also proved.

Chapter VI. Moufang Loops

1°. The main properties of Moufang loops

The most studied class of nonassociative loops is the class of Moufang loops[1]. As we saw above (see Chapter V, 3°, (5.29) and (5.30) and Corollary 1 of Theorem 5.6), a loop $Q(\cdot)$ is called a *Moufang loop* if it satisfies one of the (*Moufang identities*)

$$x(y \cdot xz) = (xy \cdot x)z, \tag{6.1}$$

$$(zx \cdot y)x = z(x \cdot yx). \tag{6.2}$$

By Theorem 5.3, *every Moufang loop is an IP-loop.* In addition, in a Moufang loop the following identities hold:

$$x \cdot xz = xx \cdot z \quad \text{(left alternativity)}, \tag{6.3}$$

$$zx \cdot x = z \cdot xx \quad \text{(right alternativity)}, \tag{6.4}$$

$$xy \cdot x = x \cdot yx \quad \text{(flexibility)}. \tag{6.5}$$

Equations (6.3) and (6.4) follow from (6.2) and (6.1) with $y = 1$, while equation (6.5) follows from (6.1) with $z = 1$.

From the Moufang identities (6.1) and (6.2) in a Moufang loop $Q(\cdot)$ we obtain the equalities

$$R_y(R_yx \cdot z) = x \cdot L_yR_yz, \quad \text{and} \quad L_y(x \cdot L_yz) = R_yL_yx \cdot z,$$

whence it follows that

$$S_y = (R_y^{-1}, L_yR_y, R_y) \tag{6.6}$$

and

$$K_y = (R_yL_y, L_y^{-1}, L_y) \tag{6.7}$$

are autotopies of $Q(\cdot)$. But if $S_y \in \mathfrak{A}_{(\cdot)}$, then Corollary 2 of Lemma 5.3 implies $P_y = (IR_y^{-1}I, R_y, L_yR_y) \in \mathfrak{A}_{(\cdot)}$.

In the third and fourth relations of (5.11),

$$R_a^{-1} = IL_aI, \quad \text{and} \quad L_a^{-1} = IR_aI$$

hold. Therefore, the autotopy P_y has the form

$$P_y = (L_yR_y, L_y, R_y), \tag{6.8}$$

whence

$$L_y x \cdot R_y z = L_y R_y (x \cdot z).$$

Consequently,

$$yx \cdot zy = y(xz \cdot y). \tag{6.9}$$

This is *the third identity that characterizes a Moufang loop, since it is equivalent to the identity* (6.1). Indeed, flexibility follows from (6.9) with $z = 1$. Next, a loop $Q(\cdot)$ satisfying the identity (6.9) is an IP-loop: If we set $y = {}^{-1}x$ in (6.9), where ${}^{-1}x \cdot x = 1$, we obtain

$$z \cdot {}^{-1}x = {}^{-1}x(xz \cdot {}^{-1}x),$$

or, by flexibility,

$$z \cdot {}^{-1}x = ({}^{-1}x \cdot xz) \cdot {}^{-1}x,$$

whence $z = {}^{-1}x \cdot xz$. Setting $y = z^{-1}$ in (6.9), we similarly obtain $xz \cdot z^{-1} = x$. Thus, $Q(\cdot)$ is an IP-loop, and all the transitions from S_y to P_y are invertible. The identity (6.9) is also called a *Moufang identity*. We have proved the following lemma [31].

Lemma 6.1. *A Moufang loop if and only if* (6.9) *holds in* $Q(\cdot)$.[2]

Thus, *the Moufang identities* (6.1), (6.2) and (6.9) *are equivalent*, and each of these identities can be taken as the basis for a definition of a Moufang loop.

Now, let $Q(\cdot)$ be a Moufang loop, and let $Q(\circ)$ be an arbitrary loop which is isotopic to $Q(\cdot)$:

$$(\circ) = (\cdot)^T.$$

Since $Q(\cdot)$ is a Moufang loop (and consequently also a Moufang quasigroup), then every loop isotopic to $Q(\cdot)$ is an IP-loop. Therefore, $Q(\circ)$ is an IP-loop.

Let $Q(*)$ be an arbitrary loop is isotopic to the loop $Q(\circ)$:

$$(\bullet) = (\circ)^S.$$

Then $(*) = (\circ)^S = ((\cdot)^T)^S = (\cdot)^{TS}$, i.e. $Q(*)$ is also an IP-loop as an isotope of the Moufang loop $Q(\cdot)$. But then $Q(\circ)$ is a Moufang quasigroup, i.e. a Moufang loop. Thus, we have proved the following theorem.

Theorem 6.1. *Each loop isotopic to a Moufang loop is itself a Moufang loop.*

Theorem 6.1 can be made more specific.

Theorem 6.2. *Let* $Q(\cdot)$ *be a Moufang loop. Then each of its loop isotopes is isomorphic to a loop* $Q(\circ)$ with

$$x \circ y = xl \cdot l^{-1}y,$$

where l is a particular element of Q.

Proof. By Chapter I, 3°, a loop $Q(\bullet)$ isotopic to the loop $Q(\cdot)$ has the form $(\bullet) = (\cdot)^{\gamma}_{a,b}$, whence

$$(\bullet)^{\gamma^{-1}} = (\cdot)_{a,b} = (\cdot)^{(R_a^{-1}, L_b^{-1}, 1)}.$$

Consider the loop $(\circ) = (\bullet)^{\gamma^{-1} R_e}$, where $e = ba$. Then

$$(\circ) = (\cdot)^{(R_a^{-1}, L_a^{-1}, 1) R_e} = (\cdot)^{(R_{a^{-1}} R_e, L_{b^{-1}} R_e, R_e)},$$

or in expanded form

$$x \circ y = R_e^{-1}(R_{a^{-1}} R_e x \cdot L_{b^{-1}} R_e y).$$

Therefore,

$$x \circ y = [(xe \cdot a^{-1})(b^{-1} \cdot ye)]e^{-1}. \tag{6.10}$$

However, $uv \cdot e^{-1} = [(ue \cdot e^{-1})v]e^{-1}$, and by the Moufang identity (6.2)

$$uv \cdot e^{-1} = ue \cdot e^{-1} v e^{-1}.$$

Applying the latter equality to (6.10),

$$x \circ y = [(xe \cdot a^{-1})e](e^{-1}[(b^{-1} \cdot ye)e^{-1}]).$$

Now, using (6.2) and (6.9),

$$x \circ y = (x \cdot ea^{-1})[(e^{-1}b^{-1})(ye \cdot e^{-1})].$$

But

$$ea^{-1} = (ba \cdot a^{-1})(ba) = b(ba) = b^2 a = l,$$

so

$$e^{-1}b^{-1} = (be)^{-1} = (b \cdot be)^{-1} = l^{-1}.$$

Thus,

$$x \circ y = xl \cdot l^{-1} y.$$

Since the loop $(\bullet)$ is isomorphic to the loop $(\circ)$, namely $(\bullet) = (\circ)^{R_e^{-1}\gamma}$, the proof of the theorem is complete. □

The question of the nuclei of a Moufang loop arises, and is answered by a more general theorem.

Theorem 6.3. *The nuclei of any IP-loop $Q(\cdot)$ coincide.*

Indeed, suppose $a \in N_l$:

$$ax \cdot y = a \cdot xy. \tag{6.11}$$

Then by (5.6) we obtain

$$y^{-1} \cdot x^{-1} a^{-1} = y^{-1} x^{-1} \cdot a^{-1},$$

i.e., $a^{-1} \in N_r$, whence also $a \in N_r$. Thus,

$$N_l \subseteq N_r.$$

The reverse inclusion is proved similarly, and then

$$N_l = N_r.$$

From (6.11), the equality

$$y = (ax)^{-1}(ax \cdot y)$$

or

$$y = (a^{-1}x^{-1})(ax \cdot y) \tag{6.12}$$

is obtained. Suppose $x = (pa)^{-1}$ and $y = pa \cdot q$, so $xy = q$. Substituting these expressions of x and y into (6.12), we obtain

$$pa \cdot q = (pa \cdot a^{-1})(aq)$$

or

$$pa \cdot q = p \cdot aq. \tag{6.13}$$

Since p and q, along with x and y, may simultaneously be arbitrary elements of Q, we have shown that $N_l \subseteq N_m$. Since the transition from (6.11) to (6.13) is reversible, we have also shown that $N_m \subseteq N_l$, whence $N_l = N_m$.

Thus, in any IP-loop, we may simply speak of the *nucleus* $N = N_l = N_m = N_r$.

2°. Inner permutations of a Moufang loop

Consider the inner permutations of a Moufang loop $Q(\cdot)$ with neutral element 1. We will consider only $I = I_1$, the group of inner permutations relative to 1, so we have (see Chapter IV, 3°):

$$\left.\begin{aligned} R_{x,y} &= R_{xy}^{-1} R_y R_x, \\ L_{x,y} &= L_{xy}^{-1} L_x L_y, \\ T_x &= L_x^{-1} R_x. \end{aligned}\right\} \tag{6.14}$$

The equalities (6.14) are obtained from (4.4) and (4.6), setting $h = 1$. In this case we have $a \bullet b = a \circ b = ab$ — compare (4.3).

Remark. *In an arbitrary lP-loop (and in particular in any Moufang loop), the inner permutations $R_{x,y}$ and $L_{x,y}$ are related by the relationship*

$$L_{x,y} = I R_{y^{-1},x^{-1}} I, \tag{6.15}$$

using $Ix = x^{-1}$. Indeed, according to (5.11),

$$L_a = I R_a^{-1} I = I R_{a^{-1}} I,$$

whence

$$L_{x,y} = I R_{xy} I \cdot I R_x^{-1} I \cdot I R_y^{-1} I = I R_{xy} R_x^{-1} R_y^{-1} I = I R_{y^{-1}x^{-1}}^{-1} R_{x^{-1}} R_{y^{-1}} I = I R_{y^{-1},x^{-1}} I.$$

Theorem 6.4. *Each inner permutation of a Moufang loop $Q(\cdot)$ is a pseudo-automorphism of $Q(\cdot)$* [31].

It suffices to prove the theorem for the inner permutations T_x, $R_{x,y}$, and $L_{x,y}$.

We consider the autotopies S_y, K_y and P_y of the loop $Q(\cdot)$ defined by the equalities (6.6) – (6.8). Then $P_y^{-1}S_y^{-1}$ is also an autotopy of $Q(\cdot)$. But

$$P_y^{-1}S_y^{-1} = (L_y^{-1}, R_y^{-1}, R_y^{-1}L_y^{-1})(R_y, R_y^{-1}L_y^{-1}, R_y^{-1})$$
$$= (T_y, L_y^{-1}R_y^{-2}, L_y^{-1}R_y^{-2}),$$

since $L_yR_y = R_yL_y$ by the flexibility (6.5). Applying Lemma 5.5, we conclude that T_y is a pseudo-automorphism.

Now

$$S_{xy}S_y^{-1}S_x^{-1} = (R_{xy}^{-1}, L_{xy}R_{xy}, R_{xy})(R_y, L_y^{-1}R_y^{-1}, R_y^{-1})(R_x, L_x^{-1}, R_x^{-1}, R_x^{-1}),$$

$$S_{xy}S_y^{-1}S_x^{-1} = (R_{xy}^{-1}R_yR_x, \lambda, \mu),$$

for certain permutations λ, μ of Q. Consequently,

$$S_{xy}S_y^{-1}S_x^{-1} = (R_{x,y}, \lambda, \mu), \tag{6.16}$$

Because $S_{xy}\ S_y^{-1}\ S_x^{-1}$ is an autotopy of the loop $Q(\cdot)$, and $R_{x,y}1 = 1$, we can apply Lemma 5.5 again: $R_{x,y}$ is a pseudo-automorphism of the loop $Q(\cdot)$. Similarly, we can prove that $L_{x,y}$ is also a pseudo-automorphism of the loop $Q(\cdot)$.

Corollary 1. Lemma 5.5 implies that $L_y^{-1}R_y^{-2}1$ is a left companion for T_y, i.e., $y^{-1}(1y^{-2}) = y^{-3}$, and the right companion is the element y^3 (see the remark to Lemma 5.4).

Further, by virtue of Lemma 5.5, $\lambda = \mu$ in (6.16), and the pseudo-automorphism $R_{x,y}$ has $\omega = \mu 1$ as its left companion. As it is evident from (6.16), $\mu = R_{xy}R_y^{-1}R_x^{-1}$, and consequently,

$$\omega = R_{xy}R_y^{-1}R_x^{-1}1 = R_{xy}R_{y^{-1}}R_{x^{-1}}1 = (x^{-1}y^{-1})(xy).$$

The element $\omega = (x^{-1}y^{-1})(xy)$ is called the *commutator* of the elements x and y, denoted by (x, y). Thus, $R_{x,y}$ has the commutator (x, y) as its left companion.

Corollary 2. Since $R_{x,y}$ is a pseudo-automorphism, $IR_{x,y} = R_{x,y}I$. Then, using (6.15), we have

$$L_{x,y} = R_{y^{-1},x^{-1}}. \tag{6.17}$$

Corollary 3. *In a commutative Moufang loop, each inner permutation is an automorphism.*[3]

Indeed, by commutativity $T_x = L_x^{-1}R_x = R_x^{-1}R_x = 1$. The inner permutation $R_{x,y}$ is a pseudo-automorphism with left companion $(x, y) = (x^{-1}y^{-1})(xy) = (yx)^{-1}(xy)$. But in a commutative Moufang loop $(x, y) = 1$, so $R_{x,y}$ is an automorphism. By (6.17), $L_{x,y}$ is also an automorphism.

Lemma 6.2. *The nucleus N of a Moufang loop is a normal subloop.*

According to Theorem 4.5, we must prove that N is invariant with respect to the group I of inner permutations. Let $\varphi \in I$. As was proved above (see Theorem 6.4), φ is a pseudo-automorphism with a right companion c, i.e., $(\varphi, R_c\varphi, R_c\varphi)$ is an autotopy of the loop $Q(\cdot)$. Let $a \in N$. Then

$$ax \cdot y = a \cdot xy.$$

Consequently,

$$\varphi(ax \cdot y) \cdot c = \varphi(ax) \cdot (\varphi y \cdot c) = \varphi a[\varphi(xy) \cdot c] = \varphi a \cdot [\varphi x \cdot (\varphi y \cdot c)],$$

whence

$$\varphi(ax) \cdot (\varphi y \cdot c) = \varphi a \cdot [\varphi x \cdot (\varphi y \cdot c)], \tag{6.18}$$

If $y = \varphi^{-1}c^{-1}$, then from (6.18) we obtain

$$\varphi(ax) = \varphi a \cdot \varphi x, \tag{6.19}$$

so (6.18) takes the form

$$(\varphi a \cdot \varphi x)(\varphi y \cdot c) = \varphi a \cdot [\varphi x \cdot (\varphi y \cdot c)].$$

Replacing φx and $\varphi y \cdot c$ with x and y respectively, we find

$$(\varphi a \cdot x)y = \varphi a \cdot xy,$$

i.e., $\varphi a \in N$. This completes the proof of the lemma.

A pseudo-automorphism φ in a Moufang loop has the following property:

$$\varphi(xyx) = \varphi x \cdot \varphi y \cdot \varphi x. \tag{6.20}$$

Indeed, there exists an element c such that

$$\varphi(xy) \cdot c = \varphi x \cdot (\varphi y \cdot c),$$

i.e., c is a right companion of the pseudo-automorphism φ. Then

$$\varphi(xyx) \cdot c = \varphi x \cdot (\varphi(yx) \cdot c) = \varphi x \cdot (\varphi y \cdot (\varphi x \cdot c)) = (\varphi x \cdot \varphi y \cdot \varphi x) \cdot c.$$

This equalities imply (6.19).

Following Bruck [31], we present the following.

Definition 1. A self-map φ of a Moufang loop satisfying (6.20) and $\varphi 1 = 1$ is called a *semi-endomorphism.*

Thus, in a Moufang loop: *Every pseudo-automorphism (and, hence, every inner permutation) is a semi-automorphism.*[4]

Note that each semi-endomorphism of a Moufang loop satisfies

$$\varphi x^{-1} = (\varphi x)^{-1}. \tag{6.21}$$

Indeed, if we set $y = x^{-1}$ in (6.20), then we obtain

$$\varphi x = \varphi(xx^{-1}x) = \varphi x \cdot \varphi x^{-1} \cdot \varphi x,$$

whence $\varphi x^{-1}\varphi x = 1$, $(\varphi x)^{-1} = \varphi x^{-1}$.

The autotopies of a Moufang loop are described by Theorem 5.7: *Each autotopy T of the Moufang loop has the form*

$$T = (L_x\theta, R_xR_c\theta, L_xR_xR_c\theta),$$

where x is an arbitrary element of Q, and θ is an arbitrary pseudo-automorphism of the loop $Q(\cdot)$ with a right companion c.

3°. Moufang's Theorem

The purpose of this section is to prove the following (*Moufang's theorem*).

Theorem 6.5. *If three elements a, b, c of a Moufang loop are connected by the law of associativity,*

$$ab \cdot c = a \cdot bc,$$

then the subloop H generated by the elements a, b, c is associative.

We will prove this theorem following Bruck [31]. For this, we need a series of lemmas.

Lemma 6.3. *Let $Q(\cdot)$ be a Moufang loop, S a non-empty set of semi-endomorphisms, F the set of all elements of Q which are invariant under each semi-endomorphism from S, and M the set of all elements m such that $mf \in F$ for each element f of F. Then:* 1) $1 \in M \subseteq F$; 2) $F = F^{-1} = \{f^{-1} \mid f \in F\}$ *and* $fFf = F$ *for every* $f \in F$; *and* 3) M *is a subloop of the loop* $Q(\cdot)$.

Proof. 1. By the definition of a semi-endomorphism φ we have $\varphi 1 = 1$, that is, $1 \in F$ and, evidently, $1 \in M$. But then $M1 \subseteq F$, i.e., $M \subseteq F$.

2. If $f \in F$, then in view of (6.21) we have

$$\varphi f^{-1} = (\varphi f)^{-1} = f^{-1}, \quad \text{i.e.,} \quad f^{-1} \in F.$$

Let f_1 be an arbitrary element of F. Then

$$\varphi(ff_1f) = \varphi f\varphi f_1\varphi f = ff_1f, \quad \text{i.e.,} \quad ff_1f \in F.$$

Conversely, suppose that $fxf = f_1$. Then $x = f^{-1}f_1f^{-1}$, i.e., $x \in F$. The equality $fFf = F$ follows.

3. Suppose that $m_1, m_2 \in M$. Then $m = m_1(m_2(m_1f^{-1})^{-1})m_1 \in F$, since

$$m_1 \in M \subset F, \quad m_1f^{-1} \in F, \quad \text{and } m_2(m_1f^{-1})^{-1} \in F.$$

But

$$m = (m_1 m_2)[(m_1 f^{-1})^{-1} m_1] = (m_1 m_2)(f m_1^{-1} \cdot m_1) = (m_1 m_2) f,$$

that is, $m_1 m_2 \in M$. Further

$$f(mf)^{-1} f \in F$$

or $f(f^{-1} m^{-1}) f \in F$ and $m^{-1} f \in F$, whence $m^{-1} \in M$. Consequently, M is a subloop of the loop $Q(\cdot)$.

The concept of an *associator* (a, b, c) plays an important role in Moufang loop theory. It is defined by

$$ab \cdot c = (a \cdot bc) \cdot (a, b, c),$$

where a, b, c are three elements arbitrary of the loop. The following two lemmas give some properties of Moufang loop associators.

Lemma 6.4. *If $(a, b, c) = 1$, then $(a', b', c') = 1$, where a', b', c' are obtained from a, b, c with some permutation, or replacement of some elements from a, b, c by their inverses.*

Proof. 1. Let $(a, b, c) = 1$. Then $Ua = a$, $Vb = b$, $Wc = c$, where U, V, W are certain inner permutations. Indeed, $ab \cdot c = a \cdot bc$ can be rewritten in the form $R_{b,c} a = a$, where $R_{b,c} = R_{bc}^{-1} R_c R_b$. Since $R_{b,c}$ is a pseudo-automorphism, $R_{b,c} a^{-1} = (R_{b,c} a)^{-1} = a^{-1}$, that is, $a^{-1} b \cdot c = a^{-1} \cdot bc$ or $(a^{-1}, b, c) = 1$. The equations

$$(a, b^{-1}, c) = (a, b, c^{-1}) = 1.$$

are proved similarly.

2. From $ab \cdot c = a \cdot bc$ it follows that

$$c^{-1} \cdot b^{-1} a^{-1} = c^{-1} b^{-1} \cdot a^{-1} \quad \text{or} \quad (c^{-1}, b^{-1}, a^{-1}) = 1.$$

From 1 we get $(c, b, a) = 1$. Further, from $ab \cdot c = a \cdot bc$ we have

$$bc \cdot a^{-1} = a^{-1}(a \cdot bc) a^{-1} = a^{-1}(ab \cdot c) a^{-1} = a^{-1}(ab \cdot c) a^{-1} = (a^{-1} \cdot ab) \cdot (ca^{-1}) = b \cdot ca^{-1},$$

that is, $(b, c, a^{-1}) = 1$, whence $(b, c, a) = 1$. From $(c, b, a) = (b, c, a) = 1$ it follows that $(a', b', c') = 1$, for a', b', c' an arbitrary permutation of the elements a, b, c. □

Lemma 6.5. *Suppose that elements a, b, c, d satisfy the equation $(x, y, z) = 1$. Then the following equations are equivalent:*

$1^\circ)$ $(ab, c, d) = 1$;
$2^\circ)$ $((ab)^2, c, d) = 1$;
$3^\circ)$ $((a, b), c, d) = 1$;
$4^\circ)$ $(cd, a, b) = 1$;
$5^\circ)$ $(bc, d, a) = 1$.

Proof. 1°) ⇒ 2°). The equality 1°) is equivalent to $U(ab) = ab$, where $U = R_{c,d}$ is an inner permutation (see the proof of Lemma 6.4) and, consequently, as proved above, U is a semi-automorphism. Thus,

$$U(ab)^2 = U(ab \cdot 1 \cdot ab) = U(ab) \cdot U1 \cdot U(ab) = (U(ab))^2 = (ab)^2,$$

whence 2°)*follows*.

2°) ⇒ 3°). Let $p = (a, b) = (a^{-1}b^{-1})(ab)$, that is,

$$ab = (ba)p, \qquad aba = (ba \cdot p)a = b \cdot apa.$$

We have

$$b \cdot apa \cdot b = aba \cdot b = (aba)(a^{-1} \cdot ab) = ab \cdot aa^{-1} \cdot ab = (ab)^2,$$

whence

$$U(ab)^2 = Ub \cdot U(apa) \cdot Ub = Ub\,(UaUpUa)\,Ub.$$

But $Ua = a$, $Ub = b$, since $(x, c, d) = 1$ for $x = a, b$. Consequently, $(ab)^2 = b(aUp \cdot a)b$, whence $Up = p$, that is, we obtain 3°).

3°) ⇒ 4°). In Corollary 1 to Theorem 6.4, it was proved that $V = R_{a,b}$ is a pseudo-automorphism with left companion $p = (a, b)$. Therefore, $V(cd)p = Vc \cdot (Vd \cdot p)$, whence $V(cd) \cdot p = c \cdot (dp)$. Here again $Vc = c$, $Vd = d$, since $(c, a, b) = (d, a, b) = 1$). But $(p, c, d) = 1$ by 3°) and, applying Lemma 6.4, we obtain $V(cd) \cdot p = cd \cdot p$, which implies $V(cd) = cd$, that is, the equality 4°).

4°) ⇒ 1°). It is enough to replace a, b, c, d by c, d, a, b respectively.

1°), 4°) ⇒ 5°). Note

$$(a \cdot bc)d = (ab \cdot c)d = ab \cdot cd$$

by 1°). Further, using the equality 4°) and $(b, c, d) = 1$, we find

$$ab \cdot cd = a(b \cdot cd) = a(bc \cdot d).$$

In this way, $(a \cdot bc)d = a(bc \cdot d)$, that is, $(a, bc, d) = 1$. Using Lemma 6.4, we obtain 5°).

5°) ⇒ 1°). Applying the transition 1°) ⇒ 5°) to $(bc, d, a) = 1$, we find the relationship $(cd, a, b) = 1$ which is equivalent to the equality 1°). □

Further, we use the following notation. Let $A, B, C \subseteq Q$. Then AB denotes the set of all products of the form ab for $a \in A$, $b \in B$, and (A, B, C) is the set of all associators of the form (a, b, c) for $a \in A$, $b \in B$, $c \in C$.

Let A be a subset of Q, and let P be a Moufang subloop of $Q(\cdot)$ containing a subset of A. We denote the set of all elements $x \in P$ such that $(A, x, P) = 1$ by A'. Then we have the following

Lemma 6.6. *The sets A' and $A^* = (A')'$ are subloops of the loop $Q(\cdot)$. Also*

$$(A, A, P) = 1 \tag{6.22}$$

implies

$$(A^*, A^*, P) = 1. \tag{6.23}$$

Proof. Let $B = A^{'}$, so

$$(A, B, P) = 1, \tag{6.24}$$

By Lemma 6.4, we obtain $B^{-1} = B$. Suppose $a \in A$, $b_1, b_2 \in B$, and $x \in P$. By (6.24), we have $(a, b_1, b_2) = 1$, and therefore

$$g = [(a \cdot b_1 b_2)x]b_2 = [(ab_1 \cdot b_2)x]b_2 = (ab_1)(b_2 x b_2).$$

But $b_2 x b_2 \in P$ (since $B \subset P$), so $(a, b_1, b_2, xb_2) = 1$ and

$$g = a[b_1(b_2 x b_2)] = a[(b_1 b_2 \cdot x)b_2].$$

Since $b_1, b_2 \in P$, we obtain $(a, b_2, b_1 b_2 \cdot x) = 1$ by (6.24). Thus, by Lemma 6.4, we obtain $(a, b_1 b_2 \cdot x, b_2) = 1$, i.e.,

$$g = [a(b_1 b_2 \cdot x)]b_2.$$

Consequently,

$$(a \cdot b_1 b_2)x = a(b_1 b_2 \cdot x),$$

i.e., $b_1, b_2 \in B$. Thus, B is a subloop and $A^* = B^{'} = (A^{'})^{'}$ is also a subloop of the loop $Q(\cdot)$.

If $(A, A, P) = 1$, then $A \subseteq A^{'}$. But $(A^{'}, (A^{'})^{'}, P) = 1$ or

$$(A^{'}, A^*, P) = 1. \tag{6.25}$$

In particular, $(A, A^*, P) = 1$, that is $A^* \subseteq A^{'}$. If now we place the subloop A^* in (6.25) instead of $A^{'}$, then we obtain (6.23). □

Corollary 1. *If we place $A^* \subseteq P$ in* (6.23) *instead of P, we obtain $(A^*, A^*, A^*) = 1$, so A^* is an associative subloop.*

Corollary 2. *If A satisfies the equality* (6.22)*, then $A \subset A^*$.* Indeed, it follows from (6.24) and Lemma 6.4 that $(B, A, P) = 1$. Thus, $A \subseteq B^{'}$, i.e., $A \subseteq (A^{'})^{'}$ or $A \subseteq A^*$.

Proof of Moufang's Theorem.[5] Let $ab \cdot c = a \cdot bc$, and let D be the set of three elements a, b, c. We define the following two subsets in Q:

$$F = \{x \mid (D, D, x) = (ab, c, x) = 1\}, \tag{6.26}$$

$$M = \{m \mid mF \subseteq F\}.$$

By Lemma 6.3, $M \subseteq F$, and M is a subloop of the loop $Q(\cdot)$. As the set S from Lemma 6.3, we take $\{R_{d,d'} \mid d, d^{'} \in D\}$. Since $(d, d^{'}, x) = 1$ or $(x, d, d^{'}) = 1$, we have $R_{d,d'}x = x$. By Lemma 6.4, we can permute the elements a, b, c in the definition of F.

1. By (6.26) and the alternative law, we have

$$(d, d, D) = (d, d, F) = (D, D, F) = 1,$$

where d stands for any of a, d, c. Besides,

$$(d, d, DF) = 1.$$

We apply Lemma 6.5 to d, d, D, F. Then

$$(d^2, D, F) = (dD, d, F) = (Dd, d, F) = 1. \tag{6.27}$$

Combining (6.26) with (6.27), we obtain

$$(DD, D, F) = 1. \tag{6.28}$$

2. From the hypothesis of the theorem and (6.26), we obtain

$$(D, D, D) = (D, D, F) = 1.$$

We apply Lemma 6.5 to D, D, D, F. Then (6.28) implies

$$(D, D, DF) = 1. \tag{6.29}$$

3. The equalities

$$(d, d, DD) = (d, d, F) = 1$$

are immediate, and from (6.28) we have

$$(DD, d, F) = 1.$$

Therefore, we can apply Lemma 6.5 to d, d, DD, F, and from the obvious equality $(d, d, DD \cdot F) = 1$ we obtain

$$(DD, d, dF) = 1. \tag{6.30}$$

4. In particular, the equalities (6.29) and (6.30) imply

$$(D, D, cF) = 1 \quad \text{and} \quad (ab, c, cF) = 1,$$

whence by the definition of F, we find that $cF \subseteq F$, i.e., $c \in M$. Similarly, we obtain $a, d \in M$, i.e., $D \subseteq M$. Since $M \subseteq F$, (6.26) implies $(D, D, M) = 1$. The assertion of Moufang's Theorem now follows from Lemma 6.6, if we take $P = M$, $A = D$ and apply Corollaries 1 and 2 of this lemma.

Corollary. *Any two elements a, b of a Moufang loop generate an associative subloop.*

Indeed, it suffices to apply Moufang's Theorem to the equality $aa \cdot b = a \cdot ab$.

A loop in which any two elements generate an associative subloop is said to be *diassociative* [31]. Thus, the preceding corollary can also be formulated as follows: *Moufang loops are diassociative.*

4°. Commutative Moufang loops

In this section we consider commutative Moufang loops. They can be characterized by the single identity

$$x^2 \cdot yz = xy \cdot xz. \tag{6.31}$$

for a loop $Q(\cdot)$. Indeed, let $y = 1$ in (6.31), so

$$x^2 \cdot z = x \cdot xz. \tag{6.32}$$

If $z = 1$, then

$$x^2 y = xy \cdot x. \tag{6.33}$$

Comparing (6.32) and (6.33), we obtain

$$x \cdot xy = xy \cdot x,$$

whence, replacing xy with y, we deduce the commutativity of the loop $Q(\cdot)$. By commutativity in (6.31) and (6.32), we find

$$x^2 \cdot yz = x(x \cdot yz) = x(yz \cdot x) = xy \cdot zx,$$

i.e., $Q(\cdot)$ is a Moufang loop.

Definition 2. An endomorphism φ of a loop $Q(\cdot)$ with nucleus $N = N_l = N_m = N_r$ is called *central* if $\varphi x \in N$ and $\varphi x \cdot y = y \cdot \varphi x$ for every x and $y \in Q$.

Lemma 6.7. *In a commutative Moufang loop $Q(\cdot)$, the mapping $x \to x^3$ is a central endomorphism.*

In other words, we must prove that x^3 lies in the nucleus N of the loop $Q(\cdot)$, and that

$$(xy)^3 = x^3 y^3. \tag{6.34}$$

By the corollary of Moufang's Theorem, the subloop generated by the elements x and y is associative and, naturally, commutative, so that (6.34) holds in it. Further, by Corollary 1 to Theorem 6.4, the inner permutation T_x is a pseudo-automorphism with left companion x^{-3}, that is, the equality

$$T_x(y \cdot z) \cdot x^{-3} = T_x y (T_x z \cdot x^{-3})$$

holds. But in a commutative loop $T_x = 1$, so

$$(yz)x^{-3} = y(zx^{-3}),$$

i.e., $x^{-3} \in N$. Consequently, x^{-3} is central.

Every loop isotopic to a commutative Moufang loop has the property of the mapping $x \to x^3$ formulated in Lemma 6.7. This assertion comes from the following theorem.

Theorem 6.6. *If the mapping $x \to x^3$ is a central endomorphism in a Moufang loop $Q(\cdot)$, then the property also holds in every loop isotopic to the loop $Q(\cdot)$.*

Proof. Suppose that for every $x, y \in Q(\cdot)$, we have $x^3 \in N$, $(xy)^3 = x^3 y^3$, and $x^3 y = y x^3$. Further, let $Q(\circ)$ be a loop isotopic to the loop $Q(\cdot)$. By Theorem 6.2, we may assume that the operation $(\circ)$ has the form

$$x \circ y = xl \cdot l^{-1} y.$$

Then

$$x^{(2)} = x \circ x = xl \cdot l^{-1}x = x^2 \tag{6.35}$$

and

$$x^{(3)} = (x \circ x) \circ x = x^2 l \cdot l^{-1}x = x^3. \tag{6.36}$$

Here we make use of the corollary to Moufang's Theorem: the elements x, l generate an associative subloop. We have

$$x^{(3)} \circ y = x^3 \circ y = x^3 l \cdot l^{-1}y = x^3(l \cdot l^{-1}y) = x^3 y. \tag{6.37}$$

Similarly, it is proved that $x \circ y^{(3)} = xy^3$. By (6.37) we conclude that

$$x^{(3)} \circ y = y \circ x^{(3)}.$$

Further we have

$$(x^{(3)} \circ y) \circ z = (x^3 y \cdot l)(l^{-1}z) = x^3(yl \cdot l^{-1}z) = x^3(y \circ z) = x^{(3)} \circ (y \circ z),$$

i.e., $x^{(3)} \in N(\circ)$ for every $x \in Q$.

Finally, we prove that $x \to x^{(3)}$ is an endomorphism of the loop $Q(\circ)$:

$$(x \circ y)^{(3)} = (xl \cdot l^{-1}y)^3 = x^3 l^3 \cdot l^{-3}y^3 = x^3 y^3.$$

Here we use the fact that $x^3 \in N$ for every $x \in Q$. Taking into account (6.37) and (6.36), the proof of the equality $(x \circ y)^{(3)} = x^{(3)} \circ y^{(3)}$ is complete. □

Now we establish a property of commutative Moufang loops that will be needed later.

Theorem 6.7. *If two commutative Moufang loops $Q(\bullet)$ and $Q(\cdot)$ are isotopic, then they are isomorphic.*

By Theorem 6.2, the loop $Q(\bullet)$ is isomorphic to a commutative Moufang loop $Q(\circ)$ with $x \circ y = xl \cdot l^{-1}y$. Since $x \circ y = y \circ x$, we have $xl \cdot l^{-1}y = yl \cdot l^{-1}x = xl^{-1} \cdot ly$, whence after replacing x and y respectively with xl and yl we obtain

$$xl^2 \cdot y = x \cdot l^2 y.$$

Consequently, l^2 lies in the nucleus N of the loop $Q(\circ)$. But by Lemma 6.7, $l^3 \in N$, so also $l \in N$. Thus, $x \circ y = xl^{-1} \cdot ly = xy$, and the loop $(\bullet)$ is isomorphic to the loop $(\circ) = (\cdot)$.

The following theorem provides a source of commutative Moufang loops.

Theorem 6.8. *Suppose that the mapping $x \to x^3$ is a central endomorphism of a Moufang loop $Q(\cdot)$. Then the groupoid $Q(\circ)$ with*

$$x \circ y = x^{-1}yx^2 \tag{6.38}$$

is a commutative Moufang loop.

Proof. The groupoid $Q(\circ)$ has the same neutral element 1 as $Q(\cdot)$. The equation $a \circ y = b$ has a unique solution. The unique solvability of the equation $x \circ a = b$ will then follow from the commutativity of the operation $(\circ)$. So, let us prove that $x \circ y = y \circ x$. By the corollary of Moufang's Theorem, brackets are not necessary in the proof.

The definition of $Q(\circ)$ implies

$$x \circ y = x^{-1}yx^{-1} \cdot x^3.$$

Then

$$\begin{aligned} y \circ x &= y^{-1}xy^{-1} \cdot y^3 = y^{-1}xy^{-1} \cdot x \cdot x^{-1}y^3 = (y^{-1}x)^2x^{-1}y^3 \\ &= (y^{-1}x)^3x^{-1}yx^{-1}y^3 = x^{-1}yx^{-1} \cdot y^3(y^{-1}x)^3 \\ &= x^{-1}yx^{-1}(y \cdot y^{-1}x)^3 = x^{-1}yx^{-1} \cdot x^3 = x \circ y. \end{aligned}$$

Consequently, $x \circ y = y \circ x$.

We now prove the validity of the identity (6.31) in $Q(\circ)$. Indeed,

$$\begin{aligned} (x \circ y) \circ (x \circ z) &= (x \circ y)^{-1}(x \circ z)(x \circ y)^{-1}(x \circ z)^3 \\ &= (x^{-1}yx^{-1} \cdot x^3)^{-1}(x^{-1}zx^{-1} \cdot x^3)(x^{-1}yx^{-1} \cdot x^3)^{-1}(x \circ y)^3 \\ &= [(xy^{-1}x)(x^{-1}zx^{-1})(xy^{-1}x)]x^{-3}(x \circ y)^3 \\ &= (xy^{-1}x \cdot x^{-1})(zx^{-1} \cdot xy^{-1}x)y^3 = (xy^{-1})(zy^{-1} \cdot x)y^3 \\ &= x(y^{-1}zy^{-1})x \cdot y^3 = x(y^{-1}zy^{-1} \cdot y^3)x. \end{aligned}$$

Consequently,

$$(x \circ y) \circ (x \circ z) = x(y \circ z)x.$$

On the other hand,

$$(x \circ x) \circ (y \circ z) = x^2 \circ (y \circ z) = x^{-2}(y \circ z)x^4 = x^{-2}(y \circ z)x \cdot x^3 = x(y \circ z)x.$$

Thus, the identity (6.31) is satisfied in $Q(\circ)$: The proof of the theorem is complete. □

Consider an isotope of a commutative Moufang loop $Q(\cdot)$. Theorem 6.2 provides an isomorphic copy $Q(\circ)$ of the isotope. By Theorem 6.6 applied to $Q(\cdot)$, the mapping $x \to x^{(3)} = x \circ x \circ x$ is a central endomorphism of $Q(\circ)$. Therefore, using (6.38) in $Q(\circ)$, we obtain a new commutative Moufang loop $Q(*)$. The following theorem explains the connection between $Q(\cdot)$ and $Q(*)$.

Theorem 6.9. *The commutative Moufang loops $Q(\cdot)$ and $Q(*)$ are isomorphic.*

By Theorem 6.2, $Q(\circ)$ has the form

$$x \circ y = xl \cdot l^{-1}y$$

for a certain element l of Q, and the neutral element 1 of $Q(\cdot)$ is also the neutral element of the loop $Q(\circ)$. We now find the inverse element $x^{(-1)}$ of an element x in $Q(\circ)$. Indeed,

$$x \circ x^{-1} = 1 \quad \text{or} \quad xl \cdot l^{-1}x^{(-1)} = 1$$

lead to

$$x^{(-1)} = l(xl)^{-1} = l \cdot l^{-1}x^{-1} = x^{-1}.$$

As shown above (6.35), we have $x^{(2)} = x \circ x = x^2$. Now we can determine $x * y$ as

$$\begin{aligned} x * y &= x^{(-1)} \circ (y \circ x^{(2)}) = x^{-1} \circ (y \circ x^2) = (x^{-1}l)[l^{-1}(yl \cdot l^{-1}x^2)] \\ &= (x^{-1}l)[(l^{-1} \cdot yl \cdot l^{-1})x^2] = (x^{-1}l)(l^{-1}y \cdot x^2) = (x^{-1}l)(l^{-1}y \cdot x^{-1} \cdot x^3) \\ &= (x^{-1}l)(l^{-1}y \cdot x^{-1})x^3 = (x^{-1}(l \cdot l^{-1}y)x^{-1})x^3 = x^{-1}yx^{-1}x^3 = xy. \end{aligned}$$

Here, the Moufang identities and diassociativity are used several times.

5°. Examples of Moufang loops

We present some specific examples of Moufang loops.

1. Let $Q(+,\cdot)$ be an *alternative ring*, where the alternative identities (6.3) and (6.6) are satisfied:

$$\left.\begin{aligned} x \cdot xy &= x^2y, \\ yx \cdot x &= yx^2. \end{aligned}\right\} \tag{6.39}$$

Flexibility follows from the second of the identities (6.39) on replacing x with $y + x$ (the process of *polarization*):

$$\begin{aligned} & [y(y+x)](y+x) = y[(y+x)(y+x)] \\ \Rightarrow \quad & (y^2 + x)(y+x) = y(y^2 + xy + yx + x^2) \\ \Rightarrow \quad & y^2 \cdot y + yx \cdot y + y^2x + yx \cdot x = y \cdot y^2 + y \cdot xy + y \cdot yx = y \cdot x^2. \end{aligned} \tag{6.40}$$

By (6.39), we have $y^2 \cdot y = y \cdot y^2$. Cancelling in (6.40), we obtain

$$yx \cdot y = y \cdot xy.$$

To simplify the subsequent calculations, we assume that 2 is invertible in $Q(+,\cdot)$.[6] Polarization of (6.39) implies the identity

$$xy \cdot z + xz \cdot y - x \cdot yz - x \cdot zy = 0. \tag{6.41}$$

We denote the left side of (6.41) by $f(x,y,z)$, and obtain the following expressions:

$$\left.\begin{aligned} f(z,x,yx) &= zx \cdot yx + (z \cdot yx)x - z(x \cdot yx) - z(yx \cdot x), \\ f(z,x,y)x &= (zx \cdot y)x + (zy \cdot x)x - (z \cdot xy)x - (z \cdot yx)x, \\ f(zx,x,y) &= (zx \cdot x)y + (zx \cdot y)x - zx \cdot xy = zx \cdot yx, \\ f(z,x,xy) &= zx \cdot xy + (z \cdot xy)x - z(x \cdot xy) - z(xy \cdot x), \\ -f(z,x^2,y) &= -zx^2 \cdot y - zy \cdot x^2 + z \cdot x^2y + z \cdot yx^2, \\ -zf(x,x,y) &= -z(xx \cdot y) - z(xy \cdot x) + z(x \cdot xy) + z(x \cdot yx). \end{aligned}\right\} \tag{6.42}$$

We now sum the equalities (6.42), and cancel terms on the right hand side of the sum. By (6.41), the left side of the sum is zero. We obtain

$$0 = 2(zx \cdot y)x - 2z(xy \cdot x).$$

Since 2 is invertible, this implies

$$(zx \cdot y)x - z(xy \cdot x) = 0$$

or

$$(zx \cdot y)x = z(xy \cdot x),$$

the Moufang identity (6.1). Consequently, if $Q(+, \cdot)$ is an alternative field (here, assuming 2 is invertible), then the set $Q \setminus \{0\}$ of non-zero elements is a Moufang loop. In particular, the set of all non-zero elements of the octonion algebra (appearing as the "Cayley-Dickson algebra" in the book of Kurosh [47]) forms a non-commutative Moufang loop under multiplication. Moreover, the 8 standard basis elements of the octonion algebra, along with their negatives, also form a non-commutative Moufang loop of order 16.[7]

2. Commutative Moufang loops can be constructed using Theorem 6.8. Let $Q(\cdot)$ be a group where $x \to x^3$ is a central endomorphism. Then $Q(\circ)$ with

$$x \circ y = x^{-1} \cdot yx^2$$

is a commutative Moufang loop. Consider the conditions under which the loop $Q(\circ)$ is associative:

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

or, by commutativity,

$$x \circ (z \circ y) = z \circ (x \circ y).$$

Thus,

$$x^{-1}(z^{-1}yz^2)x^2 = z^{-1}(x^{-1}yx^2)z^2,$$

whence

$$x^{-1}z^{-1}yz^{-1}x^{-1}z^3x^3 = z^{-1}x^{-1}yx^{-1}z^{-1}x^3z^3.$$

Consequently,

$$x^{-1}z^{-1}yz^{-1}x^{-1} = z^{-1}x^{-1}yx^{-1}z^{-1}.$$

We replace x^{-1} and z^{-1} with x and z respectively, obtaining

$$xzyzx = zxyxz. \tag{6.43}$$

If the equality (6.43) does not hold in the group $Q(\cdot)$, then $Q(\circ)$ is a non-associative commutative Moufang loop.

The equality (6.43) can be represented in the form

$$x^{-1}z^{-1}xzy = yxzx^{-1}z^{-1}$$

or

$$(x, z)y = y(x^{-1}, z^{-1}), \tag{6.44}$$

where $(x, z) = x^{-1}z^{-1}xz$ is the commutator of the elements (x, z). In the given group $Q(\cdot)$, the equality

$$(x, z) = (x^{-1}, z^{-1}),$$

holds. Indeed, $x^3z = zx^3$ implies

$$x^{-1}zx^2 = x^2zx^{-1}.$$

But

$$x^{-1}zx^2 = x \circ z = z \circ x = z^{-1}xz^2,$$

whence we obtain

$$x^{-1}z^{-1}xz = x^{-1}(z^{-1}xz^2)z^{-1} = x^{-1}(x^2zx^{-1})z^{-1} = xzx^{-1}z^{-1}.$$

Thus, the equality (6.44) takes the form

$$((x, z), y) = 1, \tag{6.45}$$

i.e., $Q(\cdot)$ is *metabelian*[*].

Now we give an example of a non-metabelian group $Q(\cdot)$ in which $x \to x^3$ is a central endomorphism. As Levi and van der Waerden proved [48], there exists a group $Q(\cdot)$ in which $x^3 = 1$ for every $x \in Q$ with n generators, and the orders of the group $Q(\cdot)$, the commutator subgroup $K(\cdot)$ and the center $Z(\cdot)$ are respectively equal to $\binom{n}{1} + \binom{n}{2} + \binom{n}{3}$, $\binom{n}{2} + \binom{n}{3}$, and $\binom{n}{3}$. In such a group the mapping $x \to x^3 = 1$ is a central endomorphism and, obviously, the group is not metabelian.

6°. Bol loops

We have seen the definition of Bol loops in the proof of Theorem 5.5.

Definition 3. A loop $Q(\cdot)$ is a *left Bol loop* if

$$(x \cdot yx)z = x(y \cdot xz) \tag{6.46}$$

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

A *right Bol loop* is defined by the identity

$$z(xy \cdot x) = (zx \cdot y)x. \tag{6.47}$$

[*]A group $Q(\cdot)$ is *metabelian* if its commutator subgroup K (the subgroup generated by all commutators of the elements of the group) is contained in the center Z (the subgroup consisting of all elements commuting with every element from Q). It is easy to see that the condition $K \subseteq Z$ is equivalent to the condition (6.45) [46].

If there is no special qualification, then by a *Bol loop* we default to a left Bol loop.[8]

We consider some elementary properties of Bol loops.

1. *Every Moufang loop is a left or right Bol loop.* This assertion follows from the fact that in every Moufang loop, flexibility (6.5) holds: $xy \cdot x = x \cdot yx$. Thus, the Moufang identity $(xy \cdot x)z = x(y \cdot xz)$ turns into (6.1). In other words, a Bol loop $Q(\cdot)$ is a Moufang loop if and only if it is flexible.

2. *A left Bol loop is a left IP-loop.* We set $y = {}^{-1}x$ in (6.46), where ${}^{-1}xx = 1$. Then

$$(x \cdot {}^{-1}xx)z = x({}^{-1}x \cdot xz), \quad \text{and} \quad xz = x({}^{-1}x \cdot xz),$$

so

$$z = {}^{-1}x \cdot xz. \tag{6.48}$$

3. ${}^{-1}x = x^{-1}$ follows from (6.48) with $z = x^{-1}$.

4. *The left alternative law $x \cdot xy = xx \cdot y$ in a Bol loop* follows from (6.46) with $y = 1$.

5. *A left Bol loop satisfies the right alternative law if and only if it is a Moufang loop.*

Indeed, suppose the right alternative law holds in a Bol loop $Q(\cdot)$. Setting $z = x$ in (6.46), we have

$$(x \cdot yx)x = x(y \cdot xx) = x(yx \cdot x).$$

Flexibility follows on replacing yx with y. Consequently, by Property 1 the loop $Q(\cdot)$ is a Moufang loop.

6. *A loop $Q(\cdot)$ that satisfies both the left and the right Bol identities is a Moufang loop.*

In this case, both alternative laws are satisfied in $Q(\cdot)$, and in view of Property 5, $Q(\cdot)$ is a Moufang loop. (See also the proof of Theorem 5.5).

7. *If a (left) Bol loop $Q(\cdot)$ is an IP-loop, then it is a Moufang loop.*

Indeed, in an IP-loop the equality

$$(xy)^{-1} = y^{-1}x^{-1}$$

holds. Consequently,

$$[(x \cdot yx)z]^{-1} = z^{-1}(x^{-1}y^{-1} \cdot x^{-1})$$

and

$$[x(y \cdot xz)]^{-1} = (z^{-1}x^{-1} \cdot y^{-1})x^{-1},$$

whence

$$z^{-1}(x^{-1}y^{-1} \cdot x^{-1}) = (z^{-1}x^{-1} \cdot y^{-1})x^{-1}.$$

Replacing x^{-1}, y^{-1}, z^{-1} respectively with x, y, z we obtain (6.47). It remains to apply Property 6.

8. *In a (left) Bol loop, the solution of the equation $ax = b$ is $x = a^{-1}b$, while the solution of $ya = b$ is $y = a^{-1}(ab \cdot a^{-1})$.*

The first assertion holds by Property 2. Now, suppose $ya = b$. If the solution y exists, then we have $(a \cdot ya)a^{-1} = ab \cdot a^{-1}$, whence $ay = ab \cdot a^{-1}$ by the left Bol law (6.46). Thus, $y = a^{-1}(ab \cdot a^{-1})$.

We may now verify that $y = a^{-1}(ab \cdot a^{-1})$ is indeed a solution of the equation $ya = b$:

$$ya = (a^{-1}(ab \cdot a^{-1}))a = a^{-1}(ab \cdot a^{-1}a) = a^{-1}(ab) = b.$$

Theorem 6.10. *A loop isotopic to a Bol loop is also a Bol loop.*

Let $Q(\cdot)$ be a Bol loop, and let $Q(\circ)$ be a principal isotope of $Q(\cdot)$. Thus, there exist permutations α and β of the set Q such that the equality

$$xy = \alpha x \circ \beta y$$

holds.

In the left Bol identity (6.46), we pass to the operation $(\circ)$

$$\alpha(\alpha x \circ \beta(\alpha y \circ \beta x) \circ \beta z) = \alpha x \circ \beta(\alpha y \circ \beta(\alpha y \circ \beta x)).$$

We replace αx, αy, and βz respectively with x, y, and z:

$$\alpha(x \circ \beta(y \circ \beta\alpha^{-1}x)) \circ z = x \circ \beta(y \circ \beta(x \circ z)).$$

Setting $z = 1$, we obtain

$$\alpha(x \circ \beta(y \circ \beta\alpha^{-1}x)) = x \circ \beta(y \circ \beta x).$$

Taking this equality into account, we may transform (6.46) into

$$(x \circ \beta(y \circ \beta x)) \circ z = x \circ \beta(y \circ \beta(x \circ z)).$$

Now we set $x = 1$:

$$\beta(y \circ \beta 1) \circ z = \beta(y \circ \beta z),$$

i.e.,

$$\beta(y \circ \beta z) = \lambda y \circ z,$$

where $\lambda y = \beta(y \circ \beta 1)$. Consequently, (6.46) takes the form

$$(x \circ (\lambda y \circ x)) \circ z = x \circ (\lambda y \circ (x \circ z)).$$

Since λ is a permutation of the set Q, we may replace λy with y:

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

so $Q(\circ)$ is a (left) Bol loop.

Notes

[1]Moufang loops were introduced by R. Moufang in [54], in connection with certain questions arising in the theory of non-Desarguesian projective planes. She also proved the main theorem (Theorem 6.4) for Moufang loops. A very detailed study of Moufang loops was carried out by Bruck. His main results are included in the monograph [31]. Chapters VII and VIII of [31] are devoted entirely to Moufang loops, and Chapter VIII is devoted to commutative Moufang loops, where the Bruck-Slaby theorem is proved: A commutative Moufang loop generated by $n > 1$ elements is centrally nilpotent of class at most $n - 1$. The results presented here are mainly contained in Chapter VII of Bruck's book [31].

[2]The equivalence of the three basic identities (6.1), (6.2), (6.9) is proved by Bol and Bruck [31].

[3]A loop in which every inner permutation is an automorphism is called an A-loop (see Bruck, Paige [30]). If $Q(\cdot)$ is *diassociative*, i.e., any two elements of the loop generate an associative subloop (see the corollary of Theorem 6.4), and $Q(\cdot)$ is an A-loop, then the conclusion of the Moufang theorem (Theorem 6.4) holds in $Q(\cdot)$. Moreover [56], if $Q(\cdot)$ is also commutative, then $Q(\cdot)$ is a Moufang loop. Some diassociative loops are considered by Ginzburg [42].

[4]The concept of a semi-automorphism can be introduced in any quasigroup: φ is a semi-automorphism of a quasigroup $Q(\cdot)$ if $\varphi(xy \cdot x) = (\varphi x \varphi y)\varphi x$. Semi-automorphisms in quasigroups were considered by Sade [71].

[5]In the proof of Moufang's Theorem (Theorem 6.5), we follow Bruck [31]. Moufang proved Theorem 6.5 by induction. For the commutative case, Bruck has a very simple proof [29]. The reader will find the connection between Moufang loops and projective planes, for example, in Hall's book [85].

[6]The fully general assertion is true: In every alternative ring, the identities (6.1) and (6.2) are satisfied (Bruck, Kleinfeld [28]).

[7]An example of a Moufang loop having 81 elements is constructed by Bol. This loop is generated by three elements.

[8]Examples of Bol loops that are not Moufang loops are given by Bol [23] and Bruck [31] (see also the example from Chapter IX, 2°).

Chapter VII. TS-quasigroups. Prolongation of quasigroups

1°. Definitions and examples

Totally symmetric (TS-)quasigroups [24] constitute a class of IP-quasigroups which are not loops.

Definition 1. A quasigroup $Q(\cdot)$ is called a *TS-quasigroup*[1] if the equality $xy = z$ implies the equality $x'y' = z'$ for any arbitrary permutation x', y', z' of the elements x, y, z.

The definition of a TS-quasigroup is equivalent to the following definition: a quasigroup $Q(\cdot)$ is called a TS-quasigroup if the identities

$$xy = yx \tag{7.1}$$

and

$$x(xy) = y \tag{7.2}$$

hold in $Q(\cdot)$.

Indeed, the first definition implies the second: If $xy = z$, then $yx = z$. If $xy = z$, then $y = xz$, so $x(xz) = z$. Conversely, suppose (7.1) and (7.2) hold in $Q(\cdot)$. If $xy = z$, then $zx = xy \cdot x = x \cdot xy = y$, implementing the permutation $x \to z \to y \to x$. On the other hand, (7.1) alone implements $x \to y \to x$. Together, these two permutations generate $\mathfrak{S}_3$.

If $Q(A)$ is a TS-quasigroup, then all six inverse operations for A coincide:

$$A = A^{-1} = {}^{-1}A = {}^{-1}(A^{-1}) = ({}^{-1}A)^{-1} = A^{*}. \tag{7.3}$$

Moreover, it is easy to see that equalities (7.3) give a new definition of total symmetry which is equivalent to the previous definitions.

Indeed, the equality $A = A^{*}$ is just the equality (7.1), and $A = A^{-1}$ is just the equality (7.2). At the same time, the equalities $A = A^{-1} = A^{*}$ imply the remaining equalities. Indeed,

$$A = A^{-1} = (A^{*})^{-1} = ([{}^{-1}(A^{-1})]^{-1})^{-1} = {}^{-1}(A^{-1}),$$

i.e.

$$A = {}^{-1}(A^{-1}).$$

Since $A^{-1} = A$, the latter equality takes the form

$$A =^{-1} A.$$

Finally,

$$(^{-1}A)^{-1} = A^{-1} = A.$$

We also have the following characterization of TS-quasigroups.

A TS-quasigroup is an IP-quasigroup with $I_r = I_l = 1$.

Indeed, if $I_r = 1$, then $A[A(x, y), y] = x$ or $^{-1}A(x, y) = A(x, y)$, i.e.

$$^{-1}A = A. \tag{7.4}$$

Similarly, $I_l = 1$ implies

$$A^{-1} = A. \tag{7.5}$$

But then all the equalities (7.3) follow from (7.4) and (7.5).

We give two more definitions:

Definition 2. A TS-loop is called a *Steiner loop*.

Definition 3. An idempotent TS-quasigroup is called a *Steiner quasigroup*.

Note that a Steiner loop is not a Steiner quasigroup.

Thus, Steiner quasigroups are particular cases of TS-quasigroups where the law of idempotency

$$x^2 = x$$

holds. Steiner quasigroups are closely related to the so-called Steiner triple systems[2] which are defined as follows. Let Q be a set, and let $Q^{(3)}$ be the set of all unordered triples (a, b, c) with $a, b, c \in Q$. A subset $S \subseteq Q^{(3)}$ is called a *Steiner triple system* (STS) if: 1) $(a, b, c) \in S$ implies that a, b, c are not pairwise equal; 2) for any pair of distinct elements $a, b \in Q$, there exists a unique triple $(a, b, c) \in S$.

Example. Let Q be the set of integers from 1 to 7. Then

$$S = \{(1,2,3),\ (1,4,5),\ (1,6,7),\ (2,4,6),\ (2,5,7),\ (3,4,7),\ (3,5,6)\}$$

is a Steiner triple system.

Let us prove the following proposition: *On a non-empty set Q, there exists a one-to-one correspondence between Steiner quasigroups and Steiner triple systems.*

Indeed, suppose we have an STS S on Q. Then we define the operation $(\cdot)$ on Q as follows:

1. If $a \neq b$, then there exists a unique triple $(a, b, c) \in S$. We define $ab = c$.
2. $a^2 = a$.

Obviously, $(\cdot)$ is a commutative operation and, moreover, $ab = c$ implies $a'b' = c'$, where a', b', c' is an arbitrary permutation of the elements a, b, c, since by the definition of Steiner triples (a', b', c') is considered to be equal to the triple (a, b, c).

Conversely, if $Q(\cdot)$ is a Steiner quasigroup, then we define a system S of unordered triples (a, b, c) in the following way: $(a, b, c) \in S$ if and only if $ab = c$ for $a \neq b$. The idempotency of the quasigroup $Q(\cdot)$ implies the distinctions $c \neq a, c \neq b$ as well, i.e., the triples from S consist of pairwise unequal elements, and each pair a, b of distinct elements belongs to one and only one triple from S.

Example. For the STS given above, the Steiner quasigroup $Q(\cdot)$ has the following Cayley table:

	1	2	3	4	5	6	7
1	1	3	2	5	4	7	6
2	3	2	1	6	7	4	5
3	2	1	3	7	6	5	4
4	5	6	7	4	1	2	3
5	4	7	6	1	5	3	2
6	7	4	5	2	3	6	1
7	6	5	4	3	2	1	7

A group $G(\cdot)$ *of exponent two* (i.e., in which every non-identity element is of order two) is an example of a Steiner loop. The group is commutative, and $x \cdot xy = x^2y = y$, i.e., it is a TS-loop (Steiner loop).

2°. Autotopy of TS-quasigroups

Let $\mathfrak{A}$ be the group of autotopies of some TS-quasigroup $Q(\cdot)$. We have the following.

Lemma 7.1. *If $T \in \mathfrak{A}$, then $T^\circ \in \mathfrak{A}$, where T° is one of T^r, T^l, T^{rl}, T^{ln}, $T^{lrl} = T^{rlr} = T^*$* (see Corollary 1 to Lemma 1.3).

Indeed, according to Lemma 5.2, T^r and T^l are autotopies of the respective quasigroups $(\cdot)^{-1}$and $^{-1}(\cdot)$. But in a TS-quasigroup, $(\cdot) = (\cdot)^{-1} = {}^{-1}(\cdot)$, so T^r and T^l are autotopies of the quasigroup $(\cdot)$. Then $(T^r)^l$ is also an autotopy of the quasigroup $(\cdot)$, and so on.

Corollary. *The sets of left, right, and principal components of all autotopies coincide.*

If α is an arbitrary component of an autotopy T, then it is a principal component of an arbitrary autotopy of the TS-quasigroup, i.e., it is a quasi-automorphism of the TS-quasigroup $Q(\cdot)$ (see Chapter II, 3°). We denote the group of all quasi-automorphisms of the TS-quasigroup $Q(\cdot)$ by K. Let us consider the groups $\mathscr{L}$, $\mathscr{R}$, and Φ of regular permutations. For TS-quasigroups we have the following.

Lemma 7.2. *The groups $\mathscr{L}$, $\mathscr{R}$, Φ of regular permutations are related by*

$$\mathscr{L} = \mathscr{R} \subseteq \Phi = \Phi^*, \tag{7.6}$$

and $\varphi_* = \varphi$ for all $\varphi \in \Phi$.

Indeed, by the definitions of $\mathscr{L}$ and $\mathscr{R}$, the equality $\mathscr{R} = \mathscr{L}$ *holds for arbitrary commutative quasigroups*. Further, consider $\lambda \in \mathscr{L}$. Then $(\lambda,\ 1,\ \lambda) \in \mathfrak{A}$. According to Lemma 7.1, we obtain $(\lambda,\ 1,\ \lambda)^r = (\lambda,\ \lambda,\ 1) \in \mathfrak{A}$, i.e., $\lambda \in \Phi$, whence $\mathscr{L} \subseteq \Phi$.

Let $\varphi \in \Phi$, i.e., $\varphi x \cdot y = x\varphi^* y$, where $\varphi^* \in \Phi^{**}$. If $x = y$, then $\varphi x \cdot x = x \cdot \varphi^* x = \varphi^* xx$, whence $\varphi^* = \varphi$.

Corollary 1. *If $\varphi \in \mathscr{L}$, then $(\varphi,\ \varphi^{-1},\ 1) \in \mathfrak{A}$.*

Indeed, $\varphi \in \Phi$ is equivalent to $(\varphi,\ (\varphi^*)^{-1},\ 1) \in \mathfrak{A}$. But $\varphi^* = \varphi$, so $(\varphi,\ \varphi^{-1},\ 1) \in \Phi$.

Corollary 2. *Let $\varphi \in \Phi$. Then $\varphi \in \mathscr{L}$ if and only if $\varphi^2 = 1$.*

Indeed, let $\varphi \in \mathscr{L}$, i.e., $(\varphi,\ 1,\ \varphi) \in \mathfrak{A}$. But $\varphi \in \Phi$, and according to Corollary 1, $(\varphi, \varphi^{-1}, 1) \in \mathfrak{A}$. However, $(\varphi, 1, \varphi) \in \mathfrak{A}$ implies $(\varphi, \varphi, 1) \in \mathfrak{A}$. Now whenever two components of two autotopies coincide, their third components also coincide.* Thus, $(\varphi,\ \varphi^{-1},\ 1) \in \mathfrak{A}$ and $(\varphi,\ \varphi,\ 1) \in \mathfrak{A}$ imply $\varphi^{-1} = \varphi$ or $\varphi^2 = 1$.

Corollary 3. *The group Φ is abelian.*

Indeed, let $\varphi,\ \psi \in \Phi$, so $(\varphi,\ \varphi^{-1},\ 1) \in \mathfrak{A}$ and $(\psi,\ \psi^{-1},\ 1) \in \mathfrak{A}$. Consequently, $(\varphi\psi,\ \varphi^{-1}\psi^{-1},\ 1) \in \mathfrak{A}$. On the other hand, $\varphi\psi \in \Phi$, so $(\varphi\psi,\ (\varphi\psi)^{-1},\ 1) \in \Phi$. Using the previous remark, we conclude that $(\varphi\psi)^{-1} = \varphi^{-1}\psi^{-1}$, whence $\varphi\psi = \psi\varphi$.

Corollary 4. *The group $\mathscr{L} = \mathscr{R}$ is abelian.*

This follows from the relationships (7.6) and Corollary 3 of Lemma 7.2.

Lemma 7.3. *If $T = (\alpha, \beta, \gamma) \in \mathfrak{A}$, then $\lambda\mu^{-1} \in \Phi$, where λ and μ are arbitrary components of the autotopy T.*

Indeed, T^*T^{-1} is an autotopy of the TS-quasigroup $Q(\cdot)$. But

$$T^*T^{-1} = (\beta,\ \alpha,\ \gamma)\ (\alpha,\ \beta,\ \gamma)^{-1} = (\beta\alpha^{-1},\ \alpha\beta^{-1},\ 1),$$

so $\beta\alpha^{-1} \in \Phi$, and so on.

Lemma 7.4. *If α is a quasi-automorphism of a TS-quasigroup $Q(\cdot)$, then there exists a unique quasi-automorphism α' such that $(\alpha,\ \alpha,\ \alpha') \in \mathfrak{A}$.*

Indeed, suppose $\alpha \in K$, i.e., there exists an autotopy T of the form (α, β, γ). According to Lemma 7.3, $\varphi = \beta\alpha^{-1} \in \Phi$, and according to Corollary 1 of Lemma 7.2, $S = (\varphi, \varphi^{-1}, 1) \in \mathfrak{A}$. Then by Lemma 1 for the penultimate equality, we have

$$T = (\alpha, \beta, \gamma) = (\alpha, \beta\alpha^{-1}\alpha, \gamma) = (\alpha, \varphi\alpha, \gamma) = (1, \varphi, \varphi^{-1})(\alpha, \alpha, \varphi\gamma)$$

$$= (\varphi, \varphi^{-1}, 1)(\alpha, \alpha, \varphi\gamma) = S(\alpha, \alpha, \varphi\gamma),$$

whence

$$(\alpha, \alpha, \beta\alpha^{-1}\gamma) = S^{-1}T \in \mathfrak{A}.$$

*For the proof of this statement, see Chapter II, 3°.

Any component of an autotopy is uniquely defined by the remaining two components of the autotopy, so $\alpha' = \beta\alpha^{-1}\gamma$ is uniquely defined by the quasi-automorphism α. The proof of the lemma is completed.

Corollary. *The group Φ is a normal subgroup of the group K of all quasi-automorphisms of a TS-quasigroup $Q(\cdot)$.*

Indeed, suppose $\varphi \in \Phi$ and $\alpha \in K$. Then there are autotopies $T_\alpha = (\alpha, \alpha, \alpha')$ and $S = (\varphi, \varphi^{-1}, 1)$. But

$$T_\alpha^{-1} S T_\alpha = (\alpha^{-1}, \alpha^{-1}, \alpha'^{-1})(\varphi, \varphi^{-1}, 1)(\alpha, \alpha, \alpha') = (\alpha^{-1}\varphi\alpha, \alpha^{-1}\varphi^{-1}\alpha, 1)$$

is also an autotopy, so $\alpha^{-1}\varphi\alpha \in \Phi$.

3°. Isotopes of TS-quasigroups

In this section we study conditions under which an isotope of a TS-quasigroup belongs to one or another class of quasigroups. It suffices to consider principal isotopes. Let $Q(\cdot)$ be a quasigroup, and $Q(\circ)$ a principal isotope:

$$x \circ y = Ux \cdot Vy \tag{7.7}$$

1. It was shown above that an arbitrary TS-quasigroup is an IP-quasigroup. We investigate conditions under which $Q(\circ)$ is also an IP-quasigroup.

Theorem 7.1. *The principal isotope (7.7) of a TS-quasigroup $Q(\cdot)$ is an IP-quasigroup if and only if $U, V \in K$ and $U^2, V^2 \in \Phi$.*

We use Theorem 5.2 for the proof: There must exist involutions I_l', I_r' of Q such that

$$\left.\begin{array}{c} T_l = (I_l \lambda I_l'^{-1} \lambda^{-1}, \nu\mu^{-1}, \mu\nu^{-1}) \in \mathfrak{A} \ \text{ and} \\ T_r = (\nu\lambda^{-1}, I_r \mu I_r'^{-1} \mu^{-1}, \lambda\nu^{-1}) \in \mathfrak{A} \end{array}\right\} \tag{7.8}$$

for the isotope is to be an IP-quasigroup. In our case $\lambda = U$, $\mu = V$, $\nu = 1$, and $I_r = I_l = 1$. Since $I_r'^2 = I_l'^2 = 1$, we obtain

$$T_l = (U I_l' U^{-1}, V^{-1}, V) \ \text{ and } \ T_r = (U^{-1}, V I_r' V^{-1}, U)$$

for (7.8). Lemmas 7.1 and 7.3 imply that $U, V \in K$ and $U^2, V^2 \in \Phi$.

By Lemma 7.4, there exists a quasi-automorphism V' such that $S = (V', V, V) \in \mathfrak{A}$. Consequently, $T_l S^{-1} \in \mathfrak{A}$. But

$$T_l S^{-1} = (U I_l' U^{-1}, V'^{-1}, V^{-2}, 1),$$

whence $U I_l' U^{-1} V'^{-1} = V^2$. Thus

$$I_l' = U^{-1} V^2 V' U. \tag{7.9}$$

In similar fashion we find

$$I_r^{'} = V^{-1}U^2U'V.$$

Thus, $I_l^{'}$ and $I_r^{'}$ are quasi-automorphisms of the TS-quasigroup $Q(\cdot)$.

Conversely, let U and V satisfy the conditions of the theorem, and let $I_l^{'}$ be defined by the equality (7.9) Then

$$I_l^{'}x \circ (x \circ y) = U(U^{-1}V^2V'Ux)(Ux \cdot Uy) = V^2V'Ux \cdot V(UxUy). \tag{7.10}$$

Since $(V', V, V) \in \mathfrak{A}$, we have $V(xy) = V'x \cdot Vy$. Similarly, since $U^2 \in \Phi$, then $(V^2, V^{-2}, 1) \in \mathfrak{A}$, whence $(V^2, 1, V^{-2}) \in \mathfrak{A}$, and so $V^2x \cdot y = V^{-2}(xy)$. Thus, from (7.10), we obtain

$$I_l^{'}x \circ (x \circ y) = V^2[V'Ux) \cdot (V'Ux \cdot V^2y)] = V^{-2}(V^2y) = y.$$

The right inverse property in the quasigroup $Q(\circ)$ is proved in similar fashion.

2. We investigate conditions under which the isotope $Q(\circ)$ is also a TS-quasigroup. As we have seen, TS-quasigroups are IP-quasigroups, and $I_r = I_l = 1$ must hold. Using the previous result, we find that T_l and T_r have the form

$$T_l = (1, V^{-1}, V), \quad T_r = (U^{-1}, 1, U),$$

whence we conclude that $U, V \in \Phi$. It is easy to see that the condition $U, V \in \Phi$ is sufficient. Thus, if $U, V \in \Phi$, then

$$U^{-1}V^{-1}(xy) = Ux \cdot Vy. \tag{7.11}$$

Indeed, since $U, V \in \Phi$, then $(U, 1, U^{-1}) \in \mathfrak{A}$ and $(1, V, V^{-1}) \in \mathfrak{A}$, whence $(U, V, U^{-1}V^{-1}) \in \mathfrak{A}$.

Let us show that $Q(\circ)$ is a TS-quasigroup. Since the group Φ is abelian (see Corollary 3 to Lemma 7.2), we have

$$\begin{aligned} x \circ (x \circ y) &= Ux \cdot V(Ux \cdot Vy) = Ux \cdot VU^{-1}V^{-1}(xy) \\ &= Ux \cdot U^{-1}(xy) = UU^{-1}(x \cdot xy) = x \cdot xy = y. \end{aligned}$$

Further, we have $x \circ y = y \circ x$. Indeed,

$$x \circ y = Ux \cdot Vy = U^{-1}V^{-1}(xy) = U^{-1}V^{-1}(yx) = Uy \cdot Vx = y \circ x.$$

Thus, we have proved the following.

Theorem 7.2. *The principal isotope (7.7) of a TS-quasigroup $Q(\cdot)$ is an IP-quasigroup if and only if $U, V \in \Phi$.*

3. We investigate conditions under which the isotope $Q(\circ)$ is a Steiner quasigroup. By Theorem 7.2, U and V must lie in Φ. Then, by (7.11), we have

$$x \circ x = Ux \cdot Vx = U^{-1}V^{-1}(xx) = U^{-1}V^{-1}x^2. \tag{7.12}$$

But in a Steiner quasigroup $x \circ x = x$, so by (7.12), we have

$$VUx = x^2. \tag{7.13}$$

By (7.11), we have

$$x \circ y = U^{-1}V^{-1}(xy),$$

whence

$$VU(x \circ y) = xy,$$

or by (7.13),

$$(x \circ y)^2 = xy. \tag{7.14}$$

Replacing y with $x \circ y$, we have

$$[x \circ (x \circ y)]^2 = x(x \circ y) \text{ and } y^2 = x(x \circ y),$$

whence

$$x \circ y = xy^2 \tag{7.15}$$

Combining (7.14) and (7.15), the identity

$$\left(xy^2\right)^2 = xy. \tag{7.16}$$

is obtained.

Conversely, suppose the identity (7.16) holds in a TS-quasigroup $Q(\cdot)$. Replacing x by x^2, we obtain

$$(x^2y^2)^2 = x^2y.$$

Interchanging x and y,

$$(y^2x^2)^2 = y^2x.$$

Consequently, $x^2y = y^2x$. Now set

$$x \odot y = x^2y = y^2x. \tag{7.17}$$

From (7.17) it follows that the operation $(\odot)$ is commutative and

$$x \odot (x \odot y) = y.$$

Indeed,

$$x \odot (x \odot y) = x^2(x \odot y) = x^2(x^2y) = y.$$

Thus $Q(\odot)$ is a TS-quasigroup. Moreover, $Q(\odot)$ is a Steiner quasigroup, since $x \odot x = x^2x = x$. If we now take an arbitrary principal isotope $Q(\circ)$ of a TS-quasigroup $Q(\cdot)$ in which the identity (7.16) holds, and $Q(\circ)$ is a Steiner quasigroup, then, repeating the arguments from the first part of ¶3, we find that $Q(\circ)$ is related to $Q(\cdot)$ by the equality (7.15). Comparing (7.15) and (7.17), we conclude that $(\circ) = (\odot)$. Thus, we have proved the following theorem.

Theorem 7.3. *The principal isotope (7.7) of a TS-quasigroup $Q(\cdot)$ is a Steiner quasigroup if and only if the identity (7.16) holds in $Q(\cdot)$. In this case, all the principal isotopes coincide.*

To conclude this section, we prove the following.

Theorem 7.4. *A Steiner quasigroup is isotopic to a commutative WIP-loop.*

Indeed, fix an arbitrary element 1 of Q. Consider the isotope

$$x \circ y = 1(xy).$$

Note that $Q(\circ)$ is a commutative loop with neutral element 1. In the loop $Q(\circ)$, the inverse element for x is $Ix = 1x$, since

$$x \circ 1x = 1[x(1x)] = 1 \cdot 1 = 1.$$

Finally, we have

$$y \circ I(x \circ y) = y \circ [1(1 \cdot xy)] = y \circ xy = 1(y \cdot xy) = 1x = Ix,$$

so $Q(\circ)$ is a WIP-loop.

4°. Admissible quasigroups

Steiner quasigroups and Steiner loops are very closely related, but the nature of this connection is distinct from isotopy or transition to an inverse operation. Before we examine this simple connection for Steiner quasigroups, we investigate a new method for obtaining quasigroups related to a given one. First of all, it is necessary to study certain concepts which are often encountered, in particular in Chapter IX.

Definition 4. Let $Q(\cdot)$ be a quasigroup. A permutation θ of the set Q is called *complete*[3] for $Q(\cdot)$ if the self-map

$$\theta' x = x \cdot \theta x \tag{7.18}$$

on the set Q is also a permutation of Q. A quasigroup is said to be *admissible* if it has at least one complete permutation.

Examples. 1. *Idempotent quasigroups* $Q(\cdot)$ (i.e., satisfying the identity $x \cdot x = x$) *are admissible,* with $\theta' = \theta = 1$.

2. *Finite groups of odd order are admissible.* Indeed, the identity permutation $\theta = 1$ is complete for a group $Q(\cdot)$ of odd order $m = 2n + 1$. Since Q is finite, it suffices to prove the injectivity: $x^2 = y^2$ implies $x = y$. We have

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

3. *Admissible groups of even order exist.* The Klein Vierergruppe $Q = \{0, a, b, c\}$ with Cayley table

	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

is admissible. Indeed, the permutation $\theta = \begin{pmatrix} 0 & a & b & c \\ 0 & b & c & a \end{pmatrix}$ is complete for $Q(\cdot)$, with $\theta' = \begin{pmatrix} 0 & a & b & c \\ 0 & c & a & b \end{pmatrix}$.

4. *An example of an imadmissible group.* The symmetric group $\mathfrak{S}_3$ of degree 3 is not admissible. Indeed, $\mathfrak{S}_3$ has a normal divisor H of order three, with coset H' giving the disjoint union $\mathfrak{S}_3 = H \uplus H'$. Suppose θ is a complete permutation of $\mathfrak{S}_3$, so that $\theta'\mathfrak{S}_3$, being equal to $\mathfrak{S}_3$, has 3 elements from H.

Now if $x \in H$ and $\theta x \in H$, then $\theta' x = x \cdot \theta x \in H$; let there be k such elements. Also, if $y \in H'$ and $\theta y \in H'$, then $\theta' y = y \cdot \theta y \in H$; there are again k such elements. Thus, $\theta'\mathfrak{S}_3$ has $2k$ elements from H, a contradiction.

We examine some simple properties of admissible quasigroups.

1. *If a quasigroup $Q(\cdot)$ is admissible, it may have multiple complete permutations.*

In fact, the following assertion is true: *Let θ be a complete permutation and let $T = (\alpha, \beta, \gamma)$ be an autotopy of the quasigroup $Q(\cdot)$. Then $\beta\theta\alpha^{-1}$ is also a complete permutation for $Q(\cdot)$.*

Indeed,

$$\gamma\theta' x = \gamma(x \cdot \theta x) = \alpha x \cdot \beta\theta x,$$

whence, replacing x by $\alpha^{-1}x$, the equation

$$\gamma\theta'\alpha^{-1}x = x \cdot \beta\theta\alpha^{-1}x$$

is obtained.

2. *Suppose that a quasigroup $Q(\cdot)$ is adrmissible. Then its inverse quasigroups are also admissible.*

Indeed, $x \cdot \theta x = \theta' x$ implies $x \backslash \theta' x = \theta x$, where $(\backslash) = (\cdot)^{-1}$; thus θ' is a complete permutation for $Q(\backslash)$.

The equality $x \cdot \theta x = \theta' x$ also implies the equality$\theta' x / \theta x = x$, whence $x/\theta\theta'^{-1}x = \theta'^{-1}x$, i.e.,$\theta\theta'^{-1}$ is a complete permutation for $Q(/)$, where $(/) = {}^{-1}(\cdot)$. It follows that the remaining quasigroups from $\Sigma_{(\cdot)}$ are admissible.

3. The following theorem characterizes admissibility of a quasigroup $Q(\cdot)$.

Theorem 7.5. *A quasigroup $Q(\cdot)$ is admissible if and only if is isotopic to an idempotent quasigroup.*[4]

Indeed, $Q(\cdot)$ is admissible if and only if there exist permutations θ and θ' such that the equality (7.18) holds. We define an isotope $Q(\circ)$ by

$$x \circ y = \theta'^{-1}(x \cdot \theta y).$$

Then $x \circ x = \theta'^{-1}(x \cdot \theta x) = \theta'^{-1}\theta' x = x$, i.e., $Q(\circ)$ is idempotent.

Conversely, let $Q(\cdot)$ be isotopic to an idempotent quasigroup $Q(\circ)$ with $x \circ y = \gamma(\alpha^{-1}x \cdot \beta^{-1}y)$, thus by isotopy $T = (\alpha, \beta, \gamma)$. Let $x = y$. Then $x = x \circ x = \gamma(\alpha^{-1}x \cdot \beta^{-1}x)$, whence $\alpha^{-1}x \cdot \beta^{-1}x = \gamma^{-1}x$. Replacing x by αx, we obtain $x \cdot \beta^{-1}\alpha x = \gamma^{-1}\alpha x$, so $\beta^{-1}\alpha$ is a complete permutation for $Q(\cdot)$.

Corollary. *Isotopes of admissible quasigroups are admissible.*

4. *If $Q(\cdot)$ is an admissible group with complete permutation θ, and $x \cdot \theta x = \theta' x$, then the groupoid $Q(A)$, with*

$$A(x, y) = x\theta'(x^{-1}y). \tag{7.19}$$

is a quasigroup.

Indeed, the equation $A(a, y) = b$ is equivalent to the equation $a\theta'(a^{-1}y) = b$, which has a unique solution $y = a\theta'^{-1}(a^{-1}b)$. We show that the equation $A(x, a) = b$ is also uniquely solvable. In fact, this equation is equivalent to the equation $x\theta'(x^{-1}a) = b$ or $x \cdot x^{-1}a \cdot \theta(x^{-1}a) = b$, whence $a\theta(x^{-1}a) = b$. Solving the equation, we have consecutively

$$a^{-1}b = \theta(x^{-1}a), \quad \theta^{-1}(a^{-1}b) = x^{-1}a, \quad \text{and} \quad x = (\theta^{-1}(a^{-1}b)a^{-1})^{-1}$$

as the unique solution of the equation $A(x, a) = b$.

5. Consider the isotope

$$B(x, y) = A(x^{-1}, y) = x^{-1}\theta'(xy)$$

of the quasigroup A from (7.19). Then: *The system*

$$\left.\begin{aligned} xy &= a, \\ B(x, y) &= b \end{aligned}\right\}$$

of equations has a unique solution for arbitrary $a, b \in Q$.

Indeed, $B(x, y) = x^{-1}\theta'(xy) = x^{-1}\theta' a = b$, so the element x is uniquely specified. Then, the element y is uniquely specified by the equation $xy = a$ we find y.

We have arrived at the following important concept.

Definition 5. Two quasigroups $Q(A)$ and $Q(B)$ are *orthogonal* if the system

$$\left.\begin{aligned} A(x, y) &= a, \\ B(x, y) &= b \end{aligned}\right\}$$

of equations is uniquely solvable for arbitrary $a, b \in Q$.[5]

Thus, the previous result can be formulated in the following form: *An admissible group has a quasigroup which is orthogonal to it.*

The converse statement is also true: *If there exists a quasigroup $Q(B)$ which is orthogonal to a group $Q(\cdot)$, then $Q(\cdot)$ is admissible.*

Indeed, for arbitrary $c \in Q$, the permutation $\theta x = B^{-1}(x, c)$ of Q is complete for $Q(\cdot)$. We consider the self-map $\theta' x = x\theta x$, and show that $\theta' x = d$ has a unique solution for an arbitrary element $d \in Q$.

The equation $\theta' x = d$ is equivalent to the equation $xB^{-1} \cdot (x, c) = d$. Let $B^{-1}(x, c) = y$. Then we obtain the system

$$\left.\begin{aligned} xy &= d, \\ B(x, y) &= c \end{aligned}\right\} \tag{7.20}$$

of equations which, by the orthogonality of $Q(B)$ and $Q(\cdot)$, has a unique solution. In particular, there exists a unique x which satisfies the system (7.20), and, consequently, the equation $\theta' x = d$.

5°. Prolongations of quasigroups[6]

Now let us move to the construction of quasigroups which was discussed at the beginning of the previous section. Let $Q(\cdot)$ be an admissible quasigroup with a complete permutation θ:

$$x\theta x = \theta' x.$$

On the set $Q' = Q \cup \{k\}$, where $k \notin Q$, we define an operation $(\circ)$ as follows:

$$x \circ y = \left\{ \begin{array}{cc} xy, & \text{if} \quad x, y \neq k,\ y \neq \theta o t x, \\ k, & \text{if} \quad x, y \neq k,\ y = \theta x, \\ \theta' x, & \text{if} \quad x \neq k,\ y = k, \\ \theta'\theta^{-1} y, & \text{if} \quad x = k,\ y \neq k, \\ k, & \text{if} \quad x = y = k. \end{array} \right\} \tag{7.21}$$

We show that $Q(\circ)$ is a *quasigroup*. Consider the equation $a \circ x = b$.

If $a = k$, then $x = k$ if $b = k$, while if $b \neq k$, the equation $k \circ x = b$ is equivalent to the equation $\theta'\theta^{-1}x = b$, defining x uniquely as $\theta\theta'^{-1}b$.

Now, suppose $a \neq k$. For $b = k$, the definition of the operation $(\circ)$ implies $x = \theta a$. If $b \neq k$, but $b = \theta' a$, then $a \circ x = \theta' a$ is solved uniquely by $x = k$. If $b \neq k$ and $b \neq \theta' a$, then $a \circ x = b$ becomes $ax = b$, whence x is again defined uniquely.

The unique solution of $x \circ a = b$ is handled in similar fashion.

Definition 6. The quasigroup $Q'(\circ)$ constructed by (7.21) is called the *prolongation* $(\circ) = (\cdot, \theta)$ *of the quasigroup* $Q(\cdot)$ *by the permutation* θ.

If Q is a finite quasigroup, then a prolongation $Q'(\circ)$ is obtained as follows. In the Cayley table for $Q(\cdot)$, we replace products $x \cdot \theta x$ with k. We add a row and a column to the resulting table, each labeled by k, which consist respectively of elements $\theta'\theta^{-1}x$ and $\theta' x$ $(x \neq k)$. Finally, we assume $k \circ k = k$. For example,

$\cdot$	0	1	2	3	4
0	0	1	2	**3**	4
1	3	**2**	0	4	1
2	**1**	4	3	0	2
3	4	3	1	2	**0**
4	2	0	**4**	1	3

$\circ$	k	0	1	2	3	4
k	k	1	2	4	3	0
0	3	0	1	2	k	4
1	2	3	k	0	4	1
2	1	k	4	3	0	2
3	0	4	3	1	2	k
4	4	2	0	k	1	3

In this example $\theta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 1 & 0 & 4 & 2 \end{pmatrix}$ and $\theta' = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 0 & 4 \end{pmatrix}$.

Note the consecutive appearance of the elements 3 2 1 0 4 (from the bottom row of θ') in bolded form down the rows of the first square. These are the products $x \cdot \theta x$. The element k appears at the corresponding places in the second table.

If $Q(\cdot)$ is an idempotent quasigroup, the prolongation $(\circ) = (\cdot, 1)$ (with 1 as the identity permutation of the set Q) has the simple form

$$x \circ y = \left\{ \begin{array}{c} xy \quad \text{for} \quad x \neq k,\ y \neq k,\ x \neq y, \\ k \quad \text{for} \quad x = y \neq k, \\ x \quad \text{for} \quad x \neq k,\ y = k, \\ y \quad \text{for} \quad x = k,\ y \neq k, \\ k \quad \text{for} \quad x = y = k. \end{array} \right\} \tag{7.22}$$

In this case $Q'(\circ)$ is a *loop with neutral element* k.

The converse statement is true: *if a prolongation* $Q'(\circ)$ *of a quasigroup* $Q(\cdot)$ *is a loop, where* $(\circ) = (\cdot, \theta)$, *then* $Q(\cdot)$ *is an idempotent quasigroup and* $\theta = 1$, i.e., the prolongation $Q'(\circ)$ has the form (7.22).

Indeed, let e be a neutral element of a loop $Q'(\circ)$. If $e \neq k$, then $e \circ k = k$ would imply the result $\theta' e = k$ which is impossible, since $\theta' e \in Q$ and $k \in Q$. Thus, $e = k$. By the definition of $(\circ)$ we have $\theta' x = x$ and $\theta' \theta^{-1} y = y$ for arbitrary $x, y \in Q$, i.e., $\theta' = 1$ and $\theta' \theta^{-1} = 1$, whence $\theta = 1$.

Theorem 7.6. *A prolongation of a quasigroup is isotopic to a group* $Q(\cdot)$ *if and only if the group* $Q(\cdot)$ *has exponent two.*

Proof. Suppose that $Q(\cdot)$ is an admissible quasigroup with a full permutation θ, and let $Q(\bullet)$ be a prolongation using θ. Suppose that $(\bullet)$ is isotopic to a group $(\circ)$:

$$x \bullet y = \bar{\gamma}^{-1}(\bar{\alpha} x \circ \bar{\beta} y),$$

where $\bar{\alpha}$, $\bar{\beta}$, and $\bar{\gamma}$ are permutations of the set $Q' = Q \cup \{k\}$. Then the definition of the prolongation $(\bullet) = (\cdot, \theta)$ implies

$$k = x \bullet \theta x = \bar{\gamma}^{-1}(\bar{\alpha} x \circ \bar{\beta} \theta x),$$

$$x \bullet k = \theta' x = \bar{\gamma}^{-1}(\bar{\alpha} x \circ \bar{\beta} k),$$

$$k \bullet x = \theta' \theta^{-1} x = \bar{\gamma}^{-1}(\bar{\alpha} k \circ \bar{\beta} x), \quad \text{and}$$

$$k = k \bullet k = \bar{\gamma}^{-1}(\bar{\alpha} k \circ \bar{\beta} k),$$

whence we obtain

$$\bar{\alpha} x \circ \bar{\beta} \theta x = \bar{\gamma} k, \tag{7.23}$$

$$\bar{\alpha} x \circ \bar{\beta} k = \bar{\gamma} \bar{\theta}' x, \tag{7.24}$$

$$\bar{\alpha} k \circ \bar{\beta} x = \bar{\gamma} \bar{\theta}' \theta^{-1} x, \quad \text{and} \tag{7.25}$$

$$\bar{\alpha} k \circ \bar{\beta} k = \bar{\gamma} k.$$

We have $x \neq k$ in all the equalities (7.23) – (7.25). We find $\bar{\alpha} x$ and $\bar{\beta} x$ from (7.23) and (7.24), and substitute into (7.25):

$$\bar{\gamma} k = \bar{\alpha} x \circ \bar{\beta} \theta x = \bar{\gamma} \bar{\theta}' x \circ (\bar{\beta} k)^{-1} \circ (\bar{\alpha} k)^{-1} \circ \bar{\gamma} \theta' \theta^{-1} (\theta x)$$

$$= \bar{\gamma}\theta' x \circ (\bar{\alpha}k \circ \bar{\beta}k)^{-1} \circ \bar{\gamma}\theta' x = \bar{\gamma}\theta' x \circ (\bar{\gamma}k)^{-1} \circ \bar{\gamma}\theta' x,$$

whence

$$\left(\bar{\gamma}\theta' x \circ (\bar{\gamma}k)^{-1}\right)^2 = 1, \tag{7.26}$$

where 1 is a neutral element of the group $Q'(\circ)$. Replace in (7.26) $\theta' x$ with x:

$$(\bar{\gamma}x \circ (\bar{\gamma}k)^{-1})^2 = 1.$$

This equality holds true for arbitrary $x \neq k$. But if $x = k$, then $\bar{\gamma}k \circ (\bar{\gamma}k)^{-1} = 1$, so the restriction $x \neq k$ can be removed. Since $x \to \bar{\gamma}x \circ (\bar{\gamma}k)^{-1}$ is a permutation of the set Q', we have shown that the group $Q(\cdot)$ has exponent two. □

The following lemma is needed for the proof of Theorem 7.7 below.

Lemma 7.5. *Consider a group $Q(\cdot)$ of order $n > 8$. If at least $n-3$ non-identity elements have order two, then all $n-1$ non-identity elements have order two.*

Consider $p \in Q$ with $p^2 \neq 1$. Then $(p^{-1})^2 \neq 1$. Consequently, all the other non-identity elements of Q should have order two. The element p^2 either does have order two, i.e., $p^4 = 1$, or does not have order two: $(p^2)^2 \neq 1$. In the latter case, since $p^2 = p$ or $p = 1$ is impossible, we have $p^2 = p^{-1}$, i.e., $p^3 = 1$. So the group $Q(\cdot)$ contains a cyclic subgroup $H = \langle p \rangle$ of order three or four. In each case, H is a normal subgroup of group $Q(\cdot)$. Indeed, $(xpx^{-1})^2 \neq 1$ for arbitrary x, since $(xpx^{-1})^2 = xp^2x^{-1} \neq 1$, and consequently $xpx^{-1} \in H$. The index of the normal subgroup H in $Q(\cdot)$ is more than two, since the order of $Q(\cdot)$ is more than eight.

We further note that

$$xpx^{-1} = p^{-1} \tag{7.27}$$

for arbitrary $x \notin H$, since then $x^2 = 1$ and $xp \notin H \;\Rightarrow\; (xp)^2 = 1 \;\Rightarrow\; xpx = p^{-1}$.

Since the index of H in $Q(\cdot)$ is more than two, the order of the quotient group $Q/H = \{\bar{x} \mid x \in Q\}$ is more than two, so there exist two elements $\bar{x}$ and $\bar{y}$ distinct from $\bar{1}$ such that $\bar{x}\bar{y} \neq \bar{1}$. In other words, in $Q(\cdot)$ there are two elements x and y not belonging to H whose product does not belong to H. Thus $x^2 = y^2 = (xy)^2 = 1$, whence, in particular, it follows that $xy = yx$.

On the other hand, (7.27) implies

$$(xy)p(xy) = p^{-1}$$

or

$$(xy)p(xy) = (xy)p(yx) = x(ypy)x = xp^{-1}x = p.$$

Thus, $p = p^{-1}$ or $p^2 = 1$, contradicting the choice of p. It follows that all the non-identity elements of the group $Q(\cdot)$ have an order two.

Remark. If the order of $Q(\cdot)$ is eight or less, the conclusion of the lemma does not hold. The dihedral group D_4 of degree 4 and order 8 serves as a counterexample.

Definition. Complete permutations φ and θ of a quasigroup $Q(\cdot)$ are *equivalent* if

$$\varphi\alpha = \beta\theta,$$

where α and β are the respective left and right components of an autotopy T of $Q(\cdot)$.

If $Q(\cdot)$ is a group, then Theorem 2.5 implies that the components α and β of the autotopy (α, β, γ) have the form

$$\alpha = L_a\nu \quad \text{and} \quad \beta = R_b\nu,$$

where a, b are elements of Q, and ν is an automorphism of the group $Q(\cdot)$. Thus the equivalence of complete permutations φ and θ means that

$$\varphi L_a\nu = R_b\nu\theta$$

or

$$\varphi = R_b\nu\theta\nu^{-1}L_a. \tag{7.28}$$

In (7.28) we have replaced a^{-1} by a.

Remark. As an example of non-equivalence of complete permutations, take $Q(\cdot)$ as a non-trivial abelian group of odd order, with a complete non-trivial automorphism φ. Now $\theta = 1$ is complete. If φ and θ are equivalent, then by (7.28), $\varphi = R_bL_a = L_bL_a = L_{ab}$. But $\varphi 1 = 1$, so $L_{ab}1 = 1$. Hence $b = a^{-1}$, i.e., $\varphi = L_1 = 1$, contradicting the choice of φ.

Theorem 7.7. Suppose that a group $Q(\cdot)$ contains at least one non-identity element of order different from two. Suppose that θ and φ are complete permutations. Then the prolongations $A = (\cdot, \theta)$ and $B = (\cdot, \varphi)$ are isotopic if and only if θ and φ are equivalent.

Proof. 1°) **Necessity.** We have to establish the equivalence of θ and φ in the presence of an isotopy

$$B = A^{\bar{T}} \tag{7.29}$$

with $\bar{T} = (\bar{\alpha}, \bar{\beta}, \bar{\gamma})$. For the prolonging element k, set

$$\bar{\alpha}k = a,\ \bar{\beta}k = b,\ \bar{\gamma}k = c, \tag{7.30}$$

$$\bar{\alpha}a_0 = k,\ \bar{\beta}b_0 = k,\ \bar{\gamma}c_0 = k.$$

By the definition of prolongation, we have the following:

$$\bar{\gamma}(xy) = A(\bar{\alpha}x, \bar{\beta}y),\ x \neq k,\ y \neq k,\ y \neq \varphi x, \tag{7.31}$$

$$c = A(\bar{\alpha}x, \bar{\beta}\varphi x),\ x \neq k, \tag{7.32}$$

$$\bar{\gamma}\varphi' x = A(\bar{\alpha}x, b),\ x \neq k, \tag{7.33}$$

$$\bar{\gamma}\varphi'\varphi^{-1}x = A(a, \bar{\beta}x),\ x \neq k, \tag{7.34}$$

$$c = A(a, b). \tag{7.35}$$

From (7.35) it follows that if two elements from a, b, c are equal to k, then the third element is also equal to k. An analogous statement follows for a_0, b_0, c_0.

There are five cases to consider:

1) $a = b = c = k$.

Let $\bar{\alpha}x = \alpha x$, $\bar{\beta}x = \beta x$, $\bar{\gamma}x = \gamma x$ for $x \neq k$, so α, β, γ are permutations of the set Q. Then (7.33) implies

$$\gamma\varphi' x = A(\alpha x, k) = \theta'\alpha x,$$

whence

$$\gamma\varphi' = \theta'\alpha. \tag{7.36}$$

From (7.32) we have

$$k = A(\alpha x, \beta\varphi x),$$

whence

$$\beta\varphi = \theta\alpha. \tag{7.37}$$

Let $x, y \in Q$ and $y \neq \varphi x$. Then from (7.31) we obtain

$$\gamma(xy) = A(\alpha x, \beta y).$$

Since $\gamma(xy) \neq k$, the definition of the prolongation A implies

$$\gamma(xy) = \alpha x \cdot \beta y$$

or

$$\gamma^{-1}(\alpha x \cdot \beta y) = xy \quad \text{for} \quad y \neq \varphi x. \tag{7.38}$$

In the case when $y = \varphi x$, we have

$$\gamma^{-1}(\alpha x \cdot \beta\varphi x) = \gamma^{-1}(\alpha x \cdot \theta\alpha x) = \gamma^{-1}\theta'\alpha x,$$

since $x \cdot \theta x = \theta' x$. But by (7.36), $\gamma^{-1}\theta'\alpha = \varphi'$. Thus

$$\gamma^{-1}(\alpha x \cdot \beta\varphi x) = \varphi' x$$

or

$$\gamma^{-1}(\alpha x \cdot \beta\varphi x) = x \cdot \varphi x. \tag{7.39}$$

Now (7.38) and (7.39) imply $\gamma^{-1}(\alpha x \cdot \beta y) = xy$ for arbitrary x and y, i.e., $T = (\alpha, \beta, \gamma)$ is an autotopy of the group $Q(\cdot)$. The equality (7.37) means that φ and θ are equivalent.

2) $c = k$, $a \neq k$, $b \neq k$.

Let $\bar{\gamma}x = \gamma x$ for $x \neq k$. The equalities (7.32), (7.33) and (7.34) respectively become

$$\left.\begin{aligned} A(\bar{\alpha}x, \bar{\beta}\varphi x) &= k, \\ A(\bar{\alpha}x, b) &= \gamma\varphi' x, \\ A(a, \bar{\beta}x) &= \gamma\varphi'\varphi^{-1}x \end{aligned}\right\} \quad \text{for} \quad x \neq k. \tag{7.40}$$
$$\tag{7.41}$$
$$\tag{7.42}$$

From (7.41) and (7.42), we have

$$A(\bar{\alpha}x, b) = A(a, \bar{\beta}\varphi x) = \gamma\varphi' x \quad \text{for} \quad x \neq k. \tag{7.43}$$

Let $\bar{\alpha}x \neq k$. Then $x \neq a_0$. Consequently, from (7.40) we have

$$bar\beta\varphi x = \theta\bar{\alpha}x, \; x \neq a_0 \quad \text{for} \quad x \neq k. \tag{7.44}$$

In particular, (7.44) implies $bar\beta\varphi x \neq k$ for $x \neq a_0$. Thus, (7.43) implies $\bar{\alpha}x \cdot b = \alpha\bar{\beta}\varphi x = \gamma\varphi' x$ for $x \neq k$ and $x \neq a_0$, whence by (7.44) we have

$$\bar{\alpha}x \cdot b = a \cdot \theta\bar{\alpha}x \quad \text{for} \quad x \neq k \quad \text{and} \quad x \neq a_0.$$

Take $x = \bar{\alpha}^{-1}y$. Then $\bar{\alpha}^{-1}y \neq k$ and $\bar{\alpha}^{-1}y \neq a_0$, whence $y \neq \bar{\alpha}k$ and $y \neq \bar{\alpha}a_0$ or $y \neq a_0$ and $y \neq k$ — see (7.30). Thus

$$y \cdot b = a \cdot \theta y,$$

whence

$$\theta y = a^{-1}yb, \tag{7.45}$$

for all $y \neq k$, $y \neq a$.

The formula (7.45) also holds for $y = a$. Indeed, for $c = k$, (7.35) implies $A(a, b) = k$, whence $\theta a = b$. The same result follows from (7.45) for $x = a$.

By (7.29), we have

$$A = B^{\bar{T}^{-1}} = B^{(\bar{\alpha}^{-1}, \bar{\beta}^{-1}, \bar{\gamma}^{-1})}.$$

If we interchange the roles of A and B, then φ and θ, and also the respective elements a, b, c and a_0, b_0,c_0, change their roles correspondingly, since $c = k \leftrightarrow c_0 = k$. Thus, we obtain a relationship for φ which is analogous to the equality (7.45):

$$\varphi y = a_0^{-1}yb_0. \tag{7.46}$$

We now determine the relation between φ and θ. From (7.45) and (7.46), we have

$$\theta(ay) = yb \quad \text{and} \quad \varphi(a_0y) = yb_0.$$

Consequently,

$$\theta(ay)b^{-1} = \varphi(a_0y)b_0^{-1},$$

whence

$$\varphi(a_0y) = \theta(ay)b^{-1}b_0$$

or

$$\varphi y = \theta(aa_0^{-1}y)b^{-1}b_0 \quad \text{and} \quad \varphi = R_c\theta L_d^{-1},$$

where $d = a_0a^{-1}$ and $c = b^{-1}b_0$. But (L_d, R_c, L_dR_c) is an autotopy of the group $Q(\cdot)$:

$$L_dx \cdot R_cy = dx \cdot yc = d(xy)c = L_dR_c(xy).$$

Consequently, φ and θ are equivalent.

3) $a = k$, $b \neq k$, $c \neq k$.

Set $\bar{\alpha}x = \alpha x$ for $x \neq k$, and $a_0 = k$. The respective equalities (7.32)—(7.34) become

$$\left.\begin{array}{rl} A(\alpha x, \bar{\beta}\varphi x) = c, & (7.47) \\ A(\alpha x, b) = \gamma\bar{\varphi}'x, & (7.48) \\ A(k, \bar{\beta}x) = \gamma\varphi'\varphi^{-1}x & (7.49) \end{array}\right\} \quad \text{for} \quad x \neq k.$$

Suppose $x \neq b_0$. Then (7.49) implies

$$\theta\theta'\bar{\beta}x = \bar{\gamma}\varphi'\varphi^{-1}x \quad \text{for} \quad x \neq b_0 \quad \text{and} \quad x \neq k. \tag{7.50}$$

The equalities (7.47) and (7.48) imply

$$\alpha x \cdot \bar{\beta}\varphi x = c \quad \text{and} \tag{7.51}$$

$$\alpha x \cdot b = \bar{\gamma}\varphi' x. \tag{7.52}$$

The equality (7.51) holds for $\bar{\beta}\varphi x \neq k$ or $\varphi x \neq \bar{\beta}^{-1}k = b_0$, whence $x \neq \varphi^{-1}b_0$. The equality (7.52) holds for $\bar{\gamma}\varphi' x \neq k$ or $\varphi' x \neq \bar{\gamma}^{-1}k = c_0$, whence $x \neq \varphi'^{-1}c_0$. But the condition $x \neq b_0$ from (7.49) is equivalent to the inequality $\bar{\gamma}\varphi'\varphi^{-1}x \neq k$, or $\varphi'\varphi^{-1}x \neq \gamma^{-1}k = c_0$, or $\varphi^{-1}x \neq \varphi'^{-1}c_0$. Thus, the inequality $x \neq \varphi'^{-1}c_0$ or $\varphi^{-1}(\varphi x) \neq \varphi'^{-1}c_0$ is equivalent to the inequality $\varphi x \neq b_0$ or $x \neq \varphi^{-1}b_0$. Consequently, the equalities (7.51) and (7.52) are true for $x \neq \varphi^{-1}b_0$ (and $x \neq k$).

From the equality (7.50), after the substitution $x = \varphi y$, we obtain

$$\theta'\theta^{-1}\bar{\beta}\varphi y = \gamma\varphi' y, \tag{7.53}$$

which holds when $\varphi y \neq b_0$ and $\varphi y \neq k$, i.e., $y \neq k$ and $y \neq \varphi^{-1}b_0$. Thus, from (7.51)—(7.53) for $x \neq k$ and $x \neq \varphi^{-1}b_0$, we have

$$\theta'\theta^{-1}\bar{\beta}\varphi x = \gamma\theta' x = \alpha x \cdot b = c(\bar{\beta}\varphi x)^{-1}b.$$

Replacing $\bar{\beta}\varphi x$ with z yields

$$\theta'\theta^{-1}z = cz^{-1}b. \tag{7.54}$$

We check for which elements z the equality (7.54) holds. First of all, $z \neq k$, this condition following from $x \neq \varphi^{-1}b_0$. Further, $x = \varphi^{-1}\bar{\beta}z$ implies $z \neq b$, since $\beta^{-1}b = k$, and $\varphi^{-1}k$ is undefined. Thus (7.54) holds for arbitrary $z \in Q$. But the equality $A(k, b) = c$ implies $c = \theta'\theta^{-1}b$. For $z = b$ in (7.54) we get the same result. From the equality (7.54) and the definition of the permutation θ' we have

$$\theta^{-1}z \cdot \theta(\theta^{-1}z) = cz^{-1}b,\ \theta^{-1}z = cz^{-1}bz^{-1}$$

or

$$\theta^{-1}z = cb^{-1}(bz^{-1})^2. \tag{7.55}$$

Arguing as in case 1, we obtain that

$$\varphi^{-1}z = c_0b_0^{-1}(b_0z^{-1})^2. \tag{7.56}$$

From (7.55) we find

$$(bz^{-1})^2 = bc^{-1}\theta^{-1}z,\ z^{-2} = bc^{-1}\theta^{-1}(zb). \tag{7.57}$$

Similarly, from (7.56) we have

$$z^{-2} = b_0c_0^{-1}\varphi^{-1}(zb_0). \tag{7.58}$$

Comparing (7.57) and (7.58), we conclude that

$$\varphi^{-1}z = e\theta^{-1}(zd^{-1}),$$

where $e = c_0b_0^{-1}bc^{-1}$ and $d = b^{-1}b_0$. Thus,

$$\varphi^{-1} = L_e\theta^{-1}R_{d^{-1}} = L^e\theta^{-1}R_d^{-1},$$

and consequently,

$$\varphi = R_d\theta L_e^{-1}.$$

Hence it follows that φ and θ are equivalent.

4) $b = k$, $a \neq k$, $c \neq k$.

Here, we may argue as in the previous case.

5) $a, b, c \neq k$.

Here, we also have $a_0, b_0, c_0 \neq k$. We examine the possible respective forms of the equalities (7.35) in a), (7.33) in b), (7.34) in c), and (7.32) in d) below, ultimately arriving at the conclusion that this particular case cannot actually arise.

a) $A(a, b) = c$.

Since all the elements a, b, c differ from k, this equation cannot hold, because the definition of the prolongation of A implies $ab = c$ and

$$\theta a \neq b, \tag{7.59}$$

since $A(a, b) = A(a, \theta a) = k$.

b) $A(\bar{\alpha}x, b) = \bar{\gamma}\varphi' x, x \neq k.$ (7.60)

Let $x = a_0$. Then $A(k, b) = \bar{\gamma}\varphi' a_0$, so

$$\theta'\theta^{-1}b = \bar{\gamma}\varphi' a_0.$$

Suppose, further, that $b = \theta\bar{\alpha}x$, i.e., $x = \bar{\alpha}^{-1}\theta^{-1}b$. Then (7.60) implies $\bar{\gamma}\varphi^{-1}\bar{\alpha}^{-1}\theta^{-1}b = k$, whence

$$\varphi'\bar{\alpha}^{-1}\theta^{-1}b = c_0. \tag{7.61}$$

This latter equality makes sense, because $\bar{\alpha}^{-1}\theta^{-1}b \neq k$. Indeed, the inequality (7.59) implies $a \neq \theta^{-1}b$, $\bar{\alpha}k \neq \theta^{-1}b$, and $k \neq \bar{\alpha}^{-1}\theta^{-1}b$. Thus, from (7.60) we have

$$\bar{\alpha}x \cdot b = \bar{\gamma}\varphi' x \quad \text{when} \quad x \neq k,\ x \neq a_0,\ x \neq \bar{\alpha}^{-1}\theta^{-1}b. \tag{7.62}$$

$c)$ $A(a, \bar{\beta}x) = \bar{\gamma}\varphi'\varphi^{-1}x,\ x \neq k.$ (7.63)

If $x = b_0$, then

$$A(a, \bar{\beta}b_0) = A(a, k) = \bar{\gamma}\varphi'\varphi^{-1}b_0,$$

whence

$$\varphi'\varphi^{-1}\bar{\beta}^{-1}\theta a = c_0. \tag{7.64}$$

The latter equality makes sense because $\theta a \neq b$ and, consequently, $\bar{\beta}^{-1}\theta a \neq \bar{\beta}^{-1}b = k$. Therefore, from (7.63) we have

$$a \cdot \bar{\beta}x = \bar{\gamma}\varphi'\varphi^{-1}x \ \text{ for } x \neq k,\ x \neq b_0,\ x \neq \bar{\beta}^{-1}\theta a. \tag{7.65}$$

We make the substitution $x = \varphi y$ in the equality (7.65):

$$a\bar{\beta}\varphi y = \bar{\gamma}\varphi' y.$$

This equality makes sense when

$$\varphi y \neq k,\ \ \varphi y \neq b_0,\ \ \varphi y \neq \bar{\beta}^{-1}\theta a,$$

or

$$y \neq k,\ \ y \neq \varphi^{-1}b_0,\ \ y \neq \varphi^{-1}\bar{\beta}^{-1}\theta a. \tag{7.66}$$

Thus,

$$a \cdot \bar{\beta}\varphi x = \bar{\gamma}\varphi' x \ \text{ for } \ x \neq k,\ \ x \neq \varphi^{-1}b_0, x \neq \varphi^{-1}\bar{\beta^{-1}}\theta a.$$

$d)$ $A(\bar{\alpha}x, \bar{\beta}\varphi x) = c,\ \ x \neq k.$ (7.67)

If $x = a_0$, then

$$A(k, \bar{\beta}\varphi a_0) = c, \tag{7.68}$$

whence $\bar{\beta}\varphi a_0 \neq k$, $\varphi a_0 \neq \bar{\beta}^{-1}k$ or

$$\varphi a_0 \neq b_0. \tag{7.69}$$

From (7.68) we obtain

$$\bar{\beta}\varphi a_0 = \theta'\theta^{-1}c. \tag{7.70}$$

If $\varphi x = b_0$ or $x = \varphi^{-1}b_0$, then

$$A(\bar{\alpha}\varphi^{-1}b_0, k) = c,$$

whence

$$\theta'\bar{\alpha}\varphi^{-1}b_0 = c. \tag{7.71}$$

In view of (7.69), the equalities (7.70) and (7.71) make sense. Thus, (7.67) implies

$$\bar{\alpha}x \cdot \bar{\beta}\varphi x = c \ \text{ for } \ x \neq k,\ \ x \neq a_0,\ \ x \neq \varphi^{-1}b_0.$$

We note that the conditions $x \neq \bar{\alpha}^{-1}\theta^{-1}b$ from (7.62) and $x \neq \varphi^{-1}\bar{\beta}^{-1}\theta a$ from (7.66) coincide with the condition $x \neq \varphi'^{-1}c_0$, since by (7.61) and (7.64) we have

$$\bar{\alpha}^{-1}\theta^{-1}b = \varphi'^{-1}c_0 \quad \text{and} \quad \varphi^{-1}\bar{\beta}^{-1}\theta a = \varphi'^{-1}c_0.$$

Thus, we find the equalities

$$\left.\begin{array}{c} \bar{\alpha}x \cdot b = \bar{\gamma}\varphi' x, \quad \text{for} \quad x \neq a_0,\ x \neq \varphi'^{-1}c_0, \\ a \cdot \bar{\beta}\varphi x = \bar{\gamma}\varphi' x, \quad \text{for} \quad x \neq \varphi^{-1}b_0,\ x \neq \varphi'^{-1}c_0, \\ \bar{\alpha}x \cdot \bar{\beta}\varphi x = c, \quad \text{for} \quad x \neq a_0,\ x \neq \varphi^{-1}b_0, \end{array}\right\} \tag{7.72}$$

all subject to the additional condition $x \neq k$. We eliminate $\bar{\alpha}x$ and $\bar{\beta}\varphi x$ from the equalities (7.72):

$$\begin{gathered} (\bar{\gamma}\varphi' x \cdot b^{-1})(a^{-1} \cdot \bar{\gamma}\varphi' x) = c, \\ \bar{\gamma}\varphi' x \cdot c^{-1} \cdot \bar{\gamma}\varphi' x = c, \\ (\bar{\gamma}\varphi' x \cdot c^{-1})^2 = 1. \end{gathered} \tag{7.73}$$

The latter equality makes sense when $x \neq a_0$, $x \neq \varphi^{-1}b_0$, and $x \neq \varphi'^{-1}c_0$. Let

$$y = \bar{\gamma}\varphi' x \cdot c^{-1}. \tag{7.74}$$

Now $x \neq a_0$ implies $y \neq \bar{\gamma}\varphi' a_0 \cdot c^{-1}$. Also $x \neq \varphi^{-1}b_0$ implies $y \neq \bar{\gamma}\varphi'\varphi^{-1}b_0 \cdot c^{-1}$, and $x \neq \varphi'^{-1}c_0$ implies $y \neq \bar{\gamma}\varphi'(\varphi'^{-1}c_0) = \bar{\gamma}c_0 = k$.

Moreover, we see that $y \neq 1$ by (7.74), because $1 = \bar{\gamma}\varphi' x \cdot c^{-1}$ would imply $\bar{\gamma}\varphi' x = c$, leading to the contradiction $\varphi' x = k$. So, the equality (7.73) takes the form $y^2 = 1$, holding when $y \neq k$, $y \neq 1$, $y \neq \bar{\gamma}\varphi'\varphi^{-1}b_0$, and $y \neq \bar{\gamma}\varphi'\varphi^{-1}b_0 \cdot c^{-1}$. If we move to the group $Q(\cdot)$, then the first two limitations can be removed. Consequently, all the non-identity elements of the group $Q(\cdot)$, with two possible exceptions, have order two. Applying Lemma 7.5, we arrive at a contradiction to the hypothesis of the theorem: All the non-identity elements of $Q(\cdot)$ have order two. Thus, case 5) cannot arise, and the necessity has been proved.

2°) **Sufficiency.** Let $Q(\cdot)$ be an admissible quasigroup. If complete permutations θ and φ are equivalent, then the prolongations $A = (\cdot, \theta)$ and $B = (\cdot, \varphi)$ are isotopic.

Indeed, let θ and φ be equivalent, so there is an autotopy $T = (\alpha, \beta, \gamma)$ of the quasigroup $Q(\cdot)$ such that

$$\theta = \beta\varphi\alpha^{-1} \tag{7.75}$$

and

$$\theta' = \gamma\varphi'\alpha^{-1}. \tag{7.76}$$

Then

$$\begin{aligned} \theta' x = x \cdot \theta x = x \cdot \beta\varphi\alpha^{-1}x &= \alpha(\alpha^{-1}x) \cdot \beta\ (\varphi\alpha^{-1}x) \\ &= \gamma(\alpha^{-1}x \cdot \varphi\alpha^{-1}x) = \gamma\varphi'\alpha^{-1}x \end{aligned}$$

for x in Q. We define three permutations $\bar{\alpha}$, $\bar{\beta}$, $\bar{\gamma}$ on the disjoint union $Q' = Q \cup \{k\}$, using $\bar{\alpha}x = \alpha x$ for $x \in Q$ and $\bar{\alpha}k = k$. We define $\bar{\beta}$ and $\bar{\gamma}$ similarly. We show $B = A^{\bar{T}}$, where $\bar{T} = (\bar{\alpha}, \bar{\beta}, \bar{\gamma})$. For this, we consider various possible cases for pairs of elements of Q'.

1) $x \neq k$, $y \neq k$, $y \neq \varphi x$:

Here, $B(x,y) = xy$. If $y \neq \varphi x$, then (7.75) implies $y \neq \beta^{-1}\theta\alpha x$, whence $\beta y \neq \theta\alpha x$. Consequently,

$$A^{\bar{T}}(x,y) = \bar{\gamma}^{-1}A(\bar{\alpha}x, \bar{\beta}y) = \bar{\gamma}^{-1}A(\alpha x, \beta y) = \gamma^{-1}(\alpha x \cdot \beta y) = x \cdot y.$$

2) $x \neq k$, $y \neq k$, $y = \varphi x$:
Here, $B(x,y) = k$. On the other hand,

$$\begin{aligned} A^{\bar{T}}(x,\varphi x) = \bar{\gamma}^{-1}A(\bar{\alpha}x, \bar{\beta}\varphi x) = \bar{\gamma}^{-1}A(\alpha x, \beta\varphi x) \\ = \bar{\gamma}^{-1}A(\alpha x, \theta\alpha x) = \bar{\gamma}^{-1}k = k. \end{aligned}$$

3) $y = k$, $x \neq k$:
Here $B(k,x) = \varphi' x$ and

$$A^{\bar{T}}(x,k) = \bar{\gamma}^{-1}A(\bar{\alpha}x, \bar{\beta}k) = \bar{\gamma}^{-1}A(\alpha x, k) = \bar{\gamma}^{-1}\theta'\alpha x = \gamma^{-1}\theta'\alpha x = \varphi' x$$

by (7.76).

4) $x = k$, $y \neq k$:
Here, $B(k,y) = \varphi'\varphi^{-1}y$, and for $A^{\bar{T}}$ we find

$$A^{\bar{T}}(k,y) = \bar{\gamma}^{-1}A(\bar{\alpha}k, \bar{\beta}y) = \bar{\gamma}^{-1}A(k, \beta y) = \bar{\gamma}^{-1}\theta'\theta^{-1}\beta y = \gamma^{-1}\theta'\theta^{-1}\beta y.$$

However, $\gamma^{-1}\theta'\theta^{-1}\beta = \gamma^{-1}(\gamma\varphi'\alpha^{-1})\ (\alpha\varphi^{-1}\beta^{-1})\beta = \varphi'\varphi^{-1}$. Thus, $A^{\bar{T}}(k,y) = B(k,y)$.

5) $x = k$, $y = k$.
Here, $B(k,k) = k$ and $A^{\bar{T}}(k,k) = \gamma^{-1}A(\bar{\alpha}k, \bar{\beta}k) = \gamma^{-1}A(k,k) = \gamma^{-1}k = k$. Thus, $A^{\bar{T}} = B$ in all possible cases. This completes the proof of the theorem. □

Remark. Note that the sufficiency part of the proof of Theorem 7.7 applies to a general admissible quasigroup $Q(\cdot)$, and not just to the groups considered in the context of the theorem.

Theorem 7.7 enables us to construct non-isotopic quasigroups, and, by Theorem 7.6, these quasigroups are not isotopic to groups.

So far, we have studied properties of prolongations of groups. To conclude this section, we return to Steiner quasigroups and prove the following proposition.

Theorem 7.8. *Let $Q(\cdot)$ be a Steiner quasigroup. Then the prolongation $(\circ) = (\cdot, 1)$ of $Q(\cdot)$ is a Steiner loop on the disjoint union $Q' = Q \cup \{k\}$.*

Being idempotent, the Steiner quasigroup $Q(\cdot)$ is admissible, and the identity permutation is complete for $Q(\cdot)$. The prolongation $Q'(\circ)$ is a loop with a neutral element k, and is easily verified to be commutative. We show that

$$x \circ (x \circ y) = y. \tag{7.77}$$

If $x = k$ and y is an arbitrary element from Q', then (7.77) holds, because k is the neutral element of a loop $Q'(\circ)$. Now, let $x \neq k$ and $y = k$. Then

$$x \circ (x \circ k) = x \circ x = k.$$

Finally, if x, y, and k are all different, we have

$$x \circ (x \circ y) = x \circ (xy) = x \cdot xy = y.$$

Thus, $Q'(\circ)$ is a Steiner loop.

Notes

[1]The concept of a TS-quasigroup was introduced by Bruck in [24], and studied in detail in [25]. The results of the sections 3° and 4° are taken mainly from these two works of Bruck.

[2]Steiner triples are studied in combinatorial analysis (see, for example, M. Hall [86], and also the literature therein). The connection between Steiner triples and Steiner quasigroups was studied by Bruck [33] and others.

[3]The concept of a complete permutation was introduced by Mann [49]in the course of a study of orthogonal quasigroups (see Definition 5).

[4]Necessary and sufficient conditions for the admissibility of groups were found by Paige [62] and by M. Hall and Paige [87]. In particular, it was shown that all symmetric groups $\mathfrak{S}_n$ are admissible for $n > 3$. Bateman [37] showed that all infinite quasigroups are admissible.

[5]If we take the two Latin squares (see Note 1 of Chapter I) corresponding to finite orthogonal quasigroups $Q(A)$ and $Q(B)$, and superimpose one on the other, then we obtain a square of the same dimension. In each cell of this square, there is a pair (a, b) of elements $a, b \in Q$. Orthogonality means that all these pairs are different. For example:

A	1	2	3
1	3	2	1
2	3	1	2
3	2	3	1

B	1	2	3
1	2	1	3
2	1	3	2
3	3	2	1

	1	2	3
1	12	21	33
2	31	13	22
3	23	32	22

The square of pairs obtained in this way is called an *Euler square*. Thus, the orthogonality of two quasigroups $Q(A)$ and $Q(B)$ of order n is equivalent to the existence of an Euler square of order n. Euler posed the first problem in this direction: To construct Euler squares of various orders. In 1779, Euler conjectured that Euler squares of order $n = 4k + 2$ do not exist (in particular, of order 6). It was not until 1901 that Tarry was able to prove that Euler's conjecture holds for $n = 6$ (the case $n = 2$ it is trivial). Since then, Euler's conjecture has been tackled by many researchers. In 1959, Parker [60] proved that there is an Euler square of order 10. Other details on Euler squares are given by M. Hall [86], as well as in the literature he cites. We also mention articles by Stein [74], Sade [68], and the author [19]. In particular, these articles consider quasigroups $Q(\cdot)$ satisfying the identity $x \cdot xy = yx$. It is easy to see that in this case, the quasigroup $Q(\cdot)$ and its opposite $Q(*)$ with $x * y = yx$ are orthogonal. Such quasigroups are also considered in [59].

[6]Prolongations of quasigroups were first considered by Bruck in [24], but only for the case where $Q(\cdot)$ is idempotent (see the definition of $Q'(\circ)$ in (7.22)). Theorem 7.8 is also proved there. Prolongation of quasigroups was also applied by Osborn in [58].

Chapter VIII. Distributive quasigroups

1°. Some elementary properties of distributive quasigroups

Definition 1. A quasigroup $Q(\cdot)$ is said to be *distributive*[1] if the following identities hold:

$$x \cdot yz = xy \cdot xz, \tag{8.1}$$

$$yz \cdot x = yx \cdot zx. \tag{8.2}$$

The identities (8.1) and (8.2) are respectively called the *left* and *right distributive laws*.

Example of a distributive quasigroup. Let $(Q, +, \cdot)$ be an associative division ring. Let us consider the operation $A(x, y) = (1 - a)x + ay, \quad a \neq 0, 1.$ in $Q(+, \cdot)$. It is easy to verify that $Q(A)$ is a distributive quasigroup. Other examples are given below.

We consider some simple properties of distributive quasigroups.

a) *A distributive quasigroup $Q(\cdot)$ is idempotent*, i.e.

$$x^2 = x$$

for all x $\in Q$. Indeed, setting $y = x$ in (8.1), we obtain $x \cdot xz = xx \cdot xz$, implying $x = xx = x^2$.

b) *The group G associated with a distributive quasigroup $Q, (\cdot)$ is a subgroup of the group of automorphisms of the quasigroup $Q(\cdot)$.*[2]

It is sufficient to prove the statement for the translations R_a and L_a, where a is an arbitrary element from Q, as R_a and L_a generate the group G. The identity of left distributivity may be rewritten as

$$L_x(yz) = L_x y \cdot L_x z,$$

showing that L_x is an automorphism of the quasigroup $Q(\cdot)$.

c) *For an arbitrary element x of a distributive quasigroup, the translations L_x and R_x commute:*

$$R_x L_x = L_x R_x y, \tag{8.3}$$

Indeed,

$$R_x L_x y = (xy)x = (xx)(yx) = x(yx) = L_x R_x y.$$

d) *Let $Q(\cdot)$ be a distributive quasigroup. Suppose that $(\cdot)^{-1} = (\backslash)$ is the right inverse operation for $(\cdot)$, and that ${}^{-1}(\cdot) = (/)$ is the left inverse operation for $(\cdot)$. Then the identities*

$$\left.\begin{aligned} x(y\backslash z) &= (xy)\backslash(xz), \\ (y/z)x &= (yx)/(zx), \\ x\backslash(yz) &= (x\backslash y)(x\backslash z), \\ (yz)/x &= (y/x)(z/x) \end{aligned}\right\} \tag{8.4}$$

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

To prove the first equality (8.4), we consider

$$x(y\backslash z) = (xy)\backslash(xz'). \tag{8.5}$$

Such an element z' exists by the invertibility of $(\cdot)$. Using the definition of the operation $(\backslash)$, we obtain

$$x(x\backslash y)x = y$$

for all $x, y \in Q$. Thus, from (8.5) we have

$$xz' = (xy)\,[x(y\backslash z)] = x\,[y(y\backslash z)] = xz,$$

which implies $z' = z$. Thus, the first of the equalities (8.4) is proved. The remainder of the equalities (8.4) are proved in similar fashion.

e) *Each coset of a subquasigroup* H *of a distributive quasigroup* $Q(\cdot)$ *is itself a subquasigroup.*[3]

Consider a coset aH, and elements $a_1, a_2 \in aH$. Then there exist elements h_1, h_2 of H such that $a_1 = ah_1$ and $a_2 = ah_2$, so $a_1a_2 = ah_1 \cdot ah_2 = a(h_1h_2) \in aH$. Now we show that the solution x of the equation $a_1x = a_2$ belongs to the same coset aH. Write the element x as ax' for some element x' of Q. Then $ah_2 = a_2 = a_1x = ah_1ax' = a\,(h_1x')$, whence $h_2 = h_1x'$. Since $H(\cdot)$ is a subquasigroup, $x' \in H$ and $x = ax' \in aH$. Similarly, we may prove that the solution y of the equation $ya_1 = a_2$ also belongs to aH.

2°. Connection with commutative Moufang loops

For an element k of Q, consider the principal isotope

$$x \cdot y = A\left(R_k^{-1}x, L_k^{-1}y\right) \tag{8.6}$$

of a distributive quasigroup $Q(A)$. The loop $Q(\cdot)$ has a neutral element $A(k,k) = k = 1$. Let us call it the loop $Q(\cdot)$ *corresponding to the distributive quasigroup* $Q(A)$ *at* k, and denote it by $Q\,[A]_k$, so $(\cdot) = [A]_k$. We now fix the element k. Further, we set

$$R = R_k \quad \text{and} \quad L = L_k.$$

The following lemma holds.

Lemma 8.1. The equalities

$$R(x \cdot y) = Rx \cdot Ry, \quad L(x \cdot y) = Lx \cdot Ly,$$

$$x(yz) = (Rx \cdot y)\,(Lx \cdot z)\,, \quad \text{and} \tag{8.7}$$

$$(yz)x = (yRx)\,(zLx) \tag{8.8}$$

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

Proof. 1. Using (8.6) and the commutativity of R and L, we have

$$R(x \cdot y) = RA\left(Rx^{-1}, L^{-1}y\right) = A\left(RR^{-1}x, RL^{-1}y\right) = A\left(R^{-1}Rx, L^{-1}Ry\right) = Rx \cdot Ry.$$

Thus, R is an automorphism of the loop $Q(\cdot)$. Similarly, L is an automorphism of the loop $Q(\cdot)$.

2. The equality (8.6) implies

$$A(x, y) = Rx \cdot Ly. \tag{8.9}$$

By (8.9) and the left distributive law for A, we obtain

$$Rx \cdot L(Ry \cdot Lz) = R\left(Rx \cdot Ly\right) L\left(Rx \cdot Lz\right)$$

and

$$Rx(LRy \cdot L^2z) = \left(R^2x \cdot RLy\right)\left(LRx \cdot L^2z\right).$$

Making the substitutions $x \to R^{-1}x$, $y \to L^{-1}R^{-1}y$ and $z \to L^{-2}z$ in the latter equality, and taking into account that $LR = RL$, we conclude

$$x(yz) = \left(Rx \cdot y\right)\left(Lx \cdot z\right).$$

The proof of the equality (8.8) is similar.

Distributive quasigroups are closely connected with Moufang loops. For distributive quasigroups, we have the following result.

Theorem 8.1. *Every distributive quasigroup is isotopic to a commutative Moufang loop.*

The proof of Theorem 8.1 is divided into the three parts.

1. *A loop $Q(\cdot)$ corresponding to the distributive quasigroup $Q(A)$ is an IP-loop.*

Consider the left distributive law for the operation A. Transform it as follows:

$$A\left[A(k, x), A(k, y)\right] = A\left[k, A(x, y)\right],$$

$$A\left\{A\left[k, A(k, y)\right], A\left[x, A(k, y)\right]\right\} = A\left[k, A(x, y)\right],$$

$$^{-1}A\left\{A\left[k, A(x, y)\right], A\left[A(x, k), A(x, y)\right]\right\} = A\left[k, A(k, y)\right].$$

Applying the second equality from (8.4) to the left side of the latter equality, we obtain

$$A\left\{^{-1}A\left[k, A(x, k)\right], A(x, y)\right\} = A\left[k, A(k, y)\right].$$

The mapping $^{-1}A(k, x)$ is a permutation. Let us denote it by L_0 :

$$L_0x = {}^{-1}A(k, x). \tag{8.10}$$

Then the equality (8.9) may be rewritten as

$$A\left[L_0Rx, A(x, y)\right] = L^2y.$$

Now we turn to the corresponding loop $Q(\cdot)$ using the formula (8.9). From the latter equality, we obtain

$$RL_0Rx \cdot L(Rx \cdot Ly) = L^2y, \quad \text{and} \quad RL_0Rx(LRx \cdot L^2y) = L^2y.$$

Replacing x with $L^{-1}R^{-1}x$ and y with $L^{-2}y$, we have

$$RL_0RL^{-1}R^{-1}x \cdot (xy) = y,$$

or

$$RL_0L^{-1}x \cdot (xy) = y. \tag{8.11}$$

Write

$$RL_0L^{-1} = I_l.$$

Then the equality (8.11) takes the form

$$I_lx \cdot (xy) = y. \tag{8.12}$$

Similarly, we prove that there exists a permutation

$$I_r = LR_0R^{-1},$$

where $R_0x = A^{-1}(x, k)$, such that the equality

$$(yx)I_rx = y \tag{8.13}$$

holds.

The equalities (8.12) and (8.13) imply that $Q(\cdot)$ is an IP-loop (see Chapter V, 1°), and, according to Property 5) of IP-loops we have

$$I_l = I_r = I,$$

where $Ix = x^{-1}$ and $x^{-1}x = xx^{-1}1$ (here, $k = 1$).

2. *A loop $Q(\cdot)$ corresponding to the distributive quasigroup $Q(A)$ is a Moufang loop.*

To prove this, we use the equality (8.7):

$$a(xy)I_rx = (Ra \cdot x)(La \cdot y). \tag{8.14}$$

Let us denote the left translation $x \to ax$ in the loop $Q(\cdot)$ by $\tilde{L}_a$, so

$$ax = \tilde{L}_ax.$$

The equality (8.14) implies

$$\tilde{L}_a(xy) = \tilde{L}_{Ra}x\tilde{L}_{La}y,$$

i.e., $(\tilde{L}_{Ra}, \tilde{L}_{La}, \tilde{L}_a)$ is an autotopy of the IP-loop $Q(\cdot)$. But then the element $a' = \tilde{L}_a1$, by the corollary to Lemma 5.5, is a Moufang element of the IP-loop $Q(\cdot)$, i.e. the element a' gives the identity

$$a'\,(y \cdot a'z) = (a'y \cdot a')\,z \tag{8.15}$$

for all $y, z \in Q$ (see the first Moufang identity (6.1) in Chapter V, 1°). But the element $a' = \tilde{L}_a 1 = a1 = a$ may be any element of the IP-loop $Q(\cdot)$, so the loop $Q(\cdot)$ is a Moufang loop.

3. *The loop $Q(\cdot)$ is commutative.*

Putting $y = 1$ in equality (8.7), we obtain

$$xz = Rx(Lxz). \tag{8.16}$$

But

$$x = RxLx,$$

by the idempotency of the distributive quasigroup $Q(A)$ and the equality (8.9). Consequently, the equality (8.16) takes the form

$$(RxLx)z = Rx(Lxz).$$

The latter equality shows that the triple of elements Rx, Lx, z of the Moufang loop $Q(\cdot)$ is associative. Then, by Moufang's Theorem (Theorem 6.5), the loop generated by the elements Rx, Lx, z, for arbitrary elements x, z, is associative, i.e. is a group. Hence in particular, we obtain

$$Rx(zLx) = (Rx \cdot z)Lx.$$

Using the equalities (8.6) and (8.7), we transform both sides of the equality (8.16):

$$Rx(zLx) = (1 \cdot Rx)(zLx) = (1 \cdot z)x = zx,$$

$$(Rx \cdot z)Lx = (Rx \cdot z)(Lx \cdot 1) = x(z \cdot 1) = xz.$$

Thus,

$$xz = zx$$

for all $x, z \in Q$. The proof of the theorem is complete.

Corollary. *Every loop which is isotopic to a distributive quasigroup $Q(A)$ is a Moufang loop $(Q, \cdot)$, and the mapping $x \to x^3$ is a central endomorphism in it.*

The validity of this statement follows from Theorem 6.1, Lemma 6.7 and Theorem 6.6.

Theorem 8.1 implies the following

Theorem 8.2. *If $Q(A)$ is a distributive quasigroup, the inverse operations A^{-1}, ${}^{-1}A$, ${}^{-1}(A^{-1})$, $({}^{-1}A)^{-1}$, $A^\star$ are all distributive. Further, the corresponding commutative Moufang loops at the same element $k = 1$ of Q coincide.*

Proof. 1. We prove the statement for the operation $A^\star$ first. It is easy to verify the left distributive law

$$A^\star\left[x, A^\star(y, z)\right] = A\left[A(z, y), x\right] = A\left[A(z, x), A(y, x)\right] = A^\star\left[A^\star(x, y), A^\star(x, z)\right].$$

The right distributive law is verified in similar fashion.

Now, we show that $[A^\star]_k = [A]_k$. According to the definition, we have

$$[A^\star]_k(x,y) = A^\star\left(R^{\star\,-1}_k x, L^{\star\,-1}_k y\right), \tag{8.17}$$

where $R^\star{}_k x = A^\star(x,k)$ and $L^\star{}_k x = A^\star(k,x)$. Since $A^\star(x,y) = A(y,x)$, we have $R^\star{}_k x = A^\star(x,k) = A(k,x) = L_k x$, i.e., $R^\star{}_k = L_k$. Similarly, one can show that $L^\star{}_k = R_k$. Thus, from the equality (8.17), we obtain

$$[A^\star]_k(x,y) = A^\star\left(L_k^{-1}x, R_k^{-1}y\right) = A\left(R_k^{-1}y, L_k^{-1}x\right) = [A]_k(y,x).$$

According to Theorem 8.1 $[A]_k$ is a commutative Moufang loop; consequently, $[A^\star]_k(x,y) = [A^\star]_k(y,x)$, whence

$$[A^\star]_k = [A]_k.$$

2. Now, we consider the operation A^{-1}.

The left distributive law for A^{-1} is proved in the same way as the equalities (8.4). The proof of the right distibutive law will use Theorem 8.1.

Let $A^{-1}(x,y) = z$. Then $A(x,z) = y$. By (8.9) we have $Rx \cdot Lz = y$. Thus

$$Lz = (Rx)^{-1}y \quad \text{and} \quad z = L^{-1}(Rx)^{-1}L^{-1}y.$$

But, since R is an automorphism of the loop $Q(\cdot)$, we have $(Rx)^{-1} = Rx^{-1}$, so

$$A^{-1}(x,y) = z = L^{-1}Rx^{-1}L^{-1}y.$$

Using this expression for A^{-1}, it is easy to prove that

$$A^{-1}\left[A(y,z),x\right] = A\left[A^{-1}(y,x), A^{-1}(z,x)\right]. \tag{8.18}$$

Indeed,

$$\begin{aligned}
A^{-1}\left[A(y,z),x\right] &= L^{-1}R(Ry\cdot Lz)^{-1}L^{-1}x \\
&= L^{-1}R\big(Lz^{-1}\cdot Ry^{-1}\big)L^{-1}x = \big(Rz^{-1}\cdot L^{-1}R^2y^{-1}\big)L^{-1}x \\
&= \big(L^{-1}R^2y^{-1}\cdot Rz^{-1}\big)L^{-1}x = \big(L^{-1}R^2y^{-1}\cdot RL^{-1}x\big)\big(Rz^{-1}\cdot LL^{-1}x\big) \\
&= R\big(L^{-1}Ry^{-1}\cdot RL^{-1}x\big)L\big(L^{-1}Rz^{-1}\cdot L^{-1}x\big) \\
&= RA^{-1}(y,x)LA^{-1}(z,x) = A\left[A^{-1}(y,x), A^{-1}(z,x)\right].
\end{aligned}$$

Since $Q\left(A^{-1}\right)$ is a quasigroup, there must exist an element z' such that

$$A^{-1}\left[A^{-1}(y,x), A^{-1}(z,x)\right] = A^{-1}\left[A^{-1}(y,z'),x\right].$$

This implies

$$A\left\{A^{-1}(y,x), A^{-1}\left[A^{-1}(y,z'),x\right]\right\} = A^{-1}(z,x).$$

By (8.18), we then have

$$A^{-1}\left\{A\left[y, A^{-1}(y,z')\right],x\right\} = A^{-1}(z,x),$$

and

$$A^{-1}(z', x) = A^{-1}(z, x),$$

i.e.,

$$z' = z.$$

Thus, the operation A^{-1} is distributive.

Now, we determine $\left[A^{-1}\right]_k$. By the definition of the loop $\left[A^{-1}\right]_k$, we have

$$\left[A^{-1}\right]_k(x, y) = A^{-1}\left({R'_k}^{-1}x, {L'_k}^{-1}y\right), \tag{8.19}$$

where

$$R'_k x = A^{-1}(x, k), \quad \text{and} \quad L'_k x = A^{-1}(k, x).$$

We find ${R'_k}^{-1}$. The equality $R'_k x = A^{-1}(x, k)$ implies $A(x, R'_k x) = k$. Replacing x with ${R'_k}^{-1}x$, we have $A\left({R'_k}^{-1}x, x\right) = k$, or ${R'_k}^{-1}x = {}^{-1}A(k, x)$. Thus, by (8.10), we obtain

$${R'_k}^{-1} = L_0.$$

From the equality $L'_k x = A^{-1}(k, x)$ we have $A(k, L'_k) = x$, or $LL'_k = 1$, i.e., ${L'_k}^{-1} = L$. Substituting these expressions for ${R'_k}^{-1}$ and ${L'_k}^{-1}$ into the equality (8.19), we obtain

$$\left[A^{-1}\right]_k(x, y) = A^{-1}(L_0 x, Ly),$$

whence

$$A\left[L_0 x, \left[A^{-1}\right]_k(x, y)\right] = Ly$$

or

$$RL_0 x \cdot L\left[A^{-1}\right]_k(x, y) = Ly,$$

so

$$L^{-1}RL_0 x \cdot L\left[A^{-1}\right]_k(x, y) = y. \tag{8.20}$$

But $RL_0L^{-1}x = I_l x = Ix = x^{-1}$, so we obtain the expression

$$L^{-1}RL_0 x = L^{-1}RL_0L^{-1}Lx = L^{-1}ILx = L^{-1}(Lx)^{-1} = L^{-1}Lx^{-1} = x^{-1}$$

for $L^{-1}RL_0$. The equality (8.20) then takes the form

$$x^{-1}\left[A^{-1}\right]_k(x, y) = y,$$

whence

$$\left[A^{-1}\right]_k(x, y) = xy$$

and

$$\left[A^{-1}\right]_k = [A]_k.$$

3. For the remaining operations, we argue as follows. It is easy to verify that

$$^{-1}A = \left[(A^\star)^{-1}\right]^\star.$$

Since the operation $A^\star$ is distributive, the operation $(A^\star)^{-1}$ is also distributive. Thus, the operation $\left[(A^\star)^{-1}\right]^\star$ is also distributive. We also have

$$\left[^{-1}A\right]_k = \left[\left[A^{\star -1}\right]^\star\right]_k = \left[A^{\star -1}\right]_k = [A^\star]_k = [A]_k.$$

Thus, the statement of the theorem is true for ^{-1}A.

4. Since the operation ^{-1}A is distributive, it follows that the operation $^{-1}(A^{-1})$ is also distributive, and

$$\left[^{-1}A^{-1}\right]_k = \left[A^{-1}\right]_k = [A]_k.$$

The result for $^{-1}(A^{-1})$ is proved in similar fashion. □

Remark. In the previous statements, the element k was fixed, and we showed that $[A]_k$ is a commutative Moufang loop. If we fix another element, say l, then we obtain another commutative Moufang loop $[A]_l$. But the loops $[A]_k$ and $[A]_l$ are isotopic (indeed, principal isotopic) to the distributive quasigroup A. Thus $[A]_k$ and $[A]_l$ are isotopic. Since $[A]_k$ and $[A]_l$ are commutative Moufang loops, then by Theorem 6.7 *the loops* $[A]_k$ *and* $[A]_l$ *are isomorphic.*

3°. Middle nuclei of distributive quasigroups

The following question arises: What is the type of a distributive quasigroup? To answer it, we prove a general statement: *If a quasigroup* $Q(\cdot)$ *is idempotent, then* $\mathscr{R} = \mathscr{L} = \{1\}$, where $\mathscr{R}$ and $\mathscr{L}$ are the respective groups of right and left regular permutations of the quasigroup $Q(\cdot)$.

Indeed, suppose $\lambda \in \mathscr{L}$. Then by the idempotency $\lambda(aa) = \lambda a$, so $(\lambda a)a = \lambda a$. But since $(\lambda a)(\lambda a) = \lambda a$, we obtain $\lambda a = a$, i.e., $\lambda = 1$. Similarly, we prove that $\mathscr{R} = \{1\}$.

Thus, the type of a distributive quasigroup is $(1, \Phi, 1)$, where Φ is the group of middle regular permutations.[4] This section examines the group Φ and the relative middle nuclei $N_m(k) = \Phi_k$ of a distributive quasigroup $Q(\cdot)$, for an arbitrary element k of Q.

Earlier, in Chapter II, 5°, the definition of a Φ-transitive quasigroup was given: A quasigroup Q is Φ-*transitive* if the group Φ acts transitively on Q.

Definition 2. A distributive quasigroup is described as *transitive* if it is Φ-transitive.

The following theorem characterizes transitivity of a distributive quasigroup.[5]

Theorem 8.3. *A distributive quasigroup $Q(A)$ is transitive if and only if it is medial.*

Proof. By Theorem 2.9, a transitive quasigroup is isotopic to a group. Therefore, the commutative Moufang loop $Q(\cdot)$ corresponding to a distributive quasigroup is an abelian group. Then, by (8.9), the equality

$$A(x,y) = Rx \cdot Ly$$

holds, defining A as an idempotent operation. As shown in Section 1°, the translations R and L of the quasigroup $Q(A)$ are automorphisms for $Q(\cdot)$, and commute: $RL = LR$. Thus,

$$A\left[A(x,y),A(u,v)\right] = A\left(Rx \cdot Ly, Ru \cdot Lv\right) = R\left(Rx \cdot Ly\right) \cdot L\left(Ru \cdot Lv\right)$$

$$= \left(R^2x \cdot RLy\right) \cdot \left(LRu \cdot L^2v\right) = \left(R^2x \cdot LRu\right) \cdot \left(RLy \cdot L^2v\right)$$

$$= RA(x,u) \cdot LA(y,v) = A\left[A(x,u),A(y,v)\right],$$

i.e., $Q(A)$ is medial.

Conversely, suppose A is medial and idempotent. Then A is left distributive:

$$A\left[x,A(y,z)\right] = A\left[A(x,x),A(y,z)\right] = A\left[A(x,y),A(x,z)\right].$$

The right distributive law is verified in similar fashion. By Lemma 2.6, the quasigroup $Q(A)$ is transitive. □

Theorem 8.3 implies that the existence of non-transitive distributive quasigroups is equivalent to the existence of non-medial distributive quasigroups.

Lemma 8.2. *In a distributive quasigroup $Q(A)$, the middle nucleus Φ_k (relative to an element k) is a normal subquasigroup.*

Indeed, suppose

$$A(x,y) = Rx \cdot Ly.$$

Then by (2.22), we have

$$\Phi_A = R^{-1}\Phi R,$$

where Φ_A and Φ are the respective groups of middle regular permutations of the quasigroup $Q(A)$ and the loop $Q(\cdot)$.

For the middle nucleus $\Phi_A 1$ of the quasigroup $Q(A)$ relative to the element $k = 1$, we have

$$\Phi_A 1 = R^{-1}\Phi R1. \tag{8.21}$$

But, $R1 = A(1,1) = 1$, and $\Phi 1 = N$ is the nucleus of the commutative Moufang loop $Q(\cdot)$. According to Theorem 6.3, the middle nucleus N_m coincides with the nucleus N of the loop $Q(\cdot)$. Furthermore, the nucleus of the loop $Q(\cdot)$ is normal (see Lemma 6.2). Note that *the nuclei of a loop are characteristic subloops*, i.e., they are invariant with respect to

arbitrary automorphisms of the loop. In particular, N is invariant with the respect to R^{-1} and therefore

$$\Phi_A 1 = N.$$

Applying Corollary 1 of Lemma 4.2, we conclude that $\Phi_A 1$ is a normal subquasigroup of $Q(A)$.

We derive a series of properties of the nucleus of the commutative Moufang loop $Q(\cdot)$ corresponding to a distributive quasigroup $Q(A)$.

Lemma 8.3. The solution of the equation $Ra = La \cdot x$ belongs to the nucleus N of the Moufang loop $Q(\cdot)$.

Indeed in the commutative Moufang loop $Q(\cdot)$, the identity

$$x^2(yz) = xy \cdot xz \tag{8.22}$$

holds for all $x, y, z \in Q$. Applying (8.7) to the identity (8.22),

$$x^2 \cdot yz = \left(Rx^2 \cdot y\right)\left(Lx^2 \cdot z\right),$$

and, comparing the right sides of the two latter equalities, we obtain

$$xy \cdot xz = \left(Rx^2 \cdot y\right)\left(Lx^2 \cdot z\right). \tag{8.23}$$

Making the substitutions $y \to x^{-1}y$ and $y \to Lx^{-2}z$, equality (8.23) becomes

$$\left[Rx^2x^{-1}y\right]z = y\left[x\left(Lx^{-2} \cdot z\right)\right]. \tag{8.24}$$

Set

$$Rx^2x^{-1}y = \phi_x y \quad \text{and} \quad x\left(Lx^{-2} \cdot z\right) = \phi_x^{\star} z.$$

Then the equality (8.24) takes the form

$$\phi_x y \cdot z = y \cdot \phi_x^{\star} z,$$

i.e., ϕ_x is a middle regular permutation of the loop $Q(\cdot)$, and $\phi_x^{\star}$ is adjoint to ϕ_x. Consequently, the element $\phi_x 1$ belongs to the nucleus of the loop $Q(\cdot)$ (see Chapter II, 2°). Set

$$\pi x = \phi_x 1 = Rx^2\left(x^{-1}1\right).$$

Then

$$\pi x = Rx^2 \cdot x^{-1}. \tag{8.25}$$

Since $\phi_x^{\star} 1 = \pi x \cdot 1$, we find one more expression for πx:

$$\pi x = x \cdot Lx^{-2}.$$

Now, we show that the solution of the equation $Ra = La \cdot x$ is πa. Indeed, (8.25) implies

$$Ra^2 = a \cdot \pi a, \tag{8.26}$$

so

$$Ra^2 \cdot La = (a \cdot \pi a)La, \quad (Ra \cdot Ra)La = (a \cdot La) \cdot \pi a,$$
$$Ra(Ra \cdot La) = (a \cdot La)\pi a, \quad Ra \cdot a = a(La \cdot \pi a).$$

Consequently,

$$Ra = La \cdot \pi a. \tag{8.27}$$

Corollary 1. *π is an endomorphism of the loop $Q(\cdot)$.*

Indeed,

$$\pi(xy) \cdot L(xy) = R(x \cdot y) = Rx \cdot Ry,$$

whence

$$\pi(xy)(LxLy) = (Lx\pi x)(Ly \cdot \pi y) = \left[(Lx\pi x)Ly\right]\pi y$$
$$= \left[(LxLy)\pi x)\right]\pi y = (LxLy)(\pi x \cdot \pi y),$$

so

$$\pi(xy) = \pi x \cdot \pi y.$$

Corollary 2. *For arbitrary x, y, the equation*

$$A(x, y) = A(y, x)\pi\left(xy^{-1}\right)$$

holds.

Indeed,

$$A(x, y) = Rx \cdot Ly = (Lx \cdot \pi x)\left[Ry \cdot (\pi y)^{-1}\right].$$

But by Corollary 1, π is an endomorphism of the loop $Q(\cdot)$, so $(\pi y)^{-1} = \pi y^{-1}$. Thus,

$$A(x, y) = (Lx \cdot \pi x)\left(Ry \cdot \pi y^{-1}\right) = (LxRy)\pi x\pi y^{-1} = (RyLx)\pi\left(xy^{-1}\right),$$

whence

$$A(x, y) = A(y, x)\pi\left(xy^{-1}\right).$$

Corollary 3. *The equality*

$$A(x,y) = x^{-1}y^2\rho\left(xy^{-1}\right),$$

holds, for some central endomorphism ρ of the commutative Moufang loop $(Q,\cdot)$.

Indeed, multiplying both sides of (8.26) by Rx, we obtain

$$Rx^2 \cdot Rx = x\pi \cdot x \cdot Rx, \quad Rx^3 = x \cdot \pi x \cdot Rx,$$

and

$$Rx = x^{-1} \cdot Rx^3 \cdot \pi x^{-1}. \tag{8.28}$$

By Lemma 6.7, the mapping $x \to x^3$ is a central endomorphism of the commutative Moufang loop, with $x^3 \in N$, so the mapping ρ defined by the equality

$$\rho x = Rx^3\pi x^{-1}$$

is also a central endomorphism:

$$\rho(xy) = R(xy)^3\pi(xy)^{-1} = Rx^3Ry^3\pi x^{-1}\pi y^{-1} = Rx^3\pi x^{-1} \cdot Ry^3\pi y^{-1} = \rho x \cdot \rho y.$$

Thus, (8.28) takes the form

$$Rx = x^{-1}\rho x.$$

By (8.29), we find

$$Lx = Rx\pi x^{-1} = x^{-1}\rho x \cdot \pi x^{-1} \tag{8.29}$$

and

$$A(x,y) = Rx \cdot Ly = x^{-1}\rho x \cdot y^{-1}\rho y \cdot \pi y^{-1} = x^{-1}y^{-1}\rho x\rho y\pi y^{-1}. \tag{8.30}$$

In particular, setting $x = y$ gives

$$y = A(y,y) = y^{-2}\rho y^2\pi y^{-1},$$

which implies

$$y^3\rho y^{-2} = \pi y^{-1}.$$

Substituting this expression for πy^{-1} in (8.30) gives

$$A(x,y) = x^{-1}y^{-1} \cdot \rho x \cdot \rho y \cdot y^3 \cdot \rho y^{-2}$$

or

$$A(x,y) = x^{-1}y^2\rho\left(xy^{-1}\right),$$

as required to complete the proof of Corollary 3.

The set of all elements of a quasigroup $Q(A)$ which commute with a given element k is called the *centralizer* Z_k of the element k. Then Lemma 8.3 implies

Corollary 4. *A centralizer Z_k in a distributive quasigroup $Q(A)$ is a commutative normal subquasigroup.*

Let $Q(\cdot)$ be the commutative Moufang loop corresponding to the element k in the quasigroup $Q(A)$. We show that $Z_k = \pi^{-1}\{1\}$, the kernel of the endomorphism π of $(Q, \cdot)$. As such, it will be a normal subloop of $(Q, \cdot)$. Indeed, if $a \in Z_k$, then

$$A(a, k) = A(k, a).$$

Thus $Ra = La$, i.e. $\pi a = 1$. The converse statement is immediate.

We now show that Z_k is invariant with respect to the automorphisms R, R^{-1}, L, and L^{-1}. We show that the equalities

$$R\pi = \pi R \quad \text{and} \quad L\pi = \pi L. \tag{8.31}$$

are satisfied. Indeed, the equality $Ra = \pi a La$ implies

$$R^2 a = R\left(\pi a \cdot La\right) = R\pi a \cdot RLa. \tag{8.32}$$

On the other hand,

$$R^2 a = R(Ra) = \pi(R \cdot a) \cdot R(La) = \pi Ra \cdot LRa. \tag{8.33}$$

Comparing the right sides of (8.32) and (8.33) we obtain the first of the equalities (8.31). The second equality is proved in the same way. Now, suppose $\pi a = 1$. Then $\pi Ra = R\pi a = R1 = 1$, i.e., $Ra \in Z_k$. Similarly, we deduce the invariance of Z_k with respect to the automorphisms R^{-1}, L, and L^{-1}.

Since Z_k is a normal subloop invariant with respect to R, R^{-1}, L, and L^{-1}, then according to Corollary 1 of Lemma 4.2 we conclude that Z_k is a normal subquasigroup of the distributive quasigroup $Q(A)$.

The proof of the commutativity of Z_k, based on (8.27), is simple. Let $a, b \in Z_k$. Then

$$A(a, b) = A(b, a)\pi\left(ab^{-1}\right).$$

But $\pi\left(ab^{-1}\right) = \pi a\left(\pi b^{-1}\right) = 1$, and consequently, $A(a, b) = A(b, a)$.

A quasigroup is called *anticommutative* if the equality $A(x, y) = A(y, x)$ holds only when $x = y$.

Theorem 8.4. *A finite anticommutative distributive quasigroup is transitive.*[6]

Indeed, let $Q(A)$ be anticommutative. Then $\pi a = 1$ holds only for $a = 1$, because the equality $Ra = La$ or $A(a, k) = A(k, a)$ holds only if $\pi a = 1 = k$. Thus, the endomorphism π is an automorphism, i.e., for any $b \in Q$, there exists $c \in Q$ such that $b = \pi c$. But πc belongs to the nucleus of the loop $Q(\cdot)$, so each element of Q lies in the nucleus of the loop $Q(\cdot)$. Thus $Q(\cdot)$ is a group, and $Q(A)$ is a transitive quasigroup.

To conclude, we prove the following lemma, which will be needed later.

Lemma 8.4. Suppose that $Q(\cdot)$ is a commutative Moufang loop. If there exist two automorphisms R and L such that for each $x \in Q$, the equation $Rx \cdot Lx = x$ holds and $Rx(Lx)^{-1}$ lies in the nucleus of $Q(\cdot)$, then $Q(\cdot)$ corresponds to a distributive quasigroup.

Let $Rx(Lx)^{-1} = \pi x$. Then $Rx = Lx\pi x$, where πx belongs to the nucleus of the loop $Q(\cdot)$. We verify (8.7) and (8.8). We have

$$(Rx \cdot y)(Lx \cdot z) = [(Lx \cdot \pi x)y]\,(Lx \cdot z) = [\pi x(Lx \cdot y)]\,(Lx \cdot z)$$

$$= \pi x \cdot [(L \cdot xy)(Lx \cdot z)] = \pi x \left[Lx^2 \cdot (yz)\right] = \left(\pi x Lx^2\right)(yz)$$

$$= \left[Rx(Lx)^{-1} \cdot Lx^2\right](yz) = (Rx \cdot Lx)(yz) = x(yz).$$

The proof of the equality (8.8) is similar.

Now L and R commute. Indeed, the equality $Rx \cdot Lx = x$ implies $R(Rx \cdot Lx) = Rx$ or $R^2x \cdot RLx = Rx$. On the other hand, substituting Rx for x in the equality $Rx \cdot Lx = x$, we obtain $R^2x \cdot LRx = Rx$. Thus, $RLx = LRx$.

Consider the operation A, defined by the formula

$$A(x, y) = Rx \cdot Ly.$$

Using (8.7) we can prove the left distributive law:

$$A\,[x, A(y, z)] = Rx \cdot L(Ry \cdot Lz) = Rx\left(LRy \cdot L^2z\right),$$

$$A\,[x, A(y, z)] = \left(R^2x \cdot LRy\right)\left(LRx \cdot L^2z\right). \tag{8.34}$$

We then have

$$A\,[x, A(y, z)] = \left(R^2x \cdot RLy\right)\left(LRx \cdot L^2z\right) = R\,(Rx \cdot Ly)\,L\,(Rx \cdot Lz)$$

$$= RA(x, y) \cdot LA(x, z) = A\,[A(x, y), A(x, z.)]$$

The proof of the right distributive law is similar.

Since $Rx = Rx \cdot L1 = A(x, 1)$ and $Lx = R1 \cdot Lx = A(1, x)$, we conclude that the loop $(Q, \cdot)$ corresponds to the distributive quasigroup $Q(A)$.

In the case of transitive distributive quasigroups, the second condition, that $Rx(Lx)^{-1}$ belongs to the nucleus, always holds.

4°. Connection with Steiner quasigroups and medial quasigroups

Let us recall that a quasigroup is a *TS-quasigroup* if the equality $A(a, b) = c$ implies the remaining five equalities obtained from the first by permutation of the elements a, b and c. For example, $A(a, c) = b$, $A(b, c) = a$, and so on. As was shown in Chapter VII, 1°,

this definition is equivalent to the following: A quasigroup $Q(A)$ is a TS-quasigroup if, for arbitrary $x, y \in Q$, the identities

$$\left.\begin{array}{c} A(x,y) = A(y,x) \text{ and} \\ A\left[x, A(x,y)\right] = y \end{array}\right\} \tag{8.35}$$

are satisfied. A Steiner quasigroup is an idempotent TS-quasigroup.

We now study the connection between distributive quasigroups and Steiner quasigroups.

The crucial importance of Steiner quasigroups for the study of distributive quasigroups results from Theorems 8.5 and 8.6 below, showing that every distributive quasigroup is an extension of a transitive distributive quasigroup by a distributive Steiner quasigroup.

Distributive Steiner quasigroups were first studied by Bruck [25]. Lemma 8.5 below is due to Bruck.

Theorem 8.5. *The quotient $Q(A)/\Phi_A k$ of a distributive quasigroup $Q(A)$ by its middle nucleus $\Phi_A k$ (relative to any given element k of Q) is a distributive Steiner quasigroup.*

Since the middle nucleus $\Phi_A k$ of the distributive quasigroup $Q(A)$ is a normal subquasigroup, we can consider its corresponding quotient $\overline{Q}(A) = \{\overline{a} \mid a \in Q\}$.

Let show that $\overline{Q}(A)$ is commutative. We use Corollary 2 to Lemma 8.3:

$$A(x,y) = A(y,x)\pi\left(xy^{-1}\right)$$

for $x, y \in Q$. Passing to the cosets, we obtain

$$A(\overline{x},\overline{y}) = \overline{A(x,y)} = \overline{A(y,x)\pi\left(xy^{-1}\right)} = \overline{A(y,x)} \cdot \overline{\pi\left(xy^{-1}\right)},$$

so

$$A(\overline{x},\overline{y}) = A(\overline{y},\overline{x})\overline{\pi\left(xy^{-1}\right)}. \tag{8.36}$$

But $\pi\left(xy^{-1}\right) \in \Phi_A k = \overline{1}$, so $\overline{\pi\left(xy^{-1}\right)} = \overline{1}$, whence, substituting in (8.36) we obtain

$$A(\overline{x},\overline{y}) = A(\overline{y},\overline{x}).$$

This commutativity, together with the observation that, by Lemma 6.7, $x^3 \in N$ or $\overline{x}^3 = \overline{1}$ for any $x \in Q$, enables application of the following simple lemma to complete the proof of Theorem 8.5.

Lemma 8.5. *Consider a commutative distributive quasigroup $Q(A)$. Then $Q(A)$ is a Steiner quasigroup if and only if each non-identity element of the corresponding commutative Moufang loop $(Q,\cdot)$ has order 3.*

Indeed, suppose $x^3 = 1$ for arbitrary $x \in Q(\cdot)$. If $Q(A)$ is a commutative, then (8.26) implies $\pi\left(xy^{-1}\right) = 1$ for all $x, y \in Q(\cdot)$, i.e., $\pi z = 1$ for all $z \in Q(\cdot)$. By (8.26), this means that $R = L$. Since $x^3 = 1$, we have $x(xx) = 1$. Passing to the operation A, we obtain

$$A\left[R^{-1}x, R^{-1}A\left(R^{-1}x, R^{-1}x\right)\right] = 1.$$

But $A\left(R^{-1}x, R^{-1}x\right) = R^{-1}x$, and

$$A\left(R^{-1}x, R^{-2}x\right) = 1,$$

whence

$$A\left(Rx, x\right) = R^2 1 = 1 = k, \quad A\left(Rx, x\right) = k, \quad \text{and} \quad A\left[x, A(x,k)\right] = k.$$

Since x and k are arbitrary elements of Q, the second equality from (8.35) is proved.

Conversely, suppose that $Q(A)$ is a distributive Steiner quasigroup. Since $Q(A)$ is commutative, $R = L$ (as proved earlier), and

$$A(a,b) = R(ab). \tag{8.37}$$

Returning to the loop $Q(\cdot)$, from (8.35) we obtain

$$R\left[a \cdot R(a,b)\right] = b,$$

which implies

$$R^{-1}a \cdot (ab) = R^{-2}b. \tag{8.38}$$

But if $a = b$ in (8.37), we find that

$$Ra^2 = a,$$

or

$$R^{-1}a = a^2. \tag{8.39}$$

Substituting (8.39) into (8.38) and setting $b = 1$ we obtain

$$a^2(a1) = 1^2,$$

or $a^3 = 1$, establishing the lemma.

A subquasigroup $H(A)$ of a quasigroup $Q(A)$ is *generated* by a subset or *alphabet* $M = \{a, b, c, \ldots\}$ if H consists of all *words*, composed of all *letters* $a, b, c, \ldots$ from the alphabet M, i.e., elements of the subset M.

The concept of a word is defined by a recursion on its *length*. For the recursion basis, *words of length* 1 are just taken as the elements of the subset M, the letters of the alphabet. If words of length $\leqslant n-1$ are already defined, then by a *word of length* n we mean an expression of the form $A^i(u,v)$, where A^i is one of the operations A, A^{-1}, or ${}^{-1}A$, and the arguments u and v are words of length $\leqslant n-1$, one of which has length exactly $n-1$.

Theorem 8.6. *If elements a, b, c, d of a distributive quasigroup satisfy the medial law equation*

$$A\left[A(a,b), A(c,d)\right] = A\left[A(a,c), A(b,d)\right], \tag{8.40}$$

then these elements generate a transitive distributive quasigroup. In other words, by Theorem 8.3, these elements generate a medial and idempotent quasigroup.

Without loss of generality, we consider $c = k = 1$. Now we turn to the operation $(\cdot)$: $xy = A\left(R^{-1}x, L^{-1}y\right)$. The equality (8.40) takes the form:

$$\left(R^2a \cdot LRb\right)\left(LR1 \cdot L^2d\right) = \left(R^2a \cdot LR1\right)\left(LRb \cdot L^2d\right)$$

or

$$\left(R^2a \cdot LRb\right)L^2d = R^2a\left(LRb \cdot L^2d\right). \tag{8.41}$$

Using (8.25), we obtain

$$LRb = L(Lb \cdot \pi b) = L^2b \cdot L\pi b = L^2b \cdot \pi Lb$$

and

$$\begin{aligned} R^2a = R(Ra) &= R(La \cdot \pi a) = R(La \cdot \pi a)\pi(La \cdot \pi a) \\ &= \left(L^2a \cdot L\pi a\right) \cdot \left(\pi La \cdot \pi^2 a\right) = L^2a \cdot \pi\left(La \cdot La \cdot \pi a\right) = L^2a \cdot \pi a. \end{aligned}$$

Substituting the values found for LRb andR^2a into the equality (8.41), we obtain

$$\left[\left(L^2a \cdot \pi a\right)\left(L^2b \cdot \pi Lb\right)\right]L^2d = \left(L^2a \cdot \pi a\right)\left[\left(L^2b \cdot \pi Lb\right)L^2d\right].$$

Since, for an arbitrary element a, the element πa belongs to the nucleus, this equality may be rewritten as

$$\left[\left(L^2a \cdot L^2b\right)L^2d\right](\pi a \cdot \pi Lb) = \left[L^2a\left(L^2b \cdot L^2d\right)\right](\pi a \cdot \pi Lb).$$

Dividing both sides by $\pi a \cdot \pi Lb$ and the automorphism L^2, we conclude

$$ab \cdot d = a \cdot bd.$$

By Moufang's Theorem, the elements a, b, d generate an associative subloop $H(\cdot)$ of the loop $Q(\cdot)$. It is easy to verify that the subloop $H'(\cdot)$ of the loop $Q(\cdot)$ generated jointly by the set $H(\cdot)$ and the nucleus of the loop $Q(\cdot)$, is also a group.

Let us denote the subquasigroup of the distributive quasigroup $Q(A)$ generated by the elements $a, b, c(= k = 1), d$ by $H_0(A)$. We will show that

$$H_0 \subseteq H'.$$

The elements $a, b, d, 1$ belong to $H'(\cdot)$. Assume that the words of length $\leqslant n-1$ from $H_0(A)$ already belong to $H'(\cdot)$. By Corollary 3 of Lemma 8.3, we have

$$A(u, v) = u^{-1}v^2\rho\left(uv^{-1}\right), \tag{8.42}$$

where for each x, the image ρx belongs to the nucleus of the loop $Q(\cdot)$. By Theorem 8.2, the commutative Moufang loops corresponding to the distributive quasigroups ${}^{-1}A$ and A^{-1} coincide with the same loop $(\cdot)$ that corresponds to the quasigroup A. Thus, for ${}^{-1}A$ and A^{-1}, we have analogous formulas:

$$\left.\begin{aligned} A^{-1}(u, v) &= u^{-1}v^2\rho_1\left(uv^{-1}\right) \\ {}^{-1}A(u, v) &= u^{-1}v^2\rho_2\left(uv^{-1}\right) \end{aligned}\right\}, \tag{8.43}$$

where ρ_1 and ρ_2 are central endomorphisms of the loop $Q(\cdot)$.

Let ω be a word of length n from $H_0(A)$. Then ω has the form

$$\omega = A^i(u, v),$$

where the arguments u and v are words of the length $\leqslant n-1$. By the induction hypothesis, $u, v \in H'(\cdot)$. By equations (8.42), (8.43), $\omega \in H'(\cdot)$, i.e., $H_0 \subset H'$.

Since $H'(\cdot)$ is a group, $H_0(\cdot)$ is also a group. This means that $H_0(A)$ is a transitive subquasigroup of the distributive quasigroup $Q(A)$.

Corollary 1. *Any three elements of a distributive quasigroup generate a transitive distributive subquasigroup.*

Indeed, the distributive and idempotent laws imply

$$A\left[A(a,b), A(c,c)\right] = A\left[A(a,b), c\right] = A\left[A(a,c), A(b,c)\right],$$

so the medial equation (8.34) holds for the quadruplea, b, c, c. Theorem 8.6 then yields the desired result.

Corollary 2. *A non-transitive distributive quasigroup requires at least four generators.*

Note that for general distributive quasigroups, the medial law does not hold. (An example is given below.) So far, we have seen that validity of the medial law in a distributive quasigroup is equivalent to its transitivity. Thus, the equation

$$A\left[A(a,b), A(c,d)\right] = A\left[A(a,x), A(b,d)\right]$$

is of great interest. Writing the solution as $[a,b,d]_c$, the medial law takes the form $[a,b,d]_c = c$ for all $a, b, c, d \in Q$.

Fixing an element c as $c = k = 1$, we write Q_k for the subquasigroup of $Q(A)$ that is generated by the set $\{[a,b,d]_k \mid a, b, d \in Q\}$. The following theorem reveals the significance of the subquasigroup $Q_k(A)$.

Theorem 8.7. *Let $Q(A)$ be a distributive quasigroup. Then the subquasigroup $Q_k(A)$ is a Steiner normal subquasigroup, and the quotient $Q(A)/Q_k(A)$ is transitive.*

Indeed, let $x = [a,b,d]_k$, so the equation

$$A\left[A(a,b), A(1,d)\right] = A\left[A(a,x), A(b,d)\right]$$

holds. Turning to the loop $Q(\cdot)$, we obtain

$$(R^2a \cdot RLb)L^2d = \left(R^2a \cdot RLx\right)\left(LRb \cdot L^2d\right). \tag{8.44}$$

Now, we transform (8.44) in the same way as was done in Theorem 8.6:

$$\left[\left(L^2a \cdot \pi a\right)\left(L^2b \cdot \pi Lb\right)\right]L^2d = \left[\left(L^2a \cdot \pi a\right) \cdot LRx\right]\left[\left(L^2b \cdot \pi Lb\right) \cdot L^2d\right],$$

$$\left[\left(L^2a\cdot L^2b\right)L^2d\right](\pi a\cdot \pi Lb)=\left[\left(L^2a\cdot LRx\right)\left(L^2b\cdot L^2d\right)\right](\pi a\cdot \pi Lb),$$
$$\left(L^2a\cdot L^2b\right)L^2d=\left(L^2a\cdot LRx\right)\left(L^2b\cdot L^2d\right),$$
$$ab\cdot d=\left(a\cdot RL^{-1}x\right)(bd). \tag{8.45}$$

At this point, we invoke the following result of Bruck [25].

Lemma 8.6. *In a commutative Moufang loop $Q(\cdot)$, write the solution of the equation*

$$ab\cdot d=(ax)(bd). \tag{8.46}$$

as $[a,b,d]$. Then the following statements hold:

1) $[\omega a,b,d]=[a,\omega b,d]=[a,b,\omega d]=[a,b,d]$, *where a,b, and d are arbitrary elements of Q, and ω is an element of the nucleus of $Q(\cdot)$;*

2) $[a,b,d]^3=1$ for all $a,b,d\in Q$.

Proof. 1. By the definition of $[a,b,d]$, we have

$$(a\omega\cdot b)d=(a[a\omega,b,d])(bd). \tag{8.47}$$

But $(a\omega\cdot b)d=(\omega a\cdot b)d=\omega(ab\cdot d)$. Transforming the right side of (8.47) and dividing it by ω, we obtain

$$(a[a,b,d])(bd)d=(a[a\omega,b,d])(bd),$$

which implies $[a\omega,b,d]=[a,b,d]$. The remaining equalities of the statement may be obtained in similar fashion.

2. By Lemma 6.7, the mapping $x\to x^3$ is a central endomorphism of the loop $Q(\cdot)$. Applying the endomorphism to (8.46) yields

$$a^3b^3\cdot d^3=\left(a^3[a,b,d]^3\right)\left(b^3d^3\right).$$

Since this equation concerns elements of the group $N(\cdot)$, the nucleus of the loop $Q(\cdot)$, it immediately gives $[a,b,d]^3=1$. □

Returning to the proof of Theorem 8.7, the equality (8.45) yields $RL^{-1}x=[a,b,d]$ or

$$[a,b,d]_k=LR^{-1}[a,b,d]. \tag{8.48}$$

By (8.46), we have

$$\varphi[a,b,d]=[\varphi a,\varphi b,\varphi d] \tag{8.49}$$

for an arbitrary automorphism ϕ of the loop $Q(\cdot)$. In particular,

$$R[a,b,d]=[Ra,Rb,Rd]. \tag{8.50}$$

Applying Lemma 8.3 to the right hand side of (8.50), we obtain

$$R[a,b,d]=[La\cdot\pi a,Lb\cdot\pi b,Ld\cdot\pi d]. \tag{8.51}$$

By Lemma 8.6, 1), we may remove the nuclear elements $\pi a, \pi b, \pi d$ from the right side of (8.51), so

$$R[a,b,d] = [La, Lb, Ld] = L[a,b,d], \tag{8.52}$$

whence

$$[a,b,d]_k = [a,b,d]$$

follows by (8.48).

Thus, $Q_k(A)$ is generated by all the solutions of the equation (8.46), where a, b, and d are arbitrary elements of Q. The corresponding Moufang loop $Q_k(\cdot)$ is generated by the all expressions $[a,b,d]$. By (8.48), the subloop $Q_k(\cdot)$ is characteristic.* Hence, $Q_k(\cdot)$ is invariant under every inner permutation, since inner permutations of a commutative Moufang loop are automorphisms, by Corollary 3 to Theorem 6.4. Thus, the subloop $Q(\cdot)$ is normal. Furthermore, $Q_k(\cdot)$ is invariant under the automortpisms R, R^{-1}, L and L^{-1}. Consequently, $Q_k(A)$ is a normal subquasigroup. By (8.52), $Q_k(A)$ is a commutative subquasigroup, and by Lemma 8.5 and Lemma 8.6, 2), we conclude that $Q_k(A)$ is a distributive Steiner subquasigroup.

Now we consider the quotient $\overline{Q}(A) = Q(A)/Q_k(A)$. By (8.46), we obtain

$$\overline{a}\overline{b} \cdot \overline{c} = (\overline{a} \cdot \overline{x}) \left(\overline{b} \cdot \overline{d}\right).$$

But $\overline{x} = \overline{1}$, so $x = [a,b,c] \in Q_k = \overline{1}$, whence,

$$\left(\overline{a} \cdot \overline{b}\right) \overline{c} = \overline{a} \left(\overline{b} \cdot \overline{c}\right).$$

Thus, the corresponding loop $\overline{Q}(A)$ is associative, which implies that it is transitive. The proof of the theorem is complete.

Theorem 8.7 offers an alternative perspective on one direction of Theorem 8.3.

Corollary 1. *A medial distributive quasigroup is transitive.*

Let $Q(A)$ be the quasigroup in question. Then $[a,b,d]_k = k$ for $a,b,d,k \in Q$, so Q_k just consists of the neutral element $k = 1$. Thus the quotient $Q(A)/Q_k(A)$ is isomorphic to $Q(A)$, which is then transitive by Theorem 8.7.

Corollary 2. *Suppose that a distributive quasigroup $Q(A)$ has no non-trivial Steiner subquasigroups. Then it is transitive.*

In fact, suppose that the only Steiner subquasigroups of the distributive quasigroup $Q(A)$ are trivial. Then, in particular, Q_k consists of just one element. Thus, the medial law holds, and $Q(A)$ is transitive by Theorem 8.3 or by Corollary 1.

*I.e., the subloop $Q_k(\cdot)$ is invariant under every automorphism of the loop $Q_k(\cdot)$.

5°. Examples of non-transitive distributive quasigroups

In this section, we present examples of non-transitive distributive quasigroups, i. e., distributive quasigroups which are not medial. To prepare for the examples, we first consider some properties of commutative distributive quasigroups. In a commutative distributive quasigroup $R = L$, so $Q(A)$ and $Q(\cdot)$ are connected by

$$A(a, b) = R(a \cdot b). \tag{8.53}$$

By (8.39),

$$R^{-1}a = a^2, \tag{8.54}$$

so squaring $a \to a^2$ is a permutation of the corresponding commutative Moufang loop. It is easy to see that the converse statement also holds.

If squaring $a \to a^2$ is a permutation on a commutative Moufang loop, then the loop corresponds to a commutative distributive quasigroup.

Indeed, according to the basic identity for commutative Moufang loops, the mapping $R^{-1}a = a^2$ is an automorphism:

$$a^2b^2 = a^2(bb) = (ab) \cdot (ab) = (ab)^2.$$

If $Ra^2 = a$, then the first hypothesis of Lemma 8.4 holds: $Ra \cdot Ra = a$. The second condition also holds: $Ra(La)^{-1}a = Ra(Ra)^{-1}$ is the nuclear element 1. Thus (8.53) determines a distributive and patently commutative quasigroup.

Theorem 8.8. *Every commutative Moufang loop of odd finite order corresponds to a commutative distributive quasigroup.*

Suppose that $Q(\cdot)$ is a commutative Moufang loop of odd finite order. Then the mapping $a \to a^2$ is a permutation. Indeed, let $x \to x^2$ and $y \to y^2$, and suppose $x^2 = y^2$. Since the elements x and y generate a commutative group, the equality $x^2 = y^2$ implies $(xy^{-1})^2 = 1$. Set $z = xy^{-1}$. Then $z^2 = 1$. But z^3 belongs to the nucleus, so $z = z^2 \cdot z = z^3$ is also nuclear. Since the nucleus of a commutative Moufang loop $A(\cdot)$ is a normal subloop of the loop, the order of the nucleus, as a divisor of an odd number, is itself an odd number. Thus, since $z^2 = 1$, we have $z = 1$, so $x = y$: the squaring $a \to a^2$ is a permutation.

Note that a Moufang loop (not necessarily commutative) of even order cannot be isotopic to any commutative distributive quasigroup, since no commutative distributive quasigroups of even order exist [78].

Theorem 8.8 implies that a commutative quasigroup of odd order corresponds to a transitive commutative distributive quasigroup.

Example of a non-transitive commutative distributive quasigroup. The required example is furnished by a non-associative commutative Moufang loop in which the mapping $x \to x^2$ is a permutation. Such an example was presented in Chapter VI, 5°. There, we considered a group $Q(\cdot)$ in which each element cubed to the identity, and defined the operation $x \circ y = x^{-1}yx^2$ to obtain a commutative non-associative Moufang loop $Q(\circ)$. Consider the operation

$$A(x, y) = R(x \circ y)$$

defined by the formula (8.53), where $R^{-1}a = a \circ a = a^{-1}$ according to (8.54). Then $Ra^{-1} = a$ or $Ra = a^{-1}$. Hence

$$A(a,b) = R(a \circ b) = (a \circ b)^{-1} = \left(a^{-1}ba^2\right)^{-1} = a^{-2}b^{-1}a.$$

But $a^3 = 1$, whence $a^{-2} = a$, and we obtain the formula

$$A(x,y) = xy^{-1}x$$

for the operation A. It is easy to show that the quasigroup $Q(A)$ is distributive but non-transitive. Moreover, it is easy to show that $Q(A)$ is a distributive Steiner quasigroup.

Notes

[1]The concept of a distributive quasigroup was introduced by C. Burstin and W. Mayer [34]. Some results of this paper were presented in the book of A.K. Sushkevich [78]. Here we mostly expound results from [16].

[2]Proposition b) implies that a distributive quasigroup has a transitive group of automorphisms: If a and b are arbitrary elements from Q, then there exists an automorphism α such that $\alpha a = b$. We can choose L_c, where $A(c, a) = b$, as α. B.Fischer [80] studied the group $R(A)$ generated by all the right translations of a distributive quasigroup. He proved that if $Q(A)$ is a finite distributive quasigroup, than $R(A)$ is a decidable group.

Also note that loops with a transitive group of automorphisms (their definition is the same as for quasigroups, with the condition that neither a nor b is the neutral element of a loop) were studied by Bruck [27]. He proved the following statement: If a loop $Q(\cdot)$ has a transitive group of automorphisms, and the descending chain condition holds for the normal subloops of $Q(\cdot)$, then $Q(\cdot)$ is a simple loop (the only normal subloops are Q and $\{1\}$.)

[3]Generally speaking, cosets of a subquasigroup H of a distributive quasigroup $Q(\cdot)$ need not posses the weak Lagrange property: aH and bH may have common elements, but not coincide. An example is provided in [20]).

[4]In [20] a non-trivial distributive quasigroup $Q(\cdot)$ of type $(1, 1, 1)$ was exhibited. There exist transitive distributive quasigroups of any order $n \neq 4k + 2$ (see the remarks in Chapter IX). Then, taking the cross-product of a such quasigroup with the quasigroup $Q(\cdot)$, we obtain distributive quasigroups with a middle nucleus of any order $n \neq 4k + 2$. A distributive quasigroup of type $(1, 1, 1)$ must be a Steiner quasigroup.

[5]Transitive medial distributive quasigroups were studied in [13]. Fulton and Stein [81] pointed out the connection between these quasigroups and conic sections. In [58] Osborn considered the relationship between Euclidean geometry and the medial quasigroup $Q(\circ)$ with $x \circ y = (1 - a)x + ay$, where $Q(+, \cdot)$ is the field of complex numbers, and $a \neq 0, 1$. In the same article the prolongation $(\cdot, \epsilon)$ of the loop $Q(\cdot)$ was studied, where ϵ is the identity map on $\mathbf{C}$ (see Definition 6 in Chapter VII, 5°). Finite medial distributive quasigroups were also studied by Sade [65].

[6]Sorkin [77] showed that a finite distributive quasigroup is either commutative, or could be obtained from a commutative quasigroup by a finite number of extensions by anticommutative quasigroups, i.e., by medial distributive quasigroups.

Chapter IX. Left-distributive quasigroups

1°. Left-distributive quasigroups which are isotopic to groups

The definition of a distributive quasigroup raises a question: Is left distributivity (8.1) independent of the right distributivity (8.2)? It transpires that this question has a positive answer: There exists a quasigroup $Q(A)$ in which the left distributive law

$$A[x, A(y, z)] = A[A(x, y), A(x, z)]$$

is satisfied, but the right distributive law is not. Such quasigroups were constructed by Stein [75] using a method of Hosszú [83].

Definition. A groupoid $Q(A)$ is called *left homogeneous*[1] *over a loop* $Q(\cdot)$ if there exists a permutation φ such that

$$A(x, y) = x \cdot \varphi(x \backslash y),$$

where $(\backslash) = (\cdot)^{-1}$, i.e., $(\backslash)$ is the right inverse operation for $(\cdot)$. Analogously, *a right homogeneous operation over* $Q(\cdot)$ is defined by

$$A(x, y) = \varphi(x/y) \cdot y.$$

In particular, if $Q(\cdot)$ is a group, a Moufang loop, or more generally an IP-loop, then a left homogeneous operation over $Q(\cdot)$ would take the form

$$A(x, y) = x \cdot \varphi(x^{-1}y),$$

since $x \backslash y = x^{-1}y$ in an IP-loop.

Using the notion of homogeneity, we formulate the following.

Theorem 9.1. *A distributive quasigroup is both right and left homogeneous over a commutative Moufang loop.*[2]

Indeed, in the previous chapter it was shown that a distributive quasigroup $Q(A)$ is isotopic to a commutative Moufang loop $Q(\cdot)$, with

$$A(x, y) = Rx \cdot Ly$$

for $x, y \in Q$, where R and L are automorphisms of the loop $Q(\cdot)$.

To prove the theorem, recall that Rx, Lx and y generate an associative subloop $H(\cdot)$ of $Q(\cdot)$. The subloop $H(\cdot)$ contains the element x (as $x = Rx \cdot Lx$). Consequently, the element x^{-1} lies in H. Thus, we have

$$(x^{-1}Lx)y = x^{-1}(Lx \cdot y)$$

Interchanging x with x^{-1} and y with Ly, we obtain

$$(xLx^{-1})Ly = x(Lx^{-1}Ly),$$

$$Rx \cdot Ly = xL(x^{-1}y), \quad \text{and}$$

$$A(x, y) = xL(x^{-1}y)$$

successively.

The following theorems provide answers to the question raised at the beginning of the section. Theorem 9.2 makes use of the concept of a *full permutation* of a quasigroup $Q(\cdot)$. Thus, a permutation ϕ of Q is *full* if, when $\phi' x \cdot \phi x = x$ holds for any $x \in Q$, then the self-map ϕ' of Q is a permutation.

Theorem 9.2. *If a left-distributive quasigroup $Q(A)$ is isotopic to a group $Q(\cdot)$, then it is left homogeneous over the group:*

$$A(x, y) = x\theta(x^{-1}y),$$

with θ as a full automorphism of the group $Q(\cdot)$. Conversely, if a groupoid $Q(A)$ is left homogeneous over a group $Q(\cdot)$, namely $A(x, y) = x\theta(x^{-1}y)$, where θ is a full automorphism of the group, then $Q(A)$ is a left-distributive quasigroup.[3]

Proof. First assume, without loss of generality, that a left distributive quasigroup $Q(A)$ is a principal isotope of a group $Q(\cdot)$, with

$$A(x, y) = \varphi x \cdot \psi y. \tag{9.1}$$

Note (9.1) with $x = \varphi^{-1}1$ implies that

$$L_{\varphi^{-1}1} = \psi,$$

whence ψ, as a left multiplication in the left distributive quasigroup $Q(A)$, is an automorphism of $Q(A)$. Again, (9.1) with $y = x$ yields

$$x = \varphi x \cdot \psi x, \tag{9.2}$$

so ψ is a full automorphism of $Q(A)$. Then

$$\psi(\varphi x \cdot \varphi y) = \varphi(\psi x) \cdot \psi(\psi y),$$

so

$$\psi(xy) = \varphi\psi\varphi^{-1}x \cdot \psi y.$$

This means that ψ is a quasiautomorphism of the group $Q(\cdot)$. By Lemma 2.5, the permutation ψ can be presented as

$$\psi x = k\theta x,$$

where θ is an automorphism of the group $Q(\cdot)$. Now φ may be recovered from the equality (9.2) as

$$\varphi x = x(\psi x)^{-1} = x(k\theta x)^{-1} = x\theta x^{-1}k^{-1}.$$

Thus,

$$A(x,y) = \varphi x \cdot \psi x = x\theta x^{-1}k^{-1} \cdot k\theta y = x\theta(x^{-1}y).$$

Here θ is a full automorphism of the group $Q(\cdot)$, because

$$x = \varphi x \cdot \psi x = (\varphi x \cdot k)\theta x = \lambda x \cdot \theta x$$

for $x \in Q$.

Conversely, suppose that a groupoid $Q(A)$ is left homogeneous over a group $Q(\cdot)$:

$$A(x,y) = x\theta(x^{-1}y),$$

with θ as a full automorphism of $Q(\cdot)$. We first show that $Q(A)$ is a quasigroup. Clearly $A(a,y) = b$ is uniquely solvable. It thus suffices to show that $A(x,a) = b$ is uniquely solvable. The equation $A(x,a) = b$ is equivalent to $x\theta(x^{-1}a) = b$ or $x\theta x^{-1} = b\theta a^{-1}$. Since θ is a full automorphism, the self-map $x \to x\theta x^{-1}$ is a permutation of the set Q. Thus, there exists a unique element x_0 such that $x_0\theta x_0^{-1} = b\theta a^{-1}$.

We now verify the left distributive law in $Q(A)$:

$$A[A(x,y),A(x,z)] = A(x\theta(x^{-1}y), x\theta(x^{-1}z))$$

$$= x\theta(x^{-1}y) \cdot \theta[(x\theta(x^{-1}y))^{-1}x\theta(x^{-1}z)] = x\theta(x^{-1}y)\theta[\theta(y^{-1}x)x^{-1} \cdot x\theta(x^{-1}z)]$$

$$= x\theta(x^{-1}y)\theta[\theta(y^{-1}x)\theta(x^{-1}z)]$$

$$= x\theta(x^{-1}y)\theta^2(y^{-1}z) = x\theta[x^{-1}y\theta(y^{-1}z)] = A[x,A(y,z)].$$

This completes the proof of the theorem. □

Theorem 9.3. *Under the equivalent conditions of Theorem 9.2, the quasigroup $Q(A)$ is distributive if and only if the group $Q(\cdot)$ is abelian.*

Indeed, if $Q(A)$ is distributive, then it is isotopic to a commutative Moufang loop $Q(+)$. On the other hand, $Q(A)$ is isotopic to a group $Q(\cdot)$ according to Theorem 9.2. Thus, the commutative Moufang loop $Q(+)$ is isotopic to the group $Q(\cdot)$, whence $Q(+)$ and $Q(\cdot)$ are isomorphic. Therefore, $Q(\cdot)$ is an abelian group.

Conversely, let $Q(\cdot)$ be an abelian group. Then

$$\lambda(xy) = xy\theta(x^{-1}y^{-1}) = xy\theta x^{-1}\theta y^{-1} = x\theta x^{-1}y\theta y^{-1} = \lambda x \cdot \lambda y,$$

so the permutation $\lambda x = x\theta x^{-1}$ is also an automorphism. The right distributive law is now easy to check.

Theorems 9.2 and 9.3 imply the existence of left distributive quasigroups which are not right distributive. It suffices to take a noncommutative group $Q(\cdot)$ which has a full automorphism.

If a group $Q(\cdot)$ is finite, the concept of a full automorphism coincides with the concept of a *special* automorphism, an automorphism θ satisying the implication $\theta c = c \Rightarrow c = 1$ for $c \in Q$. In other words, the only element of $Q(\cdot)$ left invariant by θ is the identity element.

Indeed, consider a full automorphism θ, say with $\lambda x \cdot \theta x = x$ for all $x \in Q$. Suppose $\theta c = c$ for some $c \in Q$. Then $\lambda c \cdot \theta c = c$ implies $\lambda c = 1$. In particular, $\lambda 1 \cdot \theta 1 = 1$ implies $\lambda 1 = 1$. Thus, $\lambda c = \lambda 1$, so $c = 1$. Conversely, let θ be a special automorphism, and let $\lambda x = x\theta x^{-1}$, $\lambda y = y\theta y^{-1}$. Now $\lambda x = \lambda y$ implies $x\theta x^{-1} = y\theta y^{-1}$ or $y^{-1}x = \theta y^{-1}\theta x = \theta(y^{-1}x)$. Thus $y^{-1}x = 1$ or $y = x$, by the definition of a special automorphism. Because Q is a finite set, we conclude that λ is a permutation, and thus θ is a full automorphism.

B. Neumann [55] gives an example of a finite noncommutative group with a special automorphism. So, the existence of a left distributive quasigroup which is not right distributive group is established.[4]

2°. Moufang loop cores

It is natural to ask the question: *Do other classes of left distributive quasigroups exist, not isotopic to groups?* We will provide a positive answer, using a concept introduced by Bruck [31] in the context of Moufang loops.

Definition 2. Let $Q(\cdot)$ be a loop, and let $(\cdot)^{-1} = (\backslash)$. The groupoid $Q(+)$, with the operation

$$x + y = x(y\backslash x), \tag{9.3}$$

is called the *core* of the loop $Q(\cdot)$.

In the case where $Q(\cdot)$ is a Moufang loop, (9.3) becomes

$$x + y = x(y^{-1}x),$$

unambiguously written as

$$x + y = xy^{-1}x$$

using the diassociativity of Moufang loops.

Theorem 9.4. *The core $Q(+)$ of a Moufang loop $Q(\cdot)$ is a quasigroup if and only if the squaring $x \to x^2$ is a permutation of Q.*

If $Q(+)$ is a quasigroup, the equation $x + 1 = a$ with unknown x has a unique solution, i.e., $x(1^{-1}x) = a$ or $x^2 = a$ has a unique solution for any $a \in Q$. Write this unique solution as $a^{1/2}$. Conversely, suppose that $x^2 = a$ with unknown x is uniquely solvable for any $a \in Q$. The equation

$$a + y = b$$

is equivalent to the equation

$$ay^{-1}a = b,$$

which is, obviously, uniquely solvable; its solution will be

$$y = ab^{-1}a.$$

Consider the equation

$$x + a = b \tag{9.4}$$

with unknown x Assume a solution exists:

$$x_0 + a = b$$

or

$$x_0 a^{-1} x_0 = b.$$

Multiplying by a^{-1} on the right-hand side, we obtain

$$x_0 a^{-1} x_0 a^{-1} = (x_0 a^{-1})^2 = ba^{-1},$$

whence

$$x_0 a^{-1} = (ba^{-1})^{1/2} \quad \text{or}$$

$$x_0 = (ba^{-1})^{1/2} a.$$

Thus, the uniqueness of the solution to equation (9.4) is established.

We now show that x_0 from (9.5) definitely solves equation (9.4):

$$\begin{aligned} x_0 + a = x_0 a^{-1} x_0 &= (ba^{-1})^{1/2} a \cdot a^{-1} (ba^{-1})^{1/2} a \\ &= (ba^{-1})^{1/2} \cdot (ba^{-1})^{1/2} \cdot a^{-1} = ba^{-1} \cdot a = b. \end{aligned} \tag{9.5}$$

The proof of the theorem is complete.

Theorem 9.5. *The left distributive law*

$$x + (y + z) = (x + y) + (x + z) \tag{9.6}$$

(for any $x, y, z \in Q$) holds in the core $Q(+)$ of a Moufang loop.

Proof. In the proof, we use the defining identities (6.1), (6.2), (6.9) of a Moufang loop, the identities (6.3)–(6.5), and also the fact that a Moufang loop is an IP-loop. We have

$$t = (x + y) + (x + z) = xy^{-1}x + xz^{-1}x = xy^{-1}x \cdot (xz^{-1}x)^{-1} \cdot xy^{-1}x.$$

From this it follows that

$$t = xy^{-1}x \cdot x^{-1}zx^{-1} \cdot xy^{-1}x = (xy^{-1}x \cdot x^{-1}zx^{-1})(xy^{-1}x) \quad \text{or}$$

$$t = \{x[y^{-1}(x \cdot x^{-1}zx^{-1})]\} \cdot xy^{-1}x.$$

The expression in parentheses is

$$x \cdot x^{-1}zx^{-1} = (xx^{-1} \cdot z)x^{-1} = zx^{-1}.$$

Thus,

$$\begin{aligned} t &= [x(y^{-1} \cdot zx^{-1})] \cdot xy^{-1}x = (\{[x(y^{-1} \cdot zx^{-1})]x\}y^{-1})x \\ &= \{[xy^{-1} \cdot (zx^{-1} \cdot x)]y^{-1}\}x = [(xy^{-1} \cdot z)y^{-1}]x = [x(y^{-1}zy^{-1})]x \\ &= x \cdot y^{-1}zy^{-1} \cdot x = x \cdot (y+z)^{-1}x = x + (y+z). \end{aligned}$$

The equality (9.6) is proved, and so $Q(+)$ is left-distributive. □

Theorems 9.4 and 9.5 imply the following.

Theorem 9.6. *Let $Q(\cdot)$ be a Moufang loop in which the square mapping $x \to x^2$ is a permutation. Then the core of $Q(\cdot)$ will be a left distributive quasigroup.*

The question arises: Will the left distributive quasigroup that was constructed in Theorem 9.6 also be right distributive? The answer is given by the following theorem.

Theorem 9.7. *A necessary and sufficient condition for the core of a Moufang loop $Q(\cdot)$ to be distributive is satisfaction of the equation*

$$xy^2x = yx^2y \tag{9.7}$$

for any $x, y \in Q$.

Proof. The condition (9.7) is necessary. If $x + y = xy^{-1}x$, is also right-distributive, then, in particular, we should have

$$(y + x^{-1}) + 1 = (y + 1) + (x^{-1} + 1), \tag{9.8}$$

whence $yxy + 1 = y^2 + x^{-2}$ or $(yxy)^2 = y^2x^2y^2$.

$$yxy \cdot yxy = y^2x^2y^2. \tag{9.9}$$

Dividing both sides of (9.9) by y from left and right, we obtain the condition (9.7).

The condition (9.7) is sufficient. Indeed, if we work backwards from the equality (9.9), we obtain (9.8). Let z be an element of Q. The permutation L_z^+ defined by $L_z^+a = z + a$, is an automorphism of the left distributive quasigroup $Q(+)$. Applying the automorphism L_z^+ to each side of (9.8), we obtain

$$(L_z^+y + L_z^+x^{-1}) + L_z^+1 = (L_z^+y + L_z^+1) + (L_z^+x^{-1} + L_z^+1). \tag{9.10}$$

But $L_z^+1 = z + 1 = z^2$, $L_zVy = zy^{-1}z$, and $L_z^+x^{-1} = zxz$. Replacing z^2, $zy^{-1}z$, and zxz respectively with u, v, w, from (9.10) we get $(v+w)+u = (v+u)+(w+u)$. Because u, v, w may by any elements of the loop $Q(\cdot)$, the theorem is proved. □

The next question arises: To which loops are left distributive quasigroups isotopic? When a left distributive quasigroup is the core of a Moufang loop, the following theorem gives the answer.

Theorem 9.8. *A left distributive quasigroup $Q(A)$ which is the core of a Moufang loop $Q(\cdot)$ is isotopic to a loop $Q(\circ)$ with*

$$[x \circ (y \circ x)] \circ z = x \circ [y \circ (x \circ z)], \tag{9.11}$$

i.e., a left Bol loop (see Chapter VI, 6°).

Proof. Consider the principal isotope

$$x \circ y = A(R^{-1}x, L^{-1}y), \tag{9.12}$$

of a left distributive quasigroup $Q(A)$, where $Rx = A(x, 1)$ and $Lx = A(1, x)$. Here, 1 is the unit of the Moufang loop $Q(\cdot)$). By definition of the core, the two preceding equalities take the form

$$Rx = x^2 \quad \text{and} \quad Lx = x^{-1}.$$

So, from (9.9) we find

$$A(x, y) = Rx \circ Ly = x^2 \circ y^{-1},$$

whence

$$x^2 \circ y = xyx. \tag{9.13}$$

We compute $(x^2 \circ y)^2 \circ z$ in the Moufang loop $Q(\cdot)$:

$$(x^2 \circ y)^2 \circ z = xyz \cdot z \cdot xyx = xyx \cdot (z \cdot xyx) = (x \cdot yx)[(zx \cdot y) \cdot x]$$

$$= x[yx \cdot (zx \cdot y)]x = x[y(x \cdot zx)y]x = x[y(xzx)y]x$$

$$= x[y(x^2 \circ z)y]x = x[y^2 \circ (x^2 \circ z)]x = x^2 \circ [y^2 \circ (x^2 \circ z)],$$

so

$$(x^2 \circ y)^2 \circ z = x^2 \circ [y^2 \circ (x^2 \circ z)]. \tag{9.14}$$

The unit of the loop $Q(\cdot)$ is the unit of the loop $Q(\circ)$, so setting $z = 1$ in (9.14) gives $(x^2 \circ y)^2 = x^2 \circ (y^2 \circ x^2)$ so, $[x^2 \circ (y^2 \circ x^2)] \circ z = x^2 \circ [y^2 \circ (x^2 \circ z)]$. Finally, replacing x^2 and y^2 with x and y (recalling from Theorem 9.4 that squaring is a permutation in the current context), we obtain the desired identity (9.7). □

Corollary 1. *The loop $Q(\circ)$ of Theorem 9.8 is a Moufang loop if and only if the condition (9.7) holds in the Moufang loop $Q(\cdot)$.*

Note that the equality (9.13) could be rewritten as

$$x \circ y = x^{1/2} y x^{1/2}. \tag{9.15}$$

If $Q(\circ)$ is a Moufang loop, it satisfies the right alternative law

$$y \circ (x \circ x) = (y \circ x) \circ x. \tag{9.16}$$

Passing to the loop $Q(\cdot)$ using equality (9.15), this becomes

$$y^{1/2}(x^{1/2}xx^{1/2})y^{1/2} = (y^{1/2}xy^{1/2})^{1/2}x(y^{1/2}xy^{1/2})^{1/2}.$$

Replacing $y^{1/2}$ with y yields

$$yx^2y = (yxy)^{1/2}x(yxy)^{1/2}. \tag{9.17}$$

Denote yxy by z^2. Then $y^{-1}z^2y^{-1} = y^{-1}(yxy)y^{-1} = x$. Substituting this value for x into (9.17), we obtain

$$y(y^{-1}z^2y^{-1})^2y = (z^2)^{1/2} \cdot y^{-1}z^2y^{-1} \cdot (z^2)^{1/2}, \quad \text{i.e.,}$$

$$z^2y^{-2}z^2 = zy^{-1}z^2y^{-1}z \quad \text{or} \quad zy^{-2}z = y^{-1}z^2y^{-1}.$$

Finally, replacing y^{-1} with y and taking into account that y and z are arbitrary elements, we obtain the identity (9.7).

Since all these transitions from (9.16) to (9.17) are reversible, condition (9.7) implies (9.16). However, if the left Bol loop $Q(\circ)$ is right alternative, it is a Moufang loop.

Combining Theorem 9.7 with Corollary 1 of Theorem 9.8, we obtain

Corollary 2. *If condition (9.7) holds in a Moufang loop $Q(\cdot)$, its core is a distributive quasigroup isotopic to the Moufang loop $Q(\circ)$ constructed by formula* (9.15).[5]

From Theorem 8.1, which stated that any distributive quasigroup is isotopic to a commutative Moufang loop, it follows that the operation $(\circ)$ is commutative.

From all that has been said, it follows that if we take the core $Q(+)$ of a Moufang loop $Q(\cdot)$ in which squaring $x \to x^2$ is a permutation and condition (9.7) is not satisfied, we will obtain a left distributive quasigroup which is not right distributive. The quasigroup $Q(+)$ cannot be isotopic to a group, because then, $Q(\circ)$ would be a group, while in fact it is not even a Moufang loop.

Example. Take the group $Q(\cdot)$ considered in [89, p.225]. It has order $3^\alpha q^3$, where q is a prime number of the form $3k+2$. The group has a minimal set $\{a, b, c, d\}$ of generators, subject to the system

$$a^{3^\alpha} = 1, \quad b^q = c^q = d^q = 1,$$

$$cb = bcd, , \quad a^{-1}ba = c, \quad a^{-1}ca = b^{-1}c^{-1},$$

$$da = ad, \quad db = bd, \quad dc = cd$$

of defining relations. The relations $a^{-1}ba = c$ and $a^{-1}ca = b^{-1}c^{-1}$ imply $a^{-2}ba^2 = a^{-1}(a^{-1}ba)a = a^{-1}ca = b^{-1}c^{-1}$. Multiplying from the left by b, we have $ba^{-2}ba^2 = c^{-1}$. If condition (9.7) were satisfied in this group, we could interchange $ba^{-2}b$ with $a^{-1}b^2a^{-1}$ in this latter equation:

$$c^{-1} = (a^{-1}b^2a^{-1})a^2 = a^{-1}b^2a = (a^{-1}ba)^2 = c^2,$$

whence $c^3 = 1$. This would contradict the minimality of the generating set $\{a, b, c, d\}$. Thus, condition (9.7) is not satisfied in the group, so the core of the group $Q(\cdot)$ is left distributive, but not right distributive, and is also not isotopic to a group.

As Bruck showed [31], the core of a Moufang loop is an isotopy invariant. In other words, the following theorem holds.

Theorem 9.9. *Suppose that Moufang loops $Q(\circ)$ and $Q(\cdot)$ are isotopic. Then their cores are isomorphic.*

Proof. A principal isotopy of the loops $Q(\circ)$ and $Q(\cdot)$ should have the form

$$x \circ y = R_a^{-1} x \cdot L_b^{-1} y,$$

or

$$x \circ y = xu \cdot vy,$$

because $R_a^{-1} = R_{a^{-1}} = R_u$ and $L_b^{-1} = L_{b^{-1}} = L_v$, due to the fact that every Moufang loop is an IP-loop.

Let $Q(\oplus)$ and $Q(+)$ be the respective cores of $Q(\circ)$ and $Q(\cdot)$. Then

$$x \oplus y = x \circ y^{(-1)} \circ x, \tag{9.18}$$

where $y \circ y^{(-1)} = e$ and $e = ba$. Writing the right-hand side of (9.18) in terms of the operation $(\cdot)$, we obtain

$$\begin{aligned} x \oplus y = (x \circ y^{(-1)}) \circ x &= [(xu \cdot vy^{(-1)})u](vx) \\ &= [x(u \cdot vy^{(-1)}u)] \cdot (vx) = x[(u \cdot vy^{(-1)} \cdot u)v]x, \end{aligned}$$

or

$$x \oplus y = xy_1x, \tag{9.19}$$

where

$$y_1 = (u \cdot vy^{(-1)} \cdot u)v$$

does not depend on x. Setting $y = x$ in (9.19),

$$y = y \oplus y = yy_1y,$$

whence

$$y_1 = y^{-1}$$

or

$$x \oplus y = xy_1x = xy^{-1}x = x + y,$$

as required. □

3°. Certain results on F-quasigroups

Left-distributive quasigroups are closely related to F-quasigroups (see Chapter III, 5°). More precisely, a left distributive quasigroup is a (left) F-quasigroup. Indeed, let $Q(\cdot)$ be a left distributive quasigroup:

$$x \cdot yz = xy \cdot xz. \tag{9.20}$$

It is clear that the mapping $S_a : x \to a\backslash x^*$ is a permutation. Replacing z in (9.20) with

$$S_x z = x\backslash z,$$

we obtain

$$x(y \cdot S_x z) = xy \cdot xS_x z.$$

By the definition of the operation $(\backslash)$, we have

$$xS_x z = x(x\backslash z) = z.$$

Thus, the left distributive law (9.20) takes the form

$$xy \cdot z = x \cdot yS_x z, \tag{9.21}$$

i.e. *a left distributive quasigroup is a (left) F-quasigroup.*

Note that in this case the permutations S_x are automorphisms of the quasigroup $Q(\cdot)$:

$$S_x(yz) = S_x y \cdot S_x z.$$

Indeed, it is easy to see that $S_x = L_x^{-1}$, and left translations of left distributive quasigroups are automorphisms.

On the other hand, the equality (3.32) established for any F-quasigroup gives the possibility to characterize F-quasigroups by an identity that is very close to the left distributive law. More precisely, (3.32) implies that

$$z = e_x \cdot S_x z,$$

so substituting this value for z into (9.21), we obtain

$$(xy) \cdot (e_x S_x z) = x(y \cdot S_x z),$$

or

$$(xy)(e_x z) = x(yz). \tag{9.22}$$

The equalities (9.21) and (9.22) are easily seen to be equivalent. Furthermore, (9.21) also implies that *an idempotent (left) F-quasigroup is a left distributive quasigroup*, since in this case $e_x = x$.

In Chapter III, 5° it was shown that F-quasigroups are isotopic to F-quasigroups with a left unit. Assume that $Q(\cdot)$ is an *F-quasigroup with a left unit* 1. Consider the isotope $Q(\circ)$ of the F-quasigroup $Q(\cdot)$, with

$$x \circ y = R^{-1}(x \cdot Ry), \tag{9.23}$$

where $Rx = x1$. It is easy to see that $Q(\circ)$ is a loop, with 1 as its unit element:

$$x \circ 1 = R^{-1}(x \cdot R1) = R^{-1}(x1) = R^{-1}(Rx) = x, \quad \text{and}$$

$$1 \circ x = R^{-1}(1 \cdot Rx) = R^{-1}(Rx) = x,$$

since $R1 = 1 \cdot 1 = 1$.

We will need the following result.

*Recall the equivalence of $xy = z$ and $x\backslash z = y$, i.e., $(\cdot)^{-1} = (\backslash)$.

Lemma 9.1. *There exists an automorphism $\theta_{x,y}$ of the quasigroup $Q(\cdot)$, depending on the elements x and y, such that*

$$S_x S_y = \theta_{x,y} S_{y\circ x}$$

holds for any $x, y \in Q$.

Proof. We determine $(\cdot)^{S_x S_y}$, using the equality (3.23) and bearing in mind that in the our case φ_x should be the permutation $S_{R^{-1}x}$ (see Chapter III, 4°):

$$(\cdot)^{S_{R^{-1}x} S_{R^{-1}y}} = (\cdot)_{y \cdot S^{-1}_{R^{-1}y} x},$$

or

$$(\cdot)^{S_x S_y} = (\cdot)_{Ry \cdot S_y^{-1} Rx}.$$

Then

$$Ry \cdot S_y^{-1} Rx = (y1)(S_y^{-1} Rx) = y[1 \cdot S_y(S_y^{-1} Rx)] = y \cdot Rx.$$

Thus,

$$(\cdot)^{S_x S_y} = (\cdot)_{yRx} = (\cdot)_{RR^{-1}(yRx)} = (\cdot)_{R(y\circ x)} = (\cdot)^{S_{y\circ x}},$$

i.e.

$$(\cdot)^{S_x S_y} = (\cdot)^{S_{y\circ x}},$$

or

$$(\cdot)^{S_x S_y S^{-1}_{y\circ x}} = (\cdot),$$

from which follows that the operation $(\cdot)$ has the permutation

$$\theta_{x,y} = S_x S_y S^{-1}_{y\circ x}$$

as an automorphism. □

Theorem 9.10. *The equalities*

$$(x \circ y) \circ z = x \circ (y \circ \theta_{y,x} z) \quad \text{and} \tag{9.24}$$

$$xy = x \circ (y \circ e_x^{-1}) \tag{9.25}$$

hold for any $x, y, z \in Q$.

Proof. 1. Transform the main equality (3.3) of a F-quasigroup using (9.23):

$$xy \cdot z = x \cdot y S_x z,$$

$$R[R(x \circ R^{-1} y) \circ R^{-1} z] = R[x \circ R^{-1} R(y \circ R^{-1} S_x z)],$$

$$R(x \circ R^{-1} y) \circ R^{-1} z = x \circ (y \circ R^{-1} S_x z),$$

or

$$R(x \circ y) \circ z = x \circ (Ry \circ R^{-1} S_x R z). \tag{9.26}$$

Substituting $y = 1$ in (9.26), we have

$$Rx \circ z = x \circ (R1 \circ R^{-1} S_x Rz),$$

$$Rx \circ z = x \circ R^{-1} S_x Rz. \tag{9.27}$$

Replacing x with $x \circ y$ in the latter equality, we have

$$R(x \circ y) \circ z = (x \circ y) \circ R^{-1} S_{x \circ y} Rz. \tag{9.28}$$

Equating the right hand sides of (9.26) and (9.28) yields

$$(x \circ y) \circ R^{-1} S_{x \circ y} Rz = x \circ (Ry \circ R^{-1} S_x Rz),$$

whence

$$(x \circ y) \circ z = x \circ (Ry \circ R^{-1} S_x S_{x \circ y}^{-1} Rz). \tag{9.29}$$

Using (9.27), the parenthetical expression from the right-hand side of (9.29) can be simplified as:

$$Ry \circ R^{-1} S_x S_{x \circ y}^{-1} Rz = y \circ R^{-1} S_y R \cdot R^{-1} S_x S_{x \circ y}^{-1} Rz = y \circ R^{-1} S_y S_x S_{x \circ y}^{-1} Rz,$$

or, using Lemma 9.1:

$$Ry \circ R^{-1} S_y S_x S_{x \circ y}^{-1} Rz = y \circ R^{-1} \theta_{y,x} Rz = y \circ \theta_{y,x} z,$$

since $\varphi R = R\varphi$ for any automorphism φ of the operation $(\cdot)$. Thus, from (9.29) we obtain

$$(x \circ y) \circ z = x \circ (y \circ \theta_{y,x} z).$$

2. To prove (9.25), we use the second form

$$x(yz) = (xy)(e_x z)$$

of the main equality for an F-quasigroup. Passing to the loop $Q(\circ)$, we obtain

$$R[x \circ R^{-1} R(y \circ R^{-1} z)] = R[(xy) \circ R^{-1} R(e_x \circ R^{-1} z)],$$

whence

$$(xy) \circ (e_x \circ z) = x \circ (y \circ z). \tag{9.30}$$

In particular, setting $z = 1$ we have

$$(xy) \circ e_x = x \circ y. \tag{9.31}$$

Multiplying both sides of the equality (9.31) from the right by $\theta_{e_x,xy}^{-1} e_x^{-1^*}$ gives

$$((xy) \circ e_x) \circ \theta_{e_x,xy}^{-1} e_x^{-1} = (x \circ y) \circ \theta_{e_x,xy}^{-1} e_x^{-1},$$

*Recall that u^{-1} means the right inverse element for u in a loop $Q(\circ)$.

whence, using identity (9.24), we find

$$(xy) \circ (e_x \circ e_x^{-1}) = x \circ (y \circ \theta_{y,x}\theta_{e_x,xy}^{-1} e_x^{-1}),$$

$$xy = x \circ (y \circ \theta_{y,x}\theta_{e_x,xy}^{-1} e_x^{-1}).$$

However

$$\theta_{e_x,xy} = \theta_{y,x}. \tag{9.32}$$

Indeed, computing the left-hand side of (9.31) using Lemma 9.1, we have

$$\theta_{e_x,xy} = S_{e_x} S_{xy} S_{(xy)\circ e_x}^{-1},$$

whence, by (3.31) and (9.31), we have

$$\theta_{e_x,xy} = S_{e_x} \cdot S_{e_x}^{-1} S_y S_x \cdot S_{x\circ y}^{-1} = S_y S_x S_{x\circ y}^{-1} = \theta_{y,x}.$$

Thus, the equality (9.32) is proved, meaning that the equality (9.25) is established. □

Note that (9.30) in which xy is replaced with the corresponding expression from (9.25) gives the following identity in the loop $Q(\circ)$:

$$[x \circ (y \circ e_x^{-1})] \circ (e_x \circ z) = x \circ (y \circ z).$$

Corollary. *Any F-quasigroup with a left unit is isotopic to a special loop.*

.

Recall (see Chapter III, 1°) that a loop $Q(\circ)$ is *special* if the equality (9.24) holds there for any $x, y, z \in Q$, with $\theta_{x,y}$ is an automorphism.

We show that the loop $Q(\circ)$ treated in Theorem 9.10 is actually special. In other words, we show that $\theta_{x,y}$ is also an automorphism of the loop $Q(\circ)$. To do this, note that

$$\theta_{x,y} R = R\theta_{x,y}$$

Indeed, because $\theta_{x,y}$ is an automorphism of the quasigroup $Q(\cdot)$, we find that

$$\theta_{x,y} Rz = \theta_{x,y}(z1) = \theta_{x,y} z \theta_{x,y} 1.$$

But $\theta_{x,y}1 = 1$, so we have

$$\theta_{x,y} Rz = R\theta_{x,y} z.$$

Thus,

$$\theta_{x,y}(u \circ v) = \theta_{x,y} R^{-1}(uRv) = R^{-1}(\theta_{x,y}u \cdot R\theta_{x,y}v) = \theta_{x,y}u \circ \theta_{x,y}v.$$

Remark. The corollary holds for all left F-quasigroups, since each is isotopic to a left F-quasigroup with a left unit.

4°. Left distributive quasigroups and F-quasigroups

Since each left distributive quasigroup is a left F-quasigroup, Corollary 1 of Theorem 9.10 implies the following.

Lemma 9.2. *Each left distributive quasigroup is isotopic to a special loop.*

Let $Q(A)$ be a left distributive quasigroup with a fixed element 1. Define $Lx = A(1, x)$ and $Rx = A(x, 1)$. Then the isotope

$$xy = A(x, L^{-1}y) \tag{9.33}$$

will be a left F-quasigroup with left unit 1. Combining (9.33) and (9.23), we find that

$$x \circ y = R^{-1}A(x, L^{-1}Ry), \tag{9.34}$$

where $Q(\circ)$ is a special loop according to Theorem 9.10. The isotopy referred to in Lemma 9.2 has the form

$$A(x, y) = R(x \circ R^{-1}Ly).$$

Note that L *is an automorphism both of the quasigroup* $Q(A)$ *and the loop* $Q(\circ)$. The first statement follows from the left distributivity of the quasigroup $Q(A)$. To prove the second statement, we use the equality

$$LR = RL,$$

which means that

$$A[A(1, x), 1] = A[1, A(x, 1)].$$

The latter equality comes from the left distributivity of the operation A. We have

$$L(x \circ y) = LR^{-1}A(x, L^{-1}Ry) = R^{-1}A(Lx, L^{-1}RLy) = Lx \circ Ly.$$

The second part of Theorem 9.10, i.e. the equality (9.25), provides a representation of the left distributive quasigroup $Q(A)$ with the help of the loop $Q(\circ)$. First we prove that $e_x^{-1} = Lx^{-1}$, where $xe_x = x$, whence $A(x, L^{-1}e_x) = x$ by (9.33). From the idempotency of the left distributive quasigroup we obtain $L^{-1}e_x = x$ or $e_x = Lx$, i.e. $e_x^{-1} = (Lx)^{-1} = Lx^{-1}$. Then, from the equality (9.25), we have

$$A(x, L^{-1}y) = x \circ (y \circ Lx^{-1}), A(x, y) = x \circ (Ly \circ Lx^{-1}),$$

or

$$A(x, y) = x \circ L(y \circ x^{-1}).$$

Further, we need some properties of the automorphisms $\theta_{x,y}$, defined in Lemma 9.1 for an F-quasigroup $Q(\cdot)$, related to the left distributive quasigroup $Q(A)$ by the equation (9.33).

Lemma 9.3. *The automorphisms* $\theta_{x,y}$ *commute with the translations* R *and* L.

Indeed, writing

$$\theta_{x,y}(uv) = \theta_{x,y}u \cdot \theta_{x,y}v$$

in terms of the operation A, we obtain

$$\theta_{x,y}A(u, L^{-1}v) = A(\theta_{x,y}u, L^{-1}\theta_{x,y}v). \tag{9.35}$$

Note $\theta_{x,y}1 = 1$, since $\theta_{x,y}$ is an automorphism of the quasigroup $Q(\cdot)$ which has 1 as its left unit 1. Thus, from (9.35) with $u = 1$, we find that $\theta_{x,y}L^{-1} = L^{-1}\theta_{x,y}$,whence $L\theta_{x,y} = \theta_{x,y}L$. The commutativity of R and $\theta_{x,y}$ was noted earlier, in the course of the proof of the Corollary to Theorem 9.10).

Lemma 9.4. *In the left distributive quasigroup $Q(A)$, the equation*

$$\theta_{y,x} = L_y^{-1} L L_x^{-1} L_{x\circ y} \tag{9.36}$$

represents the automorphisms $\theta_{x,y}$ in terms of left translations.

Writing (9.24) in terms of the operation A using (9.34), we have

$$R^{-1}A(x\circ y, L^{-1}Rz) = R^{-1}A[x, L^{-1}RR^{-1}A(y, L^{-1}R\theta_{y,x}z)] \quad \text{or}$$

$$A(x\circ y, L^{-1}Rz) = A[x, A(L^{-1}y, \theta_{y,x}L^{-2}Rz)],$$

because $\theta_{x,y}$ commutes with L and R. Simplifying, we obtain

$$A(x\circ y, z) = A[x, A(L^{-1}y, \theta_{y,x}L^{-1}z)].$$

Thus

$$L_{x\circ y}z = L_x L_{L^{-1}y}\theta_{y,x}L^{-1}z,$$

whence

$$\theta_{y,x} = L^{-1}_{L^{-1}y} L_x^{-1} L_{x\circ y} L. \tag{9.37}$$

But

$$L^{-1}_{L^{-1}y} = L^{-1}L^{-1}_{zy}L. \tag{9.38}$$

as follows from

$$L^{-1}_{L^{-1}y}z = A(L^{-1}y, z) = A(L^{-1}y, L^{-1}Lz) == L^{-1}A(y, Lz) = L^{-1}L_y Lz.$$

The equality (9.37) thus takes the form

$$\theta_{y,x} = L^{-1}L_y^{-1}LL_x^{-1}L_{x\bullet y}L,$$

whence

$$L\theta_{y,x}L^{-1} = L_y^{-1}LL_x^{-1}L_{x\circ y},$$

or

$$\theta_{y,x} = L_y^{-1}LL_x^{-1}L_{x\circ y}.$$

Corollary. *The automorphisms $\theta_{x,y}$ of the F-quasigroup $Q(\cdot)$ are also automorphisms of the left distributive quasigroup $Q(A)$.*

This assertion also follows from Lemma 9.3.

Lemma 9.5. *For $x, y \in Q$, we have $\theta_{Ly,Lx} = \theta_{y,x}$.*

Proof. We use the equality (9.36)

$$\theta_{Ly,Lx} = L_{Ly}^{-1}LL_{Lx}^{-1}L_{Lx\circ Ly} = L_{Ly}^{-1}LL_{Lx}^{-1}L_{L(x\circ y)}.$$

By (9.38), we have

$$L_{Ly} = LL_yL^{-1}. \tag{9.39}$$

Hence,

$$\theta_{Ly,Lx} = LL_y^{-1}L^{-1}\cdot L\cdot LL_x^{-1}L^{-1}\cdot LL_{x\circ y}L^{-1}$$

$$= LL_y^{-1}LL_x^{-1}L_{x\circ y}L^{-1} == L\theta_{y,x}L^{-1} = \theta_{y,x}.$$

Lemma 9.6. *In any special loop $Q(\circ)$ the equality*

$$x \circ (x^{-1} \circ y) = \delta_x y \tag{9.40}$$

holds, where x^{-1} is the right inverse element for x, and δ_x is some automorphism dependent on x.

Setting $y = x^{-1}$ in (9.24), we have

$$(x \circ x^{-1}) \circ z = x \circ (x^{-1} \circ \Theta_{x^1}, x^z).$$

Replacing z by $\theta^{-1}_{x^{-1},x} z$ yields (9.40), with $\delta_x = \theta^{-1}_{x^{-1},x}$.

Corollary. *If $Q(A)$ is a left distributive quasigroup, then*

$$\delta_x = L^{-1} L_x L^{-1} L_{x^{-1}}. \tag{9.41}$$

Indeed,

$$\delta_x = \theta^{-1}_{x^{-1},x} = (L^{-1}_{x^{-1}} L L^{-1}_x L_{x \circ x^{-1}})^{-1} = L^{-1}_{x \circ x^{-1}} L_x L^{-1} L_{x^{-1}}.$$

But $x \circ x^{-1} = 1$, where 1 is the neutral element of the loop $Q(\circ)$ and $L_1 = L$. So $\delta_x = L^{-1} L_x L^{-1} L_{x^{-1}}$.

Lemma 9.2 shows that each left distributive quasigroup $Q(A)$ is isotopic to a special loop $Q(\circ)$. In the loop $Q(\circ)$, we have the identity

$$[x \circ (y \circ e_x^{-1})] \circ (e_x \circ z) = x \circ (y \circ z), \tag{9.42}$$

in which e_x is the right local neutral element for x in the quasigroup $Q(\cdot)$ defined by (9.33). However, we showed that $e_x = Lx$. Thus, the identity (9.42) takes the form

$$[x \circ (y \circ Lx^{-1})] \circ (Lx \circ z) = x \circ (y \circ z). \tag{9.43}$$

Replacing z with $Lx^{-1} \circ z$ in the equality (9.42) we obtain

$$[x \circ (y \circ Lx^{-1})] \circ [Lx \circ (Lx^{-1} \circ z)] = x \circ [y \circ (Lx^{-1} \circ z)]. \tag{9.44}$$

But $Lx^{-1} = (Lx)^{-1}$, since L is an automorphism of the loop $Q(\circ)$. Hence, by Lemma 9.6, we have

$$Lx \circ (Lx^{-1} \circ z) = Lx \circ ((Lx)^{-1} \circ z) = \delta_{Lx} z.$$

On the other hand, $\delta_{Lx} = \theta^{-1}_{Lx,(Lx)^{-1}} = \theta^{-1}_{Lx,Lx^{-1}} = \theta^{-1}_{x,x^{-1}} = \delta_x$, using Lemma 9.5. Thus, (9.44) takes the form

$$[x \circ (y \circ Lx^{-1})] \circ \delta_x z = x \circ [y \circ (Lx^{-1} \circ z)]. \tag{9.45}$$

We investigate the *special case where* $L^2 = 1$, whence

$$A[1, A(1, y)] = y.$$

Applying the translation L_x of the quasigroup $Q(A)$ yields

$$L_x A[1, A(1, y)] = L_x y \quad \text{and}$$

$$A[L_x 1, A(L_x 1, L_x y)] = L_x y, \quad \text{so}$$
$$A[u, A(u, v)] = v \tag{9.46}$$

for all $u, v \in Q$. In other words,

$$L_u^2 = 1. \tag{9.47}$$

Rewriting (9.46) in terms of the loop $Q(\circ)$, we have

$$R[u \circ R^{-1}LR(u \circ R^{-1}Lv)] = v, \quad R[u \circ (Lu \circ R^{-1}v)] = v,$$

$$u \circ (Lu \circ R^{-1}v) = R^{-1}v, \quad u \circ (Lu \circ v) = v.$$

If $v = 1$, then $u = Lu = 1$, whence

$$Lu = u^{-1}. \tag{9.48}$$

Suppose that the identity (9.46) holds in the left distributive quasigroup $Q(A)$. Then in (9.43), which takes place in the special loop $Q(\circ)$ that is isotopic to the left distributive quasigroup $Q(A)$, we may replace Lx^{-1} with x, since $Lx^{-1} = L(Lx) = L^2x = x$. Consequently, in this case (9.45) takes the form

$$[x \circ (y \circ x)] \circ \delta_x z = x \circ [y \circ (x \circ z)]. \tag{9.49}$$

But (9.39), (9.41) and (9.48) imply

$$\delta_x = L^{-1}L_x L^{-1}L_{x^{-1}} = L^{-1}L_x L^{-1}L_{Lx} = L^{-1}L_x L^{-1}LL_x L^{-1} = 1.$$

From this, it follows that (9.49) reduces to the Bol identity (9.12). Thus, we have the following.

Theorem 9.11. *If $L_f^2 = 1$ in a left distributive quasigroup $Q(A)$ for some fixed element $f = 1$, then $Q(A)$ is isotopic to a left Bol loop $Q(\circ)$.*

In particular, the condition (9.47) holds in any left distributive quasigroup $Q(A)$ which is the core of a Moufang loop $Q(\cdot)$. Indeed,

$$L_x^2 y = A[x, A(x, y)] = x(xy^{-1}x)^{-1}x = x(x^{-1}yx^{-1})x = y.$$

Consequently, $Q(A)$ is isotopic to a left Bol loop (compare with Theorem 9.8).

Thus, the condition $L_x^2 = 1$ is sufficient for a left distributive quasigroup to be isotopic to a left Bol loop. Obviously, this condition is not necessary, since there are left distributive quasigroups isotopic to groups (see 1° of this chapter), but nevertheless $L_x^2 \neq 1$. This inequality holds when in Theorem 9.2 we have $\theta^2 \neq 1$. Below, we will give some necessary and sufficient conditions for the loop $Q(\circ)$ of (9.34) to be a left Bol loop. First, we prove the following assertion.

Lemma 9.7. *A special loop $Q(\circ)$[*] is a left Bol loop if and only if*

$$\theta_{x,y}\theta_{y\circ x,x} = 1 \tag{9.50}$$

for arbitrary $x, y \in Q$.

Indeed,

$$[x \circ (y \circ x)] \circ z = x \circ [(y \circ x) \circ \theta_{y\circ x,x} z],$$

whence

$$[x \circ (y \circ x)] \circ z = x \circ [y \circ (x \circ \theta_{x,y}\theta_{y\circ x,x} z)]. \tag{9.51}$$

Comparing this equation with the (left) Bol identity, we obtain the assertion of the lemma.

For a left distributive quasigroup, the condition (9.50) takes the form

$$P_{x\circ(y\circ x)} = P_x P_y P_x, \tag{9.52}$$

where $P_x = L_x L^{-1}$. In fact, by Lemma 9.4,

$$\theta_{x,y}\theta_{y\circ x,x} = L_x^{-1} L L_y^{-1} L_{y\circ x} L_{y\circ x}^{-1} L L_x^{-1} L_{x\circ(y\circ x)} = 1,$$

whence

$$L_{x\circ(y\circ x)} L^{-1} = L_x L^{-1} L_y L^{-1} L_x L^{-1}.$$

We have obtained the equality (9.52).

Thus, a necessary and sufficient condition for a left distributive quasigroup $Q(A)$ to be isotopic to a Bol loop $Q(\circ)$ is given by (9.52). In this case, the isotopy is determined by (9.34).

It is possible to find other necessary and sufficient conditions for a loop $Q(\circ)$ defined by (9.34) to be a Bol loop, and these conditions are expressed intrinsically in terms of the loop $Q(\circ)$ itself. As we have already seen above in the loop $Q(\circ)$, the identities (9.33) and (9.51) hold:

$$x \circ (y \circ z) = [x \circ (y \circ Lx^{-1})] \circ (Lx \circ z), \tag{9.53}$$

$$[x \circ (y \circ x)] \circ z = x \circ [y \circ (x \circ \psi_{x,y} z)], \tag{9.54}$$

where $\psi_{x,y} = \theta_{x,y}\theta_{y\circ x,x}$. From (9.53) we have

$$\left.\begin{aligned} [x \circ (y \circ x)] \circ z &= \{[x \circ (y \circ Lx^{-1})] \circ (Lx \circ x)\} \circ z, \\ x \circ [y \circ (x \circ \psi_{x,y} z)] &= [x \circ (y \circ Lx^{-1})] \circ [Lx \circ (x \circ \psi_{x,y} z)]. \end{aligned}\right\} \tag{9.55}$$

We introduce the notations

$$\left.\begin{aligned} t &= x \circ (y \circ Lx^{-1}), \\ \lambda x &= Lx \circ x. \end{aligned}\right\} \tag{9.56}$$

Then, (9.54) and (9.55) imply

$$(t \circ \lambda x) \circ z = t \circ [Lx \circ (x \circ \psi_{x,y} z)]. \tag{9.57}$$

[*]Here, the loop $Q(\circ)$ is not necessarily isotopic to a left distributive quasigroup.

If $t = 1$, i.e., $x \circ (y \circ Lx^{-1}) = 1$, then

$$\lambda x \circ z = Lx \circ (x \circ \varphi_x z), \tag{9.58}$$

since $\psi_{x,y} = \varphi_x$ will depend only on x. From (9.58) we find

$$Lx \circ (x \circ z) = \lambda x \circ \varphi_x^{-1} z,$$

and, consequently, the equality (9.57) takes the form

$$(t \circ \lambda x) \circ z = t \circ (\lambda x \circ \varphi_x^{-1} \psi_{x,y} z).$$

Since the loop $Q(\circ)$ is special, we finally obtain

$$\theta_{\lambda x,t} = \varphi_x^{-1} \psi_{x,y}. \tag{9.59}$$

We recall that t, y and x are connected by the relationship (9.56). By Lemma 9.7, the necessary and sufficient condition for the loop $Q(\circ)$ to be a Bol loop is

$$\psi_{x,y} = 1, \tag{9.60}$$

as can be seen from (9.59). This condition is equivalent to the condition

$$\theta_{\lambda x,t} = \varphi_x^{-1},$$

where t, x are any elements of Q. In particular, if $t = 1$ we have

$$\varphi_x = 1. \tag{9.61}$$

From here it follows that

$$\theta_{\lambda x,t} = 1. \tag{9.62}$$

It is clear that (9.61) and (9.62) are equivalent to (9.60). On the other hand, (9.62) shows that λx should belong to the middle nucleus N_m of the loop $Q(\circ)$:

$$Lx \circ x \in N_m. \tag{9.63}$$

Then (9.61) and (9.56) imply

$$(Lx \circ x) \circ z = Lx \circ (x \circ z). \tag{9.64}.$$

Summarizing, we have the following.

Theorem 9.12. *The isotope (9.34) of a left-distributive quasigroup $Q(A)$ is a Bol loop if and only if the relationships (9.63) and (9.64) hold.*

Remark. Theorem 9.12 is also true for any group $Q(\cdot)$ isotopic to a left distributive quasigroup $Q(A)$, since the loop $Q(\cdot)$, being isotopic to a left Bol loop $Q(\circ)$, is itself a left Bol loop.

Notes

[1]The concept of a homogeneous groupoid was introduced by Hosszú [84] for groups.

[2]In a further paper, Stein [76] proves the following theorem. Let $\Gamma(\cdot)$ be a group, and let S be a subset that satisfies the following conditions for any a and $b \neq c$: 1) b and c lie in distinct cosets of the centralizer of the element a; 2) $aba^{-1} \in S$. Then $S(\circ)$, where $x \circ y = xyx^{-1}$, is a left distributive quasigroup.

[3]Theorem 9.2 could also be proved on the basis of Proposition 4 of Chapter VII, 4°. As was shown there (Proposition 5), the quasigroup $B(x, y) = A(x^{-1}, y)$ and the group $(\cdot)$ are orthogonal. In Stein's paper [76] mentioned above (Note 2), it is shown that a left distributive quasigroup $(\cdot)$ and its isotope $(\circ)$ defined by the equality $x \circ y = x(ay)$ for an arbitrary element a of Q, are also orthogonal.

[4]We note here the following result of Stein [74]: Finite left distributive quasigroups of order $4k+2$ do not exist. The same assertion follows from a more general statement of Stein [74]: An idempotent quasigroup of order $4k + 2$ cannot have a transitive group of automorphisms. In this connection, it can be shown that there exist distributive (and, consequently, left distributive) quasigroups of any finite order $n \neq 4k + 2$ (see, for example, [13]).

[5]Moreover, it is easy to show that $Q(+)$ is in fact a distributive Steiner quasigroup.

Chapter X. The question of G-loops

One of the unsolved problems in the theory of quasigroups and loops is the following: Determine those loops $Q(\cdot)$ which are isomorphic to each of their loop isotopes. In Chapter III, 4°, we called such loops G-loops.*

This problem has great significance in geometry, especially in the theory of nets. Here, we just consider some of its algebraic aspects. [1]

Groups are G-loops, but there are other classes of G-loops as well. We do note that non-associative G-loops must be non-commutative loops, in view of the following theorem:

Theorem 10.1. *If a G-loop is commutative, then it is an abelian group.*

Indeed, let $Q(\cdot)$ be a commutative G-loop. Then, for any $a, b \in Q$, the isotope $Q(\cdot)_{a,b}$ must also be a commutative loop:

$$R_a^{-1}x \cdot L_b^{-1}y = R_a^{-1}y \cdot L_b^{-1}x,$$

whence

$$R_a^{-1}x \cdot L_b^{-1}y = L_b^{-1}x \cdot R_a^{-1}y, \quad R_a^{-1}L_b x \cdot y = x \cdot R_a^{-1}L_b y.$$

Arguing further, as in the proof of Lemma 2.6, we conclude that $Q(\cdot)$ is a transitive loop and, consequently, $Q(\cdot)$ is a group.

1°. Moufang G-loops.

We start with Moufang loops. The purpose of this section is to prove the following theorem of Bruck [32]:

Theorem 10.2. *Let $Q(\cdot)$ be a Moufang loop, and let $K(\cdot)$ be the subloop generated by all the nuclear elements and all the cubes x^3 (where x is an arbitrary element of Q). Then $K(\cdot)$ is a G-loop.* [2]

Proof. Denote by $(x_1x_2 \ldots x_{k-1}x_k)$ a product of the elements $x_1, x_2, \ldots, x_k$ in $Q(\cdot)$, taken in this order, with some distribution of brackets. Thus, $(x_1x_2x_3x_4x_5)$ might be, for example,

*Formally, G-loops were defined as the loops that are isomorphic to all their right and left derivatives. However, as shown by Theorem 3.8 in Chapter III, 4°, such loops are precisely those possessing the property of being isomorphic to all their loop isotopes.

$(x_1 \cdot x_2x_3)(x_4x_5)$. In this notation, there always exists $1 < s < k$ such that

$$(x_1x_2 \dots x_k) = (x_1x_2 \dots x_s)(x_{s+1} \dots x_k).$$

By the definition of $K(\cdot)$, any element of K has the form $(y_1y_2 \dots y_k)$, where $y_i = nx_i^3n'$ and $n, n' \in N$. The expression $(y_1y_2 \dots y_k)$ is called a *word of length* k.

We now recall the following properties of pseudo-automorphisms of a Moufang loop $Q(\cdot)$:

a) The sets of right and left pseudo-automorphisms of the loop $Q(\cdot)$ coincide (see Lemma 5.4);

b) Any inner permutation of the loop $Q(\cdot)$ is a pseudo-automorphism (Theorem 6.4);

c) The element x^3 is a right companion of the pseudo-automorphism $T_x = L_x^{-1}Rx$ (Corollary of Theorem 6.4);

d) The nucleus $N(\cdot)$ of the loop $Q(\cdot)$ is invariant relatively to any pseudo-automorphism (Lemma 6.2);

e) If λ is a pseudo-automorphism with right companion k, then

$$\lambda(xy) = k^{-1}(k\lambda x \cdot \lambda y).$$

This equality follows from the definition (3.19) of a right pseudo-automorphism.

After these preliminary remarks, we can proceed to the proof of the theorem. Let us prove the following assertion: *Each element of the subloop $K(\cdot)$ is a left companion of some pseudo-automorphism.* This assertion follows from the following more general assertion (A): *Each element θu, where θ is a pseudo-automorphism, and u is an element of K, is a left companion of a certain pseudo-automorphism.*

The proof of (A) will be carried out by induction on the length of the word u.

Let $n = 1$. Then $u = \theta_{y_1} = \theta(nx^3n')$. In view of (6.20), we have

$$u = \theta n\theta x^3\theta n.$$

Then by Property d), $\theta n, \theta n' \in N$. Further, any pseudo-automorphism θ of a Moufang loop is a semi-automorphism (see Chapter VI, 2°), i.e.,

$$\theta(xyx) = \theta x\theta y\theta x.$$

In particular, for $y = x$ we obtain

$$\theta x^3 = (\theta x)^3,$$

and consequently

$$u = n_1(\theta x)^3n_1' = n_1x_1^3n_1' = y_1',$$

i.e., u is a word of length one. In other words, the set of words of length one is invariant under any pseudo-automorphism. Thus, when $n = 1$, it suffices to prove that $y_1 = nx^3n'$ is a left companion of some pseudo-automorphism.

We have

$$_{y_1}(\cdot) = {}_{nx^3n'}(\cdot) = {}_n({}_{x^3}({}_{n'}(\cdot))) = {}_n({}_{x^3}(\cdot)) = {}_n((\cdot)^{T_x^{-1}}) = {}_{T_x^{-1}n}(\cdot)^{T_x^{-1}}. \tag{10.1}$$

Here we use (3.7) and (3.22):

$$_b(_a(\cdot)) = {}_{ba}(\cdot),$$

$$_a((\cdot)^{\varphi}) = ({}_{\varphi a}(\cdot))^{\varphi} = {}_{\varphi a}(\cdot)^{\varphi}.$$

Since $T_x^{-1}n \in N$, then by (10.1) we find that ${}_{y_1}(\cdot) = (\cdot)^{T_x^{-1}}$, i.e., y_1 is a left companion of the pseudo-automorphism T_x^{-1}. This completes the induction basis.

Now suppose that the assertion (A) holds for any u of length less than n. Let $u = (y_1 y_2 \dots y_n)$. Then, there exists s such that

$$u = (y_1 y_2 \dots y_s)(y_{s+1} \dots y_n) = vw.$$

The lengths of the words v and w are s and $n-s$ respectively. Since θ is simultaneously a right and left pseudo-automorphism, then let k be a right companion of the pseudo-automorphism θ:

$$(\cdot)_k = (\cdot)^{\theta^{-1}}.$$

By Property e) of pseudo-automorphisms, we obtain

$$\theta(vw) = k^{-1}(k\theta v \cdot 0w).$$

Consequently,

$${}_{\theta_u}(\cdot) = {}_{\theta_{vw}}(\cdot) = {}_{k^{-1}(k\theta v \cdot \theta w)}(\cdot) = {}_{k^{-1}}({}_{k\theta v}({}_{\theta w}(\cdot))).$$

The length of the word w is less than n. Therefore, by the induction hypothesis, there is a pseudo-automorphism α whose left companion is $\theta w : (\cdot) = (\cdot)^{\alpha-1}$. Thus,

$${}_{\theta u}(\cdot) = {}_{k^{-1}}({}_{k\theta v}((\cdot)^{\alpha-1})) = {}_{k^{-1}}({}_{k^{-1}\alpha^{-1}(k\theta v)}(\cdot)^{\alpha-1}) =$$

$$= {}_{\alpha^{-1}k^{-1}}({}_{\alpha^{-1}(k\theta v)}(\cdot))^{\alpha^{-1}} = {}_{\alpha^{-1}k^{-1}\cdot[l^{-1}(l\alpha^{-1}k\cdot\alpha^{-1}\theta v)]}(\cdot)^{\alpha-1},$$

where l is a right companion of the pseudo-automorphism α^{-1}.

Here we use (3.7) and Property e) of pseudo-automorphisms. Further, we note that

$$\alpha^{-1}k^{-1} \cdot [l^{-1}(l\alpha^{-1}k \cdot \alpha^{-1}\theta v] = (\alpha^{-1}k)^{-1}[l^{-1}(l\alpha^{-1}k \cdot \alpha^{-1}\theta v)] =$$

$$= L^{-1}_{\alpha^{-1}k} L_l^{-1} L_{l\alpha^{-1}k} \alpha^{-1}\theta v = L^{-1}_{l,\alpha^{-1}k}\alpha^{-1}\theta v = \beta v,$$

where $\beta = L^{-1}_{l,\alpha^{-1}k,l}\alpha^{-1}\theta$ is a pseudo-automorphism. So,

$${}_{\theta u}(\cdot) = {}_{\beta v}(\cdot)^{\alpha^{-1}}.$$

Again, using the induction hypothesis for v, we conclude that ${}_{\beta v}(\cdot) = (\cdot)^{\gamma}$, and, consequently,

$${}_{\theta u}(\cdot) = (\cdot)^{\gamma\alpha^{-1}}.$$

Assertion (A) is proved, and the validity of the theorem follows from the validity of this assertion. □

Corollary. *The subloop $K(\cdot)$ is normal.*[3]

2°. Loops with nuclei of index two.[4]

In this section, we exhibit G-loops which are not Moufang loops. We show that certain WIP-loops (see Definition 4 in Chapter V) are also G-loops.

Consider a loop $Q(\cdot)$ which has a nucleus N of index two, so $Q = \{N, pN\}$ with $p \in Q \setminus N$.

Lemma 10.1. *N is a normal subloop of the loop $Q(\cdot)$.*

By the corollary of Theorem 4.6, we must show that the equality

$$xN \cdot yN = (xy)N \tag{10.2}$$

holds for any $x, y \in N$. For this we note that if $a \in N$, then $aN = N$. If $a \notin N$, then

$$aN = pN.$$

Indeed, if $x = an$ with $n \in N$, we have $x \notin N$, and therefore $x \in pN$, i.e., $aN \subseteq pN$. To prove the reverse inclusion, we note that $aN = Na$. In fact, consider $yp = pn$ with $n \in N$. If $y \notin N$, then $y = pn_1 \in pN$, whence $(pn_1)p = pn$, or in view of the fact that n_1 is an element of the nucleus, we obtain $p(n_1p) = pn$ and $n_1p = n$, i.e., $p \in N$, which is impossible in view of the choice of the element p.

Now we consider the equation $ax = pn$. We have $a \notin N$, so $a = pn_2$. Consequently, we have $(pn_2)x = pn$ or $p(n_2x) = pn$, $n_2x = n$, whence $x \in N$. Thus, we have proved $pn \in aN$, i.e., $pN \subseteq aN$.

The equality (10.2) is obvious if at least one of the elements x or y belongs to the nucleus N: It follows from the properties of the nucleus N. Consequently, it suffices to prove that

$$pN \cdot pN = p^2N. \tag{10.3}$$

But $p^2 \in N$. Indeed, let $p^2 \in pN$, whence $p^2 = pn$, that is $p = n \in N$, which is impossible. So instead of (10.3) we must prove the equality:

$$pN \cdot pN = N. \tag{10.4}$$

Let $x \in pN \cdot pN$, i.e., $x = pn_1 \cdot pn_2$. We have

$$x = p(n_1 \cdot pn_2) = p(n_1p \cdot n_2).$$

There exists an element $n_3 \in N$ such that $n_1p = pn_3$, so

$$x = p(pn_3 \cdot n_2) = p(p \cdot n_3n_2) = p^2 \cdot n_3n_2 \in N,$$

i.e., $pN \cdot pN \subseteq N$. Conversely, let $n \in N$, and suppose $n = p^2x$. Obviously, $x \in N$. Then $n = p^2x = p(px) \in pN \cdot pN$, i.e., $N \subseteq pN \cdot pN$. Thus, the equality (10.4) is proved.

We saw above that $aN = Na$, and in particular $pN = Np$. This latter equality determines the following involutive self-map φ on the nucles N:

$$pn = \varphi n \cdot p.$$

Lemma 10.2. *The self-map φ is an automorphism of the nucles N.*

Indeed, let $x, y \in N$. Then

$$\varphi(xy) \cdot p = p \cdot xy = px \cdot y = (\varphi x \cdot p)y = \varphi x \cdot (py) = \varphi x(\varphi yp) = (\varphi x \varphi y)p,$$

whence

$$\varphi(xy) = \varphi x \varphi y.$$

We need the following properties of derivative operations (see Chapter III, 2^0). We formulate them for the right derivative operations $(\cdot)_a$ defined by the equality

$$ax \cdot y = a(x \cdot y)_a.$$

1) If $Q(\cdot)$ is a loop with neutral element 1, then $Q(\cdot)_a$ and $Q_a(\cdot)$ are loops with the same neutral element (Assertion 1 of Theorem 3.3);

2) $((\cdot)_a)_b = (\cdot)_{ab}$ (Assertion 2 of Theorem 3.3);

3) $(\cdot)_x = (\cdot)$ if and only if x belongs to the left nucleus.

Now we prove the main property of loops with a nucleus of index two.

Theorem 10.3. *A loop $Q(\cdot)$ with a nucleus of index two is a G-loop with the weak inverse property.*

Proof. Let N be the nucleus of $Q(\cdot)$. If $x \in N$, then $(\cdot)_x = (\cdot)$. Below we will prove that $(\cdot)_p = (\cdot)^\lambda$, where λ is some permutation of the set Q. Consider $y \in pN$, say $y = pn$. We have

$$(\cdot)_y = (\cdot)_{pn} = (\cdot)_{\varphi n \cdot p} = ((\cdot)_{\varphi n})_p = (\cdot)_p = (\cdot)^\lambda.$$

Consequently, each right derivative $Q(\cdot)_x$ of $Q(\cdot)$, with $x \in Q$, is isomorphic to the loop $Q(\cdot)$. It is similarly shown that each left derivative is isomorphic to the loop $Q(\cdot)$. Thus, the theorem will be proved if we show that $(\cdot)_p$ and ${}_p(\cdot)$ are isomorphic to $(\cdot)$.

We define the following permutation λ of the set Q:

$$\lambda n = \varphi n, \quad \lambda(pn) = p\varphi n$$

for all $n \in N$. Clearly,

$$\lambda^{-1} n = \varphi^{-1} n, \quad \lambda^{-1}(pn) = p\varphi^{-1} n.$$

We show that $(\cdot)_p = (\cdot)^\lambda$, or more specifically

$$(x \cdot y)_p = \lambda^{-1}(\lambda x \lambda y). \tag{10.5}$$

The following four cases are possible:

1) $x, y \in N$.

Then $(x \cdot y)_p = xy$ and

$$\lambda^{-1}(\lambda x \cdot \lambda y) = \lambda^{-1}(\varphi x \cdot \varphi y) = \varphi^{-1}(\varphi x \cdot \varphi y) = xy,$$

since $\varphi x, \varphi y \in N$.

2) $x \in N, y \in pN$, say $y = pn$.

We have

$$px \cdot y = px \cdot pn = p(x \cdot pn) = p(xp \cdot n) = p(p\varphi^{-1} \cdot n),$$

whence

$$(x \cdot y)_p = p\varphi^{-1}x \cdot n.$$

On the other hand, we have

$$\lambda^{-1}(\lambda x \cdot \lambda y) = \lambda^{-1}(\varphi x \cdot \lambda(pn)) = \lambda^{-1}(\varphi x \cdot p\varphi n) = \lambda^{-1}(\varphi xp \cdot \varphi n) =$$

$$= \lambda^{-1}(px \cdot \varphi n) = \lambda^{-1}(p \cdot x\varphi n) = p\varphi^{-1}(x\varphi n) = p(\varphi^{-1}x \cdot n).$$

Consequently, in this case $(x \cdot y)_p = \lambda^{-1}(\lambda x \cdot \lambda y)$.

3) $x \in pN, y \in N$, say $x = pn$. Then

$$px \cdot y = p(pn) \cdot y = p(pn \cdot y) = p(x \cdot y)_p,$$

whence

$$(x \cdot y)_p = pn \cdot y.$$

$$\lambda^{-1}(\lambda x \cdot \lambda y) = \lambda^{-1}(\lambda(pn) \cdot y) = \lambda^{-1}(p\varphi n \cdot \varphi y) = p\varphi^{-1}(\varphi n \cdot \varphi y) = p(ny).$$

Thus, in this case, the equality (10.5) is also satisfied.

4) $x \in pN, y \in pN$, say $x = pn_1$ and $y = pn_2$.

We have

$$px \cdot y = p(pn_1) \cdot pn_2 = p^2n_1 \cdot pn_2 = (p^2n_1 \cdot p)n_2.$$

But $p^2 \in N$, so

$$px \cdot y = [p\varphi^{-1}(p^2n_1)]n_2 = p[\varphi^{-1}(p^2n_1)n_2].$$

Consequently,

$$(x \cdot y)_p = \varphi^{-1}(p^2n_1) \cdot n_2.$$

On the other hand, we have

$$\lambda^{-1}(\lambda x \cdot \lambda y) = \lambda^{-1}[\lambda(pn_1) \cdot \lambda(pn_2)] = \lambda^{-1}(p\varphi n_1 \cdot p\varphi n_2)$$

$$= \lambda^{-1}[p(\varphi n_1 \cdot p\varphi n_2)] = \lambda^{-1}[p((\varphi n_1 \cdot p)\varphi n_2)] = \lambda^{-1}[p(pn_1 \cdot \varphi n_2)]$$

$$= \lambda^{-1}[p(p \cdot n_1\varphi n_2)] = \lambda^{-1}(p^2 \cdot n_1\varphi n_2) = \varphi^{-1}(p^2n_1\varphi n_2) = \varphi^{-1}(p^2n_1)n_2.$$

Thus, the equality (10.5) is established. We can prove the equality ${}_p(\cdot) = (\cdot)^{\lambda-1}$ similarly.

Now let us prove that $Q(\cdot)$ is a WIP-loop. By Property 2) of WIP-loops, it must be shown that $uv \cdot w = 1$ implies $u \cdot vw = 1$. Clearly, this assertion is satisfied if at least one of the elements u, v, w belongs to N. If none of the elements u, v, w belongs to N, then the equality $uv \cdot w = 1$ is impossible: $uv \cdot w$ belongs to pN, and cannot be equal to the neutral element that belongs to the nucleus. The proof of Theorem 10.3 is complete. □

To prove one of the corollaries of this theorem, we need the following.

Lemma 10.3. *Let F be a group with an automorphism φ whose square is an inner automorphism:*

$$\varphi^2 x = kxk^{-1} \tag{10.6}$$

for all $x \in F$ and some $k \in F$. Then $k^{-1}\varphi^{-1}k$ belongs to the center of the group F.

Indeed, $(k^{-1}\varphi^{-1}k)x = k^{-1}(\varphi^{-1}kx) = k^{-1}\varphi^{-1}(k\varphi x)$. But from (10.6) we have

$$kx = \varphi^2 x \cdot k,$$

so

$$\begin{aligned}(k^{-1}\varphi^{-1}k)x = k^{-1}\varphi^{-1}(\varphi^3 xk) = k^{-1}(\varphi^2 x \cdot \varphi^{-1}k)\\ = k^{-1}(kxk^{-1}\varphi^{-1}k) = x(k^{-1}\varphi^{-1}k).\end{aligned}$$

Corollary *For any elements $u, v, w \notin N$ there exists a fixed element $a \in N$ such that the equality*

$$uv \cdot w = (u \cdot vw)a \tag{10.7}$$

holds.

It is obvious that $a \in N$, since $uv \cdot w$ and $u \cdot vw$ cannot belong to N. Let $u = pn_1, v = pn_2, w = pn_3$ and $p^2 = k$. Computing $uv \cdot w$ and $u \cdot vw$, we have

$$uv \cdot w = (pn_1 \cdot pn_2) \cdot pn_3 = [p(n_1 \cdot pn_2)] \cdot pn_3 = [p(n_1 p \cdot n_2)] \cdot pn_3$$

$$= [p(p\varphi^{-1}n_1 \cdot n_2)] \cdot pn_3 = [(p^2 \cdot \varphi^{-1}n_1 n_2)p]n_3 = p\varphi^{-1}(k\varphi^{-1}n_1 n_2)n_3$$

and

$$u \cdot vw = pn_1 \cdot (pn_2 \cdot pn_3) = pn_1(k \cdot \varphi^{-1}n_2 n_3) = pn_1 k\varphi^{-1}n_2 n_3.$$

For given u, v, w there exists an element a such that the identity (10.7) holds. We show that a does not depend on u, v and w. Taking into account the values for $uv \cdot w$ and $u \cdot vw$, we can rewrite (10.7) as

$$p \cdot \varphi^{-1}(k\varphi^{-1}n_1 n_2)n_3 = (p \cdot n_1 k\varphi^{-1}n_2 n_3)a, \tag{10.8}$$

whence

$$\varphi^{-1}(k \cdot \varphi^{-1}n_1 n_2)n_3 = (n_1 k\varphi^{-1}n_2 n_3)a \text{ and}$$

$$\varphi^{-1}k\varphi^{-2}n_1\varphi^{-1}n_2 n_3 = (n_1 k\varphi^{-1}n_2 n_3)a.$$

Now we find $\varphi^2 n$ for $n \in N$. To this end, we compute $p(pn)$:

$$p(pn) = p(\varphi np) = (\varphi^2 np)p = \varphi^2 np^2 = \varphi^2 n \cdot k.$$

On the other hand, $p(pn) = kn$. Thus

$$\varphi^2 n = knk^{-1}. \tag{10.9}$$

The equality (10.9) determines $\varphi^{-2}n$ as

$$\varphi^{-2}n = k^{-1}nk.$$

Using this equality, we rewrite (10.8) as

$$\varphi^{-1}k \cdot k^{-1}n_1k\varphi^{-1}n_2n_3 = (n_1k\varphi^{-1}n_2n_3)a. \tag{10.10}$$

But $\varphi^{-1}k\cdot k^{-1} = k(k^{-1}\varphi^{-1}k)k^{-1}$, whence by Lemma 10.3 we conclude that $\varphi^{-1}k\cdot k^{-1}$ belongs to the center of the nucleus N. Consequently, (10.10) implies

$$(n_1k\varphi^{-1}n_2n_3)\varphi^{-1}k \cdot k^{-1} = (n_1k\varphi^{-1}n_2n_3)a,$$

whence

$$a = \varphi^{-1}k \cdot k^{-1}.$$

Theorem 10.4. *Let $Q(\cdot)$ be a loop with nucleus N. Further, suppose that the loop $Q(\cdot)$ has a normal subloop H of index two contained in the nucleus N. Then a necessary and sufficient condition for $Q(\cdot)$ to be a group is the existence of at least one element $p \notin H$ such that*

$$p^2 \cdot p = p \cdot p^2. \tag{10.11}$$

Proof. The necessity of the condition (10.11) is obvious. Sufficiency is also easily proved. By the conditions of the theorem, $H \subseteq N \subseteq Q$. Let us prove that $N = Q$. Suppose the contrary, that $N \neq Q$. Then we must have $H = N$, so $Q(\cdot)$ is a loop with a nucleus of index two, satisfying the corollary of Theorem 10.3. In particular, applying the corollary for the case $u = v = w = p$, the equality (10.7) implies $a = 1$. Consequently, $uv \cdot w = u \cdot vw$ for any $u, v, w \notin N$. Thus, $N = Q$, a contradiction.

Corollary. *A loop $Q(\cdot)$ with a nucleus of index two is not a Moufang loop.*

Indeed, in a Moufang loop each element generates an associative subloop, so (10.11) holds in $Q(\cdot)$ and, consequently, $Q(\cdot)$ must be a group. This contradicts the fact that $Q(\cdot)$ has a nucleus of index two.

The following theorem complements Theorem 10.3.

Theorem 10.5. *Let N be a group with an automorphism φ such that $\varphi^2 x = kxk^{-1}$ and $\varphi k \neq k$. Then there exists a loop $Q(\cdot)$ having N as its nucleus of index two.*

Note that the loop $Q(\cdot)$ is a G-loop with the weak inverse property which is not a Moufang loop.

Proof. Let $P(\cdot)$ be a cyclic group on the set $P = \{0, p\}$, and let $\Sigma = \{A_{a,b} \mid a, b \in P\}$ be a system of quasigroups

$$A_{a,b}(x, y) = \varphi_b^{-1}x \cdot y$$

defined on the set N, where $\varphi_0 = 1$ and $\varphi_p = \varphi$.

Consider the crossed product $Q(\circ)$ (see Chapter V), where

$$\left.\begin{aligned} Q &= P \times N, \\ (\circ) &= \langle \cdot, \Sigma \rangle. \end{aligned}\right\} \tag{10.12}$$

It is easy to see that $Q(\circ)$ is a loop with neutral element $(0,1)$, where 1 is the neutral element of the group N. Obviously, the set of all pairs $(0,x)$, where x runs through the group N, is a subloop of the loop $Q(\circ)$. It is also easy to verify that N is the nucleus of $Q(\circ)$.

We define the following permutation λ of the set Q:

$$\lambda(0,x) = (0,\varphi x), \quad \lambda(p,x) = (p,\varphi x).$$

Repeating the computations from the proof of Theorem 10.3, we see that

$$(\circ)_{(p,1)} = (\circ)^{\lambda}.$$

If x is any element of N, then it can be represented in the form $x = \varphi^{-1}y$. Thus

$$(\circ)_{(p,x)} = (\circ)_{(p,\varphi^{-1}y,1)} = (\circ)_{(0,y)\circ(p,1)} = ((\circ)_{(0,y)})_{(p,1)} = (\circ)_{(p,1)} = (\circ)^{\lambda}.$$

In order for $Q(\circ)$ to have a nucleus of index two, it is necessary to prove that $(\circ)^{\lambda} \neq (\circ)$. To this end, we evaluate the expression

$$\lambda^{-1}(\lambda(p,x)\circ\lambda(p,y)) = \lambda^{-1}((p,\varphi x)\circ(p,\varphi y))$$

$$= \lambda^{-1}(0,k\varphi^{-1}\varphi x\cdot\varphi y) = \lambda^{-1}(0,kx\varphi y) = (0,\varphi^{-1}(kx\varphi y)) = (0,\varphi^{-1}k\varphi^{-1}x\cdot y).$$

On the other hand,

$$(p,x)\circ(p,y) = (0,k\varphi^{-1}x\cdot y).$$

Since $\varphi k \neq k$, we have $(\circ)^{\lambda} \neq (\circ)$, as required □

Remark. If N is an abelian group, then the conditions of Theorem 10.5 transform into the following: $\varphi^2 = 1$, and there exists an element k such that $\varphi k \neq k$.

Examples. 1. Let $N = C_2 \times C$, where C is the additive group of integers and C_2 is the subgroup of even numbers. Thus N consists of all pairs of the form $x = (2i,j)$, where i and j are integers. Let $\varphi(2i,j) = (2i,-i-j)$. It is easy to see that φ is an automorphism of the group N with $\varphi^2 = 1$ and $\varphi(2,0) = (2,-1) \neq (2,0)$. Consequently, φ satisfies the conditions of Theorem 10.5. The elements of the loop Q form the pairs $(0,x)$ or (p,x) or, more specifically, the triples $(0;2i,j)$ and $(p;2i,j)$. This example was considered by Osborne [57].

2. Let $\mathfrak{V}_4 = \{0,a,b,c\}$ be the Klein Vierergruppe. Let $\varphi = \begin{pmatrix} 0 & a & b & c \\ 0 & b & a & c \end{pmatrix}$. The permutation φ is an automorphism of the group $\mathfrak{V}_4$, and $\varphi^2 = 1$ with $\varphi a \neq a$. One can construct a loop Q of order 8 using (10.12). The loop Q is a non-associative G-loop with the weak inverse property.

3°. An example of G-loop that is not a WIP-loop

The following example establishes the existence of G-loops that are not WIP-loops.

Let $F = F(+,\cdot)$ be a field. We consider the set $Q = F' \times F$, where F' consists of all the non-zero elements of the field F. Thus, $Q = \{(a,x) \mid a, x \in F\,,\ a \neq 0\}$. Under the operation

$$(a,x) \circ (b,y) = (ab, (a^{-1}-1)(b^{-1}-1)s + b^{-1}x + y)$$

with s as a fixed element of F, we obtain a loop $Q(\circ)$ with neutral element $e = (1,0)$.

We calculate the product $(u \circ v) \circ w$, where $u = (a,x)$, $v = (b,y)$, $w = (c,z)$. We have

$$(u \circ v) \circ w = [(a,x) \circ (b,y)] \circ (c,z)$$

$$= (ab, (a^{-1}-1)(b^{-1}-1)s + b^{-1}x + y) \circ (c,z)$$

$$= (abc, (a^{-1}b^{-1}-1)(c^{-1}-1)s + c^{-1}(a^{-1}-1)(b^{-1}-1)s + c^{-1}b^{-1}x + c^{-1}y + z)$$

or

$$(u \circ v) \circ w = (abc, (abc)^{-1}(2 - a - b - c + abc)s + b^{-1}c^{-1}x + c^{-1}y + z). \tag{10.13}$$

Similarly, we obtain

$$u \circ (v \circ w) = (abc, (abc)^{-1}(1 - ab - ac - bc + 2abc)s + b^{-1}c^{-1}x + c^{-1}y + z). \tag{10.14}$$

The solution of the equation $(u \circ v) \circ w = u \circ t$, where u, v, w are given elements from Q, must be

$$t = (\circ)_u(v,w),$$

where $(\circ)_u$ is the right derivative of the operation $(\circ)$. Let $t = (d,z')$. Then

$$u \circ t = (a,x) \circ (d,z') = (ad, (a^{-1}-1)(d^{-1}-1)s + d^{-1}x + z'). \tag{10.15}$$

Comparing (10.14) and (10.15), we find

$$\left.\begin{aligned} d &= bc, \\ z' &= (abc)^{-1}(1-b)(1-c)s + c^{-1}y + z. \end{aligned}\right\}$$

Thus,

$$(\circ)_u(v,\omega) = (bc, (abc)^{-1}(1-b)(1-c)s + c^{-1}y + z). \tag{10.16}$$

Let us show that

$$(\circ)_u = (\circ)^{\lambda_u}, \tag{10.17}$$

where $\lambda_u(b,x) = (b,ax)$.

Indeed,

$$\lambda_u^{-1}(b,x) = (b, a^{-1}x)$$

and

$$\lambda_u^{-1}(\lambda_u v \circ \lambda_u \omega) = \lambda_u^{-1}(\lambda_u(b,y) \circ \lambda_u(c,z)) = \lambda_u^{-1}((b,ay) \circ (c,az))$$

$$= \lambda_u^{-1}(bc, (b^{-1}-1)(c^{-1}-1)s + c^{-1}ay + az) = (bc, a^{-1}(b^{-1}-1) \times (c^{-1}-1)s + c^{-1}y + z).$$

Comparing this equality with (10.16), we derive the relations (10.17). Similarly, we prove that all left derived operations of $(\circ)$ are isomorphic to the operation $(\circ)$. The loop $Q(\circ)$ will be a G-loop.

Generally speaking, the constructed loop is not a WIP-loop. Indeed, suppose that $(u \circ v) \circ w = e$. By (10.13), the given equality is equivalent to the equalities

$$\left.\begin{aligned} abc = 1, \\ (2 - a - b - c + abc)s + b^{-1}c^{-1}x + c^{-1}y + z = 0. \end{aligned}\right\}$$

The loop $Q(\circ)$ will be a WIP-loop if $(u \circ v) \circ \omega = e$ implies $u \circ (v \circ \omega) = e$, i.e.,

$$\left.\begin{aligned} abc = 1, \\ (1 - ab - ac - bc + 2abc)s + b^{-1}c^{-1}x + c^{-1}y + z = 0. \end{aligned}\right\}$$

Consequently, we must have

$$\left.\begin{aligned} abc = 1, \\ (a-1)(b-1)(c-1)s = 0. \end{aligned}\right\}$$

If $s = 0$, then, as follows from (10.13) and (10.14), the loop $Q(\circ)$ is associative, i.e., it is a group. If $s \neq 0$,

$$(ab - 1)(a - 1)(b - 1) = 0 \tag{10.18}$$

for any non-zero elements of the field F. If the field F contains more than three elements, then the equality (10.18) does not hold, so $Q(\circ)$ is not a WIP-loop.

Let us show that the loop $Q(\circ)$ is special (see Chapter III, 1°), i.e., we prove that

$$(u \circ v) \circ w = u \circ (v \circ \bar{\theta} w), \tag{10.19}$$

where $\bar{\theta}$ is an automorphism of the loop $Q(\circ)$ depending on u and v.

Let $\bar{\theta} w = w' = (c', z')$. On computing the left and right sides of (10.19) using (10.13) and (10.14), and comparing the results, we find

$$c' = c \text{ and}$$

$$\begin{aligned} (abc)^{-1}&(2 - a - b - c + abc)s + b^{-1}c^{-1}x + c^{-1}y + z \\ &= (abc)^{-1}(1 - ab - ac - bc + 2abc)s + b^{-1}c^{-1}x + c{-}1y + z', \end{aligned}$$

whence

$$z' = z + l_{a,b,c},$$

with

$$l_{a,b,c} = (a - 1)(b - 1)(c - 1)s.$$

So,

$$\bar{\theta}(c, z) = (c, z + l_{a,b,c}).$$

Consequently, we have

$$\bar{\theta}(c_1, z_1) \circ \bar{\theta}(c_2, z_2) = (c_1, z_1 + l_{a,b,c_1}) \circ (c_2, z_2 + l_{a,b,c_2})$$

$$= (c_1 c_2, (c_1^{-1} - 1)(c_2^{-1} - 1)s + c_2^{-1} z_1 + c_2^{-1} l_{a,b,c_1} + z_2 + l_{a,b,c_2})$$

and

$$\bar{\theta}((c_1, z_1) \circ (c_2, z_2)) = \bar{\theta}(c_1 c_2 (c_1^{-1} - 1)(c_2^{-1} - 1)s + c_2^{-1} z_1 + z_2)$$

$$= (c_1 c_2, (c_1^{-1} - 1)(c_2^{-1} - 1)s + c_2^{-1} z_1 + z_2 + l_{a,b,c_1 c_2}).$$

For $\bar{\theta}$ to be an automorphism of the loop $Q(\circ)$, it is necessary and sufficient that

$$c_2^{-1} l_{a,b,c_1} + l_{a,b,c_2} = l_{a,b,c_1 c_2} \tag{10.20}$$

holds for any a, b, c_1, c_2. The validity of the equality (10.20) is verified by direct calculation.

4°. Universal properties of loops

A property of a loop (groupoid, etc.) is *algebraic* if it is invariant under isomorphism. A property of a loop (groupoid, etc.) is *universal* if it is invariant under isotopy. Thus, *Any algebraic property of a G-loop is universal.* We consider some simple algebraic properties, and find classes of loops for which they become universal.

1. *The following identities are universal in any loop: associativity* (Theorem 1.4), *Moufang* (Theorem 6.1), *left or right Bol* (Theorem 6.10).

2. *Commutativity is a universal property only in groups.*

Indeed, let $Q(\cdot)$ be a commutative loop. Consider a principal isotope

$$x \circ y = R_a^{-1} x \cdot L_b^{-1} y$$

which is commutative. Arguing as in the proof of Theorem 10.1, we establish the validity of the assertion 2.

3. *The inverse property is only universal in the class of Moufang loops.*

Indeed, if any loop that is isotopic to a loop $Q(\cdot)$ is an IP-loop, then $Q(\cdot)$ is a Moufang loop (Theorem 6.3). Conversely, if $Q(\cdot)$ is a Moufang loop, then it will be an IP-loop. Since any loop that is isotopic to a Moufang loop is also a Moufang loop (Theorem 6.1), the isotope also has the inverse property.

4. *If the weak inverse property is universal in a loop $Q(\cdot)$, the following identity holds*

$$xy \cdot \theta_x zx = (x \cdot yz)x,$$

where θ_x is an automorphism of the loop $Q(\cdot)$ that depends on x.

Indeed, let $Q(\cdot)$ be a WIP-loop, so

$$x(yx)^{-1} = y^{-1},$$

where $xx^{-1} = 1$. Let $Q(\circ)$ be a loop that is principally isotopic to $Q(\cdot)$, so the operation $(\circ)$ has the form

$$x \circ y = R_a^{-1}x \cdot L_b^{-1}y.$$

We find necessary and sufficient conditions for $Q(\circ)$ to have the weak inverse property. For this, we first find $x^{(-1)}$ from $x \cdot x^{(-1)} = e$, where $e = ba$ is the neutral element of the loop $Q(\circ)$. We have

$$R_a^{-1}x \cdot L_b^{-1}x^{(-1)} = e. \tag{10.21}$$

As was shown in connection with Property g of Chapter V, 5°, equation $ax = b$ has a solution $x = I(I^{-1}b \cdot a)$, where $Ix = x^{-1}$. Thus, from (10.21) we obtain

$$L_b^{-1}x^{(-1)} = I(I^{-1}e \cdot R_a^{-1}x) = IL_cR_a^{-1}x,$$

or

$$x^{(-1)} = L_bIL_cR_a^{-1}x.$$

Here $c = I^{-1}e = I^{-1}(ba)$.

Let $Q(\circ)$ be a WIP-Loop, i.e.,

$$x \circ (y \circ x)^{(-1)} = y^{(-1)}. \tag{10.22}$$

Then

$$R_a^{-1}x \cdot L_b^{-1}(y \circ x)^{(-1)} = y^{(-1)}.$$

Consequently,

$$L_b^{-1}(y \circ x)^{(-1)} = I(I^{-1}y^{(-1)} \cdot R_a^{-1}x)$$

and

$$L_b^{-1}L_bIL_cR_a^{-1}(R_a^{-1}y \cdot L_b^{-1}x) = I(I^{-1}L_bIL_cR_a^{-1}y \cdot R_a^{-1}x).$$

After cancelling, we obtain

$$L_cR_a^{-1}(y \cdot x) = I^{-1}l = L_bIL_cy \cdot R_a^{-1}L_bx. \tag{10.23}$$

Since we want (10.22) to be a universal property, (10.23) must hold for any $a, b, x, y \in Q$. Set $b = 1$. then $c = I^{-1}a$ and

$$L_{I^{-1}a}R_a^{-1}(yx) = I^{-1}ay \cdot R_a^{-1}x, \tag{10.24}$$

whence

$$I^{-1}a \cdot R_a^{-1}(yx) = I^{-1}ay \cdot R_a^{-1}x.$$

Replacing a with Ia and x with $R_{Ia}x$, we have

$$aR_{Ia}^{-1}(y \cdot xIa) = ay \cdot x. \tag{10.25}$$

In particular, for $x = a$ we obtain

$$aR_{Ia}^{-1}y = ay \cdot a. \tag{10.26}$$

Combining (10.24) with (10.25), we find

$$ay \cdot x = [a(y \cdot xIa)]\, a. \tag{10.27}$$

Let $xIa = z$. Using Property g) of the WIP-loop $Q(\cdot)$, we find $x = I^{-1}(Ia \cdot Iz)$. We define the permutation θ_a by the equality

$$I^{-1}(Ia \cdot Iz) = \theta_a z \cdot a,$$

i.e.,

$$\theta_a = R_a^{-1} I^{-1} L_{Ia} I.$$

By Property d) of WIP-loops, we obtain

$$\theta_a = I^{-1} L_a L_{Ia} I. \tag{10.28}$$

Thus, (10.26) can be rewritten in the form

$$ay \cdot \theta_a za = (a \cdot yz)a. \tag{10.29}$$

The equations (10.24) and (10.27) show that $T_1 = (L_{I^{-1}a}, R_a^{-1}, L_{Ia}^{-1} R_a^{-1})$ and $T_2 = (L_a, R_{Ia}^{-1}, R_a L_a)$ are autotopies of the loop $Q(\cdot)$. Then $T_1 T_2 = (L_{Ia}^{-1} L_a, R_a^{-1} R_{Ia}^{-1}, L_{Ia}^{-1} L_a) = (\alpha, \beta, \alpha)$ is also an autotopy of $Q(\cdot)$. But $l = \alpha 1 = L_{I-1_a} L_a 1 = I^{-1} a \cdot a = 1$ and $\beta^{-1} 1 = R_{Ia} R_a 1 = a \cdot Ia = 1$, so $k = \beta 1 = 1$.

Any autotopy of the loop $Q(\cdot)$ must have the form (2.6). Therefore, we conclude that $T_1 T_2 = (R_k^{-1}, L_l^{-1}, 1)\alpha = (1, 1, 1)\alpha = \alpha$, i.e., $\beta = \alpha$ and α is an automorphism of the loop $Q(\cdot)$. Considering this circumstance, we obtain

$$\theta_a = I^{-1} \alpha I = \alpha, \tag{10.30}$$

from (10.28), since an arbitrary automorphism α of an arbitrary loop $Q(\cdot)$ commutes with the permutation I.

Remark. The equality (10.29) reduces to the Moufang identity (6.9) if $\theta_x = 1$ for any x. The equality $\theta_x = 1$ is equivalent to the equality $L_{I^{-1}x} L_x = 1$ by (10.30), i.e., $I^{-1} x(xz) = z$. This latter equality means that $Q(\cdot)$ is a left IP-loop. Consequently: *If the weak inverse property is universal for a left IP-loop $Q(\cdot)$, then $Q(\cdot)$ is a Moufang loop.*

5. A loop $Q(\cdot)$ is called *cross-invertible*, or a *CI-loop*, if the identity

$$xy \cdot Ix = y, \tag{10.31}$$

holds, with $x \cdot Ix = 1$. Cross-invertible loops were introduced by Artzy[5].

We show that *If the crossed-inverse property is universal for a loop $Q(\cdot)$, then $Q(\cdot)$ is an abelian group.*

We first prove some elementary assertions that hold in CI-loops.

a) The identity (10.31) *is equivalent to the identity*

$$x(yIx) = y. \tag{10.32}$$

Indeed, the identity (10.31) is written in terms of translations as

$$R_{Ix}L_x = 1,$$

whence $L_xR_{Ix} = 1$. This equality is equivalent in turn to (10.32). Similarly, we can prove that (10.32) implies (10.31).

$$b) \quad R_x^{-1} = L_{I^{-1}x}, \quad L_x^{-1} = R_{Ix}. \tag{10.33}$$

Both equalities follow from (10.31).

c) The equation $ax = b$ has the solution $x = bIa$. The equation $ya = b$ has the solution $y = I^{-1}b \cdot a$.

This proposition follows from the definition of a CI-loop.

d) The permutation I is an automorphism in a CI-loop:

$$I(xy) = IxIy. \tag{10.34}$$

Indeed, from the definition (10.31) of a CI-loop it follows that

$$(xy \cdot Ix)I(xy) = Ix,$$

whence

$$yI(xy) = Ix. \tag{10.35}$$

On the basis of Property *c)* of a CI-loop, (10.35) implies (10.34). Similarly, we prove that *every CI-loop is a WIP-loop.*

Let us prove this assertion. Let $Q(\circ)$ be a loop that is isotopic to the loop $Q(\cdot)$:

$$x \circ y = R_a^{-1}x \cdot L_b^{-1}y.$$

As in the treatment 4 of universality for WIP-loops, we determine $x^{(-1)}$ from $x \circ x^{(-1)} = e$, where $e = ba$. We have

$$\begin{gathered} R_a^{-1}x \cdot L_b^{-1}x^{(-1)} = e, \\ L_b^{-1}x^{(-1)} = eI(R_a^{-1}x) = L_eIR_a^{-1}x, \\ x^{(-1)} = L_bL_eIR_a^{-1}x. \end{gathered} \tag{10.36}$$

If $Q(\circ)$ is also a CI-loop, we have

$$x \circ (y \circ x^{(-1)}) = y.$$

Interms of the operation $(\cdot)$,

$$R_a^{-1}x \cdot L_b^{-1}(R_a^{-1}y \cdot L_b^{-1}x^{(-1)}) = y.$$

Applying Property *c)*,

$$L_b^{-1}(R_a^{-1}y \cdot L_b^{-1}x^{(-1)}) = yIR_a^{-1}x,$$

whence by (10.36) we obtain

$$L_b^{-1}(R_a^{-1}y \cdot L_b^{-1}L_bL_eIR_a^{-1}x) = y \cdot IR_a^{-1}x.$$

After reduction, we find

$$L_b^{-1}(R_a^{-1}y \cdot L_ex) = yx,$$

whence

$$L_b(yx) = R_a^{-1}y \cdot L_ex,$$

or, considering (10.33), we obtain

$$b(yx) = (I^{-1}ay)(ex). \tag{10.37}$$

We write $I^{-1}a = u$ and $e = ba = v$. Consequently, $uv = I^{-1}a(ba) = b$ by (10.32). So, (10.37) becomes

$$uv \cdot yx = uy \cdot vx. \tag{10.38}$$

Thus, the loop $Q(\cdot)$ is medial. But medial loops are abelian groups. Indeed, for $x = u = 1$ we get $vy = yv$. For $y = 1$ equality (10.38) becomes $uv \cdot x = u \cdot vx$. Consequently, $Q(\cdot)$ is an abelian group.

6. Finally, we prove the following proposition: *In the loop $Q(\cdot)$, the property of left invertibility is universal if and only if $Q(\cdot)$ is a left Bol loop.*

Let $Q(\cdot)$ be a left IP loop

$$^{-1}x(xy) = y, \tag{10.39}$$

where $^{-1}xx = 1$. Consider the loop $Q(\circ)$, with

$$x \circ y = R_a^{-1}x \cdot L_b^{-1}y,$$

that is isotopic to the loop $Q(\cdot)$. Suppose that it is a left IP loop:

$$^{-1}x \circ (x \circ y) = y.$$

We transform this equality to

$$R_a^{-1}(^{(-1)}x) \cdot L_b^{-1}(R_a^{-1}x \cdot L_b^{-1}y) = y.$$

But (10.39) implies $L_b^{-1} = L_b^{-1}$, so

$$R_a^{-1}(^{(-1)}x) \cdot L_b^{-1}(R_a^{-1}x \cdot {}^{-1}by) = y.$$

Replacing ^{-1}b with c and x with $R_ax = xa$, and setting $t = R_a^{-1}(^{(-1)}(xa))$, we have

$$t\,[c(x \cdot cy)] = y. \tag{10.40}$$

The element t does not depend on y, so we set $y = 1$ in (10.40):

$$t(c \cdot xc) = 1,$$

whence

$$c \cdot xc = t^{-1}. \tag{10.41}$$

On the other hand, from (10.40), since $Q(\cdot)$ is a left IP loop, we obtain

$$c(x \cdot cy) = t^{-1}y.$$

Considering (10.41), we find

$$c(x \cdot cy) = (c \cdot xc)y.$$

Since c is an arbitrary element of Q, we have proved that $Q(\cdot)$ is a (left) Bol loop. The converse proof can be seen in Chapter VI, 6°.

Notes

[1]One of the general results concerning G-loops is the following: If A is a G-loop, then the inverse loops A^{ρ} and A^{λ} (see the definition of these inverse loops in Chapter I, 4^0) are also G-loops [18]

[2]As Bruck showed [32], Theorem 10.2 implies that any simple Moufang loop is a G-loop. Recall that a loop $Q(\cdot)$ is *simple* if it does not contain any proper, non-trivial normal subloops. Examples of simple non-associative Moufang loops were constructed by Paige [63].

[3]As an example of a G-loop which is a Moufang loop, one may consider the multiplicative loop $Q'(\cdot)$ of non-zero elements of an alternative division ring $Q(+,\cdot)$ [31].

[4]Here we follow the exposition from [21]

[5]Crossed-invertible loops (CI-loops) are a natural generalization of abelian groups. They are studied in detail by Artzy [3–6]. In the final article, autotopies of CI-loops are studied. The method of investigation is the same as that of Bruck for IP-loops (see Chapter V, 4^0).

Chapter XI. Quasigroups and nets

1°. Algebraic nets

The concept of a quasigroup has a natural interpretation using so-called nets.[1].

A *geometric net* $\mathfrak{A}$ consists of three families L_i (for $i = 1, 2, 3$) of curves having the following two properties: 1) the curves within a single family do not intersect; and 2) two curves from different families intersect precisely in one point. Using a homeomorphic transformation, i.e., using a continuous deformation, two families L_1 and L_2 can be reduced to two families L_1' and L_2' consisting of parallel lines, where the lines from L_1' are perpendicular to the lines from L_2'. In other words, L_1' and L_2' form a coordinate net. The lines from L_1' have equations $x = const$, and those from L_2', $y = const$. Then the curves from the third family L_3' are transformed into a family L_3' of level curves $z = f(x, y)$ of a function (Figure 1).

If $\mathfrak{A}$ is homeomorphic to a net $\mathfrak{A}'$ consisting of families L_i' of parallel lines, then $\mathfrak{A}$ is called a *regular net*.

The concept of a geometric net can be generalized. Thus, we define an algebraic net, or simply a net.[2]

Definition 1. A system $\mathfrak{A}$ of objects of two forms — lines and points, with an incidence relation, is called a *net* if the following conditions are satisfied.

Let the collection L of all lines from $\mathfrak{A}$ be divided into three disjoint classes L_1, L_2 and L_3. Then:

1) Two lines from different classes are incident at exectly one point of $\mathfrak{A}$;

2) Each point from $\mathfrak{A}$ is incident to one and only one line of each class.

In general usage, the word "incident" may be replaced with expressions such as "pass through," "lie on," etc.

We refer to the lines from the class L_i (for $i = 1, 2, 3$) as *i-lines*. Since by Axiom 2 the lines of any given class do not intersect, it is convenient to call them *parallel*.

We prove that there exists a one-to-one correspondence between the lines of two different classes L_i and L_j.

Indeed, we take some k-line (for $k \neq i, j$), and denote it by l. The k-line l crosses an i-line l' at only one point A. Just one j-line l'' passes through the point A. Then $l' \leftrightarrow l''$ is a one-to-one correspondence between the lines of the respective classes L_i and L_j.

Simultaneously, we have obtained the following proposition: *There exists a one-to-one correspondence between the set of points lying on any line and the set of points lying on any*

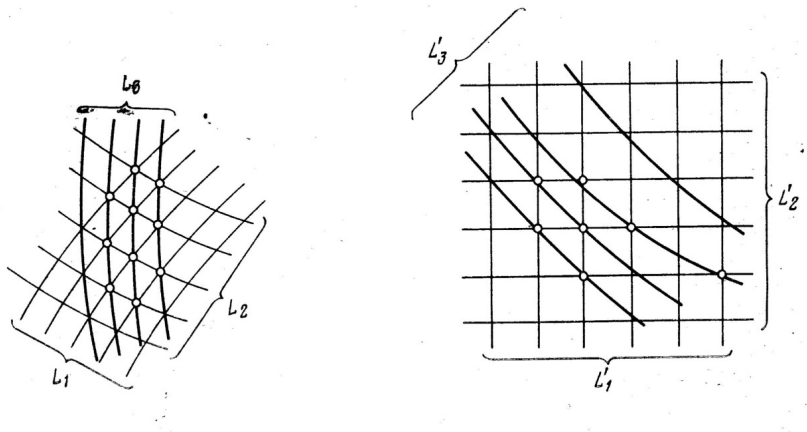


Fig. 1

other line of the same class. This proposition follows from the fact that the correspondence $l' \leftrightarrow A$, considered above, establishes a one-to-one correspondence between all the lines of the class L_i and all the points of the k-line l.

Also from this proposition we get one more one-to-one correspondence — between the respective sets of points lying on any two distinct lines (not necessarily belonging to the same class).

All these facts enable us to introduce the concept of the *order* of a net, as the cardinality of the set of lines of a given class, or the cardinality of the set of points lying on any given line.

Let $Q = \{a, b, c, \dots\}$ be a set whose cardinality coincides with the order of the given net $\mathfrak{A}$, i.e., there exists a one-to-one correspondence between the elements of the set Q and the lines of any class of $\mathfrak{A}$. This allows us to use the elements of Q as distinct labels for the i-lines. Thus, if the i-line l is labeled by the element a of Q, we denote the line by (i, a).

The set Q acquires a quasigroup structure if we endow it with the following operation. Let $a, b \in Q$. Then the lines $(1, a)$ and $(2, b)$ intersect at a single point A, and through this point there passes a single line $(3, c)$. In this case we put $c = ab$.

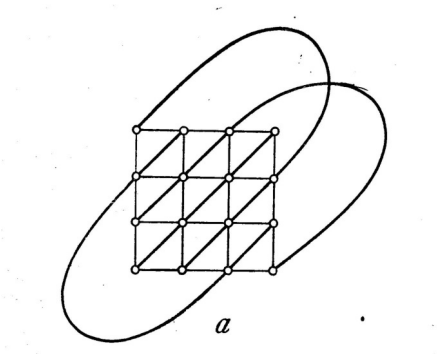
The equation $ax = b$ has a unique solution in $Q(\cdot)$. Indeed, the lines $(1, a)$ and $(3, b)$ intersect at a single point B, and through this point there passes a unique 2-line. Suppose that it is labeled by an element $d \in Q$, i.e., the line $(2, d)$ passes through B. By the definition of the operation on $Q(\cdot)$, this means that $ad = b$, i.e., the equation $ax = b$ has a unique solution $x = d$. Similarly, it is proved that the equation $ya = b$ has a unique solution. Thus, $Q(\cdot)$ is a quasigroup.

The quasigroup $Q(\cdot)$ is called a *coordinate quasigroup* for the net $\mathfrak{A}$.

Conversely, let $Q(\cdot)$ be a quasigroup. We show that it is a coordinate quasigroup of a net $\mathfrak{A}$. We define $\mathfrak{A}$ in the following way. The points of the net $\mathfrak{A}$ are ordered pairs $P = [a, b]$ of elements of Q. The pair (i, a), where $i \in \{1, 2, 3\}$ and $a \in Q$, is called an i-line. Incidence is defined as follows: the point $[a, b]$ is incident only to the lines $(1, a), (2, b), (3, ab)$. It is

easy to see that $\mathfrak{A}$ is a net, with $Q(\cdot)$ as a coordinate quasigroup.

Remark. Points $A = [a, b]$ and $B = [c, d]$ are on the same 1-line if $a = c$; on the same 2-line if $b = d$, and on the same 3-line if $ab = cd$. Therefore, 1-, 2- and 3-lines can be denoted respectively by equations $x = a$, $y = b$ and $xy = s$.



	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Fig. 2

Example. Let $Q = \{0, 1, 2, 3\}$ and let $Q(\cdot)$ be a cyclic group. Then the group $Q(\cdot)$ coordinatizes the net $\mathfrak{A}$ (Figure 2).

Here the vertical and horizontal lines are the 1- and 2-lines respectively, while the remaining lines are 3-lines. The points of the net $\mathfrak{A}$ are marked by small circles in Figure 2.

With an appropriate labeling of the lines of $\mathfrak{A}$ by elements of Q, the coordinate quasigroup $Q(\cdot)$ becomes a loop. For this, we select an arbitrary point O, and denote the lines passing through O by an element $1 \in Q$. We may label the other 3-lines as shown in Figure 3.

Take the line $(3, x)$. It crosses the lines $(1, 1)$ and $(2, 1)$ respectively at the points A and B. A single 2-line, namely $(2, x)$, passes through the point A. A single 1-line, namely $(1, x)$, passes through the point B.

Thus, all the lines from $\mathfrak{A}$ will be labeled by elements of Q. With this labeling of the lines, the coordinate quasigroup $Q(\cdot)$ will be a loop. The point A is incident with the lines $(1, 1)$, $(2, x)$ and $(3, x)$, so $1x = x$. The point B is incident with the lines $(1, x)$, $(2, 1)$ and $(3, x)$, so $x1 = x$.

For all the various labelings of the lines of the net $\mathfrak{A}$ by the elements of Q, we obtain different coordinate quasigroups. It is easy to see that *all these quasigroups are isotopic.* Indeed, if in one labeling lines $(1, x)$, $(2, y)$, $(3, z)$ pass through a point A, then with a second labeling the same lines pass through the same point, but with new labels $(1, \alpha x)$, $(2, \beta y)$, $(3, \gamma z)$, where α, β, γ are permutations of the set Q. In the first labeling we obtain a coordinate quasigroup $Q(\cdot)$, and $xy = z$, while in the second labeling we obtain a coordinate quasigroup $Q(\circ)$. In this case we have the equality $\alpha x \circ \beta y = \gamma z$ or $\alpha x \circ \beta y = \gamma(xy)$, which means that $Q(\cdot)$ and $Q(\circ)$ are isotopic. Thus, all the coordinate quasigroups of a given net $\mathfrak{A}$ are mutually isotopic.

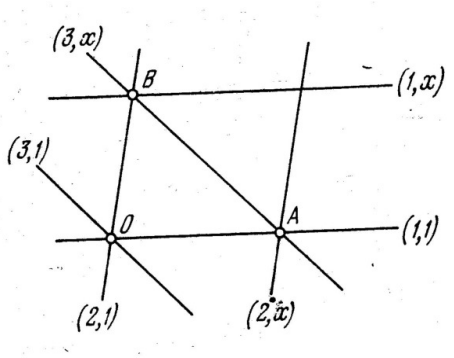


Fig. 3

It follows that the isotopy class of quasigroups on any given set Q corresponds to any net $\mathfrak{A}$ whose order is the cardinality of Q. Therefore, *to each property of the net, there corresponds a certain property of the whole class of mutually isotopic quasigroups.* In other words, the corresponding property of any coordinate quasigroup is an isotopy invariant.

We also note the following fact. As seen above, in the definition of a coordinate quasigroup, the choice of which particular family of lines is chosen to constitute the first class (class of 1-lines), and so on, plays a role. Let the lines from the net $\mathfrak{A}$ be labeled in some way, and let the lines from the classes L_i (for $i = 1, 2, 3$) be the respective i-lines. We denote the operation of the corresponding coordinate quasigroup by $(\cdot)$. Now let the lines from L_1 remain as 1-lines, but make the lines from L_2 be 3-lines, and the lines from L_3 be 2-lines. Denote the operation of the corresponding quasigroup in this situation by $(\circ)$. Let a point A be incident to the lines l_1, l_2, l_3 from the respective classes L_1, L_2, L_3 and let them be denoted by x, y, z respectively. By the choice of i-lines for $Q(\cdot)$ we have $xy = z$, while for $Q(\circ)$ we have $x \circ z = y$. Thus, $(\circ) = (\cdot)^{-1}$, i.e.,*the quasigroup $Q(\circ)$ is right inverse to the quasigroup $Q(\cdot)$.* Consequently, *renaming of the classes corresponds to choosing distinct inverse quasigroups for the coordinatization.*[3]

2°. Closure conditions

Interpretation of quasigroups by using nets makes it possible to study isotopy classes of quasigroups. One of the problems that arises here is connected with the concept of regularity of the net. A geometric net is said to be *regular* if it satisfies certain so-called closure conditions [10, 11]. Here we give a general notion of closure conditions in quasigroups and nets, and consider some of them in more detail way.

Definition 2. Let $Q(\cdot)$ be a quasigroup. We say that a closure condition (D) holds in $Q(\cdot)$ if the equalities

$$x_{p_i} \cdot y_{q_i} = x_{r_i} y_{s_i} \quad (\text{for } i = 1, 2, \ldots, k-1) \tag{11.1}$$

imply the equalities

$$x_{p_j} \cdot y_{q_j} = x_{r_j} y_{s_j} \quad (\text{for } j = k, k+1, \ldots, n), \tag{11.2}$$

with

$$x_{p_j}, x_{r_j} \in X = \{x_{p_i}, x_{r_i,\ldots}\}, \qquad y_{q_j}, y_{s_j} \in Y = \{y_{q_i}, y_{s_i,\ldots}\},$$
$$i = 1, 2, \ldots, k-1, \qquad j = k, k+1, \ldots, n.$$

Before turning to examples, we prove the following theorem:

Theorem 11.1**.** *If a closure condition (D) is satisfied in a quasigroup $Q(\cdot)$, then the closure condition (D) is also satisfied in any isotopic quasigroup. In other words, closure conditions are isotopy invariants.*

Indeed, let $Q(\cdot)$ and $Q(\circ)$ be isotopic, with

$$xy = \gamma^{-1}(\alpha x \circ \beta y),$$

Then the equalities (11.1) become

$$\gamma^{-1}(\alpha x_{p_i} \circ \beta y_{q_i}) = \gamma^{-1}(\alpha x_{n_i} \circ \beta y_{s_i}) \quad (\text{for } i = 1, 2, \ldots, k-1)$$

or

$$\alpha x_{p_i} \circ \beta y_{q_i} = \alpha x_{r_i} \circ \beta y_{s_i} \quad (\text{for } i = 1, 2, \ldots, k-1). \tag{11.3}$$

Introduce the notation: $\alpha x_l = u_l$, $\beta y_l = \upsilon_l$. Then (11.3) takes the form

$$u_{p_i} \circ \upsilon_{q_i} = u_{r_i} \circ \upsilon_{s_i} \quad (\text{for } i = 1, 2, \ldots, k-1). \tag{11.4}$$

The equalities (11.2) become

$$u_{p_j} \circ \upsilon_{q_j} = u_{r_j} \circ \upsilon_{s_j} \quad (\text{for } j = k, k+1, \ldots, n). \tag{11.5}$$

Consequently, (11.4) implies (11.5), i.e., the same condition (D) holds in $Q(\circ)$.

Consider a net $\mathfrak{A}$ coordinatized by $Q(\cdot)$. Each of the equalities (11.1) means that certain points are on certain 3-lines.

Remark. We will also say that the condition (D) is satisfied in the net $\mathfrak{A}$.

The most well-known closure conditions providing regularity in geometric nets are as follows. In 3) and 4), the horizontal lines denote implication, of the conclusion below the line from the hypotheses above the line.

1) *The Thomsen condition* (T) (Figure 4)

$$\left.\begin{aligned} x_1 y_2 &= x_2 y_1, \\ x_1 y_3 &= x_3 y_1, \end{aligned}\right\} \Rightarrow x_2 y_3 = x_3 y_2. \tag{11.6}$$

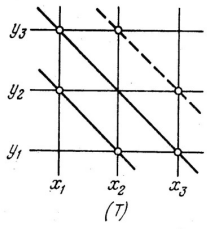


Fig. 4

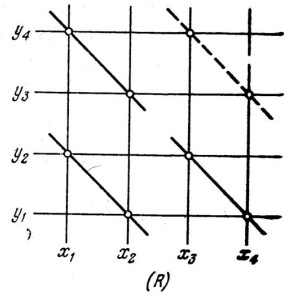


Fig.5

2) *The Reidemeister condition* (R) (Figure 5)

$$\left.\begin{aligned} x_1y_2 &= x_2y_1,\\ x_1y_4 &= x_2y_3,\\ x_3y_2 &= x_4y_1, \end{aligned}\right\} \Rightarrow x_3y_4 = x_4y_3. \tag{11.7}$$

3) *The three Bol conditions* (Figure 6)

$$\left.\begin{array}{lll} x_1y_2 = x_2y_1, & x_1y_2 = x_2y_1, & \\ x_1y_3 = x_2y_2, & x_1y_4 = x_2y_3, & x_1y_2 = x_2y_1,\\ \underline{x_3y_2 = x_4y_1,} & \underline{x_2y_2 = x_3y_1,} & \underline{x_1y_4 = x_2y_3 = x_3y_2 = x_4y_1,}\\ x_3y_3 = x_4y_2. & x_2y_4 = x_3y_3, & x_3y_4 = x_{43}y_3. \end{array}\right\} \tag{11.8}$$

The respective conditions (left Bol, right Bol, and Bol) are denoted (B_r), (B_l), (B).

4) *The hexagon condition* $(H)^4$ (Figure 7)

$$\begin{aligned} x_1y_2 &= x_2y_1,\\ \underline{x_1y_3 &= x_2y_2 = x_3y_1,}\\ x_2y_3 &= x_3y_2. \end{aligned}$$

We consider each condition separately.

1. *The Thomsen condition* (T).

Theorem 11.2. *The Thomsen condition holds in a quasigroup $Q(\cdot)$ if and only if it is isotopic to an abelian group.*

For the forward implication, it suffices by Theorem 11.1 to consider a loop $Q(\cdot)$ (with neutral element 1) in which the Thomsen condition (T) holds. We set $x_1 = 1$ in (11.6), obtaining

$$y_2 = x_2y_1 \quad \text{and} \quad y_3 = x_3y_1 \;\Rightarrow\; x_2y_3 = x_3y_2$$

or

$$x_2 \cdot x_3y_1 = x_3 \cdot x_2y_1. \tag{11.9}$$

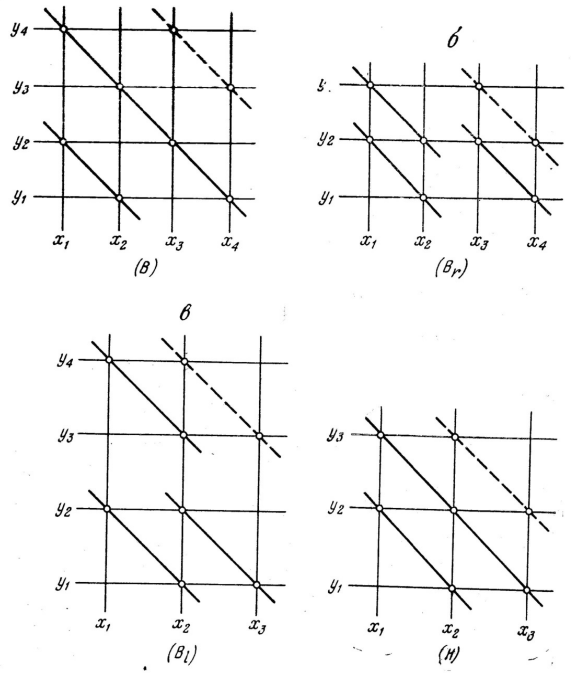


Fig. 6 (a, b, c) Fig.7

Setting $y_1 = 1$ in (11.9), we obtain $x_2x_3 = x_3x_2$, i.e., $Q(\cdot)$ is commutative. Then

$$x_2(y_1x_3) = x_2(x_3y_1) = x_3(x_2y_1) = (x_2y_1)x_3,$$

i.e., $Q(\cdot)$ is associative. Consequently, $Q(\cdot)$ is an abelian group.

Conversely, let $Q(\circ)$ be a quasigroup that is isotopic to some abelian group $Q(\cdot)$. We prove that the condition (T) holds in $Q(\circ)$. Instead of $Q(\circ)$, we again take the abelian group isotope $Q(\cdot)$, and show that the condition (T) holds in $Q(\cdot)$. Let

$$x_1y_2 = x_2y_1 \quad \text{and} \quad x_1y_3 = x_3y_1.$$

then

$$x_2y_3 = x_2(x_1^{-1}x_3y_1) = x_1^{-1}x_3 \cdot x_2y_1 = x_1^{-1}x_3 \cdot x_1y_2 = x_3y_2,$$

i.e., the condition (T) holds in $Q(\cdot)$. By Theorem 11.1 the condition (T) also holds in $Q(\circ)$, as well as in a net $\mathfrak{A}$ coordinatized by the quasigroup $Q(\circ)$.

2. *The Reidemeister condition (R).*

Theorem 11.3. *The Reidemeister condition holds in a quasigroup $Q(\cdot)$ if and only if it is isotopic to a group.*

As in the previous theorem, we may assume for the forward implication proof that $Q(\cdot)$ is a loop. In (11.7), set $x_2 = y_2 = 1$. We obtain

$$x_1 = y_1, \quad x_1y_4 = x_2y_3, \quad \text{and} \quad x_3y_2 = x_4y_1.$$

Thus

$$x_3y_4 = (x_4y_1 \cdot y_2^{-1})(x_1^{-1} \cdot x_2y_3) = x_4(y_1y_2^{-1}x_1^{-1}x_2)y_3.$$

By the first equality from (11.7), we obtain

$$x_3y_4 = x_4y_3,$$

i.e., the condition (R) holds in $Q(\cdot)$.

Conversely, suppose that the three equalities on the left hand side of (11.7) hold in a group $Q(\cdot)$. Then

$$x_3y_4 = (x_4y_1 \cdot y_2^{-1}) \cdot (x_1^{-1} \cdot x_2y_3) = x_4(y_1y_2^{-1}x_1^{-1}x_2)y_3$$

by the lower two equalities on the left hand side of (11.7). By the first of the three equalities on the left hand side of (11.7), this equality reduces to $x_3y_4 = x_4y_3$, the conclusion of the Reidemeister condition.

3. *The Bol condition* (B_l).

Theorem 11.4. *The Bol condition* (B_l) *holds in a quasigroup* $Q(\cdot)$ *if and only if it is isotopic to a left Bol loop.*

Proof. As above, let us prove the forward implication for the case where $Q(\cdot)$ is a loop. In the equalities (11.8), set $x_2 = y_2 = 1$. We obtain

$$x_1 = y_1, \quad x_1y_4 = y_3, \quad 1 = x_4y_1 \;\Rightarrow\; y_4 = x_4y_3.$$

Consequently, $x_4 = {}^{-1}y_1$ and $y_3 = x_1y_4 = y_1y_4$, whence

$$y_4 = x_4y_3 = {}^{-1}y_1 \cdot y_1y_4,$$

i.e., $Q(\cdot)$ has the left inverse property. Indeed, since an arbitrary loop isotope of the loop $Q(\cdot)$ satisfies the condition (B_l), it also has the left inverse property. Thus, by Proposition 6 of Chapter X, 4, the loop $Q(\cdot)$ must be a left Bol loop.

Conversely, we show that condition (B_l) holds in a left Bol loop $Q(\cdot)$. Suppose

$$\left.\begin{aligned} x_1y_2 &= x_2y_1, \\ x_1y_4 &= x_2y_3, \\ x_2y_2 &= x_4y_1. \end{aligned}\right\} \tag{11.10}$$

From the middle equation of (11.10), we use the left inverse property to obtain

$$y_4 = x_1^{-1} \cdot x_2y_3.$$

Consequently,

$$x_2y_4 = x_2(x_1^{-1} \cdot x_2y_3),$$

whence

$$x_2y_4 = (x_2 \cdot x_1^{-1}x_2)y_3. \tag{11.11}$$

by the left Bol identity. From the first equation of (11.10), we find

$$y_2 = x_1^{-1} \cdot x_2 y_1.$$

Thus

$$x_2 y_2 = x_2(x_1^{-1} \cdot x_2 y_1) = (x_2 \cdot x_1^{-1} x_2) y_1 \tag{11.12}$$

by the left Bol identity. Comparing (11.12) with the third equality from (11.10), we conclude that

$$x_2 x_1^{-1} x_2 = x_4. \tag{11.13}$$

Substituting this value for x_4 from (11.13) into (11.11), we obtain $x_2 y_4 = x_4 y_3$, the conclusion of the condition (B_l). The theorem has been proved.

The corresponding result for the Bol condition (B_r) is proved similarly.

Corollary. *If the closure conditions (B_l) and (B_r) hold simultaneously in a net $\mathfrak{A}$, then any coordinate quasigroup $Q(\cdot)$ of $\mathfrak{A}$ is isotopic to a Moufang loop.*

Indeed, a loop $Q(\circ)$ isotopic to the quasigroup $Q(\cdot)$ is a left and right Bol loop. By Property 6 of Bol loops (see Chapter VI, 6˙), the loop $Q(\circ)$ becomes a Moufang loop.

We now fix some notation. If a condition (D) holding in a quasigroup $Q(\cdot)$, or a net $\mathfrak{A}$ coordinatized by $Q(\cdot)$, implies that a condition (D') holds in the quasigroup $Q^{\sigma}(\cdot)$, where ${}^{\sigma}(\cdot)$ is one of the operations inverse to the operation $(\cdot)$ (see Chapter I 4˙), then we will write

$${}^{\sigma}(D) \Rightarrow (D').$$

In particular,

$$(D) \Rightarrow (D')$$

means that condition (D) in a quasigroup $Q(\circ)$ implies condition (D') in $Q(\circ)$. If $(D) \Rightarrow (D')$ and $(D') \Rightarrow (D)$, then we will write

$$(D) \Leftrightarrow (D')$$

and call the equalities (D) and (D') *equivalent*.

We turn to the study of the Bol condition (B).

4. *The Bol condition (B).*

The closure condition (B) in a quasigroup $Q(\cdot)$ states that the equalities

$$x_1 y_2 = x_2 y_1 \quad \text{and} \quad x_1 y_4 = x_2 y_3 = x_3 y_2 = x_4 y_1 \tag{11.14}$$

imply the equality

$$x_3 y_4 = x_4 y_3. \tag{11.15}$$

We have the following.

Theorem 11.5. 1) ${}^{-1}(B) \Leftrightarrow (B_l)$, 2) $(B)^{-1} \Leftrightarrow (B_r)$.

We denote the respective products from the equalities (11.14) and (11.15) by t, s and p. Thus, the first equality in (11.14) gives

$$x_1 = t/y_2 \quad \text{and} \quad x_2 = t/y_1,$$

where $a/b = c$ is equivalent to $cb = a$, i.e., $(/) = {}^{-1}(\cdot)$. Likewise, the operation $(\cdot)^{-1}$ is written as $(\backslash)$.

The second equality in (11.14) gives

$$x_1 = s/y_4, \quad x_2 = s/y_3, \quad x_3 = s/y_2, \quad x_4 = s/y_1.$$

The equality (11.15) gives

$$x_3 = p/y_4, \quad x_4 = p/y_3.$$

Thus, we have

$$\left.\begin{aligned} x_1 = t/y_2 = s/y_4, \\ x_2 = t/y_1 = s/y_3, \\ x_3 = s/y_2 = p/y_4, \end{aligned}\right\} \tag{11.16}$$

whence

$$x_4 = s/y_1 = p/y_3. \tag{11.17}$$

We denote t, s, p, y_1, y_2, y_3, y_4 respectively by x_1', x_2', x_4', y_4', y_2', y_3', y_1'. Thus, the equalities (11.16) become

$$\left.\begin{aligned} x_1'/y_2' = x_2'/y_1', \\ x_1'/y_4' = x_2'/y_3', \\ x_2'/y_2' = x_4'/y_1', \end{aligned}\right\} \tag{11.18}$$

while (11.17) becomes

$$x_2'/y_4' = x_4'/y_3'. \tag{11.19}$$

Comparing (11.18) and (11.19) with (11.8), we conclude that the condition (B_l) holds in $Q(/)$.

Theorem 11.6. *The Bol condition (B) holds in a quasigroup $Q(\circ)$ if and only if it is isotopic to a loop $Q(\cdot)$ with the identity*

$$z\,[(xy)\backslash z] = (z/y)(x\backslash z).$$

Proof. Suppose that the Bol condition (B) holds in a quasigroup $Q(\circ)$. Then it also holds in a loop $Q(\cdot)$ isotopic to the quasigroup $Q(\circ)$. In (11.14), set $y_2 = x_3^{-1}$ and $y_1 = x_4^{-1}$. Then the equalities

$$x_1 x_3^{-1} = x_2 x_4^{-1}$$

and

$$x_1 y_4 = x_2 y_3 = x_3 x_3^{-1} = x_4 y_4^{-1} = 1 \tag{11.20}$$

imply

$$x_3 x_1^{-1} = x_4 x_2^{-1},$$

since (11.20) yields $y_4 = x_1^{-1}$ and $y_3 = x_2^{-1}$. Set $x_1 = a$, $x_2 = b$, $x_3 = c$, and $x_4 = d$. Then $ac^{-1} = bd^{-1}$ implies $ca^{-1} = db^{-1}$. In particular, for $c = 1$ we see that $a = bd^{-1}$ implies $a^{-1} = db^{-1}$, i.e., the equality

$$(bd^{-1})^{-1} = db^{-1} \tag{11.21}$$

holds.

Setting $d = 1$ in (11.21), we have

$$(d^{-1})^{-1} = d.$$

Thus, replacing d by d^{-1} in (11.21), we obtain

$$(bd)^{-1} = d^{-1}b^{-1}. \tag{11.22}$$

We have proved the following proposition: *The anti-automorphic property (11.22) of the inversion permutation $I : x \to x^{-1}$ is universal in a loop $Q(\cdot)$ if the condition (B) holds in $Q(\cdot)$.*

Let $Q(\circ)$ be an arbitrary loop isotopic to the loop $Q(\cdot)$. The identity (11.22) also holds in the loop $Q(\circ)$ as

$$(x \circ y)^{(-1)} = y^{(-1)} \circ x^{(-1)}. \tag{11.23}$$

Let

$$x \circ y = R_a^{-1} x \cdot L_b^{-1} y \tag{11.24}$$

and

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

where $e = ba$. First, we find $x^{(-1)}$. We have

$$R_a^{-1} x \cdot L_b^{-1} x^{(-1)} = e. \tag{11.25}$$

We define a self-map I_e on Q from

$$x \cdot I_e x = e. \tag{11.26}$$

By (11.26), it follows that I_e is a permutation of a set Q and, in particular,

$$I_1 = I,$$

where 1 is the neutral element of the loop $Q(\cdot)$. Thus 11.25) implies

$$L_b^{-1} x^{(-1)} = I_e R_a^{-1} x,$$

whence

$$x^{(-1)} = L_b I_e R_a^{-1} x. \tag{11.27}$$

Using this equality and (11.24), we rewrite (11.23) as

$$L_b I_e R_a^{-1}(R_a^{-1} x \cdot L_b^{-1} y) = R_a^{-1}(L_b I_e R_a^{-1} y) \cdot L_b^{-1}(L_b I_e R_a^{-1} x).$$

Consequently,

$$L_b I_e R_a^{-1}(xy) = \varphi y \cdot I_e x, \tag{11.28}$$

where

$$\varphi = R_a^{-1} L_b I_e R_a^{-1} L_b.$$

The equation $(x^{-1})^{-1} = x$ is universal: it holds in any loop isotopic to the loop $Q(\cdot)$. Thus

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

whence by (11.27) we obtain

$$(L_b I_e R_a^{-1})^2 = 1.$$

Then

$$L_b I_e \varphi = L_b I_e (R_a^{-1} L_b I_e R_a^{-1} L_b) = (L_b I_e R_a^{-1})^2 L_b = L_b.$$

Consequently,

$$\varphi = I_e^{-1}.$$

Thus, (11.28) implies

$$L_b I_e R_a^{-1}(xy) = I_e^{-1} y \cdot I_e x. \tag{11.29}$$

Setting $y = 1$ in (11.29),

$$L_b I_e R_a^{-1} x = I_e^{-1} 1 \cdot I_e x.$$

We deduce $I_e^{-1} y = t$ or $I_e t = y$, since $t \cdot I_e t = ty$ and $ty = e$ — see (11.26).

In particular, for $y = 1$ we obtain $t \cdot 1 = e$. Consequently,

$$L_b I_e R_a^{-1} x = e \cdot I_e x = L_e I_e x,$$

and the identity (11.29) takes the form

$$L_e I_e(xy) = I_e^{-1} y \cdot I_e x. \tag{11.30}$$

We have already seen that the equality $I_e^{-1} y = t$ is equivalent to the equality $ty = e$, so

$$I_e^{-1} y = e/y, \tag{11.31}$$

where $(/) = {}^{-1}(\cdot)$. From (11.26) we find

$$I_e x = x\backslash e, \tag{11.32}$$

where $(\backslash) = (\cdot)^{-1}$. Thus, we can rewrite (11.30) in the following form (replacing e by z):

$$z\,[(xy)\backslash z] = (z/y)(x\backslash z). \tag{11.33}$$

Note that $z = e$ may be any element of the set Q, so the identity (11.33) holds for arbitrary $x, y, z \in Q$.

Conversely, suppose (11.33) holds in a loop $Q(\cdot)$. We will show that condition (B) holds in $Q(\cdot)$. Suppose

$$x_1 y_2 = x_2 y_1 \quad \text{and} \quad x_1 y_4 = x_2 y_3 = x_3 y_2 = x_4 y_1 = z. \tag{11.34}$$

Now (11.34) implies

$$y_4 = x_1\backslash z, \quad y_3 = x_2\backslash z, \quad x_3 = z/y_2,$$

or, by (11.31) and (11.32),

$$y_4 = I_z x_1, \quad y_3 = I_z x_2, \quad x_3 = I_z^{-1} y_2.$$

Then $x_4 y_3 = x_4 \cdot I_z x_2 = L_{x_4} I_z x_2$. The equality (11.34) implies $R_{y_1} x_2 = x_1 y_2$, whence $x_2 = R^1_{y_1}(x_1 y_2)$. Thus

$$x_4 y_3 = L_{x_4} I_z R^{-1}_{y_1}(x_1 x_2). \tag{11.35}$$

For arbitrary elements a, e from Q, we have

$$L_e I_e R_a x = L_e I_e (xa) = L_e\left[(xa)\backslash e\right] = e\left[(xa)\backslash e\right] = (e/a)(x\backslash e).$$

Here we use (11.32) and (11.33). Thus,

$$L_e I_e R_a = L_b I_e,$$

where $b = e/a$, i.e., $e = ba$. From (11.35) we find

$$L_b I_e R_a^{-1} = L_e I_e.$$

We apply this equality to (11.35), taking into account that $x_4 y_1 = z$ — see (11.34):

$$L_{x_4} I_z R^{-1}_{y_1} = L_z I_z.$$

Thus

$$x_4 y_3 = L_z I_z (x_1 y_2) = z\left[(x_1 y_2)\backslash z\right] = (z/y_2)(x_1\backslash z).$$

Taking into account (11.34), we conclude $x_4 y_3 = x_3 y_4$, i.e., the condition (B) holds in $Q(\cdot)$. The proof of the theorem is complete.

Corollary 1. *In a loop $Q(\cdot)$, the anti-automorphic property of the permutation I is universal if and only if the identity (11.33) holds in $Q(\cdot)$.*

Corollary 2. *If a loop $Q(\cdot)$ satisfies the identity (11.33), then any of its loop isotopes also satisfies the identity.*

In other words, *the identity (11.33) is universal.*

3°. Moufang-Bol axioms and loop cores

The Bol conditions (B_l) and (B_r) are closely related to the left and right IP-properties. Recall that a loop $Q(\cdot)$ with neutral element 1 has the left inverse property if for any x and y, the equality

$$^{-1}x(xy) = y$$

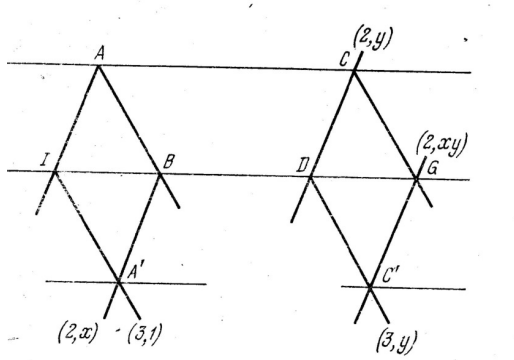


Fig. 8

holds, with ${}^{-1}xx = 1$. We will interpret this condition in a net $\mathfrak{A}$ coordinatized by $Q(\cdot)$.

Let the point I have coordinates $[1,1]$, and let AB be an arbitrary 3-line $(3,x)$. Then point A' (Figure 8) lies on the lines $(1,x')$, $(2,x)$ and $(3,1)$ for some $x' \in Q$. Consequently, $x'x = 1$, i.e., $x' = {}^{-1}x$. Consider an arbitrary point $C = [x,y]$ on the line $(1,x)$. Then $CD = (2,y)$ and $CG = (3,xy)$, while C' lies on $(1,x)$, $(2,xy)$ and $(3,y)$ for some $x'' \in Q$. Again, by the definition of the coordinate loop, we have

$$x''(xy) = y.$$

For $Q(\cdot)$ to be an IP-loop, it is necessary and sufficient that $x'' = {}^{-1}x$, i.e., the 1-line passing through A' must also pass through C', for any choice of point C on $(1,x)$. We arrive at the next concept. Fix an i-line l, and let m be an arbitrary i-line (for $i = 1,2,3$). Take an arbitrary point P on m. Through the point P we draw the remaining two lines PR and PS (Figure 9).

A single line parallel to the line PS passes through the point R, while a single line parallel to the line PR passes through S. These lines intersect at a point T. A single i-line passes through the point T. Following Bruck [33], we call the i-line n passing through T the *reflection*[5] of the line m in the line l. In particular, for $m = l$ we will assume that the reflection of m in l is also l. Generally speaking, the reflection n depends on the position of the point P. If the reflection does not depend on P, then we say that the *i-th Moufang-Bol axiom for the line l* is satisfied in the net $\mathfrak{A}$.

Let us return to the left inverse property in a loop $Q(\cdot)$. Using the concept of a line reflection, we can formulate the following statement.

Lemma 11.1. *For a loop $Q(\cdot)$ with neutral element 1 to have the left inverse property, it is necessary and sufficient that the first Moufang-Bol axiom for the 1-line $(1,1)$ holds in a net $\mathfrak{A}$ coordinatized by $Q(\cdot)$.*

The necessity has already been proven. We thus prove the sufficiency now.

Let $m = (1,x)$ and $P = [x,y]$. Consequently, the lines $(1,x)$, $(2,y)$ and $(3,xy)$ pass through P. Then $R = [1,y]$ and $S = [1,xy]$. Further, let the reflection of the line m in the

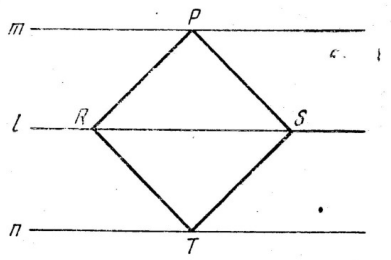


Fig. 9

line $l = (1, 1)$ be $n = (1, x')$. Thus, the lines $(1, x')$, $(2, xy)$ and $(3, y)$ pass through the point T. Consequently, $x'(xy) = y$. For $y = 1$ we obtain $x'x = 1$, i.e., $x' = {}^{-1}x$, and so we obtain the equality ${}^{-1}x(xy) = y$ establishing the left inverse property in $Q(\cdot)$.

A similar statement holds for the right inverse property.

We will say that the *i-th Moufang-Bol axiom* holds in the net $\mathfrak{A}$ if the i-th Moufang-Bol axiom holds for any i-line l in $\mathfrak{A}$.

Suppose that the first Moufang-Bol axiom holds in $\mathfrak{A}$ (Figure 10).

Let $m = (1, y)$ and $l = (1, x)$. Let n be the reflection of the 1-line m in the 1-line l. Since the first Moufang-Bol axiom holds in $\mathfrak{A}$, the position of the 1-line n does not depend on the point P, but only on the position of the 1-lines m and l. Thus, the label of the 1-line n only depends on x and y. Let $n = (1, x \overset{1}{+} y)$, where $\overset{1}{+}$ is the sign of some new operation on the set Q. Then $R = [x, p]$ and $S = [x, t]$ for some t. The point T must have coordinates $\left[x \overset{1}{+} y, t\right]$. Since PS and RT are 3-lines, we have

$$yp = xt \quad \text{and}$$

$$xp = (x \overset{1}{+} y)t. \tag{11.36}$$

Definition 3. Let $Q(\cdot)$ be a coordinate quasigroup of a net $\mathfrak{A}$ with the first Moufang-Bol axiom. Then $Q(\overset{1}{+})$ is called the *1-core* of the quasigroup.

Let $Q(\cdot)$ be a loop with neutral element 1. We choose p so that $t = 1$, i.e., $yp = x$. Then $x \overset{1}{+} y = xp = x(y \backslash x)$, and thus we recover the definition of the core from Chapter IX, 2°.

Figures 11 and 12 give the definition of 2- and *3-cores*: If the second Moufang-Bol axiom holds in $\mathfrak{A}$, then the reflection of $(2, y)$ in $(2, x)$ gives the 2-core $Q(\overset{2}{+})$, where $x \overset{2}{+} y$ depends on x and y in the following way:

$$py = tx, \quad px = t(x \overset{2}{+} y).$$

If the third Moufang-Bol axiom holds in $\mathfrak{A}$, then the reflection of $(3, y)$ in $(3, x)$ gives the definition of the 3-core $Q(\overset{3}{+})$, with

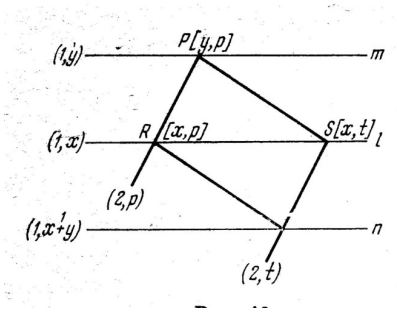


Fig. 10

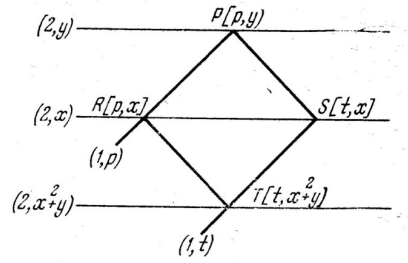


Fig.11

$$pt = y, \quad pv = vt = x, \quad vu = x \overset{3}{+} y.$$

Before proceeding to the study of the core, we prove the following theorem.

Theorem 11.7. *For $i = 1, 2$, and 3, the i-th Moufang-Bol axiom is equivalent to the respective closure conditions (B_l), (B_r), and (B).*

Let us prove the theorem for $i = 1$. Suppose the equalities

$$x_1y_2 = x_2y_1, \quad x_2y_2 = x_4y_1, \quad x_1y_4 = x_2y_3$$

hold in a coordinate quasigroup $Q(\cdot)$ of a net $\mathfrak{A}$ satisfying the first Moufang-Bol axiom.

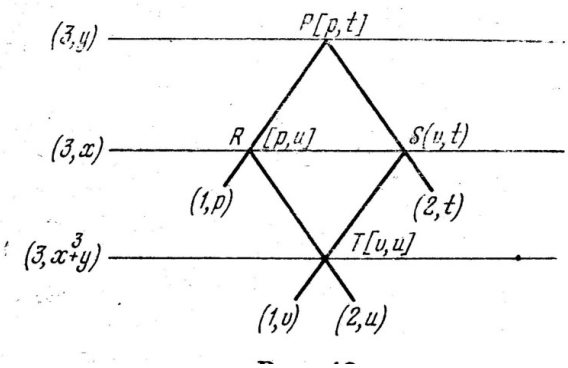


Fig. 12

By (11.36), $x_1y_2 = x_2y_1$ implies

$$x_2y_2 = (x_2 \overset{1}{+} x_1)y_1. \tag{11.37}$$

Also, $x_1y_4 = x_2y_3$ implies

$$x_2y_4 = (x_2 \overset{1}{+} x_1)y_3. \tag{11.38}$$

Comparing (11.37) with $x_2y_2 = x_4y_1$, we obtain $x_2 \overset{1}{+} x_1 = x_4$. Consequently, $x_2y_4 = x_4y_3$ follows from (11.38) and the latter equality.

Conversely, suppose the closure condition (B_l) holds in $Q(\cdot)$. Let us prove that the first Moufang-Bol axiom holds in a net $\mathfrak{A}$ coordinatized by $Q(\cdot)$. For this, it suffices to show that in the system

$$\left.\begin{aligned} yp &= xt, \\ xp &= ut \end{aligned}\right\} \tag{11.39}$$

of equations, the element u only depends on x and y, say $u = x \overset{1}{+} y$. Suppose we also have the equalities

$$\left.\begin{aligned} yp' &= xt', \\ xp' &= vt'. \end{aligned}\right\} \tag{11.40}$$

Set $x_1 = y$, $x_2 = x$, $x_4 = u$, $y_1 = t$, $y_2 = p$, $y_3 = t'$, and $y_4 = p$. Then the equalities (11.39) and first equality from (11.40) transform to the first three equalities from (11.8). But by (B_l), we obtain $x_2y_4 = x_4y_3$, i.e., $xp' = ut'$. Comparing the resulting equality with the second equality from (11.40), we find that $u = v$. This means that u does not depend on p, but only on x and y. For example, if $p' = x$, then t and, consequently, v depend only on x and y, so $u(= v)$ also only depends on x and y. Theorem 11.7 has been proved.

Corollary. Suppose that the first Moufang-Bol axiom is satisfied in a net $\mathfrak{A}$. Then each coordinatizing loop is a left Bol loop.

The statement follows from Theorem 11.4 and 11.7.

4°. Bol loop cores

We turn to the study of the core. Suppose that the first Moufang-Bol axiom holds in a net $\mathfrak{A}$. As shown above, every coordinate quasigroup is isotopic to a left Bol loop. A core is defined in any coordinate quasigroup $Q(\cdot)$ of the net $\mathfrak{A}$. The question naturally arises: What is the relationship between the cores of all the coordinate quasigroups of the net $\mathfrak{A}$?

The following theorem holds.

Theorem 11.8. *The cores* [*] *of all the coordinate quasigroups of a net $\mathfrak{A}$ with the first Moufang-Bol axiom are mutually isomorphic.*

[*] Henceforth, we only consider 1-cores. Therefore, we will omit the qualifier "1".

Let $Q(\cdot)$ and $Q(\circ)$ be two coordinate quasigroups of the net $\mathfrak{A}$, with respective cores $Q(+)$ and $Q(\oplus)$. Then by their definition, we have

$$yp = xt,$$

$$\left.\begin{array}{c} xp = (x+y)t, \\ y \circ p' = x \circ t', \\ x \circ p' = (x \oplus y) \circ t'. \end{array}\right\} \tag{11.41}$$

Let $u \circ v = \gamma^{-1}(\alpha u \cdot \beta v)$. Then the equalities (11.41) transform to

$$\gamma^{-1}(\alpha y \cdot \beta p') = \gamma^{-1}(\alpha x \cdot \beta t')$$

and

$$\gamma^{-1}(\alpha x \cdot \beta p') = \gamma^{-1}(a(x \oplus y) \cdot \beta t'),$$

whence

$$\alpha y \cdot \beta p' = \alpha x \cdot \beta t'$$

and

$$\alpha x \cdot \beta p' = \alpha(x \oplus y) \cdot \beta t'.$$

In view of the definition of the core $Q(+)$ we obtain

$$\alpha x + \alpha y = \alpha(x \oplus y),$$

which means that $Q(\oplus)$ and $Q(+)$ are isomorphic.

It is convenient to indicate the reflection of the 1-line $m = (1, y)$ in the 1-line $l = (1, x)$ as follows (see Figure 10):

$$x,\ y:\ P \to R, S, T.$$

We note here that P uniquely determines the points R, S, T. Using coordinates, we can write

$$[y,\ p] \to [x,\ p]\,, \quad [x,\ t]\,, \quad [x+y,\ t]\,,$$

with the understanding that $x + y$ currently means $x \overset{1}{+} y$.

Theorem 11.9. *The core of any coordinate quasigroup of a net $\mathfrak{A}$ with the first Moufang-Bol axiom is a left distributive groupoid.*

Proof. By Theorem 11.4, it suffices to prove the theorem for a Bol loop core.* In this case it was shown that

$$x + y = x(y\backslash x).$$

Since the Bol loop has the left inverse property, $y\backslash x = y^{-1}x$ and, consequently,

$$x + y = x(y^{-1}x). \tag{11.42}$$

*Here, we consider a left Bol loop.

Now consider the following reflections (Figure 13):

$$y,\ z:\ A \to H, E, I, \tag{11.43}$$

$$x,\ y+z:\ I \to F, K, L, \tag{11.44}$$

$$x,\ y:\ E \to F, B, G, \tag{11.45}$$

$$x,\ z:\ A \to C, B, D, \tag{11.46}$$

$$x+y,\ x+z:\ D \to G, M, L'. \tag{11.47}$$

The reflection (11.46) must have the form

$$x,\ z:\ A \to C, B', D. \tag{11.48}$$

But (11.43) and (11.44) imply that A, E, and B are on the same 3-line, and (11.48) implies that B' is on the same 3-line. Since B and B' are on the same 1-line $(1, x)$ simultaneously, they coincide.

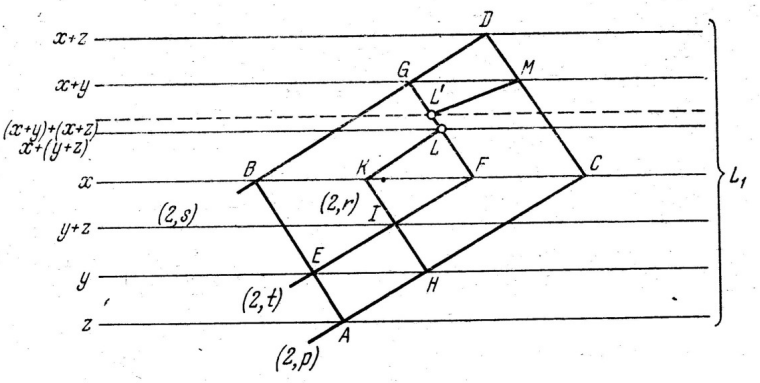


Fig. 13

In coordinates the reflections (11.43)–(11.47) have the form

$$[z,\ p] \to [y,\ p],\quad [y,\ t],\quad [y+z,\ t], \tag{11.49}$$

$$[y+z,\ t] \to [x,\ t],\quad [x,\ t],\quad [x,\ r],\quad [x+(y+z),\ r],$$
$$[y,\ t] \to [x,\ t],\quad [x,\ s],\quad [x+y,\ s],$$
$$[z,\ p] \to [x,\ p],\quad [x,\ s],\quad [x+z,\ s],$$
$$[x+z,\ s] \to [x+y,\ s],\quad [x+y,\ r'],\quad [(x+y)+(x+z),\ r'] \tag{11.50}$$

We show that

$$r = r'. \tag{11.51}$$

For this, we note that HI is a 3-line, as follows from the definition of the reflection (11.43). From (11.44) we find that IK is also a 3-line, i.e., H and K lie on the same 3-line. In this case the equality

$$yp = xr$$

holds. Since A is an arbitrary point of $(1, z)$, we set $p = 1$:

$$y = xr,$$

whence by left invertibility we find that

$$r = x^{-1}y. \tag{11.52}$$

Now (11.46) and (11.47) imply that CD and DM are 3-lines, i.e., C and M are on the same line. Consequently, we have

$$xp = (x + y)r',$$

whence in view of the equality $p = 1$ we obtain

$$(x + y)r' = x. \tag{11.53}$$

We find $(x + y)r$, taking into account (11.42), (11.52) and the Bol identity:

$$(x + y)r = (x \cdot y^{-1}x)(x^{-1}y) = x\left[y^{-1}(x \cdot x^{-1}y)\right] = x(y^{-1}y) = x.$$

Comparing the latter equality with (11.53), the equality (11.51) is established.

Now (11.44), (11.45) and (11.47) imply that FL, LG and GL' are 3-lines. Consequently, F, G, L and L' are on the same 3-line. On the other hand, from (11.43) and (11.50), and from $r = r'$, it follows that K, M, L, L' are on the same 2-line, namely on $(2, r)$. Since, the 3-line $FGLL'$ and the 2-line $KMLL'$ have common points L and L', and this is possible only if $L = L'$, whence it follows that

$$x + (y + z) = (x + y) + (x + z).$$

The proof of the theorem is complete. □

Now we find the conditions under which $Q(+)$ is a quasigroup.

Theorem 11.10. *The core of a Bol loop $Q(\cdot)$ is a quasigroup if and only if the the squaring $x \to x^2$ is a permutation of the set Q.*

The necessity of the condition is obtained immediately: if $Q(+)$ is a quasigroup, then the equation $x + 1 = a$ has a unique solution, i.e., $x(1^{-1}x) = a$ or $x^2 = a$ has a unique solution, for any $a \in Q$. Denote the solution of the equation by $a^{1/2}$.

Before proving the sufficiency of the condition formulated in the theorem, it is necessary to prove the validity of the following two relations:

$$(x^{1/2})^{-1} = (x^{-1})^{1/2}, \tag{11.54}$$

$$(x+y)^{-1} = x^{-1} + y^{-1}. \tag{11.55}$$

To prove (11.54), we use the left alternativity $x \cdot xy = x^2 \cdot y$, which holds in any Bol loop:

$$(x^{-1})^2 x^2 = (x^{-1}x^{-1})(xx) = x^{-1}(x^{-1} \cdot xx) = x^{-1}x = 1,$$

whence

$$(x^{-1})^2 = (x^2)^{-1}. \tag{11.56}$$

Let $x^2 = y$. Then (11.56) implies $(x^{-1})^2 = y^{-1}$, whence $x^{-1} = (y^{-1})^{1/2}$ or $(y^{1/2})^{-1} = (y^{-1})^{1/2}$. The element y, along with x, can be any element of the set Q, since $x \to x^2$ is a permutation of Q. We can obtain another proof, if we consider that in a Bol loop any element generates an associative subloop (see, for example, [11]).

To prove (11.55) we find $(x^{-1} + y^{-1})(x + y)$. We have

$$\begin{aligned}(x^{-1} + y^{-1})(x + y) &= (x^{-1} \cdot yx^{-1})(x \cdot y^{-1}x) \\ &= x^{-1}\left\{y\left[x^{-1}(x \cdot y^{-1}x)\right]\right\} = x^{-1}(y \cdot y^{-1}x) = x^{-1}x = 1,\end{aligned}$$

which implies the equality (11.55).

Sufficiency. Let $x \to x^2$ be a permutation of the set Q. We prove that the equality

$$a + y = b \tag{11.57}$$

has a unique solution for all $a, b \in Q$.

Let y_0 be a solution of the equation (11.57). Then (11.57), by the definition of the operation $(+)$, takes a form

$$a \cdot y_0^{-1}a = b,$$

whence

$$\begin{gathered}(a \cdot y_0^{-1}a)a^{-1} = ba^{-1}, \quad a(y_0^{-1} \cdot aa^{-1}) = ba^{-1}, \\ ay_0^{-1} = ba^{-1}, \quad y_0^{-1} = a^{-1} \cdot ba^{-1}, \\ y_0 = (a^{-1} \cdot ba^{-1})^{-1}, \end{gathered} \tag{11.58}$$

or

$$y_0 = (a^{-1} + b^{-1})^{-1}.$$

Consequently,

$$y_0 = a + b. \tag{11.59}$$

We check that y_0, defined by (11.58), is a solution of the equation (11.57):

$$a \cdot y_0^{-1}a = a\left[(a^{-1} \cdot ba^{-1})a\right] = a\left[a^{-1}(b \cdot a^{-1}a)\right] = a(a^{-1}b) = b.$$

Now consider the equation

$$x + a = b. \tag{11.60}$$

Suppose that x_0 is a solution of (11.60). Then (11.60) implies

$$x_0(a^{-1}x_0) = b. \tag{11.61}$$

Let $a^{-1} = c$. Then $(x_0 \cdot cx_0)c^{1/2} = bc^{1/2}$, whence

$$c^{1/2}\left[x_0(c \cdot x_0c^{1/2})\right] = c^{1/2} \cdot bc^{1/2}. \tag{11.62}$$

Rewriting the left side of (11.62),

$$c^{1/2}\left[x_0(c^{1/2}c^{1/2} \cdot x_0c^{1/2})\right] = c^{1/2}\left\{x_0\left[c^{1/2}(c^{1/2} \cdot x_0c^{1/2})\right]\right\}$$

$$= (c^{1/2} \cdot x_0c^{1/2})(c^{1/2} \cdot x_0c^{1/2}) = (c^{1/2} \cdot x_0c^{1/2})^2 = (c^{1/2} + x_0^{-1})^2.$$

The right side of (11.62) is equal to $c^{1/2} + b^{-1}$, since

$$c^{1/2} + x_0^{-1} = (c^{1/2} + b^{-1})^{1/2}. \tag{11.63}$$

We find x_0^{-1} from (11.63) using the equality (11.59): $x_0^{-1} = c^{1/2} + (c^{1/2} + b^{-1})^{1/2}$, whence $x_0 = \left[c^{1/2} + (c^{1/2} + b^{-1})^{1/2}\right]^{-1}$, or, using the equalities (11.54) and (11.55), we obtain

$$x_0 = (c^{1/2})^{-1} + \left[(c^{1/2} + b^{-1})^{1/2}\right]^{-1}, \quad x_0 = (c^{-1})^{1/2} + \left[(c^{-1})^{1/2} + b\right]^{1/2}.$$

Taking into account that $c = a^{-1}$, we finally find

$$x_0 = a^{1/2} + (a^{1/2} + b)^{1/2}. \tag{11.64}$$

The transitions from (11.61) to (11.63), and thence to (11.64) are invertible, whence we conclude that the solution of the equation (11.60) exists, since the equality (11.61) is nothing else than $x_0 + a = b$. This completes the proof of the theorem.

Theorems 11.9 and 11.10 generalize Theorem 9.5 and Theorem 9.4 for Moufang loops.

Note the following property of a core $Q(+)$:

$$x + (x + y) = y. \tag{11.65}$$

Indeed, combining the equality $a + y_0 = b$ and (11.58), we obtain

$$b = a + y_0 = a + (a + b).$$

The question arises: When is a loop isotopic to the core $Q(+)$ of a Bol loop $Q(\cdot)$ which satisfies the condition of Theorem 11.10?

The following theorem holds.

Theorem 11.11. *Suppose that the condition of Theorem 11.10 holds in a Bol loop $Q(\cdot)$, with core $Q(+)$. Then the quasigroup $Q(+)$ is isotopic to a Bol loop.*

The theorem is a direct corollary of Theorem 9.11: in the left-distributive quasigroup $Q(+)$ we have $L_x^2 = 1$ by virtue of the equality (11.65).

Notes

[1]The concept of a net, apparently, was first introduced by Thomsen [23] in 1929.

[2]The concept of a net given here is a particular case of the concept of a k-net for $k = 3$. A k-net is defined in the same way as a 3-net $\mathfrak{A}$, but L divides into k non-intersecting classes $L_1, L_2, \ldots, L_k$, satisfying Axioms 1 and 2. The concept of a k-net for $k \geqslant 4$ is closely connected with a system of mutually orthogonal quasigroups (see Chapter VII, 4°, Definition 5). Details about k-nets are given in Bruck [31, 33] and Pickert [61].

[3]This implies that the net $\mathfrak{A}$ defines a quasigroup up to isotopy and parastrophy (see Note 7 to Chapter I).

[4]If a loop $Q(\cdot)$ satisfies the hexagon condition (H), then $x^{-1} = {}^{-1}x$, and this property is universal. Moreover, all such loops are mono-associative, i.e., each element generates an associative subgroup (see [10], for example).

[5]Thus, a reflection is a certain transformation of the net $\mathfrak{A}$ (in the presence of the first Moufang-Bol axiom). Other transformations in nets (without additional conditions) were considered by Artzy [7], namely, transformations analogous to motions in ordinary Euclidean planes.

Problems

Let us formulate a number of problems in the theory of quasigroups, which, so far as the author knows, have not been solved and whose solution is of interest.

1. Find necessary and sufficient conditions for a special loop (Chapter III, 1°) to be isotopic to a left F-quasigroup. Is any identity fulfilled in special loops? Which loops are isotopic to bilateral F-quasigroups (Chapter III, 5°)?

2. Let $Q(\circ)$ be a group, and let $x \circ y = z_1^{\varepsilon_1} z_2^{\varepsilon_2} \dots z_n^{\varepsilon_n}$, where $z_i = x$ or y, and $\varepsilon_i = \pm 1$ (for $i = 1, 2, \dots, n$). At what values of ε_n will the groupoid $Q(\circ)$ be a quasigroup?

3. A quasigroup $Q(\cdot)$ is a *Stein quasigroup* [76], if it satisfies the identity $x \cdot xy = yx$. To which loops are Stein quasigroups isotopic?

4. A quasigroup $Q(A)$ is called a *σ-quasigroup*, if ${}^{\sigma}A = A$, where ${}^{\sigma}A$ is an inverse operation for A (Chapter I, 4°). If ${}^{\sigma}A = A^T$ (where A^T is an isotope of the quasigroup A), then will A be isotopic to some σ-quasigroup [72]?

5. To construct and develop a homotopy theory for quasigroups (Chapter IV, 4°).

6. To construct a theory of extensions for quasigroups (see Chapter V, 2°, and crossed products of quasigroups. Compare [2, 26, 90]).

7. To extend theorems of the extension of groups to any loops (in particular, to Moufang loops and to other loops classes).

8. Are there left-distributive quasigroups isotopic to loops which are not Bol loops (Chapter IX)?

9. If a positive answer is possible to the previous question, then the problem arises of describing such loops. In particular, it is required to indicate which identities they satisfied.

10. What necessary and sufficient conditions should be imposed on a loop so that its core (Chapter IX, 1° becomes a left distributive groupoid (quasigroup)?

11. In which loops is the property of being special (Chapter III, 1°) universal (Chapter X, 4°)?

12. Find G-loop classes distinct from those described in Chapter X, 1°. Describe the class of all G-loops (for example, using identities).

13. Find other conditions of closure in nets (Chapter XI, 2°). Construct a general theory of closure conditions.

14. Explore loops with the identity $z\,[(xy)\backslash z] = (z/y)(x\backslash z)$ (Chapter XI, 2°, Theorem 11.6).

15. Will an infinite anti-commutative distributive quasigroup be transitive (Chapter VIII, Theorem 8.4)?

16. Let $S(\cdot)$ be an abbreviation semigroup (i.e., $xy = xz$ or $yx = zx$ implies $y = z$). Can

it be included in a quasigroup (loop) with a nontrivial identity? (An identity is nontrivial if there is a more than one-element quasigroup in which it does not hold).*

17. What necessary and sufficient conditions must a groupoid $Q(\cdot)$ satisfy in order for it to be embedded in a Moufang loop, an IP-loop, or a distributive quasigroup*?

18. Are there any identities in a quasigroup $Q(\cdot)$ implying that $Q(\cdot)$ is a loop? (An example of such an identity is associativity.)*

19. Do there exist loops with a preassigned type $(\mathscr{L}, \Phi, \mathscr{R})$ and preassigned intersections $\mathscr{L} \bigcap \Phi, \Phi \bigcap \mathscr{R}, \mathscr{L} \bigcap \mathscr{R}, \mathscr{L} \bigcap \Phi \bigcap \mathscr{R}$?

20. In which quasigroups or loops are all (groupo) congruences are normal? (In IP-quasigroups, all congruences are normal. See [22], for example.).

*Proposed by I.E. Burmistrovich.

Bibliography

[1] A. A. Albert, Quasigroups. I, Trans. Amer. Math. Soc. **54** (1943), 507–519; MR0009962

[2] A. A. Albert, Quasigroups. II, Trans. Amer. Math. Soc. **55** (1944), 401–419; MR0010597

[3] R. Artzy, On loops with a special property, Proc. Amer. Math. Soc. **6** (1955), 448–453; MR0069804

[4] R. Artzy, Crossed-inverse and related loops, Trans. Amer. Math. Soc. **91** (1959), 480–492; MR0106958

[5] R. Artzy, On automorphic-inverse properties in loops, Proc. Amer. Math. Soc. **10** (1959), 588–591; MR0107674

[6] R. Artzy, Relations between loop identities, Proc. Amer. Math. Soc. **11** (1960), 847–851; MR0117295

[7] R. Artzy, Net motions and loops, Arch. Math. (Basel) **14** (1963), 95–101; MR0148786

[8] R. Artzy, Isotopy and parastrophy of quasigroups, Proc. Amer. Math. Soc. **14** (1963), 429–431; MR0147574

[9] J. D. Aczél, *Vorlesungen über Funktionalgleichungen und ihre Anwendungen*, Lehrbücher und Monographien aus dem Gebiete der Exakten Wissenschaften, Mathematische Reihe, Bd. 25, Birkhäuser Verlag, Basel-Stuttgart, 1961; MR0124647

[10] J. D. Aczél, Quasigroups—nets—nomograms, Mat. Lapok **15** (1964), 114–162; MR0172956

[11] J. D. Aczél, V. D. Belousov and M. Hosszú, Generalized associativity and bisymmetry on quasigroups, Acta Math. Acad. Sci. Hungar. **11** (1960), 127–136; MR0140600

[12] V. D. Belousov, Derivative operations and associators in loops, Mat. Sb. (N.S.) **45(87)** (1958), 51–70; MR0093556

[13] V. D. Belousov, Les quasi-groupes transitifs et distributifs, Ukrain. Mat. Ž. **10** (1958), no. 1, 13–22; MR0095892

[14] V. D. Belousov, Regular substitutions in quasigroups. (Russian), Uch. zap. Balti Ped. Institute, 1958, vyp. 1, 39-49.

[15] V. D. Belousov, On a class of quasigroups. (Russian), Uch. zap. Balti Ped. Institute, 1960, vyp. 5, 29-46.

[16] V. D. Belousov, The structure of distributive quasigroups, Mat. Sb. (N.S.) **50(92)** (1960), 267–298; MR0120304

[17] V. D. Belousov, On a class of left-distributive quasi-groups, Izv. Vysš. Učebn. Zaved. Matematika. (1963), no. 1(32), 16–20; MR0147573

[18] V. D. Belousov, Reciprocally-inverse quasi-groups and loops, Bul. Akad. Štiince RSS Moldoven. (1963), no. 11, 3–10 (1964); MR0212111

[19] V. D. Belousov, Systems of quasigroups with generalized identities, Uspehi Mat. Nauk **20** (1965), no. 1(121), 75–146; MR0173724

[20] V. D. Belousov, Two problems of the theory of distributive quasigroups, in *Studies in Algebra and Math. Anal. (Russian)*, pp. 109–112, Izdat. "Karta Moldovenjaske", Kishinev, ; MR0200378

[21] V. D. Belousov, Loops with a kernel of index two, in *Studies in Algebra and Math. Anal. (Russian)*, pp. 11–21, Izdat. "Karta Moldovenjaske", Kishinev, ; MR0201556

[22] G. Birkhoff, *Lattice Theory*, revised edition, American Mathematical Society Colloquium Publications, Vol. 25, Amer. Math. Soc., New York, 1948; MR0029876

[23] G. Bol, Gewebe und Gruppen. Math. Ann. 114, 414–431 (1937; JFM 63.1157.04)

[24] R. H. Bruck, Some results in the theory of quasigroups, Trans. Amer. Math. Soc. **55** (1944), 19–52; MR0009963

[25] R. H. Bruck, Contributions to the theory of loops, Trans. Amer. Math. Soc. **60** (1946), 245–354; MR0017288

[26] R. H. Bruck, An extension theory for a certain class of loops, Bull. Amer. Math. Soc. **57** (1951), 11–26; MR0039715

[27] R. H. Bruck, Loops with transitive automorphism groups, Pacific J. Math. **1** (1951), 481–483; MR0045705

[28] R. H. Bruck and E. Kleinfeld, The structure of alternative division rings, Proc. Amer. Math. Soc. **2** (1951), 878–890; MR0045099

[29] R. H. Bruck, Pseudo-automorphisms and Moufang loops, Proc. Amer. Math. Soc. **3** (1952), 66–72; MR0047635

[30] R. H. Bruck and L. J. Paige, Loops whose inner mappings are automorphisms, Ann. of Math. (2) **63** (1956), 308–323; MR0076779

[31] R. H. Bruck, *A survey of binary systems*, Reihe: Gruppentheorie Ergebnisse der Mathematik und ihrer Grenzgebiete, (N.F.), Heft 20, Springer, Berlin-Göttingen-Heidelberg, 1958; MR0093552

[32] R. H. Bruck, Some theorems on Moufang loops, Math. Z. **73** (1960), 59–78; MR0125895

[33] Bruck, R. H., What is a loop? Studies in Math., **v.2**. 59–99.

[34] C. Burstin and W. Mayer, Distributive Gruppen von endlicher Ordnung, J. Reine Angew. Math. **160** (1929), 111–130; MR1581179

[35] R. Baer, Nets and groups. II, Trans. Amer. Math. Soc. **47** (1940), 435–439; MR0002135

[36] R. Baer, The homomorphism theorems for loops, Amer. J. Math. **67** (1945), 450–460; MR0012302

[37] P. T. Bateman, A remark on infinite groups, Amer. Math. Monthly **57** (1950), 623–624; MR0040293

[38] G. E. Bates and F. Kiokemeister, A note on homomorphic mappings of quasigroups into multiplicative systems, Bull. Amer. Math. Soc. **54** (1948), 1180–1185; MR0027768

[39] G. N. Garrison, Quasi-groups, Ann. of Math. (2) **41** (1940), 474–487; MR0002150

[40] G. N. Garrison, Note on invariant complexes of a quasigroup, Ann. of Math. (2) **47** (1946), 50–55; MR0015125

[41] A. Ginzburg, Systèmes multiplicatifs de relations. Boucles quasi associatives, C. R. Acad. Sci. Paris **250** (1960), 1413–1416; MR0113962

[42] A. Ginzburg, A note on Cayley loops, Canadian J. Math. **16** (1964), 77–81; MR0164996

[43] H. Griffin, The Abelian quasi-group. Am. J. Math. 62, 725–737 (1940; JFM 66.0095.01)

[44] T. Evans, Homomorphisms of non-associative systems, J. London Math. Soc. **24** (1949), 254–260; MR0032664

[45] W. R. Cowell, Concerning a class of permutable congruence relations on loops, Proc. Amer. Math. Soc. **7** (1956), 583–588; MR0079010

[46] A. G. Kurosh, *[The theory of groups]* (Russian), Gosudarstv. Izdat. Tehn.-Teor. Lit., Moscow, 1953; MR0059266

[47] A. G. Kurosh, *[Lectures on general algebra]* (Russian), Gosudarstv. Izdat. Fiz.-Mat. Lit., Moscow, 1962; MR0141700

[48] F. W. Levi and B. L. van der Waerden, Über eine besondere Klasse von Gruppen, Abh. Math. Sem. Univ. Hamburg **9** (1933), no. 1, 154–158; MR3069591

[49] H. B. Mann, The construction of orthogonal Latin squares, Ann. Math. Statistics **13** (1942), 418–423; MR0007736

[50] G. Mattenet, Exemple d'équivalence régulière et simplifiable dans un quasi-groupe, C. R. Acad. Sci. Paris **255** (1962), 3092–3094; MR0143830

[51] D. C. Murdoch, Quasi-groups which satisfy certain generalized associative laws. Am. J. Math. 61, 509–522 (1939; JFM 65.0077.01)

[52] D. C. Murdoch, Structure of abelian quasi-groups, Trans. Amer. Math. Soc. **49** (1941), 392–409; MR0003427

[53] D. C. Murdoch, Note on normality in quasi-groups, Bull. Amer. Math. Soc. **47** (1941), 134–138; MR0003426

[54] R. Moufang, Zur Struktur von Alternativkörpern. Math. Ann. 110, 416–430 (1935).

[55] B. H. Neumann, On the commutativity of addition, J. London Math. Soc. **15** (1940), 203–208; MR0002851

[56] J. M. Osborn, A theorem on A-loops, Proc. Amer. Math. Soc. **9** (1958), 347–349; MR0093555

[57] J. M. Osborn, Loops with the weak inverse property, Pacific J. Math. **10** (1960), 295–304; MR0111800

[58] J. M. Osborn, New loops from old geometries, Amer. Math. Monthly **68** (1961), 103–107; MR0124374

[59] J. M. Osborn, Vector loops, Illinois J. Math. **5** (1961), 565–584; MR0132801

[60] E. T. Parker, Orthogonal latin squares, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 859–862; MR0104591

[61] G. Pickert, *Projektive Ebenen*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, Band LXXX, Springer, Berlin-Göttingen-Heidelberg, 1955; MR0073211

[62] L. J. Paige, Complete mappings of finite groups, Pacific J. Math. **1** (1951), 111–116; MR0043080

[63] L. J. Paige, A class of simple Moufang loops, Proc. Amer. Math. Soc. **7** (1956), 471–482; MR0079596

[64] A. Sade, Quasigroupes obéissant à certaines lois, Rev. Fac. Sci. Univ. Istanbul. Sér. A **22** (1957), 151–184; MR0106253

[65] A. Sade, Quasigroupes automorphes par le groupe linéaire et géométrie finie, J. Reine Angew. Math. **199** (1958), 100–120; MR0093554

[66] A. Sade, Quasigroupes parastrophiques. Expressions et identités, Math. Nachr. **20**, no. 1–2, (1959), 73–106; MR0114870

[67] A. Sade, Entropie demosienne de multigroupoïdes et de quasigroupes, Ann. Soc. Sci. Bruxelles Sér. I **73** (1959), 302–309; MR0124255

[68] A. Sade, Produit direct-singulier de quasigroupes orthogonaux et anti-abéliens, Ann. Soc. Sci. Bruxelles Sér. I **74** (1960), 91–99; MR0140599

[69] A. Sade, Anti-autotopie dans les quasigroupes, Ann. Soc. Sci. Bruxelles Sér. I **74** (1960), 5–11; errata, 99; MR0112914

[70] A. Sade, Paratopie et autoparatopie des quasigroupes, Ann. Soc. Sci. Bruxelles Sér. I **76** (1962), 88–96; MR0152600

[71] A. Sade, Semi-automorphisme de groupoïdes et de quasigroupes, Ann. Soc. Sci. Bruxelles Sér. I **76** (1962), 97–104; MR0152601

[72] A. Sade, Quelques problèmes non résolus dans la théorie des groupes, 1963, Neki nerešeni Problemi u Matematici, 71-72 (1963).

[73] A. Sade, Le groupe d'anti-autotopie et l'équation $Q(X, X^{-1}, 1) = QP^{12} = Q$, J. Reine Angew. Math. **216** (1964), 199–217; MR0167560

[74] S. K. Stein, On the foundations of quasigroups, Trans. Amer. Math. Soc. **85** (1957), 228–256; MR0094404

[75] S. K. Stein, On a construction of Hosszú, Publ. Math. Debrecen **6** (1959), 10–14; MR0104750

[76] S. K. Stein, Left-distributive quasi-groups, Proc. Amer. Math. Soc. **10** (1959), 577–578; MR0108547

[77] Yu. I. Sorkin, On distributive quasigroups. (Russian), Uch. zap. MZPI, 1959, 3, 82-92.

[78] A. K. Suschkewitsch, The theory of generalized groups. (Russian), Kiev, 1937.

[79] K. Toyoda, On axioms of linear functions, Proc. Imp. Acad. Tokyo **17** (1941), 221–227; MR0014105

[80] B. Fischer, Distributive Quasigruppen endlicher Ordnung, Math. Z. **83** (1964), 267–303; MR0160845

[81] C. M. Fulton and S. K. Stein, The passage from geometry to algebra, Math. Ann. **134** (1957), 140–142; MR0092983

[82] E. A. Khalezov, Automorphisms of primitive quasigroups, Mat. Sb. (N.S.) **53(95)** (1961), 319–342; MR0120303

[83] M. Hosszú, Nonsymmetric means, Publ. Math. Debrecen **6** (1959), 1–9; MR0104751

[84] M. Hosszú, Homogeneous groupoids, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **3/4** (1960/61), 95–99; MR0132799

[85] M. Hall Jr., *The theory of groups*, The Macmillan Company, New York, 1959; MR0103215

[86] M. Hall Jr., *Combinatorial theory*, Blaisdell Publishing Co. [Ginn and Co.], Waltham, Mass.-Toronto, Ont.-London, 1967; MR0224481

[87] M. Hall Jr. and L. J. Paige, Complete mappings of finite groups, Pacific J. Math. **5** (1955), 541–549; MR0079589

[88] K. Culik, Poznamky k teorii operaci.Ceasop. pestov. mat., 1960, 83, N 4, 474.

[89] O. Y. Shmidt, *[Selected works. Mathematics]* (Russian), Akad. Nauk SSSR, 1959; MR0102466

[90] S. Eilenberg and S. Mac Lane, Algebraic cohomology groups and loops, Duke Math. J. **14** (1947), 435–463; MR0021939

[91] I. M. H. Etherington, Non-associative arithmetics, Proc. Roy. Soc. Edinburgh Sect. A **62** (1949), 442–453; MR0029898

Valentin BELOUSOV

Foundations of the theory of quasigroups and loops

Bun de tipar 29.12.2025. Formatul 70x100 1/12.

Coli de tipar 25,0. Coli editorial 13,2.

Comanda. 168/25. Tirajul 150 ex.

Editura USM Str. Al. Mateevici, 60, Chișinău, MD 2009

e-mail: *editurausm@gmail.com*