MONOGRAPHS AND RESEARCH NOTES IN MATHEMATICS

Elements of Quasigroup Theory and Applications

Victor Shcherbacov

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

MONOGRAPHS AND RESEARCH NOTES IN MATHEMATICS

Elements of Quasigroup Theory and Applications

Victor Shcherbacov

Principal Researcher
Institute of Mathematics and Computer Science
Academy of Sciences
Moldova

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

A CHAPMAN & HALL BOOK

MONOGRAPHS AND RESEARCH NOTES IN MATHEMATICS

Series Editors

John A. Burns
Thomas J. Tucker
Miklos Bona
Michael Ruzhansky

Published Titles

Actions and Invariants of Algebraic Groups, Second Edition, Walter Ferrer Santos and Alvaro Rittatore

Analytical Methods for Kolmogorov Equations, Second Edition, Luca Lorenzi

Application of Fuzzy Logic to Social Choice Theory, John N. Mordeson, Davender S. Malik and Terry D. Clark

Blow-up Patterns for Higher-Order: Nonlinear Parabolic, Hyperbolic Dispersion and Schrödinger Equations, Victor A. Galaktionov, Enzo L. Mitidieri, and Stanislav Pohozaev

Bounds for Determinants of Linear Operators and Their Applications, Michael Gil′

Complex Analysis: Conformal Inequalities and the Bieberbach Conjecture, Prem K. Kythe

Computational Aspects of Polynomial Identities: Volume I, Kemer's Theorems, 2nd Edition Alexei Kanel-Belov, Yakov Karasik, and Louis Halle Rowen

A Concise Introduction to Geometric Numerical Integration, Fernando Casas and Sergio Blanes

Cremona Groups and Icosahedron, Ivan Cheltsov and Constantin Shramov

Delay Differential Evolutions Subjected to Nonlocal Initial Conditions Monica-Dana Burlică, Mihai Necula, Daniela Roşu, and Ioan I. Vrabie

Diagram Genus, Generators, and Applications, Alexander Stoimenow

Difference Equations: Theory, Applications and Advanced Topics, Third Edition Ronald E. Mickens

Dictionary of Inequalities, Second Edition, Peter Bullen

Elements of Quasigroup Theory and Applications, Victor Shcherbacov

Finite Element Methods for Eigenvalue Problems, Jiguang Sun and Aihui Zhou

Introduction to Abelian Model Structures and Gorenstein Homological Dimensions Marco A. Pérez

Iterative Methods without Inversion, Anatoly Galperin

Iterative Optimization in Inverse Problems, Charles L. Byrne

Line Integral Methods for Conservative Problems, Luigi Brugnano and Felice Iavernaro

Lineability: The Search for Linearity in Mathematics, Richard M. Aron, Luis Bernal González, Daniel M. Pellegrino, and Juan B. Seoane Sepúlveda

Modeling and Inverse Problems in the Presence of Uncertainty, H. T. Banks, Shuhua Hu, and W. Clayton Thompson

Monomial Algebras, Second Edition, Rafael H. Villarreal

Published Titles Continued

Nonlinear Functional Analysis in Banach Spaces and Banach Algebras: Fixed Point Theory Under Weak Topology for Nonlinear Operators and Block Operator Matrices with Applications, Aref Jeribi and Bilel Krichen

Partial Differential Equations with Variable Exponents: Variational Methods and Qualitative Analysis, Vicenţiu D. Rădulescu and Dušan D. Repovš

A Practical Guide to Geometric Regulation for Distributed Parameter Systems Eugenio Aulisa and David Gilliam

Reconstruction from Integral Data, Victor Palamodov

Signal Processing: A Mathematical Approach, *Second Edition*, Charles L. Byrne

Sinusoids: Theory and Technological Applications, Prem K. Kythe

Special Integrals of Gradshteyn and Ryzhik: the Proofs – Volume I, Victor H. Moll

Special Integrals of Gradshteyn and Ryzhik: the Proofs – Volume II, Victor H. Moll

Stochastic Cauchy Problems in Infinite Dimensions: Generalized and Regularized Solutions, Irina V. Melnikova

Submanifolds and Holonomy, Second Edition, Jürgen Berndt, Sergio Console, and Carlos Enrique Olmos

Symmetry and Quantum Mechanics, Scott Corry

The Truth Value Algebra of Type-2 Fuzzy Sets: Order Convolutions of Functions on the Unit Interval, John Harding, Carol Walker, and Elbert Walker

Forthcoming Titles

Groups, Designs, and Linear Algebra, Donald L. Kreher

Handbook of the Tutte Polynomial, Joanna Anthony Ellis-Monaghan and Iain Moffat

Microlocal Analysis on Rˆn and on NonCompact Manifolds, Sandro Coriasco

Practical Guide to Geometric Regulation for Distributed Parameter Systems, Eugenio Aulisa and David S. Gilliam

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2017 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed on acid-free paper
Version Date: 20170215

International Standard Book Number-13: 978-1-4987-2155-4 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Dedicated to my mother

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Contents

Foreword

This book is based on lectures which the author gave for graduate students of Charles University (Prague, Czech Republic) in autumn 2003 [779].

We hope this book will assist young (and not so young) mathematicians who would like to start their own research on the topic of quasigroup theory and especially on its applications.

In Chapters 1–4 a sufficiently elementary introduction to the theory of quasigroups and main classes of quasigroups is given. In Chapters 5–9 some results obtained mainly in the last twenty years in the branch of "pure" quasigroup theory are presented. In Chapters 10 and 11 information on applications of quasigroups in code theory and cryptology is collected.

Therefore it is possible to divide this book into three parts: Foundations, Theory, and Applications.

Chapter 1 "Elements of Quasigroup Theory" gives a short, somewhat "elementary" from the point of view of an "advanced" algebraist, and in some places only the outlined, introduction to quasigroup theory. In this chapter we try to demonstrate to the reader that there is no essentially big difference between binary and n-ary objects and that the "work" with an n-ary object is quite similar to the work with a binary object.

As it seems to the author, this introductory chapter is written in the spirit of Belousov quasigroup school: that is, attention is given especially to algebraic questions concerning quasigroup theory.

The author hopes that many questions which mainly concern loop theory will be discussed in more detail in other books.

We hope that this chapter will be comprehensible to undergraduate students (both for independent study and also for study with a teacher).

In writing this chapter, the author has tried also to take into consideration possible needs and interests of engineers, mathematicians who are non-algebraists and physicists who would like to use quasigroups in coding theory, cryptology, physics or in some other "suitable places" for application of quasigroups.

Notice, the theory of quasigroups is in the process of rapid growth and even the foundations of quasigroup theory are being changed quite quickly.

Most applications of quasigroups are connected with the fact that quasigroups often have some kind of inverse property and/or that they, like semigroups, are a generalization of the concept of a group.

Readers can find more detailed introductions to quasigroup theory in the books of V.D. Belousov [72, 80], H.O. Pflugfelder [685], and J.D.H. Smith [819]. See, also, [173, 201, 865]. Smooth quasigroups and loops are studied in [654, 727], and topological algebraic systems, including topological quasigroups, in [205].

Good introductions to the theory of Latin squares and applications can be found in [240, 490, 559, 86].

In Chapter 2 "Some Quasigroup Classes" information about the most researched quasigroup classes is included. A big part of this information is well known but there are some new results, too.

Chapter 3 is based on information from joint articles of A.D. Keedwell and

V.A. Shcherbacov concerning properties of some new classes of inverse quasigroups [486, 487, 488, 489]. There exists a sufficient basis to expect that quasigroups with these inverse properties will be applicable in cryptology.

In Chapter 4 relatively new "autotopical" approach to the nuclei and center of a quasigroup is presented.

Chapter 5 contains solutions of two problems from V.D. Belousov's book [72].

In Chapter 6 information on properties (direct decompositions, simple objects, loop isotopes) of finite left and right F-, E-, and SM-quasigroups is presented. The solutions of "1a" Belousov problem [72] and two problems of Kinyon and Phillips [520] are obtained as corollaries.

Chapter 7 contains a theorem that is a generalization of the classical Murdoch Theorem [646] on the structure of binary finite medial quasigroups. Simple n-ary medial quasigroups are also described.

In Chapter 8 information on automorphisms of binary and n-ary (mainly linear) quasigroups is given.

Chapter 9 contains a quite new approach and results concerning orthogonality of binary quasigroups. See, also [643, 213]. Various applications of the property of orthogonality of quasigroups and groupoids are described in books by J. Denes and A.D. Keedwell [240, 241, 243].

In Chapter 10 an n-ary quasigroup approach to codes with one check symbol is developed. This part is based on joint articles of G.L. Mullen and V.A. Shcherbacov [641, 642]. Information on quasigroup-based recursive MDS codes is mainly taken from [371].

Results on applications of quasigroups in cryptology are presented in Chapter 11.

The Appendix contains short historical data on quasigroup theory and information about the 20 Belousov problems [72] (formulations, information about solutions and names of solvers).

All theorems, corollaries, lemmas, remarks and formulas are identified by two numbers, the first of which specifies the chapter number. In compiling of the list of references, we tried to use mainly readily available sources. To make reading of this book more comfortable, we sometimes repeat the definitions and basic facts. We have put a few open problems in both explicit and implicit forms.

Acknowledgments. First of all, the author expresses profound gratitude to Professor A.D. Keedwell, whom he considers one of his scientific teachers. He thanks Professors Alberto Marini, Aleš Drápal and J.D. Phillips for their help. The author's work was partially supported by the grants FRVS 2733/2003, MSM 113200007, CRDF-MRDA grant and the grant 08.820.08.08 RF.

The work on this book was continued during his visit at Central European University (September, 2010–February, 2011). The author thanks the head of Mathematical Department of CEU, Prof. Gheorghe Morosanu, for his hospitality and help.

He also thanks his colleagues from the Algebra and Topology Department of the Institute of Mathematics and Computer Science of the Academy of Sciences of Republic Moldova, especially Prof. Galina Belyavskaya and Tatiana Verlan, for their help and fruitful discussions. He also thanks the staff of Shevchenko Transnistria State University.

He also thanks his family and relatives.

Victor A. Shcherbacov
Chişinău

This book was approved for publication by the Scientific Council of the Institute of Mathematics and Computer Science of the Academy of Sciences of Moldova.

2010 Mathematics Subject Classification.
Primary: 20N05 (Loops, quasigroups);
20N15 (n-ary systems).
Secondary:
20N02 (Sets with a single binary operation (groupoids));
05B15 (Orthogonal arrays, Latin squares, Room squares)
94B05 (Linear codes, general);
94A60 (Cryptography);
94A62 (Authentication and secret sharing).

Reviewer: Vladimir Arnautov, Doctor Habilitatus in Physics and Mathematics, Academician of the Academy of Sciences of Republic Moldova.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

List of Figures

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

List of Tables

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Part I

Foundations

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Chapter 1

Elements of quasigroup theory

1.1 Introduction

1.1.1 The role of definitions

In this section we adopt some remarks from the books [334, 422, 296].

In mathematics one should strive to avoid ambiguity. A very important ingredient of mathematical creativity is the ability to formulate useful definitions, ones that will lead to interesting results.

Every definition is understood to be an "if and only if" type of statement, even though it is customary to suppress the only if. Thus one may define: "A triangle is isosceles if it has two sides of equal length", really meaning that a triangle is isosceles if and only if it has two sides of equal length.

The basic importance of definitions to mathematics is also a structural weakness because not every concept used can be defined.

1.1.2 Sets

A set is well-defined collection of objects. We summarize briefly some of the things about sets we shall take for granted.

1. A set S is made up of elements, and if a is one of these elements, we shall denote this fact by $a \in S$. The order of elements in the set S is not taken into consideration, i.e., $S = \{a, b\} = \{b, a\}$.

2. There is exactly one set with no elements. It is the empty set and is denoted by $\varnothing$.

3. We may describe a set either by giving a characterizing property of the elements, such as "the set of all members of the United State Senate", or by listing the elements, for example, $\{1, 3, 4\}$ is a set.

4. A set is well defined, meaning that if S is a set and a is some object, then either a is definitely in S, denoted by $a \in S$, or a is definitely not in S, denoted by $a \notin S$. Thus one should never say "Consider the set S of some positive numbers", for it is not definite whether $2 \in S$ or $2 \notin S$.

1.1.3 Products and partitions

Definition 1.1. The Cartesian product of sets $S_1, S_2, \ldots, S_n$ is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i \in S_i$.

The Cartesian product is denoted by either $S_1 \times S_2 \times \cdots \times S_n$ or by

$$\prod_{i=1}^{n} S_i.$$

If $S_1 = S_2 = \cdots = S_n = S$, then we have $S \times S \times \cdots \times S = S^n = \{(a_1, a_2, \ldots, a_n) \,|\, a_i \in S\}$ (the n-th power of the set S).

A binary relation on a set Q is any subset of the set $Q \times Q$, a ternary relation is any subset of the set $Q \times Q \times Q$, and an n-ary relation is any subset of the set Q^n.

If φ and ψ are binary relations on Q, then their product is defined in the following way: $(a, b) \in \varphi \circ \psi$ if there is an element $c \in Q$ such that $(a, c) \in \varphi$ and $(c, b) \in \psi$. If φ is a binary relation on Q, then $\varphi^{-1} = \{(y, x) \mid (x, y) \in \varphi\}$. The operation of the product of binary relations is associative [211, 678, 813, 711].

Definition 1.2. A partition of a set is a decomposition of the set into cells such that every element of the set is in exactly one of the cells. Two cells (or sets) having no elements in common are disjoint.

Let $a \sim b$ denote that a is in the same cell as b for a given partition of a set containing both a and b. Clearly the following properties are always satisfied: $a \sim a$; if $a \sim b$, then $b \sim a$; if $a \sim b$ and $b \sim c$, then $a \sim c$, i.e., if a is in the same cell as b and b is in the same cell as c, then a is in the same cell as c.

Theorem 1.3. *Let S be a nonempty set and let $\sim$ be a relation between elements of S that satisfies the following properties:*

1. *(Reflexive) $a \sim a$ for all $a \in S$.*
2. *(Symmetric) If $a \sim b$, then $b \sim a$.*
3. *(Transitive) If $a \sim b$ and $b \sim c$, then $a \sim c$.*

Then $\sim$ yields a natural partition of S, where $\bar{a} = \{x \in S \,|\, x \sim a\}$ is the cell containing a for all $a \in S$. Conversely, each partition of S gives rise to a natural relation $\sim$ satisfying the reflexive, symmetric, and transitive properties if $a \sim b$ is defined to mean that $a \in \bar{b}$.

Definition 1.4. A relation $\sim$ on a set S satisfying the reflexive, symmetric, and transitive properties is an equivalence relation on S. Each cell $\bar{a}$ in the natural partition given by an equivalence relation is an equivalence class.

1.1.4 Maps

One of the truly universal concepts that arises in almost every part of mathematics is that of a function or a mapping from one set to another. One can safely say that there is no part of mathematics where the notion arises or plays a central role.

The definition of a function from one set to another can be given in a formal way in terms of a subset of the Cartesian product of these sets (i.e., in terms of binary relations). Instead, here, we shall give an informal and admittedly nonrigorous definition of a mapping (function) from one set to another.

Definition 1.5. Let S, T be sets; a function or mapping f from S to T is a rule that assigns a unique element $t \in T$ to each element $s \in S$.

Definition 1.6. The mapping $f : S \to T$ is onto or surjective if every $t \in T$ is the image of some $s \in S$ under f; that is, if and only if, given $t \in T$, there exists at least one $s \in S$ such that $t = f(s)$.

Definition 1.7. A mapping $f : S \to T$ is said to be one-to-one (written 1-1) or injective if for $s_1 \neq s_2$ in S, $f(s_1) \neq f(s_2)$ in T. Equivalently, f is 1-1 if $f(s_1) = f(s_2)$ implies $s_1 = s_2$.

Definition 1.8. A mapping $f : S \to T$ is said to be a 1-1 correspondence or bijection if f is both 1-1 and onto (i.e., f is both injective and surjective).

Remark 1.9. Mainly we shall use the following order of multiplication (of composition) of maps: $(\alpha\beta)(x) = \alpha(\beta(x))$, where α, β are maps. Cases when other orders of multiplication of maps are used, are also specified.

Lemma 1.10. *Let $f : A \to B$ be a map of non-empty sets. Then*

(i) the map f is injective if and only if there exists a map $g : B \to A$ such that $gf = 1_A$;
(ii) the map f is surjective if and only if there exists a map $g : B \to A$ such that $fg = 1_B$;
(iii) the map f is bijective if and only if there exists a map $g : B \to A$ such that $gf = 1_A$ and $fg = 1_B$ [312, 1. Proposition].

Here 1_A denotes the identity map of the set A. It is clear that any identity map is bijective.

Definition 1.11. Let $f : A \to B$ be a map. A left inverse map to the map f is a map $g : B \to A$ such that $gf = 1_A$. A right inverse map to the map f is a map $h : B \to A$ such that $fh = 1_B$. A left and right inverse map is called an inverse map.

It is known that if a map has an inverse, it is unique. In general this is not true for left or right inverse maps. See Example 1.13.

Lemma 1.12.
1. *Let $\varphi : A \to B$ be a map of non-empty sets. Then φ is injective if and only if φ has a left inverse map ${}^{-1}\varphi$.*
2. *Let $\psi : A \to B$ be a map of non-empty sets. Then ψ is surjective if and only if ψ has a right inverse map ψ^{-1};*
3. *Let $f : A \to B$ be a map of non-empty sets. Then f is bijective if and only if f has an inverse map f^{-1} [312, 2. Proposition].*

Example 1.13. Let $A = \{1, 2\}$, $B = \{a, b, c\}$, $\varphi = \{(1, a), (2, b)\}$. It is clear that the mapping φ is a 1-1 mapping of A into B. The left inverse mappings to the injection φ are, for example, the following surjections ($B \to A$): ${}^{-1}\varphi_1 = \{(a, 1), (b, 2), (c, 1)\}$; ${}^{-1}\varphi_2 = \{(a, 1), (b, 2), (c, 2)\}$.

Indeed, ${}^{-1}\varphi_1\varphi(1) = {}^{-1}\varphi_1(\varphi(1)) = {}^{-1}\varphi_1(a) = 1$, ${}^{-1}\varphi_1\varphi(2) = {}^{-1}\varphi_1(b) = 2$; ${}^{-1}\varphi_2\varphi(1) = {}^{-1}\varphi_1(a) = 1$, ${}^{-1}\varphi_2\varphi(2) = {}^{-1}\varphi_2(b) = 2$. Therefore ${}^{-1}\varphi_1\varphi = {}^{-1}\varphi_2\varphi = 1_A$.

Let $A = \{5, 7, 9\}$, $B = \{t, q\}$, $\psi = \{(5, t), (7, q), (9, t)\}$. The mapping ψ is a surjective mapping of A onto B. It is easy to check that the mapping $\psi^{-1} = \{(t, 5), (q, 7)\}$ is an injective mapping. Indeed, $\psi(\psi^{-1}(t)) = \psi(5) = t$, $\psi(\psi^{-1}(q)) = \psi(7) = q$. Therefore $\psi\psi^{-1} = 1_B$.

Lemma 1.14. *Let μ and ν be some maps of a non-empty set Q. If the product $\mu\nu$ of the maps is a bijective map of the set Q, then the map ν is injective and the map μ is surjective.*

Proof. If $\mu\nu = \alpha$, where α is a bijection of the set Q, then $(\alpha^{-1}\mu)\nu = 1_Q$. Then by Lemma 1.10, the map $\alpha^{-1}\mu$ is surjective and the map ν is injective. Therefore, the map μ is surjective, since the map α^{-1} is a bijective map. □

Recall, any mapping of a non-empty set Q into itself can be considered as a binary relation defined on the set Q. In this case, multiplication of mappings is a special case of the operation of multiplication of binary relations.

Lemma 1.15. *If Q is a finite set, then:*

1. any injective ($x \neq y \Rightarrow \varphi x \neq \varphi y$) map φ on this set ($\varphi(Q) \subseteq Q$) is a bijective map;

2. any surjective map ψ of this set into itself ($\psi(Q) = Q$) is a bijective map [538, Theorem 3, p. 45].

Proof. Case 1. First of all we re-write implication ($x \neq y \Rightarrow \varphi x \neq \varphi y$) in the following equivalent form:

$$\varphi x = \varphi y \Rightarrow x = y. \tag{1.1}$$

We should prove that the map φ is surjective. In other words we should prove that for any $x \in Q$ there exists an element $x' \in Q$ such that $\varphi(x') = x$.

Let $\varphi^k(x) = \varphi(\varphi^{k-1})(x)$, $k = 0, 1, \ldots$, be a sequence of elements of the set Q. Since the set Q is finite, then there exist integers m, n, $n < m$, such that $\varphi^m(x) = \varphi^n(x)$. Applying n times the relation (1.1) to the last equality, we obtain the following equality $\varphi^{m-n}(x) = x$, $\varphi(\varphi^{m-n-1}(x)) = x$. Denote the element $\varphi^{m-n-1}(x)$ by the symbol x' and finally obtain the following equality $\varphi(x') = x$.

Case 2. If the map ψ is surjective, then by Lemma 1.12 there exists a right inverse map ψ^{-1} such that $\psi\psi^{-1} = 1_Q$, i.e., $\psi\psi^{-1} = \varepsilon$, where ε denotes identity permutation of the set Q. The fact that the map ψ^{-1} is injective follows from Lemma 1.14. By Case 1 of this Lemma the mapping ψ^{-1} is bijective. Therefore the mapping ψ is bijective, too. □

We shall consider the set $A(Q)$ of all bijections of the set Q onto itself. The set $A(Q)$ forms a group relative to "usual" multiplication of these mappings. This group is called the symmetric group of degree n and it will be denoted by S_n, if the set Q has finite number n of elements. Elements of the group S_n are called permutations of the set Q. In the investigation of finite groups and quasigroups, the group S_n and its subgroups play a central role.

An n-ary operation defined on a non-empty set Q is a map $A : Q^n \longrightarrow Q$ such that $D(A) = Q^n$, i.e., this map is defined for any n-tuple. The number n is called the "arity" of operation A. If the element c corresponds to the n-tuple $(b_1, b_2, \ldots, b_n)$, then we shall write this fact in the following form $A(b_1, b_2, \ldots, b_n) = c$, or in the form $A : (b_1, b_2, \ldots, b_n) \longmapsto c$.

If $n = 2$, then the operation A is called a binary operation, if $n = 1$, then the operation A is called a unary operation. If $n = 0$, then the operation A is called a *nullary operation.* A nullary operation is a fixation of an element from the basic set Q [184].

Exercise 1.16. On a finite set of order n there exist $n^{(n^k)}$ k-ary operations. For example, on the set of order ten, there exist 10^{1000} ternary operations.

1.2 Objects

1.2.1 Groupoids and quasigroups

A binary groupoid (G, A) is a non-empty set G together with a binary operation A.

Many different symbols can be used to denote binary operations, for example, $\circ, \star, \cdot$. Thus, we can write $x \circ y$ instead of $A(x, y)$, and $x \star y$ instead of $B(x, y)$.

An n-ary groupoid (G, A) is a non-empty set G together with an n-ary operation A.

There exists a bijection (1-1 correspondence) between the set of all binary (n-ary, for fixed n) operations defined on a set Q and the set of all groupoids, defined on the set Q. Indeed, $A \longleftrightarrow (Q, A)$.

A sequence $x_m, x_{m+1}, \ldots, x_n$, where m, n are natural numbers and $m \leqslant n$, will be denoted by x_m^n, and a sequence $x, \ldots, x$ (k times) will be denoted by $\overline{x}^k$. The expression $\overline{1,n}$ designates the set $\{1, 2, \ldots, n\}$ of natural numbers [77].

We shall say that the operations A and B, which are defined on a set Q, coincide, if $A(a_1^n) = B(a_1^n)$ for all $a_i \in Q$, $i \in \overline{1,n}$.

The order of an n-ary groupoid (Q, A) is cardinality $|Q|$ (sometimes denotation $\bar{\bar{Q}}$ is used) of the carrier set Q. An n-ary groupoid $(Q, \cdot)$ is said to be finite if its order is finite.

It is possible to represent a finite n-ary groupoid (Q, A) (theoretically of any, but practically, only not a very big size) as a set of $(n+1)$-tuples $(a_1, a_2, \ldots, a_n, A(a_1^n))$.

In the binary case it is possible to define a groupoid as a set of triplets. For example, the set

$$(Q, \cdot) = \{(a,a,a), (a,b,a), (a,c,b), (b,a,b), (b,b,c), (b,c,a), (c,a,c), (c,b,a), (c,c,b)\}$$

defines a groupoid with the following multiplication table:

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

where, for example, the triple (a, c, b) defines the element $b = a \cdot c$, which appears at the intersection of the row headed by a and the column headed by c. This table is called the *Cayley table* of the groupoid $(Q, \cdot)$, where $Q = \{a, b, c\}$.

Note 1.17. Usually it is supposed that elements of carried set Q are arranged. So the groupoid $(Q, \circ)$, which is defined with the help of the following Cayley table,

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

is equal (as a set of triplets) to the groupoid $(Q, \cdot)$, but $(Q, \cdot) \neq (Q, *)$, where the groupoid $(Q, *)$ has the following Cayley table:

$*$	b	c	a
b	a	a	b
c	b	c	a
a	c	a	b

A groupoid $(Q, \circ)$ is called a *right quasigroup* if, for all $a, b \in Q$, there exists a unique solution $x \in Q$ to the equation $x \circ a = b$.

Example 1.18. Examples of right quasigroups. All columns are permutations of the set {0, 1, 2}.

$\circ$	0	1	2
0	0	0	2
1	1	1	1
2	2	2	0

$*$	0	1	2
0	0	1	2
1	1	0	1
2	2	2	0

A groupoid $(Q, \circ)$ is called a *left quasigroup* if, for all $a, b \in Q$, there exists a unique solution $y \in Q$ to the equation $a \circ y = b$.

Example 1.19. Examples of left quasigroups. All rows are permutations of the set {0, 1, 2}.

$\circ$	0	1	2
0	1	0	2
1	0	1	2
2	2	1	0

$*$	0	1	2
0	0	1	2
1	2	0	1
2	0	1	2

A left and right quasigroup is a *quasigroup*.

Example 1.20. Example of quasigroup.

$*$	0	1	2
0	1	0	2
1	0	2	1
2	2	1	0

We give a main definition of a quasigroup:

Definition 1.21. A binary groupoid $(Q, \circ)$ is called a quasigroup if for any ordered pair $(a, b) \in Q^2$ there exist unique solutions $x, y \in Q$ to the equations $x \circ a = b$ and $a \circ y = b$ [72].

Often this definition is called *existential*. Some equational (using identities) quasigroup definitions are given below (Definition 1.54).

From Definition 1.21 it follows, that any two elements from the triple $(a, b, a \circ b)$ specify the third element in a unique way. Indeed, for any elements a, b there exists a unique element $a \circ b$. This follows from the definition of operation $\circ$.

Elements $a, a \circ b$ determine the third element in a unique way since there exists a unique solution to the equation $a \circ y = b$.

Elements $b, a \circ b$ determine the third element in unique way since there exists a unique solution to the equation $x \circ a = b$.

Therefore, it is convenient to define an n-ary quasigroup in the following manner.

Definition 1.22. An n-ary groupoid (Q, A) with n-ary operation A such that in the equality $A(x_1, x_2, \ldots, x_n) = x_{n+1}$ the fact of knowing any n elements of the set $\{x_1, x_2, \ldots, x_n, x_{n+1}\}$ uniquely specifies the remaining one element is called an n-ary quasigroup [77].

If we put $n = 2$, then we obtain one more definition of a binary quasigroup.

Example 1.23. Let $Q = \{0, 1, 2, 3, 4\}$. Using the operations of addition $(+)$ and multiplication $(\cdot)$ modulo 5, we define a 4-ary quasigroup (Q, f) in the following way: $f(x_1^4) = 2 \cdot x_1 + x_2 + 4 \cdot x_3 + 3 \cdot x_4$.

Exercise 1.24. Construct a Cayley table of the quasigroup defined in Example 1.23 or list all 5-tuples that define this 4-ary quasigroup.

Definition 1.25. Let $(G, \cdot)$ be a groupoid and let a be a fixed element in G. Translation maps L_a (left) and R_a (right) are defined by $L_a x = a \cdot x$, $R_a x = x \cdot a$ for all $x \in G$.

Translations play a prominent role in quasigroup theory.

Example 1.26. Example of a quasigroup and its left and right translations.

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

For this quasigroup we have the following left and right translations:

$$L_a^\circ = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}; \quad L_b^\circ = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}; \quad L_c^\circ = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix};$$
$$R_a^\circ = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}; \quad R_b^\circ = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}; \quad R_c^\circ = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}.$$

We can express these permutations in the cycle form: $L_a^\circ = (b\,c)$; $L_b^\circ = (a\,b)$; $L_c^\circ = (a\,c)$; $R_a^\circ = \varepsilon$; $R_b^\circ = (a\,c\,b)$; $R_c^\circ = (a\,b\,c)$.

Remark 1.27. Usually the symbol of binary operation in the record of translation is omitted, i.e., it is written L_a instead of L_a°.

Notice if, for example,

$$L_a = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \text{then } L_a^{-1} = \begin{pmatrix} c & a & b \\ a & b & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix},$$

$L_a L_a^{-1} = L_a^{-1} L_a = \varepsilon$. We shall denote identity permutation by ε.

It is easy to see that in the Cayley table of a quasigroup $(Q, \cdot)$ each row and each column is a permutation of the set Q. So we may give the following definition of a quasigroup.

Definition 1.28. A groupoid $(Q, \cdot)$ is called a quasigroup if the maps $L_a : G \longrightarrow Q$, $R_a : Q \longrightarrow Q$ are bijections for all $a \in Q$ [685].

Lemma 1.29. *1. The statements "the equation $x \circ a = b$ has a unique solution for all $a, b \in Q$" and "R_a is bijection of the set Q for any $a \in Q$" are equivalent.*

2. Similarly, the conditions "the equation $a \circ y = b$ has a unique solution for all $a, b \in Q$" and "L_a is bijection of the set Q for any $a \in Q$" are equivalent.

Proof. Case 1."$\Longrightarrow$." Fix the element a and write equality $x \circ a = b$ in the following form: $R_a^\circ x = b$. Variable x takes all values in the set Q. Therefore, we have a mapping of the set Q into itself.

From the fact that equation $x \circ a = b$ has a unique solution, it follows that the mapping R_a° is injective ($(x \neq y) \to (R_a^\circ x \neq R_a^\circ y)$).

Since for any element $b \in Q$, there exists an element $x \in Q$ such that $R_a^\circ x = b$, we have that this mapping is surjective, and therefore, is a bijection of the set Q.

"$\Longleftarrow$." If translation R_a° is a bijection, then $x = (R_a^\circ)^{-1} b$.

Case 2 is proved similarly. □

Definition 1.30. An unbordered Cayley table of a finite quasigroup is called a Latin square.

Quasigroup triples have interesting combinatorial properties [571, 721].

1.2.2 Parastrophy: Quasigroup as an algebra

1.2.2.1 Parastrophy

Definition 1.31. From Definition 1.22 it follows that with a given binary quasigroup (Q, A) it is possible to associate $(3! - 1)$ others, so-called parastrophes of quasigroup (Q, A):

1. $A(x_1, x_2) = x_3 \Longleftrightarrow$
2. $A^{(12)}(x_2, x_1) = x_3 \Longleftrightarrow$
3. $A^{(13)}(x_3, x_2) = x_1 \Longleftrightarrow$
4. $A^{(23)}(x_1, x_3) = x_2 \Longleftrightarrow$
5. $A^{(123)}(x_2, x_3) = x_1 \Longleftrightarrow$
6. $A^{(132)}(x_3, x_1) = x_2$

[845, p. 230], [72, p. 18].

Notice, Cases 5 and 6 are "(12)-parastrophes" of Cases 3 and 4, respectively.
Therefore

$$A^{\sigma}(x_i, x_j) = x_k \Leftrightarrow A(x_{\sigma^{-1}i}, x_{\sigma^{-1}j}) = x_{\sigma^{-1}k}, \tag{1.2}$$

where $\sigma \in S_3$, $i, j, k \in \{1, 2, 3\}$, the numbers i, j, k are different in pairs, and $x_i, x_j, x_k \in Q$.

In the language of triplets, we have $A^{\sigma}(x_1, x_2, x_3) = A(x_{\sigma^{-1}1}, x_{\sigma^{-1}2}, x_{\sigma^{-1}3})$, i.e., in order to have the set of triplets of quasigroup A^{σ} we permute elements of any triplet by the "σ^{-1}-rule" in the set of triplets of operation A.

Then $A^{\sigma}(x_{\sigma 1}, x_{\sigma 2}) = x_{\sigma 3} \Leftrightarrow A(x_{\sigma^{-1}\sigma 1}, x_{\sigma^{-1}\sigma 2}) = x_{\sigma^{-1}\sigma 3} \Leftrightarrow A(x_1, x_2) = x_3$. For example, $A^{(132)}(x_1, x_2) = x_3 \Leftrightarrow A(x_{(123)1}, x_{(123)2}) = x_{(123)3}$. That is, $A^{(132)}(x_1, x_2) = x_3 \Leftrightarrow A(x_2, x_3) = x_1$.

Usually the operation $A^{(12)}$ is denoted as "$*$", the operation $A^{(13)}$ is denoted as "$/$", and the operation $A^{(23)}$ is denoted as "$\backslash$". Thus, if $x \cdot y = z$, then $y * x = z$, $x \backslash z = y$ and $z / y = x$. Sometimes [72, 80] it denoted ${}^{(13)}A$ instead of $A^{(13)}$, and so on. In [786] operation $A^{(123)}$ is denoted by $//$, operation $A^{(133)}$ is denoted by $\backslash\backslash$. Other denotations of these operations are used in [310].

The following convenient designation of quasigroup parastrophes (Belousov's designation [700]) is also used [80, 85]:

$$\begin{aligned}
&A^{(12)} = A^{*} = {}^{s}A,\\
&A^{(13)} = {}^{-1}A = {}^{l}A,\\
&A^{(23)} = A^{-1} = {}^{r}A,\\
&A^{(123)} = {}^{-1}(A^{-1}) = {}^{l}({}^{r}A) = {}^{\alpha}A = {}^{s}({}^{l}A),\\
&A^{(132)} = ({}^{-1}A)^{-1} = {}^{r}({}^{l}A) = {}^{\beta}A = {}^{s}({}^{r}A).
\end{aligned}$$

Note 1.32. The concept of parastrophy, especially (12)-parastrophy, can be extended to groupoids.

1.2.2.2 Middle translations

We defined left and right translations of a groupoid and, therefore, of a quasigroup. But for quasigroups it is possible to define a third kind of translation, namely, middle translations. If P_a is a middle translation of a quasigroup $(Q, \cdot)$, then $x \cdot P_a x = a$ for all $x \in Q$ [75].

Suppose that quasigroups (Q, A^{σ}) and (Q, A^{δ}) are parastrophes of a quasigroup (Q, A). Any translation of a quasigroup (Q, A^{σ}) can be expressed as a translation of a quasigroup (Q, A^{δ}) or as its inverse translation. For example, $R^{*}_a x = x * a = a \cdot x = L_a x$. Then $R^{*}_a = L_a$, $R^{*} = L$, $R^{(12)} = L$. Or

$$P^{\backslash}_a x = y \Leftrightarrow x \backslash y = a \Leftrightarrow x \cdot a = y \Leftrightarrow R_a x = y.$$

Then $P^{\backslash}_a = R_a$, $P^{\backslash} = R$, $P^{(23)} = R$.

The following table shows, for each kind of translation, the equivalent one in each of the (six) parastrophes of a quasigroup $(Q, \cdot)$. In fact, Table 1.1 is a rewritten form of results on three kinds of translations from [75]. See also [298, 786].

From Table 1.1 it follows, for example, that $R^{(132)} = L^{-1} = L^{(23)} = P^{(13)} = (R^{-1})^{(12)} = (P^{-1})^{(123)}$.

Using Table 1.1 it is possible to construct parastrophes of a quasigroup $(Q, \cdot)$. In order to construct (12)-parastrophe of a quasigroup $(Q, \cdot)$ we can write any row of the Cayley table of quasigroup $(Q, \cdot)$ as a corresponding column.

Table 1.1: Translations of quasigroup parastrophes.

	ε	(12)	(13)	(23)	(123)	(132)
R	R	L	R^{-1}	P	P^{-1}	L^{-1}
L	L	R	P^{-1}	L^{-1}	R^{-1}	P
P	P	P^{-1}	L^{-1}	R	L	R^{-1}
R^{-1}	R^{-1}	L^{-1}	R	P^{-1}	P	L
L^{-1}	L^{-1}	R^{-1}	P	L	R	P^{-1}
P^{-1}	P^{-1}	P	L	R^{-1}	L^{-1}	R

Example 1.33.

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

$\Longrightarrow$

$^{(12)}\circ$	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

In order to construct the (23)-parastrophe of a quasigroup $(Q, \cdot)$ we can replace any row of the Cayley table of quasigroup $(Q, \cdot)$ with the corresponding inverse row.

Example 1.34.

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

$\Longrightarrow$

$^{(23)}\circ$	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

In order to construct the (13)-parastrophe of a quasigroup $(Q, \cdot)$ we can replace any column of the Cayley table of quasigroup $(Q, \cdot)$ with the corresponding inverse column.

In order to construct the (123)-parastrophe of a quasigroup $(Q, \cdot)$ we can replace any row of the Cayley table of quasigroup $(Q, \cdot)$ with the corresponding inverse column.

In order to construct the (132)-parastrophe of a quasigroup $(Q, \cdot)$ we can replace any column of the Cayley table of quasigroup $(Q, \cdot)$ with the corresponding inverse row.

Exercise 1.35. Find all parastrophes of the quasigroups given in Examples 1.33 and 1.34.

1.2.2.3 Some groupoids

The class of binary quasigroups is close to the classes of binary left (right) cancellation (division) groupoids. See, for example, Lemma 1.47 and Theorem 1.58. It is known that a homomorphic image of an existential quasigroup may be only division groupoid and not a quasigroup [43].

Definition 1.36. A groupoid $(G, \cdot)$ is called a left cancellation groupoid, if the following implication is fulfilled: $a \cdot x = a \cdot y \Rightarrow x = y$ for all $a, x, y \in G$, i.e., the translation L_a is an injective map for any $a \in G$.

Definition 1.37. A groupoid $(G, \cdot)$ is called a right cancellation groupoid, if the following implication is fulfilled: $x \cdot a = y \cdot a \Rightarrow x = y$ for all $a, x, y \in G$, i.e., the translation R_a is an injective map for any $a \in G$ [462].

Definition 1.38. A groupoid $(G, \cdot)$ is called a cancellation groupoid if it is both a left and right cancellation groupoid.

Remark 1.39. In this text the terms *"cancellation groupoid"* and *"cancellative groupoid"* are synonymous.

Example 1.40. Let $x \circ y = 2x + 4y$ for all $x, y \in \mathbb{Z}$, where $(\mathbb{Z}, +, \cdot)$ is the ring of integers. The reader can check that $(\mathbb{Z}, \circ)$ is a cancellation groupoid.

Example 1.41. Let $x \circ y = 2x + 3y$ for all $x, y \in \mathbb{Z}$, where $(\mathbb{Z}, +, \cdot)$ is the ring of integers. The reader can check that $(\mathbb{Z}, \circ)$ is a cancellation groupoid.

Definition 1.42. A groupoid $(G, \cdot)$ is said to be a left (right, resp.) division groupoid if L_a (R_a, resp.) is surjective for every $a \in G$; it is said to be a division groupoid if it is both a left and right division groupoid [462].

We can give an equivalent definition of a division groupoid.

Definition 1.43. A groupoid $(G, \cdot)$ is called a division groupoid, if the equations $a \cdot x = b$ and $y \cdot a = b$ have solutions (not necessarily unique solutions) for any ordered pair of elements $a, b \in Q$.

Example 1.44. Let $x \circ y = 2 \cdot x + [y/3]$ for all $x, y \in \mathbb{Z}$, where $(\mathbb{Z}, +, \cdot)$ is the ring of integers, $[y/3] = n$, if $y = 3n$, or $y = 3n + 1$, else $y = 3n + 2$, where $n \in \mathbb{Z}$. It is possible to check that $(\mathbb{Z}, \circ)$ is a right cancellation and left division groupoid.

Example 1.45. Let $x \circ y = 1 \cdot x + [y/3]$ for all $x, y \in \mathbb{Z}$, where $(\mathbb{Z}, +, \cdot)$ is the ring of integers. It is possible to check that $(\mathbb{Z}, \circ)$ is a right quasigroup and a left division groupoid.

Example 1.46. Let $x \circ y = x^2 + y^3$ for all $x, y \in \mathbb{C}$, where $(\mathbb{C}, +, \cdot)$ is the field of complex numbers. The reader can check that $(\mathbb{C}, \circ)$ is a division groupoid.

Lemma 1.47. *A division cancellation groupoid $(Q, \cdot)$ is a quasigroup.*

Proof. The proof follows from definitions and Lemma 1.29. □

Theorem 1.48. *A finite cancellation groupoid $(G, \cdot)$ is a quasigroup; a finite division groupoid $(G, \cdot)$ is a quasigroup.*

Proof. By Lemma 1.15, if G is a finite set, then any injective ($x \neq y \Rightarrow \varphi x \neq \varphi y$) map φ on this set ($\varphi(G) \subseteq G$) is a bijective map and any surjective map ψ of this set into itself ($\psi(G) = G$) is a bijective map, too.

Since any left and right translation of a cancellation groupoid $(G, \cdot)$ is an injective map, then in the case when the set G is finite, we have that $(G, \cdot)$ is a quasigroup.

Similarly, since any left and right translation of a division groupoid $(G, \cdot)$ is a surjective map, then in the case when the set G is finite, we have that any division groupoid is a quasigroup. □

Theorem 1.49. *A finite left (right) cancellation groupoid is a left (right) quasigroup and a finite left (right) division groupoid is a left (right) quasigroup.*

Proof. The proof is similar to the proof of Theorem 1.48 and we omit it. □

1.2.2.4 Substitutions in groupoid identities

Here we give non-formal, but, we hope, relatively clear information from universal algebra about substitutions in identities. See [184] for more details. Recall that any algebraic operation is a function defined on a non-empty set Q, therefore any algebraic operation is a mapping.

Suppose that $(Q, \circ)$ is a binary groupoid. Define the set $Q \circ Q$ in the following way: $Q \circ Q = \{x \circ y \,|\, \text{for all } x, y \in Q\}$.

Definition 1.50. Let $(Q, \circ)$ be a binary groupoid. The following property

$$Q \circ Q = Q \tag{1.3}$$

of the operation $\circ$ is called *surjective*.

From Definition 1.42 it follows that the operation of left (right) division groupoid $(Q, \cdot)$ satisfies the property (1.3).

Example 1.51. The left cancellation groupoid from Example 1.40 satisfies the property $\mathbb{Z} \circ \mathbb{Z} \subsetneq \mathbb{Z}$ and it is not surjective. The cancellation groupoid from Example 1.41 satisfies the surjective property (1.3) since $g.c.d.(2; 3) = 1$ and from standard information on linear Diophantine equations [919], it follows that the equation $2x + 3y = t$ has solution for any $t \in \mathbb{Z}$.

An algebra (Q, F) will be called surjective, if any n-ary ($n \geqslant 1$) operation $f \in F$ has the surjective property, i.e., $f(Q, Q, \ldots, Q) = Q$.

In surjective binary groupoid $(Q, \cdot)$ any element $c \in Q$ can be represented as a product of two elements, say, a and b, and any variable x can be presented as a product of variables, say, y and z. Surjective medial groupoids are defined and studied in [462].

Notice, "inverse procedure" is admissible in any identity of any algebra. We have in mind that the replacement (the substitution) of, say, variable x, by suitable term T [917] in an identity of an algebra in all occurrences of an individual variable, is possible in the majority of "usual"cases.

It is clear that operation $\circ$ of quasigroup $(Q, \circ)$ has a surjective property. Similarly, any operation of quasigroup $(Q, \cdot, /, \backslash)$ (see below) has a surjective property.

1.2.2.5 Equational definitions

We recall, an algebra (or algebraic structure) is a set A together with a collection of operations defined on A [184, 212].

Bates and Kiokemeister [43] discovered that a class of quasigroups which is defined using equations (Definition 1.21) is not closed relative to homomorphic images. In the general case the quasigroup homomorphic image is only a division groupoid (see Lemma 1.280).

The problem of finding definitions of a quasigroup class such that this class is closed relative to homomorphic images was solved by Garret Birkhoff. He has defined a quasigroup using three binary operations and six identities [149, 151]. Quasigroups defined in this way often are called *equational quasigroups*. From standard universal algebraic facts (many of which also were discovered by Garret Birkhoff), it follows that class of equational quasigroups is a variety and it is closed relative to homomorphic images [151, 184].

Garrett Birkhoff [149, 151] has defined an equational quasigroup as an algebra with three binary operations $(Q, \cdot, /, \backslash)$ that satisfies the following six identities:

$$x \cdot (x\backslash y) = y, \tag{1.4}$$

$$(y/x) \cdot x = y, \tag{1.5}$$

$$x\backslash(x \cdot y) = y, \tag{1.6}$$

$$(y \cdot x)/x = y, \tag{1.7}$$

$$x/(y\backslash x) = y, \tag{1.8}$$

$$(x/y)\backslash x = y. \tag{1.9}$$

Remark 1.52. In [819] the identities (1.4)–(1.7) are called respectively (SL), (SR), (IL), (IR), since these identities guarantee that the left (L) and right (R) translations of an algebra $(Q, \cdot, /, \backslash)$ relative to the operation "$\cdot$" are surjective (S) or injective (I) mappings of the set Q.

Following this logic we can denote identity (1.8) by (SP) and identity (1.9) by (IP) since these identities guarantee that middle translations (P) are respectively surjective and injective mappings relative to the operation "$\cdot$" [786]. Indeed using Table 1.1 we see that $L_x^{/} = P_x^{-1}$.

The following lemma is well known:

Lemma 1.53. *In algebra $(Q, \cdot, \backslash, /)$ with the identities (1.4)–(1.7), the identities (1.8) and (1.9) are true [819, 779, 786].*

Proof. From the identity (1.7) $(y \to x, x \to x\backslash y)$ we have

$$(x \cdot (x\backslash y))/(x\backslash y) = x. \tag{1.10}$$

But by the identity (1.4), $x \cdot (x\backslash y) = y$. Thus from the identity (1.10) we obtain $y/(x\backslash y) = x$, i.e., we obtain (up to renaming of variables) the identity (1.8).

We can re-write identity (1.6) in the following form:

$$(x/y)\backslash((x/y) \cdot y) = y. \tag{1.11}$$

By the identity (1.5) $(x/y) \cdot y = x$. Thus from equality (1.11) we have $(x/y)\backslash x = y$, i.e., we obtain the identity (1.9). □

Therefore the following Evans equational definition of a quasigroup is usually used [307].

Definition 1.54. [150, 151, 307]. A groupoid $(Q, \cdot)$ is called a quasigroup if, on the set Q, there exist operations "$\backslash$" and "$/$" such that in the algebra $(Q, \cdot, \backslash, /)$ identities (1.4)–(1.7) are fulfilled.

Algebra $(Q, \cdot, \backslash, /)$ with identities (1.4)–(1.7) is called *e-quasigroup* (probably from the words equational quasigroup) [151, 80]. Below we shall also name an algebra $(Q, \cdot, \backslash, /)$ with identities (1.4)–(1.7) as a quasigroup $(Q, \cdot, \backslash, /)$.

A.I. Maltsev [590, 591] has called this algebra a *primitive quasigroup*. Definitions of quasigroup with the help of quasi-identities can be found in [590, 786].

Note 1.55. The identities (1.4) and (1.5) guarantee the existence of solutions of equations $a \cdot y = b$ and $x \cdot a = b$, while the identities (1.6) and (1.7) guarantee the uniqueness of solutions in these equations. See below.

Theorem 1.56. *Definitions 1.21 and 1.54 are equivalent.*

Proof. (Definition 1.21 ⇒ Definition 1.54). Let $(Q, \cdot)$ be a quasigroup. Since for every pair of elements $a, b \in Q$ there exists a unique element x such that $a \cdot x = b$, we can associate with this equation an operation on the set Q, namely $a \cdot x = b \leftrightarrow a\backslash b = x$. If we substitute

the last expression in the equality $a \cdot x = b$, then we obtain $a \cdot (a\backslash b) = b$ for all $a, b \in Q$. We obtained identity (1.4) from Definition 1.54.

Similarly, $y \cdot a = b \leftrightarrow b/a = y$, $(b/a) \cdot a = b$ for all $a, b \in Q$ and we obtain identity (1.5).

Identities (1.6) and (1.7) follow from the definitions of the operations $\backslash$ and $/$. Indeed, $x\backslash(x \cdot y) = y \leftrightarrow x \cdot y = x \cdot y$, $(y \cdot x)/x = y \leftrightarrow y \cdot x = y \cdot x$.

(Definition 1.54 $\Rightarrow$ Definition 1.21). Let $(Q, \cdot, /, \backslash)$ be an algebra with three binary operations such that in the algebra identities (1.4), (1.5), (1.6) and (1.7) hold.

We need to prove the existence and the uniqueness of solutions to the equations $a \cdot x = b$ and $y \cdot a = b$.

(Existence). Let $x = a\backslash b$. Then $a \cdot x = a(a\backslash b) \overset{(1.4)}{=} b$. Similarly, if $y = b/a$, then $y \cdot a = (b/a) \cdot a \overset{(1.5)}{=} b$.

(Uniqueness). Suppose that there exist two solutions x_1 and x_2 of equation $a \cdot x = b$, i.e., $a \cdot x_1 = b$ and $a \cdot x_2 = b$. Then $x_1 = a\backslash b$ and further we have

$$x_1 = a\backslash b = a\backslash(ax_2) \overset{(1.6)}{=} x_2.$$

Similarly, if $y_1 \cdot a = b$ and $y_2 \cdot a = b$, then $y_1 = b/a$,

$$y_1 = b/a = (y_2 \cdot a)/a \overset{(1.7)}{=} y_2.$$

□

It is possible to rewrite identities (1.4)–(1.7) in the language of translations in the following form:

$$L_x^{(\cdot)} L_x^{(\backslash)} y = y, \tag{1.12}$$

$$R_x^{(\cdot)} R_x^{(/)} y = y, \tag{1.13}$$

$$L_x^{(\backslash)} L_x^{(\cdot)} y = y. \tag{1.14}$$

$$R_x^{(/)} R_x^{(\cdot)} y = y. \tag{1.15}$$

Remark 1.57. Using Table 1.1 we can re-write identities (1.12)–(1.15) as follows:

$$L_x L_x^{-1} y = y, \tag{1.16}$$

$$R_x R_x^{-1} y = y, \tag{1.17}$$

$$L_x^{-1} L_x y = y, \tag{1.18}$$

$$R_x^{-1} R_x y = y. \tag{1.19}$$

Taking into consideration Lemma 1.14 and equalities (1.12)–(1.15) we can say that identities (1.4)–(1.7) guarantee that in a quasigroup $(Q, \cdot)$ any left and right translation is a bijection of the set Q.

In the language of translations, identities (1.9) and (1.8) take the following forms, respectively, $R_x^{(\backslash)} L_x^{(/)} y = y, L_x^{(/)} R_x^{(\backslash)} y = y$. From Table 1.1 it follows that $L_x^{(/)} = P_x^{-1}$, $R_x^{(\backslash)} = P_x$.

Algebras with identities (1.4)–(1.9) are discussed in [786, 798]. The following "equivalence" theorem is proved.

Theorem 1.58. *1. A groupoid $(Q, \cdot)$ is a left division groupoid if and only if in algebra $(Q, \cdot, \backslash)$ the identity (1.4) holds true.*

2. A groupoid $(Q, \cdot)$ is a right division groupoid if and only if in algebra $(Q, \cdot, /)$ the identity (1.5) holds true.

3. *A groupoid $(Q, \cdot)$ is a left cancellation groupoid if and only if in algebra $(Q, \cdot, \backslash)$ the identity (1.6) holds true.*

4. *A groupoid $(Q, \cdot)$ is a right cancellation groupoid if and only if in algebra $(Q, \cdot, /)$ the identity (1.7) holds true [786].*

The results about groupoids which satisfy some modifications of associative law are presented in [706, 707].

1.2.3 Some other definitions of e-quasigroups

The identities (1.8) and (1.9) play an important role in the following definitions of e-quasigroups.

Lemma 1.59. *In algebra $(Q, \cdot, \backslash, /)$ the identity (1.4) follows from the identities (1.5) and (1.8).*

Proof. If in identity (1.5) we change the variable y by the variable x, and variable x by the symbol (term) $y\backslash x$, then

$$(x/(y\backslash x)) \cdot (y\backslash x) = x. \tag{1.20}$$

By the identity (1.8) $x/(y\backslash x) = y$. Therefore we can rewrite the identity (1.20) as follows:

$$y \cdot (y\backslash x) = x. \tag{1.21}$$

Then we obtain the identity (1.4). □

Lemma 1.60. *In algebra $(Q, \cdot, \backslash, /)$ the identity (1.7) follows from the identities (1.6) and (1.8).*

Proof. We can re-write the identity (1.8) in the following form:

$$(x \cdot y)/(x\backslash(x \cdot y)) = x. \tag{1.22}$$

By the identity (1.6), $x\backslash(x \cdot y) = y$. Therefore the identity (1.22) takes the form $(x \cdot y)/y = x$ and it coincides with the identity (1.7). □

Lemma 1.61. *In algebra $(Q, \cdot, \backslash, /)$ the identity (1.6) follows from the identities (1.7) and (1.9).*

Proof. We can re-write the identity (1.9), $(x \to (x \cdot y), y \to x)$, in the following form:

$$((x \cdot y)/y)\backslash(x \cdot y) = y. \tag{1.23}$$

By the identity (1.7), $(x \cdot y)/y = x$. Therefore the identity (1.23) takes the form: $x\backslash(x \cdot y) = y$ and it coincides with the identity (1.6). □

Lemma 1.62. *In algebra $(Q, \cdot, \backslash, /)$ the identity (1.5) follows from the identities (1.4) and (1.9).*

Proof. We can re-write the identity (1.4) in the following form:

$$(x/y) \cdot ((x/y)\backslash x) = x. \tag{1.24}$$

By the identity (1.9), $(x/y)\backslash x = y$. Therefore the identity (1.24) takes the form $(x/y) \cdot y = x$ and it coincides with the identity (1.5). □

Theorem 1.63. *An algebra $(Q, \cdot, \backslash, /)$ with the identities (1.5), (1.6) and (1.8) is a quasigroup [797, 692].*

Proof. The proof follows from Lemmas 1.59 and 1.60. □

Theorem 1.64. *An algebra $(Q, \cdot, \backslash, /)$ with the identities (1.4), (1.7) and (1.9) is a quasigroup [797, 692].*

Proof. The proof follows from Lemmas 1.61 and 1.62. □

Theorem 1.65. *(1) If the $(1\,3)$-parastrophe of a groupoid (Q, A) is a groupoid, then (Q, A) is a right quasigroup.*

(2) If the $(2\,3)$-parastrophe of a groupoid (Q, A) is a groupoid, then (Q, A) is a left quasigroup.

(3) If the $(1\,2\,3)$-parastrophe of a groupoid (Q, A) is a groupoid, then (Q, A) is a quasigroup.

(4) If the $(1\,3\,2)$-parastrophe of a groupoid (Q, A) is a groupoid, then (Q, A) is a quasigroup [489].

(5) If the $(1\,2)$-parastrophe of a left quasigroup (Q, A) is a groupoid, then (Q, A) is a quasigroup.

(6) If the $(1\,2)$-parastrophe of a right quasigroup (Q, A) is a groupoid, then (Q, A) is a quasigroup.

(7) If the $(2\,3)$-parastrophe of a right quasigroup (Q, A) is a groupoid, then (Q, A) is a quasigroup.

(8) If the $(2\,3)$-parastrophe of a left quasigroup (Q, A) is a groupoid, then (Q, A) is a quasigroup [786].

Proof. Case 1. The main idea is the following: in the $(1\,3)$-parastrophe of a groupoid (Q, A) and in groupoid (Q, A), right translations are inverse in pairs. See Table 1.1. □

The definition of middle ternary relation for groupoids (an analogue of middle quasigroup translation) is given in [786].

Theorem 1.66. *A groupoid $(Q, \cdot)$ is a quasigroup if and only if all middle translations of $(Q, \cdot)$ are bijective maps of the set Q.*

Proof. Let a, b be a pair of fixed elements of the set Q. Since translation P_b of groupoid $(Q, \cdot)$ is a bijective map, then we have that for the element a of set Q there exists a unique element $x \in Q$ such that $P_b\, a = x$, i.e., $a \cdot x = b$. Since all middle translations of $(Q, \cdot)$ are bijective maps, then for any fixed elements $a, b \in Q$ there exists a unique element x such that equation $a \cdot x = b$ has a unique solution.

If a translation P_b is a bijective map, then translation P_b^{-1} also is a bijective map. Further we have that for any fixed element a of the set Q there exists a unique element $y \in Q$ such that $P_b^{-1} a = y$, i.e., $y \cdot a = b$. Therefore, equation $y \cdot a = b$ has a unique solution in $(Q, \cdot)$ for any fixed elements $a, b \in Q$.

Converse. From Table 1.1 it follows that middle translations of a quasigroup are bijective mappings. See, also, [75]. □

Some other definitions of a quasigroup are given in [590, 819, 786].

Example 1.67. Define binary groupoid $(\mathbb{Z}, *)$ $x * y = x + 2y$ for all $x, y \in \mathbb{Z}$, where $(\mathbb{Z}, +, \cdot)$ is the ring of integers.

It is easy to check that groupoid $(\mathbb{Z}, *)$ is a right quasigroup with the left cancellative property.

From Theorem 1.58 it follows that groupoid $(\mathbb{Z}, *)$ satisfies the identities (1.5), (1.6), and (1.7).

We prove that groupoid $(\mathbb{Z}, *)$ satisfies the identity (1.9). If $x * y = x + 2y$, then the set of solutions of the equation $a * y = b$ is described in the following way: $y = a\backslash b = \frac{b-a}{2}$. It is clear that a solution of this equation exists only for any pair of elements of equal parity from the set of integers.

Solution of equation $x * a = b$ has the following form $x = b/a = b - 2a$. Then

$$(a/b)\backslash a = (a - 2b)\backslash a = \frac{a - a + 2b}{2} = b.$$

Therefore $(a/b)\backslash a = b$ for all $a, b \in \mathbb{Z}$, groupoid $(\mathbb{Z}, *)$ satisfies identities (1.5), (1.6), (1.7), and (1.9) and it is not a quasigroup.

Remark 1.68. In Example 1.67 both the sub-term a/b and the term $(a/b)\backslash a = b$ are defined for all $a, b \in Q$.

1.2.4 Quasigroup-based cryptosystem

References [601, 602] proposed using quasigroups for secure encryption.

A quasigroup $(Q, \cdot)$ and its (23)-parastrophe $(Q, \backslash)$ satisfy the following identities $x\backslash(x \cdot y) = y,\ x \cdot (x\backslash y) = y$ (identities (1.4) and (1.6)). It is proposed to use this property of the quasigroups to construct a stream cipher.

Algorithm 1.69. Let A be a non-empty alphabet, k be a natural number, $u_i, v_i \in A$, $i \in \{1, ..., k\}$. Define a quasigroup $(A, \cdot)$. It is clear that the quasigroup $(A, \backslash)$ is defined in a unique way. We take a fixed element l ($l \in A$), which is called a leader.

Let $u_1u_2...u_k$ be a k-tuple of letters from the alphabet A. The authors propose the following ciphering procedure $v_1 = l \cdot u_1, v_i = v_{i-1} \cdot u_i$, $i = 2, ..., k$. Therefore we obtain the following ciphertext $v_1v_2 \dots v_k$.

The enciphering algorithm is constructed in the following way: $u_1 = l\backslash v_1, u_i = v_{i-1}\backslash v_i, i = 2, ..., k$.

We shall name this algorithm the Markovski algorithm.

In this encryption procedure, a private key for both sender and receiver is quasigroup $(A, \cdot)$ and leader element l. Therefore this is a cryptosystem with symmetric keys. The authors claim that this cipher is resistant to the brute force attack (exhaustive search) and to the statistical attack (in many languages some letters appear together more frequently, than other letters).

Example 1.70. Let alphabet A consist of the letters a, b, c. We construct the following quasigroup $(A, \cdot)$:

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

Then quasigroup $(A, \backslash)$ has the following Cayley table:

$\backslash$	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

Let $l = a$ and the open text is $u = b\,b\,c\,a\,a\,c\,b\,a$. Then the ciphertext is $v = c\,b\,b\,c\,a\,a\,c\,a$. Applying the decoding function to v we get $b\,b\,c\,a\,a\,c\,b\,a = u$.

Remark 1.71. In this construction n-ary quasigroups and their parastrophes can also be used. See Algorithm 11.10 or [684]. Notice, row-Latin squares can be used by construction of a cryptosystem with non-symmetric keys. See Section 11.7.5.

1.2.5 Identity elements

1.2.5.1 Local identity elements

Definition 1.72. An element $f(b)$ of a quasigroup $(Q, \cdot)$ is called a left local identity element of an element $b \in Q$, if $f(b) \cdot b = b$. Therefore $f(b) = b/b$, or $f(b) = R_b^{-1} b$.

An element $e(b)$ of a quasigroup $(Q, \cdot)$ is called a right local identity element of an element $b \in Q$, if $b \cdot e(b) = b$. Therefore $e(b) = b\backslash b$, or $e(b) = L_b^{-1} b$.

An element $s(b)$ of a quasigroup $(Q, \cdot)$ is called a middle local identity element of an element $b \in Q$, if $b \cdot b = s(b)$. Therefore $s(b) = L_b b = R_b b$ [764, 767].

In a quasigroup there exists a unique left (right, middle) local identity element of any fixed element a. Indeed, if $f(b) \cdot a = f(a) \cdot a$, then $f(b) = f(a)$. And so on.

Exercise 1.73. Construct a quasigroup with at least two left (right, middle) local identity elements.

1.2.5.2 Left and right identity elements

Definition 1.74. An element $f \in Q$ ($e \in Q$) is a left (right) identity element for quasigroup $(Q, \cdot)$ means that $f = f(x)$ for all $x \in Q$ (respectively, $e = e(x)$ for all $x \in Q$). An element $s \in Q$ is a middle identity element for quasigroup $(Q, \cdot)$ means that $s = s(x)$ for all $x \in Q$.

Definition 1.75. An element f is a left identity element of a quasigroup $(Q, \cdot)$ means that $f(x) = f$ for all $x \in Q$, i.e., all left local elements of quasigroup $(Q, \cdot)$ coincide.

An element e is a right identity element of a quasigroup $(Q, \cdot)$ means that $e(x) = e$ for all $x \in Q$, i.e., all right local elements of quasigroup $(Q, \cdot)$ coincide.

An element e is an identity element of a quasigroup $(Q, \cdot)$ means that $e(x) = f(x) = e$ for all $x \in Q$, i.e., all left and right local elements of quasigroup $(Q, \cdot)$ coincide.

Lemma 1.76. *1. In a quasigroup $(Q, \cdot)$ there exists a unique left identity element.*
2. In a quasigroup $(Q, \cdot)$ there exists a unique right identity element.
3. In a quasigroup $(Q, \cdot)$ there exists a unique identity element.

Proof. Case 1. If $f_1 x = f_2 x = x$ for all $x \in Q$, then $f_1 = f_2$. Case 2. If $x e_1 = x e_2 = x$ for all $x \in Q$, then $e_1 = e_2$. Case 3. The proof follows from Cases 1 and 2. □

1.2.5.3 Loops

Definition 1.77. A quasigroup $(Q, \cdot)$ with a left identity element $f \in Q$ is called a *left loop*.
A quasigroup $(Q, \cdot)$ with a right identity element $e \in Q$ is called a *right loop*.
A quasigroup $(Q, \cdot)$ with a middle identity element $s \in Q$ is called a *unipotent quasigroup*.
A quasigroup $(Q, \cdot)$ with an identity element $e \in Q$ is called a *loop*.

Example 1.78. We give an example of a non-associative unipotent loop.

$\circ$	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	4	0	1	3
3	3	2	4	0	1
4	4	3	1	2	0

Unipotent loops are studied in [504].

Define in a quasigroup $(Q, \cdot)$ the following mappings: $f : x \mapsto f(x)$, where $f(x) \cdot x = x$; $e : x \mapsto e(x)$, where $x \cdot e(x) = x$; $s : x \mapsto s(x)$, where $s(x) = x \cdot x$.

Remark 1.79. In a left loop $|f(Q)| = 1$, in a right loop $|e(Q)| = 1$, in a unipotent quasigroup $|s(Q)| = 1$.

1.2.5.4 Identity elements of quasigroup parastrophes

Connections between different kinds of local identity elements in various parastrophes of a quasigroup $(Q, \cdot)$ are given in the following table [504, 764, 767].

Table 1.2: Local identity elements of parastrophic quasigroups.

	ε	(12)	(13)	(23)	(123)	(132)
f	f	e	s	f	e	s
e	e	f	e	s	s	f
s	s	s	f	e	f	e

In Table 1.2, for example, $s^{(123)} = f^{(\cdot)}$.

Definition 1.80. A quasigroup $(Q, \cdot)$ with identity $x \cdot x = x$ is called an *idempotent quasigroup*. An element x with this property is called *idempotent element*.

Remark 1.81. It is easy to see that any parastrophe of an idempotent quasigroup is an idempotent quasigroup. In an idempotent quasigroup, the mappings e, f, s are identity permutations of the set Q. Moreover, if one of these three mappings is an identity permutation, then all other ones are identity permutations, too.

1.2.5.5 The equivalence of loop definitions

Definition 1.82. A quasigroup $(Q, \cdot, /, \backslash)$ with identity

$$x/x = y/y \tag{1.25}$$

is called a left loop.

Lemma 1.83. *A quasigroup $(Q, \cdot)$ is a left loop if and only if quasigroup $(Q, \cdot, /, \backslash)$ is a left loop.*

Proof. Suppose that quasigroup $(Q, \cdot)$ has the left identity element, i.e., there exists an element f such that the equality $f \cdot z = z$ is true for any $z \in Q$. We can re-write equality

$f \cdot z = z$ in the following form: $z/z = f$ for any $z \in Q$. Therefore $x/x = y/y = f$ and the following identity is true $x/x = y/y$.

Suppose that quasigroup $(Q, \cdot, /, \backslash)$ satisfies the identity (1.25). Therefore we have $(x/x) \cdot z \overset{(1.25)}{=} (z/z) \cdot z \overset{(1.5)}{=} z$. Thus quasigroup $(Q, \cdot)$ has the left identity element $f = x/x$. The uniqueness follows from Lemma 1.76. □

Recall identity (1.5) is true in any right division groupoid (Theorem 1.58). Therefore in any right division groupoid with the identity (1.25) there exists at least one left identity element.

Definition 1.84. A quasigroup $(Q, \cdot, /, \backslash)$ with identity

$$x\backslash x = y\backslash y \tag{1.26}$$

is called a right loop.

Exercise 1.85. Prove the analogue of Lemma 1.83 for right loops.

Definition 1.86. A quasigroup $(Q, \cdot, /, \backslash)$ with identity

$$x\backslash x = y/y \tag{1.27}$$

is called a loop.

Theorem 1.87. *Quasigroup $(Q, \cdot)$ is a loop if and only if quasigroup $(Q, \cdot, /, \backslash)$ is a loop [591, p. 97].*

Proof. A quasigroup $(Q, \cdot)$ is a loop means that there exists an element, say 1, such that the following equalities $1 \cdot x = x$ and $y \cdot 1 = y$ are true for any $x, y \in Q$. Therefore $x/x = 1$, $y\backslash y = 1$, and $x/x = y\backslash y$ for all $x, y \in Q$.

Let $x\backslash x = y/y$ in quasigroup $(Q, \cdot, /, \backslash)$. Prove the existence of the left and right identity element in quasigroup $(Q, \cdot)$. We have: $(x\backslash x) \cdot z \overset{(1.27)}{=} (z/z) \cdot z \overset{(1.5)}{=} z$; $z \cdot (x/x) \overset{(1.27)}{=} z \cdot (z\backslash z) \overset{(1.4)}{=} z$.

The uniqueness of the identity element follows from Lemma 1.76. □

1.2.5.6 Identity elements in some quasigroups

Lemma 1.88. *[819, Proposition 1.3]. A nonempty quasigroup $(Q, \cdot, /, \backslash)$ is a loop if and only if it satisfies the "slightly associative identity"*

$$x(y/y) \cdot z = x \cdot (y/y)z. \tag{1.28}$$

Proof. If $(Q, \cdot, /, \backslash)$ is a loop with identity element e relative to the operation " $\cdot$ ", then $y/y = e$ and identity (1.28) follows.

Conversely, if identity (1.28) is true, then setting $z = y$ we obtain $x(y/y) \cdot y = x \cdot (y/y)y = xy$ (since by identity (1.5) $(y/y)y = y$). Further we have $x(y/y) \cdot y = xy$. After cancellation from the right we have $x(y/y) = x$, $x\backslash x = y/y$. □

Corollary 1.89. *A quasigroup $(Q, \cdot)$ with identity*

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{1.29}$$

(identity of associativity) has the identity element, i.e., this quasigroup is a group [549].

Proof. In identity associativity we can put $y := y/y$ and after this apply Lemma 1.88. □

Notice that in [72] V.D. Belousov posed the following problem (Problem 18): "From what identities, that are true in a quasigroup $Q(\cdot)$, does it follow that the quasigroup $Q(\cdot)$ is a loop?" More detailed information on Belousov problems is given in Chapter 5.

The following identities are called Moufang identities: $x(y \cdot xz) = (xy \cdot x)z$, $(zx \cdot y)x = z(x \cdot yx)$, $yx \cdot zy = y(xz \cdot y)$, $yx \cdot zy = (y \cdot xz)y$.

Theorem 1.90. *A quasigroup $(Q, \cdot)$ with any of Moufang identities is a loop [545, 794].*

From Theorem 1.90 and the well-known result that in a loop all Moufang identities are equivalent [173, 72], it follows that in a quasigroup all Moufang identities are equivalent.

Definition 1.91. A quasigroup with identity $xy \cdot uv = xu \cdot yv$ is called *medial*, and a quasigroup with equality $yz \cdot x = yf(x) \cdot zx$ is called *right F-quasigroup* [80].

Problem 1.1. It is easy to see that in loops $1 \cdot ab = 1a \cdot 1b$. Describe quasigroups with the property $f(ab) = f(a)f(b)$ for all $a, b \in Q$, where $f(a)$ is a left local element of element a.

Medial and right F-quasigroups have this property [80].

The identity $x(y \cdot xz) = (x \cdot yx)z$ is called the left Bol identity. A loop with the left Bol identity is called a left Bol loop.

Lemma 1.92. *A quasigroup $(Q, \cdot)$ with the left Bol identity has a right identity element.*

Proof. Indeed, if we put $z := e_x$ in identity $x(y \cdot xz) = (x \cdot yx)z$, then we obtain $x \cdot yx = (x \cdot yx)e_x$ for all $x, y \in Q$. □

Notice, there exist right loops with the left Bol identity:

$*$	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

1.2.5.7 Inverse elements in loops

Let $(Q, \circ)$ be a loop. Let I_r, I_l be the following maps: $I_r(x) = x^{-1}$, where $x \circ x^{-1} = 1$; $I_l(x) = {}^{-1}x$, where ${}^{-1}x \circ x = 1$, for all $x \in Q$.

Lemma 1.93. *In any loop $(Q, \circ)$, $I_l = I_r^{-1}$.*

Proof. In a loop $(Q, \circ)$ we have $x \circ I_r x = 1$, i.e., $P_1 x = I_r x$, $I_r = P_1$. Similarly we have $I_l x \circ x = 1$, i.e., $P_1^{-1} x = I_l x$, $I_l = P_1^{-1}$. Therefore $I_l = I_r^{-1}$ in any loop. □

1.2.6 Multiplication groups of quasigroups

Let $(Q, \cdot)$ be a quasigroup. With every element $a \in Q$ it is possible to associate left (L_a), right (R_a) and middle (P_a) translations. These translations are some permutations of the set Q. They can be considered as elements of the symmetric group S_Q.

With any quasigroup $(Q, \cdot)$ we can associate the sets of all left translations $(\mathbb{L})$, right translations $(\mathbb{R})$, and middle translations $(\mathbb{P})$. Denote the groups generated by all left, right, and middle translations of a quasigroup $(Q, \cdot)$ as $LM(Q, \cdot)$, $RM(Q, \cdot)$, and $PM(Q, \cdot)$, respectively.

The group generated by all left and right translations of a quasigroup $(Q,\cdot)$ is called (following A.A. Albert [10, 11]), a multiplication group of quasigroup. Usually this group is denoted by $M(Q,\cdot)$. A multiplication group of a quasigroup plays an important role by the study of quasigroups, especially in the study of loops.

By $FM(Q,\cdot)$ we shall denote a group generated by sets $\mathbb{L},\mathbb{R},\mathbb{P}$ of a quasigroup $(Q,\cdot)$. Information about the group $FM(Q,\cdot)$ in the case when $(Q,\cdot)$ is an IP-loop (a Moufang loop, a group) is presented in [758].

We can see on a quasigroup $(Q,\cdot)$ of a finite order n, as on a set $\mathbb{T}$ of permutations of the group S_n with the following property: if $\alpha,\beta\in\mathbb{T}$ and there exists an element $x\in Q$ such that $\alpha^{-1}\beta x=x$, then $\alpha=\beta$.

Definition 1.94. A set $\mathbb{T}$ of permutations on a finite set Q is called sharply transitive, if for any pair of elements $a,b\in Q$ there exists exactly one permutation $\alpha\in\mathbb{T}$ such that $\alpha a=b$.

Sets of all left, right and middle translations of a quasigroup $(Q,\cdot)$ give us examples of sharply transitive sets of permutations on the set Q.

We shall use the following fact about the properties of groups that act transitively on a set Q: if a group G acts transitively on a set Q, then stabilizers of any two elements $a,b\in Q$ are isomorphic subgroups and $|G|=|St(a)|\cdot|Q|$ [471].

Multiplication groups play an important role in quasigroup theory for the following reason: groups are algebraic objects which are much better known than quasigroups. Often it is possible to express some quasigroup properties in the language of corresponding groups.

For example, the theory of normality of quasigroups, and especially of loops, can be expressed in terms of corresponding subgroups of its multiplication group [10, 11].

Properties of multiplication groups of quasigroups and loops are described in many articles, see, for example, [280, 268, 269]. In [268] the following result is proved. Let W be a free loop with a basis $X\neq\varnothing$. Then the left multiplication group $LM(W)$ is a free group of infinite rank and a Frobenius permutation group [435]. Notice, for the group $M(W)$ this fact is not true [268, 280]. Multiplication groups of free and free commutative quasigroups are also described in [360, 361].

Let $(Q,\cdot)$ be a quasigroup. The group $I_h=\{\alpha\in M(Q,\cdot)|\alpha h=h\}$ is called an inner mapping group of a quasigroup $(Q,\cdot)$ relative to element $h\in Q$. The group I_h is a stabilizer of element h by action of the group $M(Q,\cdot)$ on the set Q.

In the loop case the group $I_1(Q,\cdot)=I(Q,\cdot)$ is usually studied, where 1 is the identity element of a loop $(Q,\cdot)$.

It is possible to define the "inner mapping groups" for the groups $LM(Q,\cdot)$, $RM(Q,\cdot)$, $PM(Q,\cdot)$, $FM(Q,\cdot)$ of a quasigroup $(Q,\cdot)$, namely, it is possible to define the groups $LI_h(Q,\cdot)$, $RI_h(Q,\cdot)$, $PI_h(Q,\cdot)$, $FI_h(Q,\cdot)$ for any element $h\in Q$.

Example 1.95. We use quasigroup from Example 1.20. It is easy to check that $L_0=(01)$, $L_1=(12)$, $L_2=(02)$, $LM(Q,\cdot)=\{\varepsilon,(0\,1),(0\,2),(1\,2),(0\,1\,2),(0\,2\,1)\}$, $LI_0(Q,\cdot)=\{\varepsilon,(1\,2)\}$, $LI_1(Q,\cdot)=\{\varepsilon,(0\,2)\}$, $LI_2(Q,\cdot)=\{\varepsilon,(0\,1)\}$, $LM(Q,\cdot)\cong S_3$, $LI_0(Q,\cdot)\cong Z_2$.

Of course, it is possible to define "inner mapping groups" for other "multiplication groups" of a quasigroup $(Q,\cdot)$.

Since all the above listed multiplication groups of a quasigroup $(Q,\cdot)$ act transitively on the set Q, inner mapping groups relative to different elements of the set Q are isomorphic.

For example, $PI_h(Q,\cdot)\cong PI_g(Q,\cdot)$, $FI_h(Q,\cdot)\cong FI_g(Q,\cdot)$ and so on. If $|Q|$ is finite, then $|M(Q,\cdot)=|Q||I_h(\cdot)|$ and so on.

Exercise 1.96. Construct various multiplication groups and inner multiplication groups for a quasigroup of order 4 or (and) 5.

1.2.7 Transversals: "Come back way"

Definition 1.97. Suppose we have a partition of a set Q into cosets A_i. The set of representatives $\{a_i \mid a_i \in A_i\}$ (a unique element from any coset) is called a transversal of the set Q relative to the partition A_i.

The term "transversal" is used in combinatorics. See, for example, [409, Chapter V].

Let $(Q,\cdot)$ be a quasigroup. It is clear that $LI_h(Q,\cdot) \subseteq LM(Q,\cdot)$, and that a unique left translation lies in any left coset class of the group $LM(Q,\cdot)$ by the group $LI_h(Q,\cdot)$. Therefore we have the following partition of the group $LM(Q,\cdot)$ through the group $LI_h(Q,\cdot)$ (for brevity, we omit the expression $(Q,\cdot)$)

$$\begin{aligned} LM = a_1 \cdot LI_h \sqcup a_2 \cdot LI_h \sqcup a_3 \cdot LI_h \sqcup \dots a_n \cdot LI_h \sqcup \dots = \\ L_{a_1} \cdot LI_h \sqcup L_{a_2} \cdot LI_h \sqcup L_{a_3} \cdot LI_h \sqcup \dots L_{a_n} \cdot LI_h \sqcup \dots \end{aligned} \tag{1.30}$$

It is clear that the situation with other multiplication groups and corresponding inner multiplication groups is similar.

Notice, the ordered set of translations $\{L_{a_1}, \dots, L_{a_n}, \dots\}$ defines the Cayley table of quasigroup $(Q,\cdot)$ in a unique way.

Example 1.98. We continue Example 1.95. We have $LM = L_0 \cdot LI_0 \sqcup L_1 \cdot LI_0 \sqcup L_2 \cdot LI_0$, where $LI_0 = \{\varepsilon, (12)\}$, $L_0 \cdot LI_0 = \{(01), (012)\}$, $L_1 \cdot LI_0 = \{\varepsilon, (12)\}$, $L_2 \cdot LI_0 = \{(02), (021)\}$.

This situation can be generalized in the following way. Let $(G,\cdot)$ be a group, and $(H,\cdot)$ be its subgroup. A complete system T of representatives of the left cosets aH, $a \in G$ is called a left transversal in group $(G,\cdot)$ to subgroup $(H,\cdot)$.

In other words, from any coset $a_i \cdot H$ we take only one element, for example, element a_i. Thus $G = a_1 \cdot H \sqcup a_2 \cdot H \sqcup a_3 \cdot H \sqcup \dots a_n \cdot H \sqcup \dots = \sqcup a_i \cdot H$ [471], and $T = \{a_1, a_2, \dots, a_n, \dots\}$ is a left transversal.

Define operation $*$ on the set T in the following way:

$$a * b = a \cdot b \pmod{H}. \tag{1.31}$$

Lemma 1.99. *Groupoid $(T,*)$ is a left quasigroup, i.e., equation $a * x = b$ has a unique solution for any $a, b \in T$.*

Proof. Indeed, left translations L_d^*, $d \in T$, defined by the equality (1.31), correspond to permutations (this fact is easy to check or see [407, Theorem 5.3.1. (a)], [471, 12.2.1 Theorem]) by the following action of the element d on the set of cosets $d(a_j \cdot H) = d \cdot a_j \cdot H$, where $a_j \cdot H \in \sqcup a_i \cdot H$. □

R. Baer, by definition of transversal, supposed that $1 \in T$, where 1 is the identity element of the group G [24, 25]. In this case the left quasigroup has the identity element 1, i.e., $1 * x = x * 1 = x$ for all $x \in T$.

Notice, the set of left translations of the groupoid $(T,*)$ is a subset of the set of permutations S of the group G by its subgroup H (permutation presentation of the group G by its subgroup H) [407, Theorem 5.3.1. (a)], [471, 12.2.1 Theorem]).

It is known [407, 471] that the set S forms a group relative to standard multiplication of permutations and this group is isomorphic to the group $G/(ker\, H)$, where $kerH$ is the largest normal subgroup of the group G, which is contained in H.

Lemma 1.100. *If $L_a^* = L_b^*$ in the left quasigroup $(T,*)$, then $a = b$.*

Proof. If $L_a^* x = L_b^* x$ for all $x \in T$, then, using equality (1.31), we have $a \cdot x = b \cdot x \pmod{H}$, $x = a^{-1}bx \pmod{H}$, $a^{-1}b \in H$, $a = b \pmod{H}$, i.e., $a = b$ in left quasigroup $(T,*)$. □

Corollary 1.101. *In the Cayley table of the left quasigroup* $(T, *)$*, all rows are pairwise different.*

Proof. The proof follows from Lemma 1.100. □

The conditions when a transversal T is a loop transversal, i.e., $(T, *)$ is a loop, are given in [24, 25, 658].

Example 1.102. Let $G = S_3 = \langle a, b \,|\, a^3 = b^2 = (ab)^2 = 1 \rangle$, $S_3 = \{1, a, a^2, b, ab, a^2b\}$, $H = \langle b \rangle$. We have the following set of left cosets: $H = \{1, b\}$, $aH = \{a, ab\}$, $a^2H = \{a^2, a^2b\}$. Elements $\{b, ab, a^2\}$ form the left transversal T. We can construct a Cayley table of the left quasigroup $(T, *)$.

$*$	b	ab	a^2
b	b	a^2	ab
ab	ab	b	a^2
a^2	a^2	b	ab

If we denote b as 1, ab as 2, a^2 as 3, then we obtain the following Cayley table:

$*$	1	2	3
1	1	3	2
2	2	1	3
3	3	1	2

In [556, Theorem 3.4] it is proved that every right quasigroup with identity element can be embedded as a right transversal in a group which is universal in some sense.

Transversals are studied in [449, 450, 447, 448]. These objects are used in construction of codes [429, 433]. Loop transversal is based on a loop and some its subloop. Such transversals are introduced and studied in [553, 554].

1.2.8 Generators of inner multiplication groups

We start this subsection from the following Belousov theorem, which is a generalization of the corresponding Bruck theorem, which was proved for loop case [167]. Taking into consideration the importance of these theorems for the development of quasigroups and especially loop theory, we decided to name these theorems for their discoverers.

Theorem 1.103. *Belousov theorem. In a quasigroup* $(Q, \cdot)$

$$I_h(Q, \cdot) = \langle R_{a,b}, L_{a,b}, T_a \,|\, a, b \in Q \rangle ,$$

where $R_{a,b} = R^{-1}_{a \bullet b} R_b R_a$, $h(a \bullet b) = (ha)b$, $L_{a,b} = L^{-1}_{a \circ b} L_a L_b$, $(a \circ b)h = a(bh)$, $T_a = L^{-1}_{\sigma a} R_a$, $\sigma = R^{-1}_h L_h$ *[72].*

Theorem 1.104. *Bruck theorem. In a loop* $(Q, \cdot)$ *with identity element* 1

$$I_1(Q, \cdot) = \langle R_{a,b}, L_{a,b}, T_a \,|\, a, b \in Q \rangle ,$$

where $R_{a,b} = R^{-1}_{ab} R_b R_a$, $L_{a,b} = L^{-1}_{ab} L_a L_b$, $T_a = L^{-1}_a R_a$ *[167].*

Theorem 1.103 and Theorem 1.104 are proved in [72, 167] using induction. Theorem 1.103 and Theorem 1.104 play important roles in definition of normal subloops and subquasigroups.

It is possible to prove analogs of these theorems using Theorem 1.106. This plan, for example, was realized in [772]. Namely, in Theorem 1.106 induction is hidden. Properties of the group $FM(Q, \cdot)$ and generators of the group $FI_h(Q, \cdot)$ are given in [75].

Theorem 1.105. *In a quasigroup* $(Q,\cdot)$

$$FI_h(Q,\cdot)=\langle L_{a,b},T_{a,b},P_{a,b}\,|\,a,b\in Q\rangle\,,$$

where $L_{a,b}=L^{-1}_{a\circ b}L_aL_b$, $(a\circ b)h=a(bh)$, $T_{a,b}=L^{-1}_{a\star b}R_aL_b$, $(a\star b)h=bh\cdot a$, $P_{a,b}=L^{-1}_{a\bullet b}P_aL_b$, $(a\bullet b)h=a/(bh)$.

Proof. Firstly we note that group $FM(Q,\cdot)$ of a quasigroup $(Q,\cdot)$ acts transitively on the set Q. Really, for any fixed elements $a,b\in Q$ there exists an element c, such that $L_ca=b$ since the equation $x\cdot a=b$ has a unique solution in a quasigroup $(Q,\cdot)$ for any fixed elements $a,b\in Q$.

A stabilizer of element h in group FM of a quasigroup $(Q,\cdot)$ is group FI_h. Moreover, we can write

$$FM(Q,\cdot)=L_{f(h)}(FI_h)\sqcup L_{a_1}(FI_h)\sqcup L_{a_2}(FI_h)\sqcup\cdots\,, \tag{1.32}$$

where $f(h)\cdot h=h$.

In [471, 14.3.1. Theorem] the following Otto Schreier Theorem is proved:

Theorem 1.106. *Let T be a set of generators of a group G, H be a subgroup of the group G, $f:u\to\overline{u}$ be a function such that any element $u\in G$ corresponds to a fixed element $\bar{u}$ from the set uH, and S be a set of selected representatives (one element from any coset). Then $H=\langle\overline{ps}^{\,-1}ps\mid s\in S,p\in T\rangle$.*

We apply this theorem for obtaining a generator set of the group FI_h of a quasigroup $(Q,\cdot)$. The set $T=\mathbb{L}\cup\mathbb{R}\cup\mathbb{P}$ is a generator set of the group $FM(Q,\cdot)$ of a quasigroup $(Q,\cdot)$.

Let a set of selected representatives from every left coset of subgroup FI_h of a group $FM(Q,\cdot)$ be the following set: $S=\{L_a\mid a\in Q\}$. Therefore we defined the "selecting" function f.

Finally, we specify elements of the form $\overline{ps}^{\,-1}$. They must have the form L_z^{-1}. We can find the element z knowing elements p and s.

(i) Let $p=L_a,s=L_b$. We need to specify element z such that $L_aL_bh=L_zh$, $a(bh)=zh$. We have $z=R_h^{-1}(a\cdot bh)$. We can re-write the last relation as a binary operation with variables $a,b\in Q$ in the following form $(a\circ b)h=(a\cdot bh)$.

(ii) Let $p=R_a,s=L_b$. We need to specify element z such that $R_aL_bh=L_zh$, $(bh)a=zh$. Further we have $z=R_h^{-1}((bh)a)$. We can re-write the last relation as a binary operation with variables $a,b\in Q$ in the following form $(a\star b)h=(bh\cdot a)$.

(iii) Let $p=P_a,s=L_b$. We need to specify element z such that $P_aL_bh=L_zh$, $P_a(bh)=zh$. Further we have $zh\cdot bh=a$, $zh=a/bh$. We can re-write the last relation as a binary operation with variables $a,b\in Q$ in the following form $(a\bullet b)h=a/(bh)$. □

Corollary 1.107. *In a quasigroup* $(Q,\cdot)$,

$$I_h(Q,\cdot)=\langle L_{a,b},T_{a,b}\,|\,a,b\in Q\rangle\,,$$

where $L_{a,b}=L^{-1}_{a\circ b}L_aL_b$, $(a\circ b)h=a(bh)$, $T_{a,b}=L^{-1}_{a\star b}R_aL_b$, $(a\star b)h=bh\cdot a$.

Proof. The proof follows from Theorem 1.105. □

Corollary 1.108. *In a loop* $(Q,\cdot)$,

$$\begin{aligned}FI_1(Q,\cdot)&=\langle L_{a,b},T_{a,b},P_{a,b}\,|\,a,b\in Q\rangle\,,\\ I_1(Q,\cdot)&=\langle L_{a,b},T_{a,b}\,|\,a,b\in Q\rangle\,,\end{aligned} \tag{1.33}$$

where $L_{a,b}=L^{-1}_{a\cdot b}L_aL_b$, $T_{a,b}=L^{-1}_{b\cdot a}R_aL_b$, $P_{a,b}=L^{-1}_{a/b}P_aL_b$.

Proof. It is sufficient to put $h = 1$ in conditions of Theorem 1.105, where the symbol 1 denotes identity element of loop $(Q, \cdot)$. □

Notice, $\langle L_{a,b}, T_{a,b} \,|\, a, b \in Q\rangle \subseteq \langle R_{a,b}, L_{a,b}, T_a \,|\, a, b \in Q\rangle$. Indeed,

$$(L_{ba}^{-1} R_{ba})(R_{ba}^{-1} R_a R_b)(R_b^{-1} L_b) = L_{ba}^{-1} R_a L_b.$$

The proof of inverse inclusion is more complicated.

Lemma 1.109. *In a quasigroup* $(Q, \cdot)$

$$LI_h(Q, \cdot) = \langle L_{a,b} \,|\, a, b \in Q\rangle\,,$$

where $L_{a,b} = L_{a\circ b}^{-1} L_a L_b$, $(a \circ b)h = a(bh)$ *[816, 772].*

Proof. The proof follows from Theorem 1.105. □

Exercise 1.110. Construct two more triples of generators of the group FI_h of a quasigroup $(Q, \cdot)$, $h \in Q$.

Lemma 1.111. *In a loop* $(Q, \cdot)$,

$$PI_h(Q, \cdot) = \langle P_{a,b} \,|\, a, b \in Q\rangle\,,$$

where $P_{a,b} = P_{a\backslash b}^{-1} P_a P_b$ *[767].*

Proof. The proof is similar to the proof of Theorem 1.105. □

The following results are known: a permutation group G of a set Q is the multiplication group of some quasigroup if and only if there is a loop $(Q, +)$ and permutations f and g of Q such that $\langle Mlt(Q, +), f, g\rangle = G$ [438]; any Hamiltonian group (finite non-abelian groups with only normal subgroups [407, p. 213]) cannot be a multiplication group of a loop [438].

Problem 1.2. Describe groups that can be or cannot be a multiplication group of a loop (of a quasigroup). We hope our readers will be able to generalize this problem on other "multiplication groups" of quasigroups and loops (or left quasigroups).

We notice, there are many articles in which properties of quasigroups (or loops) are studied with various conditions on their various inner multiplication groups. Mainly, these are the articles of T. Kepka, A. Drapal, M. Niemenmaa and their pupils and followers.

1.3 Morphisms

1.3.1 Isotopism

We start from a traditional definition of isotopism (of isotopy).

Definition 1.112. n-Ary groupoid (G, f) is an isotope of an n-ary groupoid (G, g) (*in other words* (G, f) *is an isotopic image of* (G, g)), if there exist permutations $\mu_1, \mu_2, \ldots, \mu_n$, μ of the set G such that

$$f(x_1, x_2, \ldots, x_n) = \mu^{-1} g(\mu_1 x_1, \ldots, \mu_n x_n) \tag{1.34}$$

for all $x_1, \ldots, x_n \in G$. We can also write this fact in the form $(G, f) = (G, g)T$ where $T = (\mu_1, \mu_2, \ldots, \mu_n, \mu)$. The ordered $(n + 1)$-tuple T is called *isotopy* of n-ary groupoids.

If in equality (1.34) $f = g$, then $(n+1)$-tuple $(\mu_1, \mu_2, \ldots, \mu_n, \mu)$ of permutations of the set G is called an *autotopy of n-groupoid* (Q, f). The last component of an autotopy of an n-groupoid is called a *quasiautomorphism* (by analogy with binary case).

A set of all autotopies of a groupoid (Q, f) forms the group of autotopies relative to the usually defined operation on this set: if $T_1 = (\mu_1, \mu_2, \ldots, \mu_n, \mu)$ and $T_2 = (\nu_1, \nu_2, \ldots, \nu_n, \nu)$ are autotopies of groupoid (Q, f), then $T_1T_2 = (\mu_1\nu_1, \mu_2\nu_2, \ldots, \mu_n\nu_n, \mu\nu)$ is an autotopy of groupoid (Q, f). Autotopy group of a groupoid (Q, f) will be denoted as $\mathfrak{T}(Q, f)$.

If in (1.34) $\mu_1 = \mu_2 = \cdots = \mu_n = \mu$, then groupoids (Q, f) and (Q, g) are isomorphic.

At last, if in (1.34) the n-ary operations f and g are equal and $\mu_1 = \mu_2 = \cdots = \mu_n = \mu$, then we obtain an *automorphism of groupoid* (Q, f), i.e., a permutation μ of the set Q is called an automorphism of an n-groupoid (Q, f) if for all $x_1, \ldots, x_n \in Q$ the following relation is fulfilled: $\mu f(x_1, \ldots, x_n) = f(\mu_1 x_1, \ldots, \mu_n x_n)$. We denote by $Aut(Q, f)$ the automorphism group of an n-ary groupoid (Q, f). If $n = 2$, we obtain the following definition of isotopism.

Definition 1.113. Binary groupoid $(G, \circ)$ is an isotopic image of a binary groupoid $(G, \cdot)$, if there exist permutations α, β, γ of the set G such that $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$.

We list some properties of isotopisms. As usual, ε denotes the identity permutation.

Lemma 1.114. *If (α, β, γ) is an isotopism, then*

$$(\alpha, \beta, \gamma) = (\alpha, \beta, \varepsilon) * (\varepsilon, \varepsilon, \gamma) = (\alpha, \varepsilon, \varepsilon) * (\varepsilon, \beta, \varepsilon) * (\varepsilon, \varepsilon, \gamma) = (\varepsilon, \beta, \varepsilon) * (\varepsilon, \varepsilon, \gamma) * (\alpha, \varepsilon, \varepsilon)$$

and so on.

Lemma 1.114 helps to construct a Cayley table of isotopic images of a finite quasigroup (groupoid).

Lemma 1.115. *If $(Q, \circ) = (Q, \cdot)(\alpha, \varepsilon, \varepsilon)$, i.e., $x \circ y = \alpha x \cdot y$ for all $x, y \in Q$, then $L^{\circ}_x = L^{\cdot}_{\alpha x}$ for all $x \in Q$.*

If $(Q, \circ) = (Q, \cdot)(\varepsilon, \beta, \varepsilon)$, i.e., $x \circ y = x \cdot \beta y$ for all $x, y \in Q$, then $R^{\circ}_y = R^{\cdot}_{\beta y}$ for all $y \in Q$.

If $(Q, \circ) = (Q, \cdot)(\varepsilon, \varepsilon, \gamma)$, i.e., $x \circ y = \gamma^{-1}(x \cdot y)$ for all $x, y \in Q$, then $P^{\circ}_z = P^{\cdot}_{\gamma z}$ for all $z \in Q$.

Proof. Case 3. We can re-write equality $(Q, \circ) = (Q, \cdot)(\varepsilon, \varepsilon, \gamma)$ in the form $x \circ y = \gamma^{-1}(x \cdot y)$ for all $x, y \in Q$. Therefore, if $x \circ y = \gamma^{-1}(x \cdot y) = z$, then $P^{\cdot}_z x = y$, $P^{\circ}_{\gamma^{-1} z} x = y$, $P^{\cdot}_z = P^{\circ}_{\gamma^{-1} z}$. □

Lemma 1.115 helps to find the Cayley table of isotopic images of a groupoid in the following way: if we have isotopy (α, β, γ), then we permute rows by the rule $L^{\circ}_x = L^{\cdot}_{\alpha x}$, after this we permute columns by the rule $R^{\circ}_y = R^{\cdot}_{\beta y}$, and finally we rename elements in the Cayley table by the following rule: if $x \cdot y = a$, then $x \circ y = \gamma^{-1} a$. As it follows from Lemma 1.114, we can change the order of execution of steps 1, 2, and 3.

Example 1.116. Let $T = ((1234), (12)(34), (123))$. Let a quasigroup $(Q, \cdot)$ have the following Cayley table:

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

If we apply isotopy $((1234), \varepsilon, \varepsilon)$ to this quasigroup (it changes the rows), then we obtain the following Cayley table

$*$	1	2	3	4
1	1	4	2	3
2	2	1	3	4
3	3	2	4	1
4	4	3	1	2

Further, if we apply the isotopy $(\varepsilon, (12)(34), \varepsilon)$ to the obtained quasigroup (we change the order of columns in the previous Cayley table), then we have quasigroup:

$\circ$	1	2	3	4
1	4	1	3	2
2	1	2	4	3
3	2	3	1	4
4	3	4	2	1

Finally, with the help of isotopy $(\varepsilon, \varepsilon, (123))$ $(\gamma^{-1} = (132))$, we rename elements inside the last Cayley table:

$\circ$	1	2	3	4
1	4	3	2	1
2	3	1	4	2
3	1	2	3	4
4	2	4	1	3

Definition 1.117. An isotopism of the form $(\alpha, \beta, \varepsilon)$ is called a principal isotopism.

Usually we shall write the fact that groupoids (Q, A) and (Q, B) are isotopic in this form: $(Q, A) \sim (Q, B)$

Lemma 1.118. *Any isotopism up to isomorphism is a principal isotopism.*

Proof. Suppose that (Q, A) and (Q, B) are isotopic groupoids. If $(Q, B) = (Q, A)$ (α, β, γ), then $(Q, B)(\gamma^{-1}, \gamma^{-1}, \gamma^{-1}) = (Q, A)(\alpha\gamma^{-1}, \beta\gamma^{-1}, \varepsilon)$. Thus $(Q, C) = (Q, A)$ $(\alpha\gamma^{-1}, \beta\gamma^{-1}, \varepsilon)$, where $(Q, C) = (Q, B)$ $(\gamma^{-1}, \gamma^{-1}, \gamma^{-1})$. □

Definition 1.119. Isotopy of the form $(R_a^{-1}, L_b^{-1}, \varepsilon)$, where L_b, R_a are left and right translations of a quasigroup $(Q, \cdot)$, is called LP-isotopy (loop isotopy) [72, 80].

Theorem 1.120. *Any LP-isotope of a quasigroup $(Q, \cdot)$ is a loop.*

Proof. Prove that quasigroup $(Q, \circ)$, where $x \circ y = R_a^{-1}x \cdot L_b^{-1}y$, is a loop. Let $1 = b \cdot a$. If we take $x = 1$, then $1 \circ y = R_a^{-1}ba \cdot L_b^{-1}y = R_a^{-1}R_a b \cdot L_b^{-1}y = b \cdot L_b^{-1}y = L_b L_b^{-1}y = y$.

If we take $y = 1$, then we have $x \circ 1 = R_a^{-1}x \cdot L_b^{-1}ba = R_a^{-1}x \cdot a = R_a R_a^{-1}x = x$. Element 1 is the identity element of the quasigroup $(Q, \circ)$. □

Lemma 1.121. *1. If $(Q, \circ) = (Q, \cdot)(\alpha, \beta, \varepsilon)$ and $(Q, \circ)$ is a loop, then there exist elements $a, b \in Q$ such that $\alpha = R_a^{-1}$, $\beta = L_b^{-1}$, where $R_a x = x \cdot a$, $L_b x = b \cdot x$ ([80], Lemma 1.1).*

2. If $(Q, \circ) = (Q, \cdot)(\alpha, \varepsilon, \gamma)$ and $(Q, \circ)$ is a unipotent left loop, then there exist elements $a, b \in Q$ such that $\alpha = P_a^{-1}$, and $\gamma = L_b$.

3. If $(Q, \circ) = (Q, \cdot)(\varepsilon, \beta, \gamma)$ and $(Q, \circ)$ is a unipotent right loop, then there exist elements $a, b \in Q$ such that $\beta = P_a$, and $\gamma = R_b$.

Proof. 1. Let $x \circ y = \alpha x \cdot \beta y$. If $x = 1$, then we have $1 \circ y = y = \alpha 1 \cdot \beta y$. Therefore $L_{\alpha 1}\beta = \varepsilon$, $\beta = L_{\alpha 1}^{-1}$. If we take $y = 1$, then we have $x \circ 1 = x = \alpha x \cdot \beta 1$, $R_{\beta 1}\alpha = \varepsilon$, $\alpha = R_{\beta 1}^{-1}$.

2. Let $x \circ y = \gamma^{-1}(\alpha x \cdot y)$. If $x = 1$, then we have $y = \gamma^{-1}(\alpha 1 \cdot y)$. Therefore $\gamma y = L_{\alpha 1} y$. If $x = y$, then $1 = \gamma^{-1}(\alpha \cdot x)$, $\gamma 1 = \alpha x \cdot x$, $P_{\gamma 1}^{-1} x = \alpha x$. In order to obtain the claimed in this case, we denote $\alpha 1$ by b, and $\gamma 1$ by a.

3. Let $x \circ y = \gamma^{-1}(x \cdot \beta y)$. If $y = 1$, then we have $x = \gamma^{-1}(x \cdot \beta 1)$. Therefore $\gamma x = R_{\beta 1} x$. If $x = y$, then $1 = \gamma^{-1}(x \cdot \beta x)$, $\gamma 1 = x \cdot \beta x$, $P_{\gamma 1} x = \beta x$. In order to obtain the claimed in conditions of the lemma, we denote $\beta 1$ by b, and $\gamma 1$ by a.

□

Lemma 1.122. *(i) If $(Q, \cdot)$ is a binary quasigroup, L_a, R_b are some of its left and right translations, $\varphi \in Aut(Q, \cdot)$, then $\varphi L_a = L_{\varphi a}\varphi$, $\varphi R_b = R_{\varphi b}\varphi$.*

(ii) If $(Q, +)$ is a group, then $L_a R_b = R_b L_a$, $L_a^{-1} = L_{-a}, R_a^{-1} = R_{-a}$.

(iii) If $(Q, +)$ is a group, then $R_d = L_d I_d$, where I_d is the inner automorphism of the group $(Q, +)$, i.e., $I_d x = -d + x + d$ for all $x \in Q$.

Proof. (i) We have $\varphi L_a x = \varphi(a \cdot x) = \varphi a \cdot \varphi x = L_{\varphi a}\varphi x$, $\varphi R_b x = \varphi(x \cdot b) = \varphi x \cdot \varphi b = R_{\varphi b}\varphi x$.

(ii) $L_a R_b x = a + (x + b) = (a + x) + b = R_b L_a x$. $L_a^{-1} = L_{-a}$ since $L_a^{-1} L_a x = x = -a + a + x = L_{-a} L_a x$.

(iii) $R_d x = x + d = d - d + x + d = L_d I_d x$. □

Theorem 1.123. *Generalized Albert theorem. If $(Q, \circ) = (Q, \cdot)(\alpha, \beta, \varepsilon)$, $(Q, \cdot)$ is a group, and $(Q, \circ)$ is a loop, then $(Q, \circ)$ is a group isomorphic to group $(Q, \cdot)$ [80, 10, 11, 72, 548, 685, 779].*

Proof. By Lemma 1.121 $\alpha = R_a^{-1}$, $\beta = L_b^{-1}$. However in a group $R_a^{-1} = R_{a^{-1}}$, $L_b^{-1} = L_{b^{-1}}$ (Lemma 1.122).

Therefore $x \circ y = R_a^{-1} x \cdot L_b^{-1} y = x a^{-1} \cdot b^{-1} y = x(a^{-1} b^{-1}) y$. Denote the element $a^{-1} b^{-1}$ as c. Then $(x \circ y) \cdot c = (x \cdot c) \cdot (y \cdot c)$, $R_c(x \circ y) = R_c x \cdot R_c y$.

Hence $(Q, \circ) \cong (Q, \cdot)$. If $a \cdot b = 1$, then $(Q, \circ) = (Q, \cdot)$. □

Exercise 1.124. Find the form of isotopy between quasigroups from Example 1.34.

1.3.2 Group action

We recall some definitions from [334, 471, 911].

Definition 1.125. A group G acts on a set M if for any pair of elements (g, m), $g \in G, m \in M$, an element $(gm) \in M$ is defined. Moreover, $g_1(g_2(m)) = (g_1 g_2)m$ and $em = m$ for all $m \in M$, $g_1, g_2 \in G$. Here e is the identity element of the group G.

The set $Gm = \{gm \mid g \in G\}$ is called an orbit of element m. For every m in M, we define the stabilizer subgroup of m as the set of all elements in G that fix m: $G_m = \{g \mid gm = m\}$.

Theorem 1.126. *Let x and y be two elements in M, and let g be a group element such that $y = g(x)$. Then the two stabilizer groups G_x and G_y are related by $G_y = g G_x g^{-1}$ [911].*

Proof. By definition, $h \in G_y$ if and only if $h(g(x)) = g(x)$. Applying g^{-1} to both sides of this equality yields $(g^{-1} h g)(x) = (g^{-1} g)(x) = x$; that is, $g^{-1} h g \in G_x$. □

The aforesaid gives us that the stabilizers of elements in the same orbit are conjugate to each other. Thus, one can associate a conjugacy class of a subgroup of G (i.e., the set of all conjugates of the subgroup) to each orbit.

The orbits of any two elements of the set M coincide or are not intersected. Then the set M is divided into a set of non-intersected orbits. In other words, if we define a binary relation $\sim$ on the set M as:

$$m_1 \sim m_2 \text{ if and only if there exists } g \in G \text{ such that } m_2 = gm_1,$$

then $\sim$ is an equivalence relation on the set M.

Every orbit is an invariant subset of M on which G acts transitively. The action of G on M is transitive if and only if all elements are equivalent, meaning that there is only one orbit.

A partition θ of the set M on disjoint subsets $\theta(x)$, $x \in M$ is called a partition on blocks relative to the group G, if for any $\theta(a)$ and any $g \in G$ there exists a subset $\theta(b)$ such that $g\theta(a) = \theta(b)$. It is obvious that there exist trivial partitions of the set M, namely, partitions into one-element blocks and partitions into unique blocks.

If there does not exist a partition of the set M into non-trivial blocks, then the group G is called primitive.

Definition 1.127. The action of G on M is referred to as follows:

1. Faithful (or effective), if for any two distinct $g, h \in G$ there exists an $x \in M$ such that $g(x) \neq h(x)$; or equivalently, if for any $g \neq e \in G$ there exists an $x \in M$ such that $g(x) \neq x$. Intuitively, different elements of G induce different permutations of M;

2. Free (or semiregular), if for any two distinct $g, h \in G$ and all $x \in M$ we have $g(x) \neq h(x)$; or equivalently, if $g(x) = x$ for some x, then $g = e$;

3. Regular (or simply transitive), if it is both transitive and free; this is equivalent to saying that for any two x, y in M there exists precisely one g in G such that $g(x) = y$. In this case, M is known as a principal homogeneous space for G or as a G-torsor [911].

1.3.3 Isotopism: Another point of view

Here we present another point of view on the concept of isotopism using the concept of action of a group.

Definition 1.128. An ordered $(n+1)$-tuple of permutations (bijections) of a set G is called an *isotopism (an isotopy).*

Lemma 1.129. *Set $\mathfrak{T}$ of all isotopisms of a set Q forms the group $S_Q^{n+1} = S_Q \times S_Q \times \cdots \times S_Q$, which is the direct sum of $(n+1)$ copies of the group S_Q relative to the following operation (componentwise multiplication of $(n+1)$-tuples): $(\mu_1, \mu_2, \ldots, \mu_{n+1}) * (\nu_1, \nu_2, \ldots, \nu_{n+1}) = (\mu_1\nu_1, \mu_2\nu_2, \ldots, \mu_{n+1}\nu_{n+1})$.*

Let $\mathcal{G}$ be a class of all n-ary groupoids (arity is fixed) defined on a set Q. By $\mathcal{Q}$ we denote a quasigroup class defined on the set Q. Define the action of elements of the group $\mathfrak{T}$ on classes $\mathcal{G}, \mathcal{Q}$ in the following way: if (Q, f) is n-ary groupoid, $T = (\nu_1, \nu_2, \ldots, nu_n, n_{n+1}) \in \mathfrak{T}$, then $(Q, f)T = \nu_{n+1}^{-1} f(\nu_1 x_1, \nu_2 x_2, \ldots, \nu_n x_n)$ for all $x_1, x_2, \ldots, x_n$.

Theorem 1.130. *(i) $\mathcal{G}\mathfrak{T} = \mathcal{G}$, (ii) $\mathcal{Q}\mathfrak{T} = \mathcal{Q}$.*

Proof. (i). If (Q, f) is an n-ary groupoid, $T = (\nu_1, \nu_2, \ldots, nu_n, n_{n+1}) \in \mathcal{T}$, then $(Q, f)T$ defines some other n-ary groupoid (Q, g) since the operation $g(x_1^n) = \nu_{n+1}^{-1} f(\nu_1 x_1, \nu_2 x_2, \ldots, \nu_n x_n)$ is defined for all $x_1, \ldots, x_n \in Q$.

(ii). Prove this theorem for the binary case. For n-ary ($n > 2$) the proof is similar. Let $(Q, \cdot)$ be a quasigroup and $T = (\alpha, \beta, \gamma)$ – an isotopy. Prove that operation $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$ is a quasigroup operation. From (i) it follows that $(Q, \circ)$ is a binary groupoid.

For any fixed element x, the map L_x° is a permutation of the set Q, since $L_x^\circ y = \gamma^{-1} L_{\alpha x}^{\cdot} \beta y$ and the product of permutations is a permutation. Similarly, the map $R_y^\circ x = \gamma^{-1} R_{\beta y}^{\cdot} \alpha x$ is a permutation. Taking into consideration Definition 1.28, we conclude that groupoid $(Q, \circ)$ is a quasigroup. □

Corollary 1.131. *Any isotope of a left (right) quasigroup $(Q, \circ)$ is a left (right) quasigroup.*

Remark 1.132. Researches of quasigroup classes closed relative to all isotopisms or isotopisms of a fixed kind (for example, LP-isotopisms) form a direction in quasigroup theory [72, 401, 400, 869, 870, 866].

Quasigroup isotopism has a relatively clear geometrical [76] and automata theory [400] interpretation.

1.3.4 Autotopisms of binary quasigroups

Theorem 1.133. *If n-ary quasigroups (Q, f) and (Q, g) are isotopic with isotopy T, i.e., $(Q, f) = (Q, g)T$, then $Avt\,(Q, f) = T^{-1} Avt\,(Q, g) T$ [77].*

Proof. Quasigroups (Q, f) and (Q, g) are in one orbit (they are isotopic) by action of the group $\mathcal{T}$ on the set $\mathcal{Q}$ of all quasigroups of a fixed arity n. Autotopy groups of these quasigroups are stabilizers of elements (Q, f) and (Q, g) by this action. It is known that stabilizers of elements of a set S from one orbit by action of a group G on the set S are isomorphic [471, 334], moreover, they are conjugate subgroups of the group S_Q^3. □

Automorphisms and automorphism groups of some binary and n-ary quasigroups are studied in many articles, see, for example, [646, 461, 462, 736, 760, 769, 290, 772, 832, 444, 524, 525, 600].

It is clear that any automorphism is an autotopy with equal components. So, if we know the structure of autotopies of a "good" n-ary quasigroup (Q, f) and the form of isotopy T, then we have a possibility to obtain information on autotopies and automorphisms of n-ary quasigroup $(Q, g) = (Q, f)T$.

This observation was used by the study of automorphism groups of quasigroups isotopic to groups in [762].

In the binary case, Theorem 1.133 allows us (up to isomorphism) to reduce the study of autotopy group of a quasigroup to the study of autotopy group of an LP-isotope of this quasigroup, i.e., to the study of autotopy group of a loop.

Definition 1.134. An autotopism (sometimes we shall refer to autotopism as autotopy) is an isotopism of a quasigroup $(Q, \cdot)$ into itself, i.e., a triple (α, β, γ) of permutations of the set Q is an autotopy if the equality $x \cdot y = \gamma^{-1}(\alpha x \cdot \beta y)$ is fulfilled for all $x, y \in Q$.

We denote the set of all autotopies of a quasigroup $(Q, \cdot)$ as $Avt\,(Q, \cdot)$. It is clear that the defined on this set (on the set $Avt\,(Q, \cdot)$) operation $\star$ of autotopies multiplication

$$(\alpha_1, \beta_1, \gamma_1) \star (\alpha_2, \beta_2, \gamma_2) = (\alpha_1 \alpha_2, \beta_1 \beta_2, \gamma_1 \gamma_2)$$

is a group operation. Then we have a possibility to speak on the group $(Avt(Q, \cdot), \star)$. This

group has more than one denotation. The following denotation $Top(Q,\cdot)$ of the group of autotopism of a quasigroup $(Q,\cdot)$ will be also used.

Lemma 1.135. *The set of all the first (second, third) components of autotopies of a quasigroup $(Q,\cdot)$ forms a group.*

We shall denote the group of all the first components of autotopisms of a quasigroup $(Q,\cdot)$ as $AC_1(Q,\cdot)$ (the letters "A"and "C"are initial letters of the words autotopy component), of all the second components as $AC_2(Q,\cdot)$, and the set of all the third ones as $AC_3(Q,\cdot)$. The group $AC_3(Q,\cdot)$ is called the group of quasiautomorphisms of a quasigroup $(Q,\cdot)$.

Definition 1.136. The third component of any autotopism is called a *quasiautomorphism.*

Lemma 1.137. *If T is a quasigroup autotopy, then its two components uniquely determine the third one.*

Proof. If (α_1,β,γ) and (α_2,β,γ) are autotopies, then $(\alpha_2^{-1},\beta^{-1},\gamma^{-1})$ is an autotopy and $(\alpha_1\alpha_2^{-1},\ \beta\beta^{-1},\gamma\gamma^{-1}) = (\alpha_1\alpha_2^{-1},\varepsilon,\varepsilon)$ is an autotopy too. We can re-write the last form of autotopy in this form: $\alpha_1\alpha_2^{-1}x\cdot y = x\cdot y$, then $\alpha_1=\alpha_2$.

If $(\varepsilon,\varepsilon,\gamma_1\gamma_2)$ is an autotopy, then we have $x\cdot y = \gamma_1\gamma_2^{-1}(x\cdot y)$. If we put in the last equality $y=e(x)$, then we obtain $x=\gamma_1\gamma_2^{-1}x$ for all $x\in Q$, i.e., $\gamma_1=\gamma_2$. □

Corollary 1.138. *If two components of a quasigroup autotopy are identity mappings, then the third component is also an identity mapping.*

Proof. The proof follows from Lemma 1.137 because in any quasigroup there exists identity autotopy $(\varepsilon,\varepsilon,\varepsilon)$. □

A stronger result than Lemma 1.137 is proved by I.V. Leakh [580].

Theorem 1.139. *Leakh theorem. Any autotopy $T=(\alpha_1,\alpha_2,\alpha_3)$ of a quasigroup $(Q,\circ)$ is uniquely defined by its autotopy component α_i, $i\in\{1,2,3\}$, and by element $b=\alpha_j a$, where a is any fixed element of set Q, $i\neq j$ [580].*

Proof. Case 1. $i=1, j=2$. If we have autotopies $(\alpha,\beta_1,\gamma_1)$ and $(\alpha,\beta_2,\gamma_2)$ such that $\beta_1 a=\beta_2 a=b$, then we have $\alpha x\circ\beta_1 a=\gamma_1(x\circ a)$ and $\alpha x\circ\beta_2 a=\gamma_2(x\circ a)$. Since the left sides of the last equalities are equal, then we have $\gamma_1(x\circ a)=\gamma_2(x\circ a)$, $\gamma_1 R_a x=\gamma_2 R_a x$, $\gamma_1=\gamma_2$ and by Lemma 1.137, $\beta_1=\beta_2$.

Case 2. $i=1, j=3$. Suppose there exist autotopies $(\alpha,\beta_1,\gamma_1)$ and $(\alpha,\beta_2,\gamma_2)$ such that $\gamma_1 a=\gamma_2 a=b$ for some fixed element $a\in Q$. Since $(Q,\circ)$ is a quasigroup, then for any element $x\in Q$ there exists a unique element $x'\in Q$ such that $x\circ x'=a$. Using the concept of middle quasigroup translation we can re-write the last equality in the form $P_a x=x'$ and say that P_a is a permutation of the set Q.

For all pairs x,x' we have $\alpha x\circ\beta_1 x'=\gamma_1(x\circ x')=b$ and $\alpha x\circ\beta_2 x'=\gamma_2(x\circ x')=b$. Since the right sides of the last equalities are equal, we have $\alpha x\circ\beta_1 x'=\alpha x\circ\beta_2 x'$, $\beta_1 x'=\beta_2 x'$ for all $x'\in Q$. The variable x' takes all values from the set Q since P_a is a permutation of the set Q. Therefore $\beta_1=\beta_2$ and by Lemma 1.137, $\gamma_1=\gamma_2$.

All other cases are proved in a similar way as Cases 1 and 2. □

Lemma 1.140. *If $(Q,\cdot)$ is a loop, then its autotopy has the form*

$$(\alpha,\beta,\gamma)=(R_b^{-1},L_a^{-1},\varepsilon)(\gamma,\gamma,\gamma), \tag{1.35}$$

where $\gamma 1=a\cdot b$, γ is some bijection of the set Q.

Proof. Let $T = (\alpha, \beta, \gamma)$ be an autotopy of a loop $(Q, \cdot)$, i.e., $\alpha x \cdot \beta y = \gamma(x \cdot y)$. If we put $x = 1$, then we obtain $\alpha 1 \cdot \beta y = \gamma y$, $\gamma = L_{\alpha 1}\beta$, $\beta = L_{\alpha 1}^{-1}\gamma$. If we put $y = 1$, then, by analogy, we obtain, $\alpha = R_{\beta 1}^{-1}\gamma$. Then $T = (R_{\beta 1}^{-1}\gamma, L_{\alpha 1}^{-1}\gamma, \gamma) = (R_b^{-1}, L_a^{-1}, \varepsilon)(\gamma, \gamma, \gamma)$, where $\beta 1 = b$, $\alpha 1 = a$. If we put $x = y = 1$, then $\alpha 1 \cdot \beta 1 = \gamma 1$. □

Corollary 1.141. *If $(Q, \cdot)$ is a loop, then any its autotopy has the form*

$$(\alpha, \beta, \gamma) = (\gamma, \gamma, \gamma)(R_b, L_a, \varepsilon), \tag{1.36}$$

where γ is some bijection of the set Q.

Proof. We use Lemma 1.140. We have

$$\begin{aligned}(\alpha_1, \beta_1, \gamma_1) = T^{-1} = (\alpha^{-1}, \beta^{-1}, \gamma^{-1}) \overset{(1.35)}{=} (\gamma^{-1}, \gamma^{-1}, \gamma^{-1})(R_b, L_a, \varepsilon) = \\ (\gamma^{-1}, \gamma^{-1}, \gamma^{-1})(R_b, L_a, \varepsilon).\end{aligned} \tag{1.37}$$

□

Remark 1.142. In some articles, loop autotopy presented in the form (1.36) is called crypto-automorphism. See for example [6].

Theorem 1.143. *The order of autotopy group of a finite quasigroup Q of order n is a divisor of the number $n! \cdot n$.*

Proof. The proof follows from Theorem 1.133 (we can prove the loop case), Lemma 1.137 and Lemma 1.140 (we can take the second and the third components of loop autotopy). □

Example 1.144. The order of autotopy group of the group $Z_2 \times Z_2$ is equal to $4 \cdot 4 \cdot 6 = 4! \cdot 4$, i.e., in this case the order of autotopy group is equal to the upper bound.

There exist quasigroups (loops) with identity autotopy group [245], i.e., $|Avt(Q, \cdot)| = 1$.

Example 1.145. We give examples of such loops of order seven and nine. In this case the autotopy group is of minimal order. The proof is based on the analyses of cycle structure of quasigroup (loop) translations.

·	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	1	7	6	4	5	3
3	3	6	1	2	7	4	5
4	4	5	2	1	3	7	6
5	5	7	4	3	6	2	1
6	6	3	5	7	2	1	4
7	7	4	6	5	1	3	2

·	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	3	1	8	6	7	5	9	4
3	3	1	2	9	7	5	6	4	8
4	4	5	6	7	9	8	1	3	2
5	5	6	4	2	1	9	8	7	3
6	6	4	5	3	8	1	9	2	7
7	7	8	9	5	3	2	4	6	1
8	8	9	7	1	4	3	2	5	6
9	9	7	8	6	2	4	3	1	5

Lemma 1.146. *For any loop autotopy (α, β, γ) the following equality is true*

$$(\alpha, \beta, \gamma) = (R_b^{-1}, R_b^{-1}, R_b^{-1})(\varepsilon, R_b, R_b)(L_a, \varepsilon, L_a)(L_a^{-1}, L_a^{-1}, L_a^{-1})(\gamma, \gamma, \gamma), \tag{1.38}$$

where $a = \alpha 1$, $b = \beta 1$.

Proof. In order to check equality (1.38) it is sufficient to multiply factors in the right side of this equality and to compare the obtained result with the right side of equality (1.35). □

Remark 1.147. Notice in the conditions of Lemma 1.146 that $\gamma 1 = \alpha 1 \cdot \beta 1$. Comparison of Lemma 1.146 and Theorem 1.148 demonstrates that in the decomposition of autotopies of a loop and a group there are triples corresponding to the elements of the left and right nucleus.

We can obtain more detailed information on autotopies of a group, and since autotopy groups of isotopic quasigroups are isomorphic, on autotopies of quasigroups that are group isotopes.

Theorem 1.148. *Any autotopy of a group $(Q,+)$ can be decomposed in the following product of autotopies:*

$$(L_a\delta, R_b\delta, L_aR_b\delta) = (L_a, \varepsilon, L_a)(\varepsilon, R_b, R_b)(\delta, \delta, \delta), \tag{1.39}$$

where L_a is a left translation of the group $(Q,+)$, R_b is a right translation of this group, and δ is an automorphism of the group $(Q,+)$ [80].

Proof. Let $T = (\alpha, \beta, \gamma)$ be an autotopy of a group $(Q,+)$, i.e., for all $x, y \in Q$ the following equality

$$\alpha x + \beta y = \gamma(x + y) \tag{1.40}$$

is true.

If in equality 1.40 we put $x = y = 0$, then we obtain $\alpha 0 + \beta 0 = \gamma 0$.

If in equality 1.40 we put only $x = 0$, then $\alpha 0 + \beta y$, $L_{\alpha 0}\beta = \gamma$, $\beta = L_{-\alpha 0}\gamma$.

If in equality 1.40 we put only $y = 0$, then $\alpha x + \beta 0 = \gamma x$, $R_{\beta 0}\alpha = \gamma$, $\alpha = R_{-\beta 0}\gamma$.

Now we can re-write equality 1.40 in this form: $R_{-\beta 0}\gamma x + L_{-\alpha 0}\gamma y = \gamma(x + y)$, i.e., $\gamma x - \beta 0 - \alpha 0 + \gamma y = \gamma(x + y)$. Denote $-\beta 0 - \alpha 0$ as c, and it is easy to conclude that $-c = \alpha 0 + \beta 0$. From the last equality we have $\gamma x + c + \gamma y + c = \gamma(x + y) + c$, i.e., $R_c\gamma$ is an automorphism of the group $(Q,+)$.

Let $\theta = R_c\gamma$. Then $\gamma = R_{-c}\theta$, $\alpha x = R_{-\beta 0}\gamma x = R_{-\beta 0}R_{-c}\theta x = \theta x + \alpha 0 + \beta 0 - \beta 0 = \theta x + \alpha 0 = \alpha 0 - \alpha 0 + \theta x + \alpha 0 = L_{\alpha 0}I_{\alpha 0}\theta x$, where $I_{\alpha 0}x = -\alpha 0 + x + \alpha 0$ is an inner automorphism of the group $(Q,+)$.

Similarly,

$$\beta x = L_{-\alpha 0}\gamma x = L_{-\alpha 0}R_{-c}\theta x = -\alpha 0 + \theta x + \alpha 0 + \beta 0 = R_{\beta 0}I_{\alpha 0}\theta x.$$

We can also write the permutation γ in the following form: $\gamma x = \theta x + \alpha 0 + \beta 0 = \alpha 0 - \alpha 0 + \theta x + \alpha 0 + \beta 0 = L_{\alpha 0}R_{\beta 0}I_{\alpha 0}\theta x$.

If we rename $\alpha 0$ as a, $\beta 0$ as b, and $I_{\alpha 0}\theta$ as δ, then we obtain the following form of any autotopy of a group $(Q,+)$:

$$(L_a\delta, R_b\delta, L_aR_b\delta).$$

□

Corollary 1.149. *1. If $L_a\delta = L_aR_b\delta$, then $R_b = \varepsilon$. 2. If $R_b\delta = L_aR_b\delta$, then $L_a = \varepsilon$. 3. If $L_a\delta = R_b\delta$, then $a \in C(Q,+)$.*

Proof. 3. We have $a + \delta x + a + \delta y = a + a + \delta x + \delta y$, $\delta x + a = a + \delta x$ for all $x \in Q$. □

Corollary 1.150. *Any group quasiautomorphism has the form $L_d\varphi$, where $\varphi \in Aut(Q,+)$ [769].*

Proof. We have $L_aR_b\,\delta x = a + \delta x + b = a + b - b + \delta x + b = L_{a+b}I_b\,\delta x = L_d\,\varphi$, where $d = a + b$, $\varphi = I_b\delta$, $I_b\,x = -b + x + b$. □