М І Ф

Математика, Інформатика, Фізика: Наука та Освіта, Том 3, № 1 (2026), с. 65–77.
Mathematics, Informatics, Physics: Science and Education, Volume 3, No. 1 (2026), pp. 65–77.
Journal homepage: https://intranet.vspu.edu.ua/miph

UDC 512.548.7

SAC loops and loops of order five

Fedir Sokhatsky

Pidstryhach Institute for Applied Problems of Mechanics and Mathematics,
Department of Algebra, Lviv, Ukraine
fmsokha@ukr.net
https://orcid.org/0000-0003-4969-5651

Abstract. In this article, we continue the analytical research loops of small orders. Namely, we investigate loops of order 5. Recall that an element of a loop is called *unipotent* if its square is the neutral element. A loop is called *unipotent* if all its elements are unipotent. It is well known that there are six loops of order 5 up to isomorphy relation. One of these loops is a semisymmetric anticommutative loop (SAC loop). The following property is true: "*If a unipotent loop is isotopic to an SAC loop, then the components of the isotopism coincide, so the loops are isomorphic.*" Since any SAC loop is unipotent, any isotopism (autotopism) is an isomorphism (respectively, an automorphism) in the class of SAC loops. This property allowed us to describe the isomorphy relation on the isotopes of the SAC loop. As a corollary, we obtain a complete classification of loops of order 5 and their automorphism groups. In addition, we managed to solve the recognition problem for all six loops of order 5. For example, a loop of order 5 is isomorphic to: 1) the group if and only if the squares of all elements are pairwise distinct; 2) SAC loop if and only if it has at least three unipotents.

Keywords: quasigroup, loop, isotope, SAC loop, loops of small orders, loop of order 5.

1. Introduction

Despite the growing use of Latin squares, in particular in such relatively new areas as information coding and encryption, their research is mainly carried out by computer methods and mainly combinatorial properties are studied. And the results of such research are quantitative characteristics and some construction methods [1, 2]. Systematic analytical research of small-order quasigroups is almost missing. So, for example, it is known that the set of loops of order 5 are divided into 6 isomorphy classes and 5 of them are isotopic to each other, but it is not known to which algebraic classes of loops they belong.

e-ISSN 3041-1955 DOI: https://doi.org/10.31652/3041-1955-2026-03-01-06
2020 Mathematics Subject Classification: 20N05, 05B15.

This article is devoted to the systematic study of loops of order 5. In the class of SAC loops, a property holds that is very similar to the corresponding property in the variety of groups: "If a unipotent loop is isotopic to an SAC loop, then the components of the isotopy coincide, so the loops are isomorphic." Recall that an element of a loop is called a unipotent if its square is the neutral element. A loop is called unipotent if all its elements are unipotent. Since any SAC loop is unipotent, in the class of SAC loops any isotopism (autotopism) is an isomorphism (respectively, an automorphism) (Theorem 8). This property allowed us to describe the isomorphism relation on the isotopes of any SAC loop (Lemma 10). If the group of automorphisms of an SAC loop is transitive on the set of pairs of distinct nonzero elements, then the isotopes of the SAC loop are divided into 5 subsets by the isomorphy relation (Theorem 11). Since all nonassociative loops of order 5 are isotopic to an SAC loop, we obtain a complete classification of loops of order 5 and a description of their automorphism groups (Theorem 14). In addition, we managed to solve the recognition problem for all six loops of order 5. For example, a 5-order loop is isomorphic to the group $\mathbb{Z}_5$ if and only if the squares of all elements are pairwise distinct. These results were reported in [6].

2. Preliminaries

Let $(\cdot)$ be a binary operation defined on a set Q. The pair $(Q;\cdot)$ is called a *quasigroup* if for all a and b in Q each of the equations

$$x \cdot a = b, \qquad a \cdot y = b$$

has a unique solution. In this case, the set Q is called a *carrier set* or a *carrier*, and the operation $(\cdot)$ is called an *invertible* or a *quasigroup operation*.

A quasigroup is called a *loop* if it has a *neutral element*, that is, an element e such that $e \cdot x = x \cdot e = x$ for all $x \in Q$. The loop is also called an *e-loop* and is denoted by $(Q;\cdot,e)$. An element a of an e-loop is called: *unipotent* if $a^2 = a \cdot a = e$; *right inverse* to b if $b \cdot a = e$. An element a of a quasigroup is called *idempotent* if $a^2 = a \cdot a = a$. It is clear that only the neutral element is idempotent in a loop.

Isotopy relation. S_Q denotes the symmetry group of the set Q, that is, the group of all bijections of the set Q. Two operations f and g defined on Q are called *isotopic* if there exist bijections α_1, α_2, $\alpha_3 \in S_Q$ such that

$$g(x,y) = \alpha_3 f(\alpha_1^{-1}(x), \alpha_2^{-1}(y))$$

for all x, y in Q, the triplet $\bar{\alpha} := (\alpha_1, \alpha_2, \alpha_3)$ is called an *isotopism*, and α_3 is its *principal component*. These operations are called *isomorphic* if $\alpha_1 = \alpha_2 = \alpha_3$. The operation g is called the *isotope* of the operation f and is denoted by ${}^{\bar{\alpha}}f$. Every operation that is isotopic to an invertible operation is also invertible. The equalities

$${}^{\bar{\alpha}}\left({}^{\bar{\beta}}f\right) = {}^{\bar{\alpha}\bar{\beta}}f, \qquad {}^{\bar{\iota}}f = f, \qquad \bar{\iota} := (\iota,\iota,\iota)$$

imply that the group $S_Q^3 := S_Q \times S_Q \times S_Q$ and the group S_Q act on the set of all binary operations and on the subset Δ of all invertible binary operations defined on Q. Therefore, the sets of all autotopisms $\mathrm{Autt}(f)$ and the sets of all automorphisms $\mathrm{Aut}(f)$ of an operation f are its stabilizers under these actions and therefore they are subgroups of the groups S_Q^3 and S_Q, respectively. The cardinal $m := |Q|$ is called *order* of f where Q is its carrier. If the order is finite, then the carrier is denoted by $Z_m := \{0,1,\dots,m-1\}$ and $\mathbb{Z}_m := (Z_m;+,0)$ denotes the group of integers modulo m.

Lemma 1. *1. Every loop $(Q;*,e)$ of order m is isomorphic to some loop $(Z_m;\star,0)$:*

$$x\star y := \varphi(\varphi^{-1}(x) * \varphi^{-1}(y)),$$

where $\varphi : Q \to Z_m$ is an arbitrary bijection with the property $\varphi(e) = 0$.
2. Every quasigroup $(Q;\star)$ is isotopic to some loop $(Q;\bullet, a\star b)$, where

$$x \bullet y := \rho_b^{-1}(x) \star \lambda_a^{-1}(y),$$

where $\lambda_0(x) := 0\star x$, $\rho_b(x) := x\star b$.

Proof. It is easy to verify. □

Therefore, considering loops of order m up to isomorphism, it suffices to consider 0-loops on the set Z_m.

Let us highlight a well-known trivial statement which is well known as a corollary of Albert's theorem.

Lemma 2. *Every loop isotopic to a group is isomorphic to it. Every isotopism (α,β,γ) of a loop $(A;*,0)$ on a commutative group $(B;+,e)$ has the form*

$$(\alpha,\beta,\gamma) = (R_a\theta, R_b\theta, R_{a+b}\theta)$$

for some elements a, b of the group $(B;+,e)$ and an isomorphism θ of the loop on the group, where $R_a(x) := x + a$.

Proof. Let (α,β,γ) be an isotopism of a loop $(A;*,e)$ onto a commutative group $(B;+,0)$, i.e.

$$\alpha(x) + \beta(y) = \gamma(x * y). \tag{1}$$

Denote $a := \alpha(e)$, $b := \beta(e)$, $c := \gamma(e)$, then $a + b = c$. Let's define

$$\theta_1(x) := -c + \alpha(x) + b, \qquad \theta_2(y) := -b + \beta(y), \qquad \theta(x) := -c + \gamma(x).$$

Substituting the relations in (1) we obtain $\theta_1(x) + \theta_2(y) = \theta(x * y)$. Therefore, $\theta_1 = \theta_2 = \theta$, because $\theta_1(e) = \theta_2(e) = \theta(e) = 0$ and so θ is an isomorphism. □

Theorem 3 ([2])**.** *There exist exactly two loops of order 5 up to isotopy.*

Theorem 4. *Every loop of order $m = 2, 3, 4$ is isomorphic to one of the following group $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$. A loop of order 4 is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ if and only if it is unipotent.*

Quasigroups of order 4 are described in [5, 7].

Theorem 5 ([4])**.** *If Q is a quasigroup of order m and P is its proper subquasigroup of order k, then $2k \leqslant m$.*

3. SAC loops

In this section, we introduce the concept of SAC loops and study some of their properties that allow us to analytically describe all loops of order 5.

Definition 6. A loop $(Q;\circ,0)$ is called:

- *semisymmetric* if it satisfies the identity $x \circ (y \circ x) = y$ or the equivalent identity $(x \circ y) \circ x = y$;
- *anticommutative* if for all distinct nonzero elements $x \circ y \neq y \circ x$ holds. In other words, if it satisfies the condition

$$x \circ y = y \circ x \Leftrightarrow (x = 0 \vee y = 0 \vee x = y);$$

- *SAC loop* if it is semisymmetric and anticommutative. We will denote the SAC loop of order m by $\mathbb{L}_m$ or $\mathbb{L}$.

Let $\mathbb{L} := (Q; \circ, 0)$ be an SAC loop and $a, b \in Q$, then the quasigroup defined by

$$x \underset{ab}{\triangle} y := (b \circ x) \circ (y \circ a) \tag{2}$$

is called (a, b)-*loop* and denoted it by $(Q; \underset{(a,b)}{\triangle}, a \circ b)$. If there is no misunderstanding, we will simplify the notation and write *ab-loop* and $(Q; \underset{ab}{\triangle}, a \circ b)$, respectively. The neutral element in this loop is $a \circ b$. Indeed,

$$(a \circ b) \underset{ab}{\triangle} y = (b \circ (a \circ b)) \circ (y \circ a) = a \circ (y \circ a) = y,$$

$$x \underset{ab}{\triangle} (a \circ b) = (b \circ x) \circ ((a \circ b) \circ a) = (b \circ x) \circ b = x.$$

The defining identities

$$x \circ (y \circ x) = y \quad \text{and} \quad (x \circ y) \circ x = y$$

of semisymmetric loops can be written as $L_x R_x = \iota$ and $R_x L_x = \iota$, i.e.

$$L_x^{-1} = R_x \quad \text{and} \quad R_x^{-1} = L_x.$$

Hence, each translation of a semisymmetric loop has only two directions [8, 9].

Every semisymmetric loop is unipotent. Indeed, if $y = 0$, then $x \circ x = 0$. In other terminology [3], it is a three-sided loop, i.e. its neutral element is left, right and middle neutral. Therefore, all parastrophes of a unipotent loop are loops with the same neutral element.

3.1. Isotopes of SAC loops. It is well known that any loop that is isotopic to a group is also a group that is isomorphic to that group. Here, in Theorem 8, we prove a similar property for SA-loops.

Lemma 7. *Let (α, β, θ) be an isotopism of some e-loop onto the SAC loop $(Q; \circ, 0)$. Then $\alpha = L_b\theta$, $\beta = R_a\theta$, where $a := \alpha(e)$ and $b := \beta(e)$.*

Proof. Let (α, β, θ) be an isotopism of the loop $(A; *, e)$ onto the SAC loop $(Q; \circ, 0)$, i.e.

$$\alpha(x) \circ \beta(y) = \theta(x * y) \tag{3}$$

for all x, y in A. The equality $a \circ b = \theta(e)$ follows from (3) for $x = y = e$. Substituting $y = e$ and $x = e$ in turn, we obtain

$$\alpha = R_b^{-1}\theta = L_b\theta, \qquad \beta = L_a^{-1}\theta = R_a\theta. \tag{4}$$

□

Theorem 8. *Any isotopism of a unipotent loop onto an SAC loop is an isomorphism.*

Proof. Let (α, β, θ) be an isotopism of some unipotent loop $(A; *, e)$ onto an SAC loop $\mathbb{L} := (Q; \circ, 0)$, i.e. the equality (3) holds. By Lemma 7 we obtain

$$L_b\theta(x) \circ R_a\theta(y) = \theta(x * y).$$

Replace x with $\theta^{-1}(x)$ and y with $\theta^{-1}(y)$:

$$(b \circ x) \circ (y \circ a) = \theta(\theta^{-1}(x) * \theta^{-1}(y)). \tag{5}$$

Since the loop $(A;*,e)$ is unipotent, i.e. $u*u=e$ for all u,

$$\theta(\theta^{-1}(x)*\theta^{-1}(x))=\theta(e)=\theta(e*e)\overset{(3)}{=}\alpha(e)\circ\beta(e)=a\circ b.$$

Therefore, the equality (5) for $x=y$ can be written as

$$(b\circ x)\circ(x\circ a)=a\circ b. \tag{6}$$

If $x=0$, then $b\circ a=a\circ b$. As the loop $(Q;\circ,0)$ is anticommutative, then

$$a=0 \quad\vee\quad b=0 \quad\vee\quad a=b.$$

For each of these cases, (6) can be written as

$$(b\circ x)\circ x=b \quad\vee\quad x\circ(x\circ a)=a \quad\vee\quad (a\circ x)\circ(x\circ a)=0,$$

respectively. Using the operation $(\circ)$, we apply: 1) the element x on the left to the first equality; 2) the element x from the right of the second equality; and 3) the element $a\circ x$ from the right of the third equality:

$$x\circ((b\circ x)\circ x)=x\circ b \quad\vee\quad (x\circ(x\circ a))\circ x=a\circ x \quad\vee\quad ((a\circ x)\circ(x\circ a))\circ(a\circ x)=a\circ x.$$

Since the loop $\mathbb{L}$ is semisymmetric,

$$b\circ x=x\circ b \quad\vee\quad x\circ a=a\circ x \quad\vee\quad x\circ a=a\circ x.$$

The value of the variable x can be chosen in such a way that $x\notin\{0,a,b\}$. Therefore, from the first equality it follows that $b=0$, and from the second and third $a=0$. Therefore, each of these three cases leads to the equalities $a=b=0$ and therefore the equalities $\alpha=L_b\theta$, $\beta=R_a\theta$ lead to $\alpha=\beta=\theta$, i.e. the isotopism (α,β,θ) is an isomorphism. □

Corollary 9. *Any autotopism of an SAC loop is its automorphism.*

Proof. Each SAC loop is unipotent therefore by Theorem 8, any autotopism of an SAC loop is its automorphism. □

3.2. Isomorphy relation on SAC loops. In this subsection we will give a complete analytical description of the isomorphy relation on loops order 5 using only the fact that they are divided into two isotopy classes. First, we prove the following lemma.

Lemma 10. *Let $\mathbb{L}:=(Q;\circ,0)$ be an SAC loop. Then*

1. *every loop isotopic to a loop $\mathbb{L}$ is isomorphic to some ab-loop;*
2. *the triplet (α,β,θ) is an autotopism of the ab-loop if and only if θ is an automorphism of the loop $\mathbb{L}$ and $\alpha=R_b\theta L_b$, $\beta=L_a\theta R_a$;*
3. *the bijection θ of the set Q is an isomorphism of the operations $\underset{ab}{\triangle}$ and $\underset{a'b'}{\triangle}$ if and only if $a'=\theta(a)$ and $b'=\theta(b)$;*
4. *the bijection θ of the set Q is an automorphism of the operation $\underset{ab}{\triangle}$ if and only if $\theta(a)=a$ and $\theta(b)=b$.*

Proof. **1.** Let a loop $(A;*,e)$ be isotopic to the SAC loop $\mathbb{L}$. It means that there exist bijections α, β, θ of the set A onto the set Q such that the equality (3) holds. Using Lemma 7, we obtain (5), and taking into account notations (2), we have

$$x\underset{ab}{\triangle}y=\theta(\theta^{-1}(x)*\theta^{-1}(y)), \quad \text{i.e.} \quad \theta(x)\underset{ab}{\triangle}\theta(y)=\theta(x*y)$$

for all x, y in Q. Therefore, θ is an isomorphism of the loops $(A;*,e)$ and $(Q;\underset{ab}{\triangle},a\circ b)$.

Let the triplet of bijections α, β, θ of the set Q be an isotopism of the operations $\underset{ab}{\triangle}$ and $\underset{a'b'}{\triangle}$, i.e.

$$\theta\left(x \underset{ab}{\triangle} y\right) = \alpha(x) \underset{a'b'}{\triangle} \beta(y)$$

for all x, $y \in Q$. Using the equality (2), we have

$$\theta\left(L_b(x) \circ R_a(y)\right) = L_{b'}\alpha(x) \circ R_{a'}\beta(y).$$

Replacing x with $L_b^{-1}(x)$ and y with $R_a^{-1}(y)$, we obtain

$$\theta\left(x \circ y\right) = L_{b'}\alpha L_b^{-1}(x) \circ R_{a'}\beta R_a^{-1}(y).$$

Hence, $(L_{b'}\alpha L_b^{-1}, R_{a'}\beta R_a^{-1}, \theta)$ is an autotopism of the SAC loop $\mathbb{L}$. By Theorem 8

$$L_{b'}\alpha L_b^{-1} = R_{a'}\beta R_a^{-1} = \theta. \tag{7}$$

Therefore, θ is an automorphism of the SAC loop $\mathbb{L}$.

2. If the triplet (α, β, θ) is an autotopism of the operation $\underset{ab}{\triangle}$, then for $a' = a$ and $b' = b$ we obtain

$$\alpha = L_b^{-1}\theta L_b = R_b\theta L_b, \qquad \beta = R_a^{-1}\theta R_a = L_a\theta R_a.$$

3. If the triplet (α, β, θ) is an isomorphism of the operations $\underset{a'b'}{\triangle}$ and $\underset{ab}{\triangle}$, then $\alpha = \beta = \theta$ and (7) implies

$$\theta = L_{b'}\theta L_b^{-1} = L_{b'}L_{\theta(b)}^{-1}\theta, \qquad \theta = R_{a'}\theta R_a^{-1} = R_{a'}R_{\theta(a)}^{-1}\theta.$$

Therefore, $L_{b'} = L_{\theta(b)}$, $R_{a'} = R_{\theta(a)}$, which is equivalent to $b' = \theta(b)$, $a' = \theta(a)$.

4. It follows from **3.** when $a' = a$ and $b' = b$. □

Theorem 11. *If the automorphism group of an SAC loop $(Q; \circ, 0)$ is transitive on the set of pairs of distinct nonzero elements, then every loop that is isotopic to $(Q; \circ, 0)$ is isomorphic to exactly one of the following loops:*

$$(Q; \circ, 0), \quad (Q; \underset{01}{\triangle}, 1), \quad (Q; \underset{10}{\triangle}, 1), \quad (Q; \underset{11}{\triangle}, 0), \quad (Q; \underset{23}{\triangle}, 2 \circ 3).$$

Proof. If the automorphism group $Aut(\circ)$ of the SAC loop $(Q; \circ, 0)$ is transitive on the set of pairs of distinct nonzero elements, then the action of the group $Aut(\circ)$ on the set Q^2 has five orbits:

$$\{(0,0)\}, \qquad \{(0,y) \mid y \neq 0\}, \qquad \{(x,0) \mid x \neq 0\},$$

$$\{(x,x) \mid x \neq 0\}, \qquad \{(x,y) \mid 0 \neq x \neq y \neq 0\}.$$

A set of representatives of these orbits are the pairs $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$, $(2,3)$. It remains to use item 3 of Lemma 10. □

4. Loops of order five

Each semisymmetric loop is unipotent since $x \circ x = x \circ (0 \circ x) = 0$. Formally speaking, the smallest order of an SAC loop is 2. We call this case degenerate.

4.1. Elementary properties. In this subsection, we prove some elementary properties of loops of order 5.

Lemma 12. *The smallest order of a nondegenerate SAC loop is 5. The loop* $\mathbb{L}_5 := (Z_5; \circ, 0)$, *where*

$\circ$	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

(8)

is an SAC loop.

Proof. Theorem 4 implies that the loops of the order 2 and 3 are commutative and therefore they are not SAC loops. It is easy to verify that the loop $\mathbb{L}_5$ is anticommutative and satisfies the identity $x \circ (y \circ x) = y$. □

Let $\mathbb{L}_5 := (Z_5; \circ, 0)$ denote the SAC loop given in (8), $L_a(x) := a \circ x$, $R_a(x) := x \circ a$ and S'_4 (A'_4) denotes a symmetric (alternating) group of degree 4, i.e. the group of all (respectively, even) bijections of the set $\{1, 2, 3, 4\}$. Before giving a final theorem in which we describe the basic concepts in each loop of order 5, we prove the following statement.

Lemma 13. *If* a, b *are distinct nonzero elements of the loop* $\mathbb{L}_5$, *then*

(1) $Z_5 = \{0, a, b, a \circ b, b \circ a\}$;
(2) $a \circ (a \circ b) = b \circ a$;
(3) $(a \circ b) \circ (b \circ a) = a$.

Proof. By the condition, the elements 0, a, b are distinct; by the definition of the SAC loop, $a \circ b \neq b \circ a$. Suppose $b \circ a = 0$ or $a \circ b = 0$, but $a \circ a = 0$, therefore $b = 0$. A contradiction. So, $b \circ a \neq 0$ and $a \circ b \neq 0$. Finally, $b \neq a \circ b \neq a$ since $a \circ 0 = a$ and $0 \circ b = b$.

The element $a \circ (a \circ b)$ is not equal to any of the elements 0, a, b, $a \circ b$, therefore $a \circ (a \circ b) = b \circ a$ by item 1. To obtain item 3, we multiply the equality $a \circ (a \circ b) = b \circ a$ by $a \circ b$ on the left and use the semisymmetry identity. □

Theorem 14. *Let* $\mathbb{L}_5 := (Z_5; \circ, 0)$ *be the SAC loop ginen in* (8). *The following statements are true:*

(1) *every autotopism of* $\mathbb{L}_5$ *is its automorphism, namely,*

$$\operatorname{Aut} \mathbb{L}_5 = \{\theta_{ab} \mid \ a \neq b, \ a, b = 1, 2, 3, 4\} = A'_4, \tag{9}$$

$$\text{where} \quad \theta_{ab} := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & a & b & a \circ b & b \circ a \end{pmatrix}; \tag{10}$$

(2) *every loop of order 5 is isomorphic to exactly one of the following loops:*

$$\mathbb{L}_5, \quad (Z_5; \underset{01}{\triangle}, 1), \quad (Z_5; \underset{10}{\triangle}, 1), \quad (Z_5; \underset{11}{\triangle}, 0), \quad (Z_5; \underset{23}{\triangle}, 1), \quad \mathbb{Z}_5. \tag{11}$$

(3) *the autotopism group of the loop* $(Q; \underset{ab}{\triangle})$, *where* $ab \in \{01, 10, 11, 23\}$, *is*

$$\operatorname{Autt} (\underset{ab}{\triangle}) = \{(R_b \theta L_b; \ R_a \theta L_a; \ \theta) \mid \theta \in \operatorname{Aut} \mathbb{L}_5\} \simeq A'_4;$$

(4) *the automorphism group of the loop* $(Z_5; \underset{23}{\triangle}, 1)$ *is trivial:* $\operatorname{Aut} (\underset{23}{\triangle}) = \{\iota\}$;

(5) *the automorphism group of the loop* $(Q; \underset{ab}{\triangle})$, *where* $ab \in \{01, 10, 11\}$, *is*

$$\operatorname{Aut}(\underset{ab}{\triangle}) = \{\iota, (234), (243)\} \simeq A'_3;$$

(6) *each autotopism* (α, β, γ) *of the group* $\mathbb{Z}_5$ *has the form*

$$\alpha(x) = kx + a, \qquad \beta(x) = kx + b, \qquad \gamma(x) = kx + a + b.$$

The group of autotopisms is a subgroup of the group $\mathcal{L} \times \mathcal{L} \times \mathcal{L}$, *where* $\mathcal{L}$ *denotes the group of linear transformations of the field* $\mathbb{Z}_5$.

(7) *Each loop of order 5 has only trivial normal subloops, i.e. they are simple loops; each proper subloop of a loops is a subloops generated by a nonzero unipotent.*

Proof. (1). Theorem 8 implies that every autotopism of an SAC loop is its automorphism. Suppose that φ is an automorphism of the loop $\mathbb{L}_5$ and let $a := \varphi(1)$ and $b := \varphi(2)$, then

$$\varphi(3) \overset{(8)}{=} \varphi(1 \circ 2) = \varphi(1) \circ \varphi(2) = a \circ b,$$

$$\varphi(4) \overset{(8)}{=} \varphi(2 \circ 1) = \varphi(2) \circ \varphi(1) = b \circ a.$$

Therefore, every automorphism can be represented in the form (10).

Vice versa, let a transformation θ_{ab} be defined by the equality (10) for some distinct nonzero elements a and b of the loop $\mathbb{L}_5$. Lemma 13 implies that θ_{ab} is a bijection of the set Z_5. Let us prove that

$$\theta_{ab}(x \circ y) = \theta_{ab}(x) \circ \theta_{ab}(y) \tag{12}$$

is true for all x, y in Z_5. In the cases $x = 0$, $y = 0$, $x = y$ the equality (12) is obvious.

Consider the case $x = 1$. The equality (12) can be written as follows:

$$\theta_{ab}(1 \circ y) = a \circ \theta_{ab}(y).$$

If $y = 2$, then the equality is $a \circ b = a \circ b$. If $y = 3$, then we have the equality $b \circ a = a \circ (a \circ b)$ which is proved in item 2 of Lemma 13. If $y = 4$, then we get $b = a \circ (b \circ a)$, which follows from the identity $x \circ (y \circ x) = y$.

In the cases $x = 2$, $x = 3$ and $x = 4$, the equality (12) can be written as:

$$\theta_{ab}(2 \circ y) = b \circ \theta_{ab}(y), \quad \theta_{ab}(3 \circ z) = (a \circ b) \circ \theta_{ab}(z), \quad \theta_{ab}(4 \circ u) = (b \circ a) \circ \theta_{ab}(u).$$

Let us consider only the non-obvious cases: if $y = 1$, then $a \circ b = b \circ (b \circ a)$; if $z = 2$, then $b \circ a = (a \circ b) \circ b$; if $u = 3$, then $b = (b \circ a) \circ (a \circ b)$. All these items are proved in the Lemma 13. Hence, the trasformation θ_{ab} is an automorphism of $\mathbb{L}_5$.

Therefore, the loop $\mathbb{L}_5$ has as many automorphisms as there are pairs of nonzero elements, i.e. 12. There is only one subgroup in the group S'_4 with 12 elements. Hence, $\operatorname{Aut} \mathbb{L}_5 = A'_4$.

(2). Theorem 3 implies that every loop is isotopic to either the group $\mathbb{Z}_5$ or the SAC loop $\mathbb{L}_5$. If a loop is isotopic to a group, then it is isomorphic to it, therefore it is a group (Lemma 2). Consequently, all nonassociative loops of order 5 are isotopic to SAC loop $\mathbb{L}_5$.

From the just proved item 1) it follows that for any distinct nonzero elements a, $b \in Z_5$ the automorphism θ_{ab} maps the pair (1,2) to an arbitrary pair (a, b) of distinct non-zero elements. Therefore, the automorphism $\theta_{cd}\theta_{ab}^{-1}$ maps the pair (a, b) to the pair (c, d). It means that the automorphism group $\operatorname{Aut} \mathbb{L}_5$ is transitive on the set of all pairs of distinct nonzero elements of the set Z_5. By Theorem 11, every nonassociative loop is isomorphic to exactly one of the specified loops, except $\mathbb{Z}_5$.

(3). Item 2 of Lemma 10.

(4). According to item 4 of Lemma 10, the automorphism of the operation $\underset{23}{\triangle}$ is the bijection φ which satisfies the conditions $\varphi(0) = 0$, $\varphi(2) = 2$, $\varphi(3) = 3$. Consequently, $\varphi(1) = \varphi(2 \circ 3) = \varphi(2) \circ \varphi(3) = 2 \circ 3 = 1$. Hence, $\varphi = \iota$ and

$$\mathrm{Aut}\left(\underset{23}{\triangle}\right) = \{\iota\}.$$

(5). The general form of the automorphism θ of the operations $\underset{01}{\triangle}$, $\underset{10}{\triangle}$, $\underset{11}{\triangle}$ is

$$\varphi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & x & 1 \circ x & x \circ 1 \end{pmatrix}, \quad x = 2, 3, 4.$$

Therefore,

$$\mathrm{Aut}\left(\underset{01}{\triangle}\right) = \mathrm{Aut}\left(\underset{10}{\triangle}\right) = \mathrm{Aut}\left(\underset{11}{\triangle}\right) = \{\iota, (234), (243)\}.$$

(6). It follows from Lemma 2.

(7). Since the order of the normal subloop divides the order of the loop, the loop of order 5 has only trivial normal subloops $\{0\}$ and Z_5. Since the order of its own subquasigroup does not exceed half the order of the quasigroup (Theorem 5), the only proper subloops of loops of order 5 are subloops generated by unipotents. □

4.2. Recognition of loops of order 5. In this subsection, we find a criterion for each of the six loops (11).

Theorem 15. *An arbitrary loop of order 5 is isomorphic to:*

(1) *the group if and only if the squares of all elements are pairwise different;*
(2) *a loop-23 if and only if it has exactly one unipotent and the squares of some other elements coincide;*
(3) *the loop-11 if and only if it has exactly two unipotents and the squares of some other elements coincide;*
(4) *the loop-01 if and only if it has exactly two unipotents, the squares of the other elements are pairwise different and the right inverse of some element is its square;*
(5) *the loop-10 if and only if it has exactly two unipotents, the squares of the other elements are pairwise different, and the right inverse of some nonunipotent is not its square;*
(6) *the SAC loop if and only if it has at least three unipotents.*

Proof. Recall that an element of a loop is called *unipotent* if its square is the unit of the loop. All unipotents is on the main diagonal of the respective Latin square. It is obvious that the number of equal squares (in particular, unipotents) and so distinct suares in a finite loop are

invariant under any isomorphism. The table

unit	square	0	1	2	3	4	the number of unipotents	the number of distinct squares
0	$x+x$	0	2	4	1	3	1	5
1	$x \underset{23}{\triangle} x$	4	1	4	4	0	1	3
0	$x \underset{11}{\triangle} x$	0	0	1	1	1	2	3
1	$x \underset{01}{\triangle} x$	1	1	4	2	3	2	4
1	$x \underset{10}{\triangle} x$	1	1	3	4	2	2	4
0	$x \circ x$	0	0	0	0	0	5	1

and the equalities

$$2 \underset{01}{\triangle} 2^2 = (1\circ 2)\circ 4 = 3\circ 4 = 1, \quad 3 \underset{01}{\triangle} 3^2 = (1\circ 3)\circ 2 = 4\circ 2 = 1, \quad 4 \underset{01}{\triangle} 4^2 = (1\circ 4)\circ 3 = 2\circ 3 = 1,$$

$$2 \underset{10}{\triangle} 2^2 = 2\circ(3\circ 1) = 2\circ 2 = 0, \quad 3 \underset{10}{\triangle} 3^2 = 3\circ(4\circ 1) = 3\circ 3 = 0, \quad 4 \underset{10}{\triangle} 4^2 = 4\circ(2\circ 1) = 4\circ 4 = 0.$$

imply that each of these six operations (11) satisfies exactly one of the conditions given in items (1)–(6).

For example, let consider item (2). Two operations have exactly one unipotent $+$ and $\underset{23}{\triangle}$, but the sequence all squares of $+$ are repetition-free and $0 \underset{23}{\triangle} 0 = 4 = 2 \underset{23}{\triangle} 2$. Therefore, the condition of item 2 uniquely defines the operation $\underset{23}{\triangle}$.

Now, consider item (4). There are two operations which have exactly two unipotents and the squares of the other elements are pairwise different. Those operations are $\underset{01}{\triangle}$ and $\underset{10}{\triangle}$. Moreover, the right inverse to 2 is 2^2: $2 \underset{01}{\triangle} 2^2 = 1$ and none of 2^2, 3^2, 4^2 is the right inverse respectively to 2, 3, 4 under the operation $\underset{10}{\triangle}$. □

Corollary 16. *Let $(Q;\diamond)$ be a quasigroup of order 5 and u be its arbitrary element. Then $(Q;\diamond)$ is a group isotope if and only if the mapping γ_u defined by $\gamma_u(x) := R_u^{-1}(x) \diamond L_u^{-1}(x)$ is a bijection of the set Q.*

Proof. Every quasigroup is isotopic to a loop of the same order (Lemma 1). Theorem 15 implies that every loop is isotopic to either a group or SAC loop.

Since a loop isotopic to a group is also isomorphic to it (Lemma 2), the group and the SA-loop are not isotopic. Lemma 1 implies that the quasigroup $(Q;\bullet)$, where

$$x \bullet y := R_u^{-1}(x) \diamond L_u^{-1}(x), \qquad L_u(x) := u \diamond x, \quad R_u(y) := y \diamond u,$$

is a loop with neutral element $u \diamond u$. In this loop, the square of the element x is equal to $x \bullet x = \gamma_u(x)$. According to Theorem 15, a loop is a group if and only if the squares of all elements are pairwise distinct, i.e. γ_u is a bijection of the set Q. □

4.3. Some applications of Theorem 15. Consider the quasigroups $(Z_5;*,2)$, $(Q;\diamond)$ and $(Z_5;\circledast)$ which are defined by the following Cayley tables:

$*$	0	1	2	3	4
0	4	2	0	1	3
1	3	0	1	4	2
2	0	1	2	3	4
3	1	4	3	2	0
4	2	3	4	0	1

$\diamond$	a	b	c	d	e
a	b	c	a	e	d
c	a	e	d	c	b
b	c	d	b	a	e
e	d	a	e	b	c
d	e	b	c	d	a

$\circledast$	0	1	2	3	4
0	4	3	0	1	2
1	2	1	3	4	0
2	3	2	4	0	1
3	1	0	2	3	4
4	0	4	1	2	3

,

Example 1. To which loop the loop $(Z_5;*,2)$ is isomorphic?

From the Cayley table, it follows that the neutral element of the loop $(Z_5;*,2)$ is 2, therefore only 2 and 3 are unipotents: $2*2=2$ and $3*3=2$. The squares of the elements 0, 1, 4 are respectively equal to 4, 0, 1, therefore they are pairwise distinct. The right inverse of 0 is not its square. Indeed, the element $4=0*0$ and $0*4\neq 2$. Hence, the loop $(Z_5;*,2)$ is isomorphic to the 10-loop.

Example 2. To which loop is isotopic the quasigroup $(Q;\diamond)$?

We use Corollary 16. Consider the case $u=a$, then

$$R_a=\begin{pmatrix} a & b & c & d & e\\ b & a & c & d & e\end{pmatrix},\qquad L_a=\begin{pmatrix} a & b & c & d & e\\ b & c & a & e & d\end{pmatrix}.$$

$$\gamma_a(a)=R_a^{-1}(a)\diamond L_a^{-1}(a)=b\diamond c=b;\qquad \gamma_a(b)=R_a^{-1}(b)\diamond L_a^{-1}(b)=a\diamond a=b.$$

Since $\gamma_a(a)=\gamma_a(b)$, the transformation γ_a is not a bijection of the set Z_5. By Corollary 16, the quasigroup $(Q;\diamond)$ is not isotopic to a group, so it is isotopic to the SAC loop.

Example 3. Is the quasigroup $(Z_5;\circledast)$ a group isotope?

Again, we use Corollary 16. Let $u=0$, then

$$R_0=\begin{pmatrix} 0 & 1 & 2 & 3 & 4\\ 4 & 2 & 3 & 1 & 0\end{pmatrix},\qquad L_0=\begin{pmatrix} 0 & 1 & 2 & 3 & 4\\ 4 & 3 & 0 & 1 & 2\end{pmatrix}.$$

Let's find the values of the function $\gamma_0(x)=R_0^{-1}(x)\circledast L_0^{-1}(x)$, $x=0,1,2,3,4$:

$$\gamma_0(0)=R_0^{-1}(0)\circledast L_0^{-1}(0)=4\circledast 2=1,\quad \gamma_0(1)=R_0^{-1}(1)\circledast L_0^{-1}(1)=3\circledast 3=3,$$
$$\gamma_0(2)=R_0^{-1}(2)\circledast L_0^{-1}(2)=1\circledast 4=0,\quad \gamma_0(3)=R_0^{-1}(3)\circledast L_0^{-1}(3)=2\circledast 1=2,$$
$$\gamma_0(4)=R_0^{-1}(4)\circledast L_0^{-1}(4)=0\circledast 0=4.$$

The quasigroup $(Z_5;\circledast)$ is isotopic to the group $\mathbb{Z}_5$, because all values of the function γ_0 are different.

Conflict of interest and ethics. The author is a member of the editorial board of this journal. To avoid a conflict of interest, the manuscript underwent an appropriate peer-review process by independent reviewers, and the decision on publication was made by an independent editor. The author also declares full adherence to all journal research ethics policies.

Acknowledgements. Theorem 15 of this paper has been inspired by a teaching material of Aleš Drápal in which he discusses loops of order 5. The author thanks Aleš Drápal for agreeing to use his ideas in this paper of mine. The author also declares no special funding for this work.

References

1. Keedwell, A. D., Dénes, J. (2015). *Latin Squares and their Application* (2nd ed.), Elsevier B.V., Amsterdam. https://doi.org/10.1016/C2014-0-03412-0
2. McKay, B.D., Wanless, I.M. (2005). *On the Number of Latin Squares,* Ann. Comb., **9**, 335–344. https://doi.org/10.1007/s00026-005-0261-7
3. Sokhatsky, F. M. (2016). *Parastrophic symmetry in quasigroup theory,* Bull. of DonNU., Ser. A. Natural Sciences, No. 1–2, 70-–83.
4. Wall, D.W. (1957). *Subquasigroups of finite quasigroups,* Pasific Journal of Mathematics, **7** (4), 1711–1714.
5. Sokhatsky, F.M., Krainichuk, H.V., Luzhetsky, V.A. (2024). *Canonical and matrix figuration of quasigroups of the fourth order,* Applied problems of mechanics and mathematics, **22**, 95–105. [in Ukrainian]. https://doi.org/10.15407/apmm2024.22.95-105
6. Sokhatsky, F. (2025). *Quasigroups and loops up to order 5,* ConfQRS-2025: Book of Abstracts (Chisinau, July 2–4, 2025), 41–45.
7. Sokhatsky, F.M., Lutsenko, A.V., Fryz, I.V. (2024). *Construction of Quasigroups with Invertibility Properties,* J. Math. Sci., **279**, 115–132. https://doi.org/10.1007/s10958-024-06999-0
8. Sokhatsky, F., Lutsenko, A. (2020). *Classification of quasigroups according to directions of translations I,* Comment. Math. Univ. Carolin., **61** (4), 567–579. http://dx.doi.org/10.14712/1213-7243.2021.002
9. Sokhatsky, F., Lutsenko, A. (2021). *Classification of quasigroups according to directions of translations II,* Comment. Math. Univ. Carolin., **62** (3), 309–323. http://dx.doi.org/10.14712/1213-7243.2021.021

UDC 512.548.7

SAC лупи і лупи п'ятого порядку

Федір Сохацький

Анотація. У цій статті ми продовжуємо аналітичне дослідження луп малих порядків. А саме, ми досліджуємо лупи порядку 5. Нагадаємо, що елемент лупи називається *уніпотентним*, якщо його квадрат нейтральний. Лупа називається *уніпотентною*, якщо всі її елементи уніпотентні.

Одна з луп порядку 5 є напівсиметричною антикомутативною лупою (SAC-лупа). Виконується така властивість: «Якщо уніпотентна лупа ізотопна SAC-лупі, то компоненти ізотопії збігаються, отже, лупи ізоморфні». Оскільки будь-яка SAC-лупа є уніпотентною, то будь-який ізотопізм (автотопізм) є ізоморфізмом (відповідно, автоморфізмом) у класі SAC-луп. Ця властивість дозволила нам описати відношення ізоморфізму на ізотопах SAC-лупи. Як наслідок ми отримуємо повну класифікацію луп порядку 5 та кожну з їхніх груп автоморфізмів. Крім того, нам вдалося вирішити проблему розпізнавання для всіх шести луп порядку 5. Наприклад, лупа порядку 5 ізоморфна: 1) групі тоді і тільки тоді, коли квадрати всіх її елементів попарно різні; SAC лупі тоді і тільки тоді, коли вона має принаймні три уніпотенти.

Ключові слова: квазігрупа, лупа, ізотоп, SAC лупа, квазігрупи малих порядків, лупи малих порядків, лупа порядку 5.

Список використаних джерел

1. Keedwell A. D., Dénes J. Latin Squares and their Application. 2nd ed. Amsterdam: Elsevier B.V., 2015. 424 p. DOI: https://doi.org/10.1016/C2014-0-03412-0
2. McKay B.D., Wanless I.M. On the Number of Latin Squares. *Ann. Comb.* 2005. Vol. 9. P. 335–344. DOI: https://doi.org/10.1007/s00026-005-0261-7

3. Sokhatsky F. M. Parastrophic symmetry in quasigroup theory. *Вісн. ДонНУ., Сер. А. Природничі науки.* 2016. No. 1–2. С. 70–83.
4. Wall D.W. Subquasigroups of finite quasigroups. *Pasific Journal of Mathematics.* 1957. Vol. 7, No. 4. P. 1711–1714.
5. Сохацький Ф.М., Крайнічук Г.В., Лужецький В.А. Канонічні та матричні задання квазігруп четвертого порядку. *Прикладні проблеми механіки та математики.* 2024. Вип. 22. С. 95–105. DOI: https://doi.org/10.15407/apmm2024.22.95-105
6. Sokhatsky F. Quasigroups and loops up to order 5. ConfQRS-2025: Book of Abstracts (Chisinau, July 2–4, 2025). P. 41–45.
7. Sokhatsky F.M., Lutsenko A.V., Fryz I.V. Construction of Quasigroups with Invertibility Properties. *J. Math. Sci.* 2024. Vol. 279. P. 115–132. DOI: https://doi.org/10.1007/s10958-024-06999-0
8. Sokhatsky F., Lutsenko A. Classification of quasigroups according to directions of translations I. *Comment. Math. Univ. Carolin.* 2020. Vol. 61, No. 4. P. 567–579. DOI: http://dx.doi.org/10.14712/1213-7243.2021.002
9. Sokhatsky F., Lutsenko A. Classification of quasigroups according to directions of translations II. *Comment. Math. Univ. Carolin.* 2021. Vol. 62, No. 3. P. 309–323. DOI: http://dx.doi.org/10.14712/1213-7243.2021.021

Про автора / About the author

Федір Сохацький, доктор фізико-математичних наук, старший науковий співробітник, відділ алгебри, Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача Національної академії наук України, вул. Наукова, 3 Б, м. Львів, 79060, Україна;

Fedir Sokhatsky, Doctor of Science in Physics and Mathematics, Senior Researcher, Department of Algebra, Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, National Academy of Sciences of Ukraine, 3-b Naukova Str., Lviv 79060, Ukraine.

Отримано / Received 31.03.2026
Прийнято до друку / Accepted 07.05.2026
Опубліковано / Published 27.05.2026