Proceedings of the International Conference IMCS-60, MSU
October 10–13, 2024, Chisinau, Republic of Moldova

About AC-Groupoids

Vladimir Izbas, Ana-Maria Izbas

Abstract

The concept of a right (left) AC-groupoid over an arbitrary group is defined and studied. Necessary and sufficient conditions which transform a right (left) AC-groupoid into a quasigroup are given. The AC-groupoids form a wide class of special groupoids and quasigroups that have a transitive subset of automorphisms.

Keywords: groupoid, automorphism, quasigroup, group, AC-groupoid.

1 Introduction

The concept of "automorphic by the cyclic group" groupoid (AC-groupoid) was introduced by A. Sade [2]. The author considers the problem of defining a single-valued binary operation ($\times$) on a cyclic group G, such that the mapping $x \to x + t$ is an automorphism of $(G, \times)$ for each t in G. Quasigroups of finite order n, automorphic by the cyclic group, exist for every odd n, does not exist for even n and, could not be groups. Based on the idea of A. Sade [2], we introduse the concepts of right (left) AC-groupoids over an arbitrary group, generalizing the concept of groupoid "automorphic by the cyclic group". The properties of right (left) AC-groupoids are investigated in the present paper, and as a result, a wide class of groupoids with the transitive automorphism group is obtained. We find the conditions when the AC-groupoid is a quasigroup (either idempotent or comutative one). A right AC-quasigroup is constructed over the Frobenius group of order 21 (the smallest non-Abelian group of odd order). Note that AC-quasigroups are of interest for cryptography.

©2024 by Vladimir Izbas, Ana-Maria Izbas

2 Right (left) AC-groupoids

Definition 1. *A groupoid $(Q,*)$ is called a right AC-groupoid (respectively a left AC-groupoid), if there exists a group $(Q,+)$ such that the right translations*

$$R_a^+ : R_a^+(x) = x + a$$

(respectively left translations $L_a^+ : L_a^+(x) = a + x$) of the group $(Q,+)$ are automorphisms of $(Q,*)$.

Theorem 2. *A groupoid $(Q,*)$ is a right AC-groupoid (respectively, left AC-groupoid) over a group $(Q,+)$, if and only if for any $x, y \in Q$ we have*

$$x * y = f(x - y) + y \tag{1}$$

(respectively,

$$x * y = x + g(-x + y)), \tag{2}$$

where $f(x) = x * 0$ (respectively, $g(x) = 0 * x$), 0 is the neutral element of the group $(Q,+)$ and "$-$" is the inverse operation of "$+$".

Proof. Let $(Q,*)$ be a right AC-groupoid over the group $(Q,+)$. As $R_a^+ \in Aut(Q,*)$ for any $a \in Q$, we have

$$x * a = [(x - a) + a] * [(a - a) + a] = [(x - a) + a] * [0 + a] =$$

$$= [(x - a) * 0] + a = f(x - a) + a,$$

for every $x \in Q$. Thus, $x * y = f(x - y) + y$, $\forall x, y \in Q$.

Conversely, if $(Q,+)$ is a group, then $(Q,*)$, defined in (1), is a right AC-groupoid over the group $(Q,+)$. Indeed, for any $a \in Q$ we have

$$(x*y)+a = [f(x-y)+y]+a = f(x-y)+(y+a) = f(x+a-a-y)+(y+a) =$$

$$= f((x + a) - (y + a) + (y + a) = (x + a) * (y + a).$$

So $R_a^+ \in Aut(Q,*)$ for any $a \in (Q,*)$. Thus, the right AC-groupoid $(Q,*)$ is determined by the mapping $f : Q \to Q, f(x) = x * 0$ and

the group $(Q,+)$ with the neutral element 0, by the formula $x * y = f(x-y)+y$, for any $x, y \in Q$. We will denote this groupoid by $(Q, *_f)$ or $(Q, *_f, +, 0)$. For a left AC-groupoid the proof is similar and we will denote the corresponding groupoid by $(Q,_g *)$ or $(Q,_g *, +, 0)$. □

So

$$x *_f y = f(x-y)+y \tag{3}$$

$$x_g * y = x + g(-x+y) \tag{4}$$

for any $x, y \in Q$.

It is clear that two binary operations Δ and ∇ defined on the same set Q are different if and only if there are elements $m, n \in Q$ such that $m\Delta n \neq m\nabla n$.

Theorem 3. *There is a one-to-one correspondence between the set of right AC-groupoids defined over a group $(Q,+)$ and the set $F(Q)$ of all mappings defined on the set Q. For $|Q| = n$ there are exactly n^n right AC-groupoids defined over the group $(Q,+)$.*

Similar statements are true for left AC-groupoids as well.

Theorem 4. *There is a one-to-one correspondence between the set of the left AC-groupoids defined on a group $(Q,+)$ and the set $F(Q)$ of all mappings defined on the set Q. For $|Q| = n$ there are exactly n^n left AC-groupoids defined over the group $(Q,+)$.*

3 Some properties of right (left) AC-groupoids

Proposition 5. *In any right (left) AC-groupoid, defined over a group $(Q,+)$, the mapping $x \to x * x$ is a bijection.*

Remark 6. *In the Cayley table of a finite right (left) AC-groupoid all elements on the main diagonal are different.*

Proposition 7. *An automorphism φ of the group $(Q,+)$ is an automorphism of the right AC-groupoid $(Q, *_f)$ (left AC-groupoid $(Q,_g *)$) if and only if φ and f (respectively φ and g) are commutative, that is, for any $x \in Q$, $\varphi(f(x)) = f(\varphi(x))$ (respectively $\varphi(g(x)) = g(\varphi(x))$).*

Proposition 8. *Let* $(Q, *_f)$ ($(Q,_g *)$) *be a right (left) AC-groupoid defined over a group* $(Q, +)$. *Then* $g(x) = f(-x)+x$, $(f(x) = x+g(-x))$ *for any* $x \in Q$.

Theorem 9. *A right AC-groupoid* $(Q, *_f)$ *(left AC-groupoid* $(Q,_g *)$*), defined over the group* $(Q, +)$ *with the neutral element* 0 *is commutative if and only if* $x *_f 0 = 0 *_f x$ *for any* $x \in Q$ *(respectively,* $0_g * x = x_g * 0$ *for any* $x \in Q$*).*

Proposition 10. *If the group* $(Q, +)$ *has an element of order two, then any right AC-groupoid* $(Q, *_f)$ *(respectively left AC-groupoid* $(Q,_g *)$*) is not commutative.*

Corollary 11. *Any right AC-groupoid* $(Q, *_f)$ *(left AC-groupoid* $(Q,_g *)$*) of even order is not commutative.*

Theorem 12. *A right AC-groupoid* $(Q, *_f)$ *(left AC-groupoid* $(Q,_g *)$*), defined over the group* $(Q, +)$ *with the neutral element* 0 *is idempotent if and only if* $f(0) = 0$ *(respectively* $g(0) = 0$*).*

4 Right (left) *AC*-quasigroups

Theorem 13. *Let* $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) *be a right (left) AC-groupoid defined over the group* $(Q, +)$. *Then:*

1. $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) *is a right-reducible groupoid if and only if the mapping* $f(x) = x * 0$ *is injective;*

2. $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) *is a groupoid with right divisibility if and only if the mapping* $f(x) = x * 0$ *is surjective;*

3. $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) *is a right quasigroup if and only if the the mapping* $f(x) = x * 0$ *is bijective.*

4. $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) *is a groupoid with left reduction if and only if the mapping* $g(x) = 0 * x$ *is injective;*

5. $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) *is a groupoid with left divisibility if and only if the mapping* $g(x) = 0 * x$ *is surjective;*

6. $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) *is a left quasigroup if and only if the the mapping* $g(x) = 0 * x$ *is bijective.*

7. $(Q, *_f, +, 0)$ ($(Q,_g *, +, 0)$) *is a quasigroup if and only if the mappings* $g(x) = 0 * x$ *and* $f(x) = x * 0$ *are bijective.*

Figure 2 contains a right $AC-$quasigroup constructed over the Frobenius group of order 21 given in Figure 1.

°	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	2	0	13	14	12	4	5	3	16	17	15	7	8	6	19	20	18	10	11	9
2	2	0	1	8	6	7	14	12	13	20	18	19	5	3	4	11	9	10	17	15	16
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	0	1	2
4	4	5	3	16	17	15	7	8	6	19	20	18	10	11	9	1	2	0	13	14	12
5	5	3	4	11	9	10	17	15	16	2	0	1	8	6	7	14	12	13	20	18	19
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	0	1	2	3	4	5
7	7	8	6	19	20	18	10	11	9	1	2	0	13	14	12	4	5	3	16	17	15
8	8	6	7	14	12	13	20	18	19	5	3	4	11	9	10	17	15	16	2	0	1
9	9	10	11	12	13	14	15	16	17	18	19	20	0	1	2	3	4	5	6	7	8
10	10	11	9	1	2	0	13	14	12	4	5	3	16	17	15	7	8	6	19	20	18
11	11	9	10	17	15	16	2	0	1	8	6	7	14	12	13	20	18	19	5	3	4
12	12	13	14	15	16	17	18	19	20	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	12	4	5	3	16	17	15	7	8	6	19	20	18	10	11	9	1	2	0
14	14	12	13	20	18	19	5	3	4	11	9	10	17	15	16	2	0	1	8	6	7
15	15	16	17	18	19	20	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	15	7	8	6	19	20	18	10	11	9	1	2	0	13	14	12	4	5	3
17	17	15	16	2	0	1	8	6	7	14	12	13	20	18	19	5	3	4	11	9	10
18	18	19	20	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	18	10	11	9	1	2	0	13	14	12	4	5	3	16	17	15	7	8	6
20	20	18	19	5	3	4	11	9	10	17	15	16	2	0	1	8	6	7	14	12	13

Figure 1.

Acknowledgments. Institutional Research Program of the Moldova State University for 2024-2027, subprogram 011303, has supported part of the research for this paper.

$\times_f$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	2	1	6	17	10	12	11	19	18	5	7	3	20	16	9	14	4	15	8	13
1	2	1	0	11	7	15	20	13	9	8	19	3	17	4	18	5	10	12	14	16	6
2	1	0	2	16	9	8	10	18	14	4	6	20	19	15	5	13	3	11	7	12	17
3	18	11	16	3	5	4	9	20	13	15	14	1	0	8	10	6	2	19	12	17	7
4	17	19	9	5	4	3	14	10	18	2	16	12	11	1	6	20	7	0	8	13	15
5	10	15	20	4	3	5	19	12	11	13	0	17	7	9	2	1	18	8	16	6	14
6	15	20	10	0	14	19	6	8	7	12	2	16	18	17	4	3	11	13	9	5	1
7	11	16	18	20	1	12	8	7	6	17	13	0	5	19	15	14	4	9	2	10	3
8	19	9	17	13	18	2	7	6	8	1	15	14	16	3	20	10	12	5	4	0	11
9	12	8	4	18	2	13	3	17	1	9	11	10	15	5	19	0	20	7	6	14	16
10	5	13	6	14	19	0	2	4	15	11	10	9	20	16	3	8	1	18	17	7	12
11	7	3	14	1	12	20	16	0	5	10	9	11	4	18	17	19	6	2	13	15	8
12	9	17	19	15	11	7	0	5	16	6	20	4	12	14	13	18	8	1	3	2	10
13	20	10	15	8	16	9	17	1	3	5	7	18	14	13	12	2	19	6	11	4	0
14	16	18	11	10	6	17	4	15	2	19	3	8	13	12	14	7	0	20	1	9	5
15	6	15	13	12	20	1	18	14	10	3	8	19	9	2	7	15	17	16	0	11	4
16	14	17	15	7	8	6	19	20	18	10	11	9	1	2	0	13	14	12	4	5	3
17	4	15	16	2	0	1	8	6	7	14	12	13	20	18	19	5	3	4	11	9	10
18	3	14	7	9	8	16	15	2	4	0	17	13	6	11	1	12	5	10	18	20	19
19	8	4	12	17	10	6	5	16	0	14	1	15	2	7	9	11	13	3	20	19	18
20	13	6	5	7	15	11	1	3	17	16	12	2	10	0	8	4	9	14	19	18	20

Figure 2.

References

[1] V. Belousov. *Foundations of quasigroup and loop theory*. Moscow, Nauka, 1967. (in Russian).

[2] A. Sade. *Groupoides automorphes par le groupe cyclique*. Can. J. Math., 1957, vol. 9, pp. 321–335.

Vladimir Izbas[1], Ana Maria Izbas[2]

[1]Vladimir Andrunachievici Institute of Mathematics and Computer Science, USM
E–mail: vladimir.izbas@math.md
ORCID: https://orcid.org/0009-0002-4684-405X

[2] University of Groningen
E–mail: anamaria.izbas@gmail.com