Journal of Prime Research in Mathematics Vol. **11***(2015), 77-84*

ON MULTIPLICATION GROUP OF AN AG-GROUP

M. SHAH[1], A. ALI[2], I. AHMAD[3] AND V. SORGE[4]

Abstract. We are investigating the multiplication group of a special class of quasigroup called AG-group. We prove some interesting results such as: The multiplication group of an AG-group of order n is a non-abelian group of order $2n$ and its left section is an abelian group of order n. The inner mapping group of an AG-group of any order is a cyclic group of order 2.

Key words : multiplication group, inner mapping group, translations.
AMS SUBJECT : Primary 14H50, 14H20, 32S15.

1. Introduction

A groupoid G is an *AG-group* if (i) $(xy)z = (zy)x$ for all $x, y, z \in G$, (ii) There exists left identity $e \in G$ (that is $ex = x$ for all $x \in G$), (iii) For all $x \in G$ there exists $x^{-1} \in G$ such that $x^{-1}x = xx^{-1} = e$. x and x^{-1} are called inverses of each other. AG-group is a subclass of cancellative AG-groupoids [9]. Some basic properties of AG-groups have been derived in [8].

AG-group is a generalization of abelian group and is a special quasigroup. AG-groups have been counted computationally in [11] and algebraically in [10]. The counting of AG-groups up to order 6 can also be found in [1]. AG-groups have been studied as a generalization of abelian group as well as a special case of quasigroups in [10]. The present paper studies the multiplication group and inner mapping group of an AG-group and thus is related to both aspects of AG-group.

[1,2]DEPARTMENT OF MATHEMATICS, QUAID-I-AZAM UNIVERSTY, ISLAMABAD, PAKISTAN.
Email: mshahmaths@gmail.com, Email: dr_asif_ali @hotmail.com
[3]DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MALAKAND, DIR.
Email: iahmaad@hotmail.com
[4]SCHOOL OF COMPUTER SCIENCE, UNIVERSITY OF BIRMINGHAM, UK.
Email: V.Sorge@cs.bham.ac.uk.

Multiplication group and inner mapping group of a loop have been investigated in a number of papers for example [2, 13, 5, 6, 7]. This has always been remained the most interesting topic of group theorists in loop theory. Multiplication group of quasigroup has also been considered in quite a few papers for example [12, 3]. Quasigroup does not have inner mapping group because it does not have an identity element unless it is not a loop. An AG-group though not a loop but has a left identity and thus has a multiplication group as well as an inner mapping group. We will prove here some interesting results about the multiplication group and inner mapping group of an AG-group that do not hold in case of a loop. For example for an AG-group G of order n the L_S is an abelian group of order n. Its multiplication group is a nonabelian group of order $2n$. The inner mapping group of an AG-group is always a cyclic group of order 2 regardless of its order. The following lemma of [8] will be used to prove various results.

Lemma 1. *Let G be an AG-group G. Let $a, b, c, d \in G$ and e is the left identity in G. Then the following conditions hold in G.*

(i) $(ab)(cd) = (ac)(bd)$ *medial law;*
(ii) $ab = cd$. *This implies that* $ba = dc$;
(iii) $a \cdot bc = b \cdot ac$;
(iv) $(ab)(cd) = (db)(ca)$ *paramedial law;*
(v) $(ab)(cd) = (dc)(ba)$;
(vi) $ab = cd$. *This implies that* $d^{-1}b = ca^{-1}$;
(vii) *If e the right identity in G then it becomes left identity in G, i.e,* $ae = a$. *This implies that* $ea = a$;

Let G be an AG-group and $a \in G$ be an arbitrary element. The mapping $L_a : G \to G$ defined by $L_a(x) = ax$ is called left translation on G and the mapping $R_a : G \to G$ defined by $R_a(x) = xa$ is called right translation on G.

Our first result discusses the relations between a left translation and a right translation.

Lemma 2. *Let G be an AG-group. Let $a, b \in G$ and e is left identity in G. Then*

(i) $L_aR_b = R_{ab}$.
(ii) $R_aR_b = L_{ab}$.
(iii) $L_aL_b = R_{(ae)}R_b$.
(iv) $L_aL_b = L_{(ae)b} = L_{(be)a}$.
(v) $R_aL_b = R_{(ae)b}$.
(vi) $L_aL_b = L_bL_a$.
(vii) $R_aL_b = R_bL_a$.

Proof. (i) $L_aR_b(x) = L_a(xb) = a(xb) = x(ab) = R_{ab}(x)$. $\Rightarrow L_aR_b = R_{ab}$.

(ii) $R_aR_b(x) = R_a(xb) = (xb)a = (ab)x = L_{ab}(x)$. $\Rightarrow R_aR_b = L_{ab}$.

(iii) $L_aL_b(x) = L_a(bx) = a(bx) = (ea)(bx) = (xb)(ae) = R_{(ae)}(xb) = R_{(ae)}R_b(x)$. This implies that $L_aL_b = R_{(ae)}R_b$.

(iv) By (ii) and (iii) and left invertive law.

(v) $R_aL_b(x) = R_a(bx) = (bx)a = (bx)(ea) = (ae)(xb) = L_{ae}(xb) = L_{ae}R_b(x)$. This implies that $R_aL_b = L_{ae}R_b$. This implies that $R_aL_b = R_{(ae)b}$ by (i).

(vi) $L_aL_b = L_{(be)a}$ by (iv). This implies that $L_aL_b = L_bL_a$ again by (iv).

(vii) $R_aL_b = R_{(ae)b}$ by (v). This implies that $R_aL_b = R_{(be)a}$ by left invertive law. This implies that $R_aL_b = R_bL_a$ again by (v).

□

Remark 1. *From Lemma 2 we note that if G is an AG-group, then the left translation L_a and the right translation R_a behave like an even permutation and an odd permutation respectively, that is;*

$$L_aL_a = L_a, R_aR_a = L_a, L_aR_a = R_a, R_aL_a = R_a.$$

Next we recall the following definition.

Definition 1. *Let G be an AG-group. Then the set $L_S = \{L_a : L_a(x) = ax \text{ for all } x \in G\}$ is called* ***left section*** *of G and the set $R_S = \{R_a : R_a(x) = xa \text{ for all } x \in G\}$ is called* ***right*** *section of G.*

We remark that left section of a loop is not a group but left section of an AG-group does form a group as the following theorem claims.

Theorem 3. *Let G be an AG-group of order n. Then L_S is an abelian group of order n.*

Proof. By definition $L_S = \{L_a : L_a(x) = ax \text{ for all } x \in G\}$. Let $L_a, L_b \in L_S$ for some $a, b \in G$. Then by Lemma 2 Part(iv), we have $L_aL_b = L_{(ae)b} \in L_S \Rightarrow L_S$ is an AG-groupiod. $L_eL_a = L_{(ee)a} = L_a$ and $L_aL_e = L_{(ae)e} = L_{(ee)a} = L_a$. Therefore, L_e is the identity in L_S.

Let $L_a, L_b, L_c \in L_S$. Consider $(L_aL_b)L_c = L_{(ae)b}L_c = L_{[\{(ae)b\}e]c} = L_{(ce)((ae)b)}$ $= L_{(ce)((be)a)} = L_{(ae)((be)c)} = L_aL_{(be)c} = L_a(L_bL_c)$. Let $L_a \in L_S \Rightarrow a \in G \Rightarrow a^{-1} \in G \Rightarrow a^{-1}e \in G$. Let $a^{-1}e = b$ then $L_b \in L_S$.

Now $L_aL_b = L_{(ae)b} = L_{(ae)(a^{-1}e)} = L_e = L_bL_a \Rightarrow L_b$ is the inverse of L_a. Thus L_S is a group. Since from Lemma 2, we have $L_aL_b = L_bL_a$. Therefore L_S is an abelian group. □

We illustrate the above result by an example.

Example 1. *An AG-group of order* 3 :

$\cdot$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

The Multiplication group of the AG-group given in Example 1 is isomorphic to S_3, the symmetric group of degree 3 as the following example shows.

Example 2. *Multiplication group of the AG-group given in Example 1.*

$\cdot$	L_0	L_1	L_2	R_0	R_1	R_2
L_0	L_0	L_1	L_2	R_0	R_1	R_2
L_1	L_1	L_2	L_0	R_2	R_0	R_1
L_2	L_2	L_0	L_1	R_1	R_2	R_0
R_0	R_0	R_1	R_2	L_0	L_1	L_2
R_1	R_1	R_2	R_0	L_2	L_0	L_1
R_2	R_2	R_0	R_1	L_1	L_2	L_0

Here $L_S = \{L_0, L_1, L_2\}$ which is an abelian group as the following table shows:

$\cdot$	L_0	L_1	L_2
L_0	L_0	L_1	L_2
L_1	L_1	L_2	L_0
L_2	L_2	L_0	L_1

But $R_S = \{R_0, R_1, R_2\}$ does not form an AG-group as the following table shows:

$\cdot$	R_0	R_1	R_2
R_0	L_0	L_1	L_2
R_1	L_2	L_0	L_1
R_2	L_1	L_2	L_0

Remark 2. *Right section does not form even an AG-groupoid.*

Definition 2. *Let G be an AG-group. The set $\langle L_a, R_a : a \in G\rangle$ forms a group which is called multiplication group of the AG-group G and is denoted by $M(G)$ i.e $M(G) = \langle L_a, R_a : a \in G\rangle$.*

Lemma 2 guarantees that for an AG-group G, $M(G) = \langle L_a, R_a : a \in G\rangle = \{L_a, R_a : a \in G\}$

Theorem 4. *Let G be an AG-group of order n. The set $\{L_a, R_a : a \in G\}$ forms a non-abelian group of order $2n$ which is called multiplication group of the AG-group G and is denoted by $M(G)$ i.e $M(G) = \{L_a, R_a : a \in G\}$.*

Proof. From Lemma 2, it is clear that $M(G)$ is closed. L_e plays the role of identity as $L_aL_e = L_eL_a = L_a$ and $R_aL_e = R_{(ae)e} = R_{(ee)a} = R_a = R_{ea} = L_eR_a$. By Theorem 3, $L_a \in M(G)$ has an inverse $L_{a^{-1}} \in M(G)$. Let $R_a \in M(G) \Rightarrow a \in G \Rightarrow a^{-1} \in G \Rightarrow R_{a^{-1}} \in M(G)$ and $R_aR_{a^{-1}} = L_{aa^{-1}} = L_e = L_{a^{-1}a} = R_{a^{-1}}R_a$. Therefore $R_{a^{-1}}$ of R_a is in $M(G)$. Associativity in $M(G)$ follows from the associativity of mappings. Thus $M(G)$ is a group. Note that $M(G)$ is non-abelian because $R_aR_b \neq R_bR_a$. □

To make things a bit more clear, we consider the following example.

Example 3. *An AG-group of order* 4.

$\cdot$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	3	2	1	0
3	2	3	0	1

Its multiplication group is:

Example 4. *Multiplication group of the AG-group in Example 3.*

$\cdot$	L_0	L_1	L_2	L_3	R_0	R_1	R_2	R_3
L_0	L_0	L_1	L_2	L_3	R_0	R_1	R_2	R_3
L_1	L_1	L_2	L_3	L_0	R_3	R_0	R_1	R_2
L_2	L_2	L_3	L_0	L_1	R_2	R_3	R_0	R_1
L_3	L_3	L_0	L_1	L_2	R_1	R_2	R_3	R_0
R_0	R_0	R_1	R_2	R_3	L_0	L_1	L_2	L_3
R_1	R_1	R_2	R_3	R_0	L_3	L_0	L_1	L_2
R_2	R_2	R_3	R_0	R_1	L_1	L_2	L_3	L_0
R_3	R_3	R_0	R_1	R_2	L_2	L_3	L_0	L_1

From Example 3 we observe that: (i) The multiplication group of an AG-group is not necessarily dihedral. For example, $(L_1 \cdot R_3)^2 = R_2^2 = L_3 \neq L_0$. So here $M(G)$ is not D_4. From Examples 1 and 3 we observe that: (ii) The left sections in both the examples are C_3 and C_4 respectively.

Theorem 5. *Let G be an AG-group. Let a be an element of G distinct from e. Then a is self-inverse $\Longleftrightarrow R_a^{-1} = R_a$ is self-inverse.*

Proof. Suppose a is self-inverse. Since $R_a(x) = xa$, then R_a is of order 2, as $R_a(R_a(x)) = (xa)a = (xa)a^{-1} = x$ this implies $R_a^2 = L_e$ this further implies $R_a^{-1} = R_a$.

Conversely let $R_a^2 = L_e$ then $R_a^2(x) = L_e(x)$ for all $x \in G$. This implies that $(xa)a = ex = x$. Now by left invertive law, $a^2x = x$. This by right cancellation implies $a^2 = e$ or $a^{-1} = a$. □

Remark 3. *R_a cannot fix all the elements of AG-group G. For if we suppose that R_a fixes all the elements. That is; $R_a(x) = x$ for all $x \in G$. This implies $xa = x$ for all $x \in G$. Hence a is the right identity and thus G is abelian.*

Theorem 6. *The inner mapping group of every AG-group G is $Inn(G) = \{L_0, R_0\} \cong C_2$.*

Proof. As $R_a(0) = 0a = a$. This implies that only R_0 maps 0 on 0. On the other hand $L_0(0) = 0$ and no other L_a can map 0 on 0. Because let $L_a(0) = 0$ where $a \neq 0$. Then $a0 = 0$. This implies $R_0(a) = 0$. But $R_0(0) = 0$. This implies that R_0 is not a permutation which is a contradiction. Hence $Inn(G) = \{L_0, R_0\} \equiv C_2$. The following table verifies the claim.

$\cdot$	L_0	R_0
L_0	L_0	R_0
R_0	R_0	L_0

Hence the proof. □

Again the following are some quick observations:

(i) The $Inn(G)$ is not necessarily normal in $M(G)$ for example consider the multiplication group of the AG-group given in 3. Here $L_1 \{L_0, R_0\} = \{L_1, R_3\} \neq \{L_1, R_1\} = \{L_0, R_0\} L_1$.

(ii) For every AG-group G, L_S being of index 2 is normal in $M(G)$ and hence $M(G)/L_S \equiv C_2$.

(iii) For every AG-group G, left multiplication group of G coincides with L_S and right multiplication group of G coincides with $M(G)$.

A non-associative quasigroup can be left distributive as well as right distributive but a non-associative AG-group can neither be left distributive nor right distributive as the following theorem shows.

Theorem 7. *Every left distributive AG-group and every right distributive AG-group is abelian group.*

Proof. Let G be a left distributive AG-group. Then for all $a, b, c \in G$, we have

$$\begin{aligned} a(bc) &= (ab)(ac) \\ &= (aa)(bc) \text{ by Lemma 1 Part(i)} \\ \text{which implies that } a &= aa \text{ by right cancellation.} \end{aligned}$$

This further implies that G is an abelian group. The second part is similar. A non-associative quasigroup can be left distributive as well as right distributive but a non-associative AG-group can neither be left distributive nor right distributive as the following theorem shows. □

Theorem 8. *If G is an AG-group then the $M(G)$ cannot be the group of automorphisms of L.*

Proof. Assume that the $M(G)$ is the group of automorphisms of G. It means that every element of $M(G)$ is an automorphism of G. Since $L_a, R_a \in M(G)$ for all $a \in G$. Thus L_a and R_a are both automorphisms of G. So we can write

$$\begin{aligned} (xy)L_a &= (x)L_a \cdot (y)L_a \because L_a \text{ is homomorphism} \\ &\Rightarrow a(xy) = (ax)(ay) \text{ for all } x, y \in G \\ &\Rightarrow G \text{ is left distributive} \end{aligned}$$

Similarly,

$$\begin{aligned} (xy)R_a &= (x)R_a \cdot (y)R_a \because R_a \text{ is homomorphism} \\ &\Rightarrow (xy)a = (xa)(ya) \text{ for all } x, y \in G \\ &\Rightarrow G \text{ is right distributive.} \end{aligned}$$

Thus G is distributive which is a contradiction to Theorem 7. Hence our supposition is wrong and thus $M(G)$ of an AG-group G cannot be the group of automorphisms of G. □

Theorem 9. *Let G be an AG-group and $M(G)$ its multiplication group. Let $x, y \in G$ and e be the identity element in G. Then*

(i) $R_x^{-1} = R_{x^{-1}}$;
(ii) $L_x^{-1} = L_{x^{-1}e}$.

Proof. (i) Since G satisfies right inverse property. Therefore,

$$\begin{aligned} (yx)x^{-1} &= y \\ &\Rightarrow R_{x^{-1}}R_x(y) = y = L_e(y), \forall x, y \in G \\ &\Rightarrow R_{x^{-1}}R_x = L_e \\ &\Rightarrow R_x^{-1} = R_{x^{-1}}. \end{aligned}$$

(ii) By Lemma 2 Part (iv)

$$\begin{aligned} L_x L_{x^{-1}e} &= L_{(xe)(x^{-1}e)} = L_{(xx^{-1})e} = L_e \\ &\Rightarrow L_x^{-1} = L_{x^{-1}e}. \end{aligned}$$

□

Future Work: We have proved that an AG-group G of order n has its multiplication group as a nonabelian group of order $2n$ and its L_S is an abelian group of order n. It is now an interesting question which nonabelian group can occur as a multiplication group of an AG-group G and which cannot and which abelian group can occur as its left section and which cannot. Similar work has been done for loops for example see [4].

References

[1] A. Distler, M. Shah, V. Sorge: *Enumeration of AG-groupoids*, Lecture Notes in Computer Science, 2011, Volume 6824/2011, $1-14$.

[2] A. Drápal: *Multiplication groups of finite loops that fix at most two points*, Journal of Algebra, Volume 235, Issue 1, January 2001, Pages $154-175$.

[3] A. Drápal, *On multiplication groups of relatively free quasigroups isotopic to Abelian groups*, Czechoslovak Mathematical Journal 3-2005, 55(1), $61-86$.

[4] A. Vasanan, *The group $PSL(2,q)$ is not the multiplication group of a loop*, Communications in Algebra, $22(4):1177-1195, 1994$.

[5] M. Niemenmaa: *Finite loops with nilpotent inner mapping groups are centrally nilpotent*, Bulletin of the Australian Mathematical Society $(2009), 79:109-114$.

[6] M. Niemenmaa: *On loops which have dihedral 2-groups as inner mapping groups*, Bulletin of the Australian Mathematical Society $(1995), 52:153-160$.

[7] M. Niemenmaa: *On finite loops whose inner mapping groups are abelian*, Bulletin of the Australian Mathematical Society $(2002), 65:477-484$.

[8] M. Shah, A. Ali: *Some structural properties of AG-groups*, International Mathematical Forum, Vol. $6, 2011$, no. $34, 1661-1667$.

[9] M. Shah, T. Shah, A. Ali: *On the cancellativity of AG-groupoids*, International Mathematical Forum, $6(44):2187-2194, 2011$.

[10] M. Shah: *A theoretical and computational study of AG-groups*, PhD thesis,Quaid-i-Azam University Islamabad, 2012.

[11] M. Shah, C. Gretton, V. Sorge: *Enumerating AG-groups with an introduction to Samarandache AG-groups*, International Mathematical Forum, Vol.$6, 2011, no.62, 3079-3086$.

[12] T. Ihringer: *On multiplication groups of quasigroups*, Europ. J. Combinatorics (1984)5, $137-141$.

[13] T. Kepka: *M. Niemenmaa, On loops with cyclic inner mapping groups*, Archiv der Mathematik, 1993 - Springer,Volume 60, Number $3, 233-236$, DOI: $10.1007/BF01198806$.