Decomposition of AG*-groupoids

Qaiser Mushtaq and Madad Khan

Abstract

We have shown that an AG*-groupoid $S$ has associative powers, and $S/\rho$, where $a\rho b$ if and only if $ab^n = b^{n+1}$, $ba^n = a^{n+1} \forall a,b \in S$, is a maximal separative commutative image of $S$.

An Abel-Grassmann's groupoid [9], abbreviated as an AG-groupoid, is a groupoid $S$ whose elements satisfy the invertive law:

$$(ab)c = (cb)a. \quad (1)$$

It is also called a left almost semigroup [3, 4, 5, 7]. In [1], the same structure is called a left invertive groupoid. In this note we call it an AG-groupoid. It is a useful non-associative algebraic structure, midway between a groupoid and a commutative semigroup, with wide applications in the theory of flocks.

An AG-groupoid $S$ is medial [2], i.e., it satisfies the identity

$$(ab)(cd) = (ac)(bd). \quad (2)$$

It is known [3] that if an AG-groupoid contains a left identity then it is unique. It has been shown in [3] that an AG-groupoid contains a left identity then it is unique. It has been proved also that an AG-groupoid with right identity is a commutative monoid, that is, a semigroup with identity element.

If an AG-groupoid satisfy one of the following equivalent identities:

$$(ab)c = b(ca) \quad (3)$$

$$(ab)c = b(ac) \quad (4)$$

2000 Mathematics Subject Classification: 20M10, 20N99
Keywords: LA-semigroup, AG*-groupoid, invertive law, medial law, congruence.
then it is called an $AG^*$-groupoid [10].

Let $S$ be an $AG^*$-groupoid and a relation $\rho$ be defined in $S$ as follows. For a positive integer $n$, $ab$ if and only if $ab^n = b^{n+1}$ and $ba^n = a^{n+1}$, for all $a$ and $b$ in $S$.

In this paper, we have shown that $\rho$ is a separative congruence in $S$, that is, $a^2\rho a b$ and $ab\rho b^2$ implies that $ab$ when $a, b \in S$.

The following four propositions have been proved in [10].

**Proposition 1.** Every $AG^*$-groupoid has associative powers, i.e., $aa^n = a^n a$ for all $a$.

**Proposition 2.** In an $AG^*$-groupoid $S$, $a^m a^n = a^{m+n}$ for all $a \in S$ and positive integers $m, n$.

**Proposition 3.** In an $AG^*$-groupoid $S$, $(a^m)^n = a^{mn}$ for all $a \in S$ and positive integers $m, n$.

**Proposition 4.** If $S$ is an $AG^*$-groupoid, then for all $a, b \in S$, $(ab)^n = a^n b^n$ and positive integer $n \geq 1$ and $(ab)^n = b^n a^n$ for $n > 1$.

**Theorem 1.** Let $S$ be an $AG^*$-groupoid. If $ab^m = b^{m+1}$ and $ba^n = a^{n+1}$ for $a, b \in S$ and positive integers $m, n$ then $apb$.

**Proof.** For the sake of definiteness assume that $m < n$ and $m > 1$. Then by multiplying, $ab^m = b^{m+1}$ by $b^{-m}$ and successively applying Proposition 1, identities (1) and (2), we obtain

$$
b^{m+1} b^{-m} = (ab^m) b^{-m} = a b^{m-1} b = (b^{m-1} a) b^{-m} = (b^{m-1} a) b^{-m} = b^{m-1} (b^{m-1} a) = b^{m-1} (b^{m-1} a) = \cdots = ab^n.
$$

Thus $ab^n = b^{n+1}$, $ba^n = a^{n+1}$ and so $ab$.

**Theorem 2.** The relation $\rho$ on an $AG^*$-groupoid is a congruence relation.

**Proof.** Evidently $\rho$ is reflexive and symmetric. For transitivity we may proceed as follows.

Let $apb$ and $bpc$ so that there exist positive integers $n, m$ such that,

$$
ab^n = b^{n+1}, \quad ba^n = a^{n+1} \quad \text{and} \quad bc^m = c^{m+1}, \quad cb^m = b^{m+1}.
$$
Let $k = (n+1)(m+1) - 1$, that is, $k = n(m+1) + m$. Using identities (1), (2) and Propositions 2 and 3, we get

$$ac^k = ac^{n(m+1)+m} = a(c^{n(m+1)}c^m) = a((bc^m)^m) = a((bc)^m) = (b^n a)(c^{n(m+1)-1}c)
= (b^n c^{n(m+1)-1})(ac) = ((ac)c^{n(m+1)-1})b^n = (c(ac)^{n(m+1)-1})b^n
= b^{n+1}c^{n(m+1)+1} = c^{(m+1)(n+1)} = c^{k+1}.
$$

Similarly, $ca^k = a^{k+1}$. Thus $\rho$ is an equivalence relation. To show that $\rho$ is compatible, assume that $a \rho b$ such that for some positive integer $n$,

$$ab^n = b^{n+1} \quad \text{and} \quad ba^n = a^{n+1}.
$$

Let $c \in S$. Then by identity (2) and Propositions 4 and 1, we get

$$(ac)(bc)^n = (ac)(b^n c^n) = (ab^n)(c^a) = b^{n+1}c^{n+1}.
$$

Similarly, $(bc)(ac)^n = (ac)^{n+1}$. Hence $\rho$ is a congruence relation on $S$. \hfill \Box

**Theorem 3.** The relation $\rho$ is separative.

**Proof.** Let $a, b \in S$, $abpa^2$ and $abpb^2$. Then by definition of $\rho$ there exist positive integers $m$ and $n$ such that,

$$(ab)(a^2)^m = (a^2)^{m+1}, \quad a^2(ab)^m = (ab)^{m+1},
(ab)(b^2)^n = (b^2)^{n+1}, \quad b^2(ab)^n = (ab)^{n+1}.
$$

Now using identities (3), (2), (1) and Proposition 1, we get

$$ba^{2m+1} = b(a^{2m}a) = (ab)a^{2m} = (ab)(a^m a^m) = (aa^m)(ba^m)
= a^m(ba^m) = (ba^{m+1})a^m = (b(a^m a)a^m = ((a^{m}b)a)a^m
= (a^m a)(a^m b) = (aa^m)(a^m b) = a^m(a^m b)
= a^m((ba)a^m) = ((ba)a^m)a^m = ((a^m b)a)a^m
= (a^{m+1}b)a^m = b(a^{m+1}a^m) = ba^{2m+1} = b(a^{2m}a)
= (ab)a^{2m} = (ab)(a^2)^m = (a^2)^{m+1} = a^{2m+2}.$$
Using identities (3), (2) and (1) and Theorem 2, 3, we get
\[ ab^{2n+1} = a(b^{2n}b) = (ba)b^{2n} = (ba)(b^n b^n) = (bb^n)(ab^n) \]
\[ = (b^n(bb^n))a = ((b^n b^n)b)a = (ab)(b^n b^n) \]
\[ = (ab)(b^{2n}) = (ab)(b^n)^2 = (b^2)^{n+1} = b^{2n+2}. \]

Now by Theorem 1, \( a \rho b \). Hence \( \rho \) is separative.  

The following Lemma has been proved in [10]. We re-state it without proof for use in our later results.

**Lemma 1.** Let \( \sigma \) be a separative congruence on an \( AG^* \)-groupoid \( S \), then for all \( a, b \in S \) it follows that \( a \sigma ba \).

**Theorem 4.** Let \( S \) be an \( AG^* \)-groupoid. Then \( S/\rho \) is a maximal separative commutative image of \( S \).

**Proof.** By Theorem 3, \( \rho \) is separative, and hence \( S/\rho \) is separative. We now show that \( \rho \) is contained in every separative congruence relation \( \sigma \) on \( S \). Let \( a \rho b \) so that there exists a positive integer \( n \) such that,
\[ ab^n = b^{n+1} \quad \text{and} \quad ba^n = a^{n+1}. \]

We need to show that \( a \sigma b \), where \( \sigma \) is a separative congruence on \( S \). Let \( k \) be any positive integer such that,
\[ ab^k \sigma b^{k+1} \quad \text{and} \quad ba^k \sigma a^{k+1}. \]

Suppose \( k \geq 2 \). Putting \( ab^0 = a \) in the next term (if \( k = 2 \))
\[ (ab^{k-1})^2 = (ab^{k-1})(ab^{k-1}) = a^2 b^{2k-2} = (aa)(b^{k-2}b^k) \]
\[ = (ab^{k-2})(ab^k) = (ab^{k-2})b^{k+1}, \]
i.e., \( ab^{k-2})(ab^k) \sigma (ab^{k-2})b^{k+1} \).

Using identity (1) and Proposition 2 we get
\[ (ab^{k-2})b^{k+1} = (b^{k+1}b^{k-2})a = b^{2k-1}a = (b^k b^{k-1})a = (ab^{k-1})b^k, \]
\[ (ab^{k-1})b^k = (b^k b^{k-1})a = b^{2k-1}a = (b^{k-1}b^k)a = (ab^k)b^{k-1}. \]

Thus \( (ab^{k-1})^2 \sigma (ab)^{b^{k-1}}. \)

Since \( ab^k \sigma b^{k+1} \) and \( (ab^k)b^{k-1} \sigma b^{k+1}b^{k-1} \), hence \( (ab^{k-1})^2 \sigma (b^k)^2 \). It further implies that, \( (ab^{k-1})^2 \sigma (ab^{k-1})b^k \sigma (b^k)^2 \). Thus \( ab^{k-1} \sigma b^k \). Similarly, \( ba^{k-1} \sigma a^k \).
Thus if (1) holds for \( k \), it holds for \( k + 1 \). By induction down from \( k \), it follows that (1) holds for \( k = 1 \), \( ab \sigma b^2 \) and \( ba \sigma a^2 \). Hence by Lemma 1 and separativity of \( \sigma \) it follows that \( a \sigma b \).

**Lemma 2.** If \( xa = x \) for some \( x \) and for some \( a \) in an \( AG^* \)-groupoid, then \( x^n a = x^n \) for some positive integer \( n \).

**Proof.** Let \( n = 2 \), then identity (3) implies that
\[
x^2 a = (xx)a = x(xa) = xx = x^2.
\]
Let the result be true for \( k \), that is \( x^k a = x^k \). Then by identity (3) and Proposition 1, we get
\[
x^{k+1} a = (xx^k)a = x^k(xa) = x^k x = x^{k+1}.
\]
Hence \( x^n a = x^n \) for all positive integers \( n \).

**Theorem 5.** Let \( a \) be a fixed element of an \( AG^* \)-groupoid \( S \), then
\[
Q = \{ x \in S \mid xa = x \text{ and } a = a^2 \}
\]
is a commutative subsemigroup.

**Proof.** As \( aa = a \), we have \( a \in Q \). Now if \( x, y \in Q \) then by identity (2),
\[
xy = (xa)(ya) = (xy)(aa) = (xy)a.
\]
To prove that \( Q \) is commutative and associative, assume that \( x \) and \( y \) belong to \( Q \). Then by using identity (1), we get \( xy = (xa)y = (ya)x = yx \), and commutativity gives associativity. Hence \( Q \) is a commutative subsemigroup of \( S \).

**Theorem 6.** Let \( \eta \) and \( \xi \) be separative congruences on an \( AG^* \)-groupoid \( S \) and \( x^2 a = x^2 \), for all \( x \in S \). If \( \eta \cap (Q \times Q) \subseteq \xi \cap (Q \times Q) \), then \( \eta \subseteq \xi \).

**Proof.** If \( x\eta y \), then
\[
(x^2(xy))^2 \eta(x^2(xy))(x^2y^2)\eta(x^2y^2)^2.
\]
It follows that \( (x^2(xy))^2, (x^2y^2)^2 \in Q \). Now by identities (2), (1), (3), respectively and Lemma 2, it means that,
\[
(x^2(xy))(x^2y^2) = (x^2x^2)((xy)y^2) = (x^2x^2)(y^3x) = x^4(y^3x) = (xx^4)y^3 = x^5y^3,
\]
\[
(x^5y^3)a = (x^5y^3)(aa) = (x^5a)(y^3a) = x^5y^3.
\]
So, \(x^2(xy)(x^2y^2) \in Q\). Hence \((x^2(xy))^2 \xi (x^2(xy)(x^2y^2)) \xi (x^2y^2)^2\) implies that \(x^2(xy) \xi x^2y^2\).

Since \(x^2y^2 \eta x^4\) and \(x^2a = x^2\) for all \(x \in S\), so \((x^2y^2), x^4 \in Q\). Thus \(x^2y^2 \xi x^4\) and it follows from Proposition 4 that \(x^2y^2 = (xy)^2\). So \((x^2)^2 \xi (x^2(xy))^2 \xi (xy)^2\) which means that \(x^2 \xi xy\). Finally, \(x^2 \eta y^2\) and \(x^2, y^2 \in Q\), means that \(x^2 \xi y^2, x^2 \xi xy \xi y^2\). As \(\xi\) is separative so \(x \xi y\). Hence \(\eta \subseteq \xi\) and by Lemma 1, \(S/\eta\) is the maximal separative commutative image of \(S\). □

References


Received October 9, 2006
Revised December 18, 2006

Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mail: qmushtaq@isb.apollo.net.pk