THE INVERSE MONOID ASSOCIATED TO A GROUP 
AND THE SEMIDIRECT PRODUCT OF GROUPS 

N. GHADBANE *

ABSTRACT. In this paper, we construct an inverse monoid $M(G)$ 
associated to a given group $G$ by using the notion of the join of 
subgroups and then, by applying the left action of monoid $M$ on 
a semigroup $S$, we form a semigroup $S\omega M$ on the set $S \times M$. 
The finally result is to build the semi direct product of groups 
associated to the group action on another group.

1. INTRODUCTION AND PRELIMINARIES

Semigroups and monoids are convenient algebraic systems for stating 
theorems on groups and playing an important role in algebra and in 
many other branches of science. In semigroup theory, by using the 
actions of semigroups, we can introduce new algebraic structures which 
may employ in other area like computer science. The same is true for 
the wreath product as a specialized product of two groups. It helps 
to construct interesting examples of groups and can be applicable in 
semigroups as well. For example, it is used to prove the theorem on 
the decomposition of every finite semigroup automation into a step wise 
combination of flip-flop and simple group automata. With the help of 
these notions, we introduce new algebraic structures.

In this Section, we recall some requisite definitions and then, in Sec-
tion 2, we construct an inverse monoid $M(G)$ associated to the group 

MSC(2010): Primary: 20M18; Secondary: 20AXX, 20BXX
Keywords: Semigroup, group, idempotents of semigroup, inverses of semigroup, Cayley 
table, symmetric inverse semigroup.
Received: 24 September 2018, Accepted: 4 October 2019.
*Corresponding author.
Let $S$ be a non-empty set. A binary operation on $S$ is a mapping of $S \times S$ into $S$ denoted by a dot "·" such that the image of the ordered pairs $(a, b)$ in $S \times S$ is $a \cdot b$. For the sake of simplicity, we shall omit the dot and write $ab$. A semigroup $S$ is a non-empty set equipped with a binary operation as above such that for all $x, y$ and $z$ of $S$, $(xy)z = x(yz)$. A familiar example of semigroup is the set of functions on a non-empty set $X$ under the operation of composition.

A semigroup $S$ with the identity element is called monoid. By given an arbitrary semigroup $S$, we define $S^1$ to be $S$ if $S$ is a monoid and to be $S \cup \{1\}$ if it is not a monoid where $1x = x1 = x$, for all $x$ in $S$. In this way, $S^1$ is a monoid. An element $e$ in $S$ is called an idempotent if $e^2 = ee = e$. The set of idempotents of $S$ is denoted by $E(S)$. An element $a$ in $S$ is called regular, if and only if $a$ in $aSa$, i.e., $a = axa$ for some $x$ in $S$. A semigroup $S$ is called regular if every element of $S$ is regular. A semigroup $S$ is said to be an inverse semigroup if for every element $a$ in $S$, there is a unique element $a^{-1}$ in $S$ in the sense that $aa^{-1}a = a$ and $a^{-1}aa^{-1} = a^{-1}$. The element $a^{-1}$ is usually called an inverse of $a$ in $S$. We recall that the following conditions on a regular semigroup $S$ are equivalent: (i) idempotents commute and (ii) inverses are unique. We also note that to each $a$ in $S$ there corresponds a pair of idempotents $e$ and $f$ such that

$$aa^{-1} = e, a^{-1}a = f, ea = a, af = a$$

The idempotents $e$ and $f$ are called respectively the left and right units of $a$. Moreover, for any two elements $a, b$ in $S; (ab)^{-1} = b^{-1}a^{-1}$. Alternatively, inverse semigroup are precisely regular semigroups whose idempotents commute.

A subset $T$ of $S$ is an inverse subsemigroup of $S$ if $T$ is closed under the operations of $S$, that is, for all $t_1$ and $t_2$ of $T, t_1t_2$ in $T$ and $t_1^{-1}$ in $T$. If $e$ in $E(S)$ then we denote by $Se$, the inverse subsemigroup $eSe$ (See [8, 13, 1]).

A partial permutation on a set $X$ is a bijection map from a subset of $X$ to a subset of $X$. The set of partial one-to-one transformations on a non-empty set $X$ under the operation of composition is an important example of inverse semigroup. This semigroup is called the symmetric inverse semigroup on $X$ and denoted by $I(X)$. By a theorem of Vagner [15] and Preston [14] every inverse semigroup $S$ is isomorphic to an inverse subsemigroup of $I(X)$ for a suitable set $X$. 

G. Finally, we draw our conclusions in Section 3. Throughout the article, our notations are based on [3, 5, 7] and [11].
Let $S$ be an inverse semigroup. For each $s$ in $S$ take $\tau_s$ in $I(S)$ where $\tau_s(x) = sx$, $x$ in $Ss^{-1}$. Then the mapping $\tau : S \rightarrow I(S)$ defined by $\tau(s) = \tau_s$ is an embedding of $S$ into $I(S)$.

Let $S$ be a semigroup and $M$ be a monoid with 1 as an identity. To simplify notation, we will write $S$ additively, without assuming that $S$ is commutative. A left action of $M$ on $S$ is a mapping of $M \times S$ into $S$ defined by $(m, s) \mapsto ms$ and satisfying for all $s, s_1$ and $s_2$ in $S$, $m, m_1$ and $m_2$ in $M$:

(i) $m(s_1 + s_2) = ms_1 + ms_2$,
(ii) $m_1(m_2s) = (m_1m_2)s$,
(iii) $1s = s$.

Of course, this just amounts to giving a morphism from $M$ to the monoid of endomorphisms acting on the left of $S$. This action is used to form a semigroup $S\omega M$ on the set $S \times M$ with the multiplication defined by $(s, m)(s', m') = (s + ms', mm')$. Note that $S\omega M$ is called a semidirect product of $S$ and $M$ [4]. Moreover, if the elements of $S \times M$ are represented by matrices of the form $\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}$ where $s \in S$ and $m \in M$ then the previous formula can be written as

$$\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s + ms' & mm' \end{pmatrix}.$$ 

If the elements of $S \times M$ are denoted by $(s, m)$, then one can define the product $M\omega S$ by $(m, s)(m', s') = (mm', sm' + s')$. If the elements of $M \times S$ are represented by matrices of the form $\begin{pmatrix} m & 0 \\ s & 1 \end{pmatrix}$ then the formula can be written as

$$\begin{pmatrix} m & 0 \\ s & 1 \end{pmatrix} \begin{pmatrix} m' & 0 \\ s' & 1 \end{pmatrix} = \begin{pmatrix} mm' & 0 \\ sm' + s' & 1 \end{pmatrix}.$$ 

Recall that, if $S$ is a semilattice and let $G$ is a group, then $S\omega M$ is an inverse semigroup for any left action of $G$ on $S$. (See [13, 2, 9, 12])

A group $G$ is an ordered pair $(G, \cdot)$ consisting of a non void set $G$ equipped with a binary operation $\cdot$" which satisfies the following properties:

(i) For all elements $x, y$ and $z$ of $G$, $(xy)z = x(yz)$,
(ii) There exists an element $1_G$ in $G$ such that for all $x \in G$, $1_Gx = x1_G = x$,
(iii) For each $x$ in $G$, there exists an element $x^{-1} \in G$ such that $x^{-1}x = xx^{-1} = 1_G$.

A non empty subset $H$ of a group $G$ is called a subgroup of $G$, denoting by $H \leq G$, if and only if for all $x, y \in H$, $xy \in H$ and $x^{-1}$ in $H$. We may use $Sub(G)$ to stand for the set of all subgroups of the group $G$. 
Theorem 2.1. Let $G$ be a group and let the inclusion $\subseteq$ be totally ordered relation on $\text{Sub}(G)$. Consider the set

$$M(G) = \{Ha : H \subseteq G, a \in G\},$$

and define an operation ”$*$” on $M(G)$ by $Ha*Kb = (H \triangleright aK^{-1})ab$. Then the followings hold:

(i) The set $(H \triangleright aK^{-1})ab$ is the smallest element of $M(G)$ containing the product $HaKb$,
(ii) $(M(G),*)$ is an inverse monoid.
(iii) $\text{Sub}(G)$ is the set of idempotents.

Proof. Since the inclusion relation $\subseteq$ is totally ordered on $\text{Sub}(G)$ then we have $(H \triangleright aK^{-1}) = H$ or $(H \triangleright aK^{-1}) = aK^{-1}$. Moreover, for all $K \in \text{Sub}(G)$ and $a \in G$, $aK^{-1} \in \text{Sub}(G)$ because the set $M(G)$ is closed under the operation $\triangleright$. Let $x = hakb \in HaKb$ arbitrarily where $h$ in $H$ and $k$ in $K$. Since $h$ is an element of $H \subseteq H \triangleright aK^{-1}$ and $aka^{-1} \in aK^{-1} \subseteq H \triangleright aK^{-1}$ so $x = (haka^{-1})ab$ in $(H \triangleright aK^{-1})ab$ which yields that $HaKb \subseteq (H \triangleright aK^{-1})ab$. Let $Lc \in M(G)$ contains $HaKb$. Since $HaKb \subseteq Lc$, $1_G \in H$ and $1_G \in K$ so $1_G a1_G b = ab \in Lc$. Moreover $HaKb \subseteq Lc$ and $1_G \in K$, implies $Hab \subseteq Lc$. On the other hand, $HaKb = (HaK^{-1})ab \subseteq Lc$ and $1_G \in H$ implies $(aK^{-1})ab \subseteq Lc$. Therefore we get $(H \triangleright aK^{-1})ab \subseteq Lc$ which completes the proof of (i). By considering elements $Ha, Kb$ and $Lc$ of $M(G)$ we have

$$((Ha*Kb)\ast Lc = ((H \triangleright aK^{-1})ab)\ast Lc,$$

$$= (H \triangleright aK^{-1}) (abL^{-1}) (ab)c,$$

$$= (H \triangleright aK^{-1} \triangleright abL^{-1}a^{-1}) abc.$$ 

Also, we get

$$Ha \ast (Kb \ast Lc) = Ha \ast (K \triangleright bL^{-1}) bc,$$

$$= (H \triangleright a \triangleright (K \triangleright bL^{-1})a^{-1}) abc,$$

$$= (H \triangleright aK^{-1} \triangleright abL^{-1}a^{-1}) abc.$$
This shows that the operation $*$ is associative and so $M(G)$ is a semigroup. If $Ha \in M(G)$ then

$$Ha \ast \{1_G\} = \{1_G\} \ast Ha = Ha,$$

where $\{1_G\} = \{1_G\} 1_G \in Sub(G) \cap M(G)$. So, the identity element for $(M(G), *)$ is $\{1_G\}$. For the elements $Ha$ and $(a^{-1}Ha) a^{-1}$ of $M(G)$ we have

$$(Ha \ast (a^{-1}Ha) a^{-1)) \ast Ha = (H \ast a (a^{-1}Ha) a^{-1)) aa^{-1} \ast Ha,$$

$$= (H \ast H) 1_G \ast Ha = H \ast Ha = Ha.$$

And

$$(a^{-1}Ha) a^{-1} \ast Ha \ast (a^{-1}Ha) a^{-1} = (a^{-1}Ha) a^{-1},$$

which show that $(a^{-1}Ha) a^{-1}$ is an inverse of $Ha$ in monoid $(M(G), *)$. So the proof of (ii) is completed. For (iii) suppose that $Ha$ is idempotent:

$$Ha = Ha \ast Ha = (H \ast aHa^{-1}) a^2,$$

Then, in particular, $a^2 = 1_G a^2 \in Ha$, i.e. $a^2 = ha$ for some $h \in H$. Hence $a = h \in H$ so $Ha = H$. This means that the idempotents of $(M(G), *)$ are precisely the subgroups of $G$. Since for any two subgroups $H, K$ of $G$, $H \ast K = K \ast H = H \vee K$ thus the idempotents commute and so $(M(G), *)$ is an inverse monoid.

**Remark 2.2.** For each $Ha \in M(G)$, the map $\tau_{Ha} : M(G) \rightarrow M(G)$ defined by $\tau_{Ha}(Kb) = (H \ast aKa^{-1}) ab$ where $Kb \in M(G) \ast (a^{-1}Ha) a^{-1}$ is an element of $I(M(G))$. Moreover, the map $\tau : M(G) \rightarrow I(M(G))$ defined by $\tau(Ha) = \tau_{Ha}$ is an embedding of $M(G)$ into $I(M(G))$.

**Proof.** $(M(G), *)$ is an inverse monoid and by using the inverse of $Ha \in M(G)$, i.e. $(Ha)^{-1} = (a^{-1}Ha) a^{-1}$ the proof is complete. \(\square\)

**Remark 2.3.** (i) For all $H \in Sub(G)$, $H \ast M(G) \ast H$ is the inverse subsemigroup of $(M(G), *)$. (ii) For all $Ha \in M(G)$,

$$Ha \ast (a^{-1}Ha) a^{-1} \ast M(G) \ast Ha \ast (a^{-1}Ha) a^{-1},$$

and

$$(a^{-1}Ha) a^{-1} \ast Ha \ast M(G) \ast (a^{-1}Ha) a^{-1} \ast Ha,$$

are the inverse subsemigroups of $(M(G), *)$.

**Proof.** For (i) we use the fact that $E_{M(G)} = Sub(G)$. (ii) Since for all $Ha \in M(G)$, we have $(Ha)^{-1} = (a^{-1}Ha) a^{-1}$,

$$Ha \ast (a^{-1}Ha) a^{-1} \ast Ha \ast (a^{-1}Ha) a^{-1} \in E_{M(G)},$$
and 
\[(a^{-1}Ha)^{-1} * Ha * (a^{-1}Ha)^{-1} * Ha \in E_{M(G)},\]
so the proof is complete. \(\Box\)

**Theorem 2.4.** Let \(G\) be a group such that for all \(H, K \in \text{Sub}(G), HK = KH\). Define an operation "\(\Delta\)" on \(M(G)\) by \(Ha\Delta Kb = (HK)ab\). Then the followings hold:

(i) \((M(G), \Delta)\) is an inverse monoid.

(ii) \(\text{Sub}(G)\) is the set of idempotents.

**Proof.** (i) Obviously \(M(G)\) is closed with respect to \(\Delta\) since for all \(H, K \in \text{Sub}(G), HK \in \text{Sub}(G)\). If \(Ha, Kb, Lc \in M(G)\) then
\[(Ha\Delta Kb) \Delta Lc = ((HK)ab) \Delta Lc = ((HK) L)(ab)c = (HKL)abc,
And
\[Ha \Delta (Kb \Delta Lc) = Ha \Delta (KL)bc = (H(KL))abc = (HKL)abc,
so the \(\Delta\) is an associative operation.

The identity element in \(M(G)\) is \(\{1_G\}\). Indeed, if \(Ha \in M(G)\) then we have \(Ha\Delta \{1_G\} = \{1_G\} \Delta Ha = Ha\). Since
\[Ha\Delta Ha^{-1} \Delta Ha = HHa^{-1} \Delta Ha = H1_G \Delta Ha = H\Delta Ha = Ha\]
and \(Ha^{-1} \Delta Ha \Delta Ha^{-1} = H^{-1}\), so \(Ha^{-1}\) is an inverse of \(Ha\) in the monoid \((M(G), \Delta)\). Now, suppose that \(Ha\) is idempotent, i.e. \(Ha = Ha\Delta Ha = Ha^2\). Then in particular, \(a^2 = 1_G a^2 \in Ha\), i.e. \(a^2 = ha\) for some \(h \in H\). Hence \(a = h \in H\) and so \(Ha = H\). In fact the idempotents of \((M(G), \Delta)\) are precisely the subgroups of \(G\). For any two subgroups \(H, K\) of \(G\), \(H \Delta K = K \Delta H = HK\). Thus idempotents commute and so \((M(G), \Delta)\) is an inverse monoid. \(\Box\)

**Remark 2.5.** For each \(Ha \in M(G)\), let \(\tau_{Ha} \in I(M(G))\) defined by \(\tau_{Ha}(Kb) = (HK)ab\), for all \(Kb \in M(G)\). Then the mapping \(\tau : M(G) \rightarrow I(M(G))\) defined by \(\tau(Ha) = \tau_{Ha}\) is an embedding of \(M(G)\) into \(I(M(G))\).

**Proof.** The proof yields from the fact that \((M(G), \Delta)\) is an inverse monoid and for \(Ha \in M(G)\), we have \((Ha)^{-1} = Ha^{-1}.\) \(\Box\)

**Remark 2.6.** (i) For all \(H \in \text{Sub}(G), H \Delta M(G) \Delta H\) is the inverse subsemigroup of \((M(G), \Delta)\). (ii) For all \(Ha \in M(G), Ha \Delta Ha^{-1} \Delta M(G) \Delta Ha^{-1},\)
and
\[Ha^{-1} \Delta Ha \Delta M(G) \Delta Ha^{-1} \Delta Ha,
are inverse subsemigroups of \((M(G), \Delta)\).
Theorem 2.7. Let \((S, +, 0)\) and \((M, \cdot, 1)\) be two monoids and consider the left action of \(M\) on \(S\): 
\[
\begin{align*}
M \times S & \longrightarrow S \\
(m, s) & \longmapsto ms,
\end{align*}
\]
such that it satisfies
- \(m (s_1 + s_2) = ms_1 + ms_2\),
- \(m_1 (m_2 s) = (m_1 m_2) s\),
- \(1s = s\),
- \(m0 = 0\).
for all \(s, s_1, s_2 \in S\) and \(m, m_1, m_2 \in M\). Then the followings hold
  
(i) For all \(m \in M\); the map \(\theta_m : S \longrightarrow S, s \longmapsto ms\) is an element of \(\text{End}(S)\),
  
(ii) The map \(\theta : (M, \cdot, 1) \longrightarrow (\text{End}(S), \circ, \text{id}_S), m \longmapsto \theta_m\) is a morphism of monoids.
  
(iii) The set \(S \times M\) with the multiplication \((s, m) (s', m') = (s + ms', mm')\) is a monoid.
  
(iv) If \(K = \{(1_{s_m}, s) \in S, m \in M\}\), then \((K, \times)\) is a monoid.
  
(v) The map \(h : (S \times M, \cdot) \longrightarrow (K, \times), (s, m) \longmapsto (1_{s_m} 0)\) is an isomorphism of monoids.

Proof. For all \(s, s' \in S\), \(\theta (s + s') = m (s + s') = ms + ms' = \theta (s) + \theta (s')\) and \(\theta (0) = m0 = 0\) so \(\theta_m \in \text{End}(S)\) and this proved (i). Since for all \(s \in S\), \(\theta_{mm'} (s) = (mm') s\) and \((\theta_m \circ \theta_{m'}) (s) = \theta_m (m's) = m (m's)\) so \(\theta (mm') = \theta (m) \circ \theta (m)\) where \(m, m' \in M\) which left the part (ii) proved. For (iii), the closure property follows from the definition of multiplication as follows. Take elements \((s, m), (s', m')\) and \((s'', m'')\) of \(S \times M\). Then 
\[
((s, m) (s', m')) (s'', m'') = (s + ms', mm') (s'', m'') = (s + ms' + (mm') s'', (mm') m'').
\]
Also, we have in the same manner that, 
\[
(s, m) ((s', m') (s'', m'')) = (s, m) (s' + m's'', m'm'') = (s + m (s' + m's''), m (m'm'')) = (s + ms' + (mm') s'', m (m'm'')).
\]
Hence the multiplication is associative. Moreover, for all \((s, m) \in S \times M\)
\[
(s, m) \cdot (0, 1) = (0, 1) \cdot (s, m) = (s, m).
\]
This implies that identity element exists so \(S \times M\) is a monoid. For elements \((\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix})\) and \((\begin{pmatrix} 1 & 0 \\ s'' & m'' \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ s''' & m''' \end{pmatrix})\) of \(K\) we have
\[
\begin{align*}
\left[\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix}\right] \times \begin{pmatrix} 1 & 0 \\ s'' & m'' \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ s + ms' & mm' \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s'' & m'' \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ s + ms' + mm's'' & (mm')m'' \end{pmatrix}.
\end{align*}
\]
And
\[
\begin{align*}
\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \times \left[\begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s'' & m'' \end{pmatrix}\right] &= \begin{pmatrix} 1 & 0 \\ s + ms' + mm's'' & (mm')m'' \end{pmatrix}.
\end{align*}
\]
Obviously, the identity element of \((K, \times)\) is \((\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})\). So \((K, \times)\) is a monoid. For (v), it is easy to see that \(h\) is a bijective. Also for all \((s, m), (s', m') \in S \times M:\)
\[

h[(s, m)(s', m')] = h(s + ms', mm') = \begin{pmatrix} 1 & 0 \\ s + ms' & mm' \end{pmatrix},
\]
\[
= \begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix},
\]
\[
= h(s, m) \times h(s', m').
\]

\[\square\]

**Theorem 2.8.** Let \((S, \cdot, 0)\) and \((M, \cdot, 1)\) be two groups. Let the left action of \(M\) on \(S\) \(M \times S \rightarrow S, (m, s) \mapsto ms\) which satisfies the following conditions for all \(s, s_1, s_2 \in S\) and \(m, m_1, m_2 \in M\)

- \(m(s_1 + s_2) = ms_1 + ms_2,\)
- \(m_1(m_2 s) = (m_1m_2)s,\)
- \(1s = s,\)
- \(m0 = 0,\)
- \(m^{-1}(s) = m(-s) = -ms.\)

Then we have

(i) For all \(m \in M, \theta_m : S \rightarrow S, s \mapsto ms, \theta_m \in \text{End}(S),\)

(ii) The mapping \(\theta : (M, \cdot, 1) \rightarrow (\text{End}(S), \circ, \text{id}_S), m \mapsto \theta_m\) is a morphism of groups,

(iii) The set \(S \times M\) with multiplication \((s, m)(s', m') = (s + ms', mm')\) is a group.

(iv) If \(K = \{(\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}, s \in S, m \in M\}, then (K, \times)\) is a group,
(v) The mapping \( h : (S \times M, \cdot) \rightarrow (K, \times), (s, m) \mapsto (1, 0, s, m) \) is an isomorphism of groups.

**Proof.** It is suffices to show that, for each \((s, m) \in S \times M\), there exists \((s', m') \in S \times M\) such that \((s, m)(s', m') = (s', m')(s, m) = (0, 1)\). We have
\[
(s, m)(-m^{-1}s, m^{-1}) = (s + m(-m^{-1}s), mm^{-1}) = (0, 1),
\]
and
\[
(-m^{-1}s, m^{-1})(s, m) = (-m^{-1}s + m^{-1}s, m^{-1}m) = (0, 1).
\]
We also have
\[
\begin{pmatrix}
1 & 0 \\
1 & 0
\end{pmatrix}
\begin{pmatrix}
1 & 0 \\
-m^{-1}s & m^{-1}
\end{pmatrix}
\begin{pmatrix}
1 & 0 \\
1 & 0
\end{pmatrix}
\begin{pmatrix}
1 & 0 \\
1 & 0
\end{pmatrix} = \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}.
\]


\[\square\]

### 3. Conclusion

In this paper, we present some notes on the inverse monoid \( M(G) \) associated to a group \( G \). Also we construct the semidirect product of groups associated to the group action on another group.

### References


Nacer Ghadbane
Laboratory of Pure and Applied Mathematics, Department of Mathematics, University of M’sila, B.P 166, Msila, Algeria.
Email: nasser.ghadbane@univ-msila.dz