Let $A$ be a ring with identity. The generalized affine transformation monoid $\text{Gaff}(A)$ is defined as the set of all transformations on $A$ of the form $x \mapsto xu + a$ (for all $x \in A$), where $u, a \in A$. We study the algebraic structure of the monoid $\text{Gaff}(A)$ on a finite Galois ring $A$. The following results are obtained: an explicit description of Green's relations on $\text{Gaff}(A)$; and an explicit description of the Schützenberger group of every $H$-class, which is shown to be isomorphic to the affine transformation group for a smaller Galois ring.

Copyright © 2006 Hindawi Publishing Corporation. All rights reserved.

1. Introduction and preliminaries

It is interesting to characterize algebra systems by use of semigroup theory. For an algebra system $\Omega$ with underlying set $S$, we consider special subsemigroups of the transformation semigroup on the set $S$, where every transformation in these subsemigroups is dependent on the algebra structure of $\Omega$. The studies of special transformation subsemigroups on $S$ may provide relationships between the algebra structure of $\Omega$ and semigroup theory.

Let $A$ be a ring with identity and $U(A)$ the group of units of $A$. We consider a transformation $\alpha$ on the set $A$ defined by the following: there exist $u, a \in A$ such that $(x)\alpha = xu + a$ for all $x \in A$, and we denote this transformation by $\langle u, a \rangle$ in this paper. If $u \in U(A)$, then $\langle u, a \rangle$ is an affine transformation and $\text{Aff}(A) := \{\langle u, a \rangle \mid u \in U(A), a \in A\}$ is the affine transformation group on the ring $A$ (see [6]). For any $u \in A$, we call $\langle u, a \rangle$ a generalized affine transformation on the ring $A$. If $v, b \in A$, we have $\langle u, a \rangle = \langle v, b \rangle$ if and only if $u = v$ and $a = b$, and that $\langle u, a \rangle \langle v, b \rangle = \langle uv, av + b \rangle$ as transformations on $A$. Let $\text{Gaff}(A) = \{\langle u, a \rangle \mid u, a \in A\}$. Then $\text{Gaff}(A)$ is a monoid with respect to the transformation multiplication. We call $\text{Gaff}(A)$ the generalized affine transformation monoid on the ring $A$. Since the structure of Galois rings has been fully studied, it is easy to determine the explicit structure of generalized affine transformation monoids on Galois rings. So we will study the algebraic structure of the monoid $\text{Gaff}(A)$ on a Galois ring $A$ in this note.

We conclude this section by recalling some of the basic properties of Galois rings. These have been well documented in [5, 7]. There is a number of equivalent descriptions.
of Galois rings: they are the separable extensions of finite, unital, local, commutative rings and the unramified extensions of such rings. Let $T$ be a finite, local, commutative ring with unity and has a maximal ideal $(p)$ for some prime $p$. A polynomial $h(x) \in T[x]$ is called basic irreducible if it is irreducible modulo $p$. We construct the Galois ring as a quotient ring of $\mathbb{Z}_{p^n}[x]$ as follows. Let $n$ and $m$ be positive integers and let $h(x) \in \mathbb{Z}_{p^n}[x]$ be a monic basic irreducible polynomial of degree $m$. The quotient ring $\mathbb{Z}_{p^n}[x]/(h(x))$, denoted $GR(p^n, p^{nm})$, is called the Galois ring of order $p^{nm}$ and characteristic $p^n$. Moreover, the integers $p$, $n$, and $m$ chosen as above determined uniquely (up to isomorphism) the Galois ring $GR(p^n, p^{nm})$ [7, page 207]. For the remainder of the text the symbol $A$ will denote the Galois ring $GR(p^n, p^{nm})$. It is known that all ideals of $A$ are given by $(0) = (p^n) \subset (p^{n-1}) \subset \cdots \subset (p) \subset (p^0) = A$ and that the ideal $(p^i)$, $0 \leq i \leq n$, has cardinality $p^{(n-i)m}$. By [8, Theorem 14.8] there exists an element $\xi \in A$ of multiplicative order $p^m - 1$, which is a root of a basic primitive polynomial $h(x)$ of degree $m$ over $\mathbb{Z}_{p^n}$ and dividing $x^{p^m - 1} - 1$ in $\mathbb{Z}_{p^n}[x]$, and every element $a \in A$ can be written uniquely as $a = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$, $a_0, a_1, \ldots, a_{n-1} \in \mathcal{F}$, where $\mathcal{F} = \{0, 1, \xi, \ldots, \xi^{p^n-2}\}$. Moreover, $a$ is a unit if and only if $a_0 \neq 0$, and $a$ is a zero divisor or $0$ if and only if $a_0 = 0$. Using notation of [2], we define the $p$-exponent of $a$ by $\nu_p(0) = n$ and $\nu_p(a) = i$ if $a = a_i p^i + \cdots + a_0 p^{n-i}$ with $a_i \neq 0$. By [8, Corollary 14.9], $U(A) \cong \langle \xi \rangle \times \{1 + (p)\}$, where $\langle \xi \rangle$ is the cyclic group of order $p^m - 1$ and $1 + (p) = \{1 + x \mid x \in (p)\}$ is the one-group of Galois ring $A$, so $|U(A)| = (p^m - 1)p^{(n-1)m}$.

2. Main results

Let $S$ be a monoid. As in [4], Green’s relations $\mathcal{R}$, $\mathcal{L}$, $\mathcal{J}$, $\mathcal{H}$, and $\mathcal{D}$ are defined on $S$ by $\mathcal{R} := \{(a, b) \in S \times S \mid a S = b S\}$, $\mathcal{L} := \{(a, b) \in S \times S \mid S a = S b\}$, $\mathcal{J} := \{(a, b) \in S \times S \mid S a S = S S b S\}$, $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$, and $\mathcal{D} = \mathcal{R} \vee \mathcal{L}$, respectively. An element $a$ of $S$ is called regular if $axa = a$ for some $x \in S$ [3, page 26]. A $\mathcal{D}$-class $D$ of $S$ is called regular if every element of $D$ is regular [3, page 58]. It is known that a $\mathcal{D}$-class $D$ of a semigroup is regular if $D$ contains a regular element [3, Theorem 2.11]. Now, we list Green’s relations, properties, and structure of the monoid $Gaff(A)$ as follows. Firstly, since $Gaff(A)$ is a finite semigroup, by [4, Proposition 2.3] we have $\mathcal{J} = \mathcal{D}$.

Theorem 2.1. Let $u, v, a, b \in A$. Then

1. $(\langle u, a \rangle \mathcal{R} \langle v, b \rangle)$ in the monoid $Gaff(A) \Rightarrow \nu_p(u) = \nu_p(v)$;
2. $(\langle u, a \rangle \mathcal{L} \langle v, b \rangle)$ in the monoid $Gaff(A) \Rightarrow \nu_p(u) = \nu_p(v)$ and $a \equiv b \mod(p^i)$, where $i = \nu_p(u)$;
3. $\mathcal{H} = \mathcal{L}$ and $\mathcal{D} = \mathcal{R}$;
4. there are exactly $n + 1$ $\mathcal{D}$-classes in $Gaff(A) : D^{(i)} := \{\langle u, a \rangle \mid \nu_p(u) = i, u, a \in A\}$, $i = 0, 1, \ldots, n$;
5. for every $0 \leq i \leq n$, there are exactly $p^{nm}$ $\mathcal{H}$-classes contained in the $\mathcal{D}$-class $D^{(i)}$ of $Gaff(A) : H^{(i, \omega)} := \{\langle u, a \rangle \mid \nu_p(u) = i, a + (p^i) = \omega, u, a \in A\}$, where $\omega$ is a residue class of $A$ modulo its ideal $(p^i)$, that is, $\omega \in A/\langle p^i \rangle$;
6. there are exactly 2 regular $\mathcal{D}$-classes in $Gaff(A) : D^{(0)}$ and $D^{(n)}$, where $D^{(0)} = Aff(A)$ is the affine transformation group over $A$ and $D^{(n)} = \{\langle 0, a \rangle \mid a \in A\}$ is an ideal of $Gaff(A)$ and a right zero band;
(7) let $D^* := \bigcup_{i=1}^{n} D^{(i)}$. Then $D^*$ is a maximal ideal of Gaff(A) and the maximal nil-extension of the right zero band $D^{(n)}$ in Gaff(A);

(8) the Rees quotient semigroup of Gaff(A) modulo its ideal $D^*$ is given by Gaff(A)/D* = Aff(A) \cup \{0\}. Thus Gaff(A) is an ideal extension of $D^*$ by Aff(A) \cup \{0\}.

Proof. (1) Let $\langle u, a \rangle R \langle v, b \rangle$ in the monoid Gaff(A). Then there exist $x, y, c, d \in A$ such that $(u, a) \langle x, c \rangle = (v, b)$ and $\langle v, b \rangle \langle y, d \rangle = (u, a)$. Hence $ux = v$ and $vy = u$, so $(u) = (v) = (p^i)$ as ideals of Gaff(A) for some $0 \leq i \leq n$. Thus $\nu_p(u) = \nu_p(v) = i$.

Conversely, let $\nu_p(u) = \nu_p(v) = i$. Then there exist $s, t \in U(A)$ such that $u = p^is$ and $v = p^it$. Select $c = b - as^{-1}t$, $d = a - bt^{-1}s \in A$. Then $(u, a) \langle s^{-1}t, c \rangle = (p^i as^{-1}t, as^{-1}t + c) = (v, b)$ and $(v, b) \langle t^{-1}s, d \rangle = (p^i tt^{-1}s, bt^{-1}s + d) = (u, a)$. Hence $(u, a) R \langle v, b \rangle$ in the monoid Gaff(A).

(2) Let $\langle u, a \rangle L \langle v, b \rangle$ in the monoid Gaff(A). Then there exist $x, y, c, d \in A$ such that $x, c \langle u, a \rangle (v, b)$ and $\langle y, d \rangle \langle v, b \rangle \langle u, a \rangle$, that is, $v = xu$, $u = yv$, $b = uc + a$ and $a = vd + b$. Hence $(u) = (v) = (p^i)$ for some $0 \leq i \leq n$ and $a - b \in (p^i)$, so $\nu_p(u) = \nu_p(v) = i$ and $a \equiv b (\text{mod}(p^i))$.

Conversely, let $\nu_p(u) = \nu_p(v) = i$ and $a - b \in (p^i)$. Then there exist $s, t \in U(A)$ and $c, d \in A$ such that $u = p^is$, $v = p^it$, $a - b = dv$, and $b - a = cu$. Hence $\langle ts^{-1}, c \rangle \langle u, a \rangle = \langle ts^{-1} p^is, uc + a \rangle = (v, b)$ and $\langle st^{-1}, d \rangle \langle v, b \rangle = (st^{-1} p^it, vd + b) = (u, a)$, so $\langle u, a \rangle L \langle v, b \rangle$ in the monoid Gaff(A).

Then (3) follows because $L \subseteq R$ by (1) and (2), and (4) follows by (1).

(5) For every $0 \leq i \leq n$, by (1) and (2) we see that all distinct $\mathcal{H}$-classes contained in $R^{(i)}$ of Gaff(A) are given by $H^{(i, \omega)}$, $\omega \in A/(p^i)$. Hence the number of $\mathcal{H}$-classes contained in $R^{(i)}$ is equal to $|A/(p^i)| = p^{nm}/p^{(n-i)m} = p^{im}$.

(6) We consider idempotents of the monoid Gaff(A) first. Let $u, a \in A$ satisfying $\langle u, a \rangle^2 = \langle u, a \rangle$, that is, $u(u - 1) = 0$ and $ua = 0$. If $u$ is invertible in $A$, then by $u(u - 1) = 0$ and $ua = 0$, we have $u = 1$ and $a = 0$. Otherwise, $u - 1$ is invertible in $A$, from which we obtain $u = 0$ by $u(u - 1) = 0$. Hence all idempotents of Gaff(A) are given by $(1, 0)$ and $(0, 0)$, $a \in A$.

Since $\nu_p(1) = 0$, $D^{(0)} = R^{(0)} = \{ \langle u, a \rangle \mid \nu_p(u) = 0, u, a \in A \} = \{ \langle u, a \rangle \mid u \in U(A), a \in A \} = \text{Aff}(A)$, that is, the $\mathcal{R}$-class of Gaff(A) containing the idempotent $(1, 0)$. Hence $D^{(0)}$ is regular and equal to the affine transformation group over $A$. For every $a \in A$, since $\nu_p(0) = n$, $D^{(n)} = R^{(n)} = \{ \langle u, b \rangle \mid \nu_p(u) = n, u, b \in A \} = \{ \langle 0, b \rangle \mid b \in A \}$, that is, the $\mathcal{R}$-class of Gaff(A) containing the idempotent $(0, a)$. So $D^{(n)}$ is regular. For any $u, a, b \in A$, since $\langle u, a \rangle \langle 0, b \rangle = \langle 0, b \rangle \in R^{(n)}$ and $\langle 0, b \rangle \langle u, a \rangle = \langle 0, ub + a \rangle \in D^{(n)}$, we see that $D^{(n)}$ is an ideal of Gaff(A) and a right zero band.

Then (7) and (8) follow immediately from (1)–(6) and semigroup theory [3, page 137] and [1, page 62–64].

Then we give an explicit description of every $\mathcal{H}$-class of the monoid Gaff(A).

**Lemma 2.2.** For any $1 \leq i \leq n$ and $\omega \in A/(p^i)$, there is a bijection from the set $U(A/(p^{n-i})) \times (p^i)$ onto the $\mathcal{H}$-class $H^{(i, \omega)}$ of the monoid Gaff(A).

Proof. Let $a_0 \in A$ satisfying $\omega = a_0 + (p^i)$. Define $\phi : U(A/(p^{n-i})) \times (p^i) \to H^{(i, \omega)}$ via $(s + (p^{n-i}), b) \mapsto (p^s a_0 + b)$. We show firstly that $\phi$ is well defined. If $s_1, s_2 \in A$ satisfying
Let \( A \) be a commutative ring with unity. Then the multiplication 
\[ p^i st \in (p^{n-i}) \]
for all \( i \in [0, n) \) and \( s + (p^{n-i}) \in U(A/(p^{n-i})) \) and \( b \in (p^i) \). Then \( a_0 + b + (p^i) = a_0 + (p^i) = \omega \) and \( p^i s \in (p^i) \). Since \( s + (p^{n-i}) \in U(A/(p^{n-i})) \), there exists \( t \in A \) such that \( st \equiv 1 \) (mod \( p^{n-i} \)), which is equivalent to \( p^i (st - 1) = 0 \). Hence \( p^i = p^i st \in (p^i s) \) and so \( (p^i s) = (p^i) \). Thus \( \langle p^i s, a_0 + b \rangle \in H^{(i, \omega)} \) by Theorem 2.1(5). So \( \phi \) is well defined. Now, we prove that \( \phi \) is a bijection. Obviously, \( \phi \) is injective. For any \( \langle u, d \rangle \in H^{(i, \omega)} \), by Theorem 2.1(5) we have \( v_p(u) = i \) and \( d + (p^i) = a_0 + (p^i) \). Since \( v_p(u) = i \), there exist \( t, s \in A \) such that \( u = p^i s \) and \( p^i \neq ut \). Then \( p^i = p^i st \) and so \( st - 1 \in (p^{n-i}) \). Hence \( s + (p^{n-i}) \in U(A/(p^{n-i})) \). From \( d + (p^i) = a_0 + (p^i) \) we obtain \( d - a_0 \in (p^i) \). Then \( (s + (p^{n-i}), d - a_0) \phi = \langle u, d \rangle \). So \( \phi \) is surjective.

Now, for every \( 1 \leq i \leq n \), let \((G, \circ)\) be the semidirect product \( U(A/(p^{n-i})) \ltimes (p^i) \) of the multiplicative group \( U(A/(p^{n-i})) \) on the additive group \((p^i)\) with respect to the action of \( U(A/(p^{n-i})) \) on \((p^i)\) defined by \( c t^{(p^{n-i})} = ct \) for all \( c \in (p^i), t + (p^{n-i}) \in U(A/(p^{n-i})) \). Then the multiplication “\( \circ \)” on \( G \) is given by the following: for any \( (s + (p^{n-i}), b), (t + (p^{n-i}), d) \in G \), \( (s + (p^{n-i}), b) \circ (t + (p^{n-i}), d) = (st + (p^{n-i}), bt + d) \).

**Lemma 2.3.** For every \( 1 \leq i \leq n \), \( U(A/(p^{n-i})) \ltimes (p^i) \) is isomorphic to the affine transformation group on the Galois ring \( GR(p^{n-i}, p^{(n-i)m}) \).

**Proof.** Let \((G, \circ) = U(A/(p^{n-i})) \ltimes (p^i)\). We first prove that \( U(A/(p^{n-i})) \cong GR(p^{n-i}, p^{(n-i)m}) \) as multiplicative groups. Recall that for the Galois ring \( A = GR(p^n, p^m) \), there exists \( \xi \in A \) of multiplicative order \( p^m - 1 \) such that \( \xi \) is a root of a certain basic primitive polynomial \( h(x) \in \mathbb{Z}_{p^n}[x] \) of degree \( m \) satisfying \( h(x)(x^{p^m - 1} - 1) \). So \( A = \mathbb{Z}_{p^n}[\xi] = \mathbb{Z}_{p^n}[x]/(h(x)) \) up to ring isomorphism. Let \( \sigma : c + (p^{n-i}) \rightarrow c + (p^{n-i}) \) for all \( c \in \mathbb{Z} \) be the natural surjective ring homomorphism from \( \mathbb{Z}_{p^n} \) onto \( \mathbb{Z}_{p^{n-i}} \). Then \( \sigma \) induces a surjective ring homomorphism \( \tilde{\sigma} \) from \( \mathbb{Z}_{p^n}[x] \) onto \( \mathbb{Z}_{p^{n-i}}[x] \) defined by \( \tilde{\sigma} : \Sigma c_k x^k \rightarrow \Sigma [c_k \sigma] x^k \) (for all \( \Sigma c_k x^k \in \mathbb{Z}_{p^n}[x] \)). For any \( f(x) \in \mathbb{Z}_{p^n}[x] \), denote \( \tilde{f}(x) = (f(x)) \tilde{\sigma} \). Obviously, \( \tilde{h}(x) \) is a basic primitive polynomial in \( \mathbb{Z}_{p^{n-i}}[x] \) of degree \( m \). Hence we have \( GR(p^{n-i}, p^{(n-i)m}) = \mathbb{Z}_{p^{n-i}}[x]/(\tilde{h}(x)) \) up to ring isomorphism. Define mapping \( \tau : A \rightarrow GR(p^{n-i}, p^{(n-i)m}) \) via \( f(x) + (h(x)) \rightarrow \tilde{f}(x) + (\tilde{h}(x)) \) for all \( f(x) \in \mathbb{Z}_{p^n}[x] \). Then \( \tau \) is a surjective ring homomorphism from \( A \) onto \( GR(p^{n-i}, p^{(n-i)m}) \) with kernel \( \ker(\tau) = p^{n-i} - A = (p^{n-i}) \). Then we have a ring isomorphism \( A/(p^{n-i}) \cong GR(p^{n-i}, p^{(n-i)m}) \), which induces a multiplicative group isomorphism \( U(A/(p^{n-i})) \cong U(GR(p^{n-i}, p^{(n-i)m})) \).

Similarly, define a mapping \( \theta : (p^i) = p^i A \rightarrow GR(p^{n-i}, p^{(n-i)m}) \) via \( p^i f(x) + (h(x)) \rightarrow \tilde{f}(x) + (\tilde{h}(x)) \) for all \( f(x) \in \mathbb{Z}_{p^n}[x] \). It is a routine matter to show that \( \theta \) is an additive group surjective homomorphism from \((p^i)\) onto \( GR(p^{n-i}, p^{(n-i)m}) \) with kernel \( \ker(\theta) = \{0\} \). Hence \((p^i, +) \cong (GR(p^{n-i}, p^{(n-i)m}), +) \).

Finally, we prove that \((G, \circ)\) is isomorphic to the affine transformation group \( \text{Aff}(GR(p^{n-i}, p^{(n-i)m})) \). Define a mapping \( \zeta : G \rightarrow \text{Aff}(GR(p^{n-i}, p^{(n-i)m})) \) by

\[
(\alpha) \zeta = \left( \tilde{f_1}(x) + (\tilde{h}(x)), \tilde{f_2}(x) + (\tilde{h}(x)) \right) = \left( \left[ f_1(x) + (h(x)) \right] \tau, \left[ p^i f_2(x) + (h(x)) \right] \theta \right)
\]

for all \( \alpha = (f_1(x) + (h(x)) + p^{n-i}A, f_2(x) + (h(x))) \in G \), where \( f_1(x), f_2(x) \in \mathbb{Z}_{p^n}[x] \). Obviously, \( \zeta \) is a bijection. Moreover, for any \( g_1(x), g_2(x) \in \mathbb{Z}_{p^n}[x] \), and \( \beta = (g_1(x) + (h(x)) + p^{n-i}A, g_2(x) + (h(x))) \in G \), by definitions and properties of \( \tilde{\sigma}, \tau, \) and \( \theta \), we
We have
\[(\alpha \circ \beta)\zeta = \left( [f_1(x) + (h(x))] [g_1(x) + (h(x))] + p^{n-i} A, [p^i f_2(x) + (h(x))] \right) \]
\[\times \left[ [g_1(x) + (h(x))] + p^i g_2(x) + (h(x)) \right] \zeta \]
\[= (f_1(x) g_1(x) + (h(x)) + p^{n-i} A, p^i [f_2(x) g_1(x) + g_2(x)] + (h(x))) \zeta \]
\[= \left( [f_1(x) g_1(x)] \tilde{\sigma} + (\tilde{h}(x)), [f_2(x) g_1(x) + g_2(x)] \tilde{\sigma} + (\tilde{h}(x)) \right) \]
\[= \left( \tilde{f}_1(x) \tilde{g}_1(x) + (\tilde{h}(x)), \tilde{f}_2(x) \tilde{g}_1(x) + \tilde{g}_2(x) + (\tilde{h}(x)) \right) \]
\[= \left( \tilde{f}_1(x) + (\tilde{h}(x)), \tilde{f}_2(x) + (\tilde{h}(x)) \right) \tilde{g}_1(x) + (\tilde{h}(x)), \tilde{g}_2(x) + (\tilde{h}(x)) \right) \]
\[= \left( (\alpha) \zeta \right) \left[ (\beta) \zeta \right]. \]

Hence \(\zeta\) is a group isomorphism from \((G, \circ)\) onto \(\text{Aff}(GR(p^{n-i}, p^{(n-i)m})).\)

Let \(S\) be a semigroup and \(H\) an \(\mathcal{H}\)-class of \(S^1\). As in [4], the submonoid \(T_r(H)\) of \(S^1\), defined by \(T_r(H) = \{x \in S^1 \mid Hx = H\}\), is called the right stabilizer of \(H\). The quotient monoid \(\Gamma_r(H) = T_r(H)/\eta\) of \(T_r(H)\) by its congruence \(\eta\), defined by \(\eta = \{(x, y) \mid (\exists h \in H)hx = hy, x, y \in T_r(H)\}\), is a transitive group of permutations of \(H\). It is known that \(\Gamma_r(H_1)\) and \(\Gamma_r(H_2)\) are equivalent permutation groups for any two \(\mathcal{H}\)-classes \(H_1\) and \(H_2\) contained in the same \(\mathcal{D}\)-class of \(S\). The abstract group \(\Gamma_r(H)\) is called the Schützenberger group of the \(\mathcal{D}\)-class containing \(H\).

**Theorem 2.4.** For every \(1 \leq i \leq n\), the Schützenberger group of the \(\mathcal{D}\)-class \(D(i)\) of Gaff \((A)\) is isomorphic to the affine transformation group on the Galois ring \(GR(p^{n-i}, p^{(n-i)m})\). Then \(|H^{(i, \omega)}| = (p^m - 1)p^{(2n-2i-1)m}\) for any \(\omega \in A/(p^i)\).

**Proof.** By Lemma 2.3 we need only to show that the Schützenberger group of \(D(i)\) is isomorphic to \((G, \circ) = U(A/(p^{n-i})) \rtimes (p^i)\). Consider the \(\mathcal{H}\)-class \(H^{(i, \bar{b})}\) contained in \(D(i)\), where \(\bar{b} = (p^i) \in A/(p^i)\). In view of Lemma 2.2, \(H^{(i, \bar{b})} = \{(p^i s, b) \mid s + (p^{n-i}) \in U(A/(p^{n-i}))\}, b \in (p^i)\}. Now, we denote \(H^{(i, \bar{b})}\) by \(H\) for brevity. First, we determine the right stabilizer \(T_r(H) = \{\langle t, c \rangle \mid H.t, c \in A\}\) of \(H\). By properties of \(\mathcal{H}\)-classes in semigroup theory [4, Lemma 3.2, page 32], for any \(t, c \in A\), \(\langle t, c \rangle \in T_r(H)\) if and only if there exist \(s + (p^{n-i}) \in U(A/(p^{n-i}))\) and \(b \in (p^i)\) such that \(\langle p^i s, b \rangle (t, c) = \langle p^i s t, b t + c \rangle \in H\), which is equivalent to \((p^i s t) = (p^i)\) and \(b t + c = b t + c - 0 \in (p^i)\) by Theorem 2.1(5). Since \(b \in (p^i)\), \(b t + c \in (p^i)\) is equivalent to \(c \in (p^i)\). Since \(s + (p^{n-i}) \in U(A/(p^{n-i}))\), \(\langle p^i s t, b \rangle = (p^i)\) is equivalent to \(s t w \equiv 1 \pmod{(p^{n-i})}\) for some \(w \in A\), that is, \(t + (p^{n-i}) \in U(A/(p^{n-i}))\). Therefore, we have
\[T_r(H) = \{\langle t, c \rangle \mid t + (p^{n-i}) \in U(A/(p^{n-i})), c \in (p^i), t \in A\}.\]

Now, define mapping \(\psi : T_r(H) \rightarrow G\) by \(\langle t, c \rangle \psi = (t + (p^{n-i}), c)\) for all \(t + (p^{n-i}) \in U(A/(p^{n-i})), c \in (p^i)\). Then \(\psi\) is surjective, and for any \(\alpha_i = \langle t_i, c_i \rangle \in T_r(H), i = 1, 2,\) we have \(\alpha_1 \alpha_2 \psi = \langle t_1 t_2, t_2 c_1 + c_2 \rangle \psi = (t_1 t_2 + (p^{n-i}), t_2 c_1 + c_2) = (t_1 + (p^{n-i}), c_1) \circ (t_2 + (p^{n-i}), c_2) = (\alpha_1 \psi) \circ (\alpha_2 \psi).\) Hence \(\psi\) is a surjective semigroup homomorphism from \(T_r(H)\) onto \((G, \circ)\). Moreover, in view of semigroup theory [4, page 32] we have \((\alpha_1, \alpha_2) \in \eta\) if and only if
there exist \( s + (p^{n-i}) \in U(A/(p^{n-i})) \) and \( b \in (p^i) \) such that \( \langle p^i s, b \rangle \alpha_1 = \langle p^i s, b \rangle \alpha_2 \), that is, \( \langle p^i s t_1, t_1 b + c_1 \rangle = \langle p^i s t_2, t_2 b + c_2 \rangle \), which is equivalent to \( p^i s t_1 = p^i s t_2 \) and \( t_1 b + c_1 = t_2 b + c_2 \). Since \( s + (p^{n-i}) \in U(A/(p^{n-i})) \), we have

\[
p^i s t_1 = p^i s t_2 \iff s t_1 \equiv s t_2 \mod (p^{n-i}) \iff t_1 \equiv t_2 \mod (p^{n-i})
\]

(2.4)

and that \( t_1 b + c_1 = t_2 b + c_2 \) is equivalent to \( c_2 - c_1 = b(t_1 - t_2) \in (p^i)(p^{n-i}) = \{0\} \), that is, \( c_1 = c_2 \). Therefore, \( (\alpha_1, \alpha_2) \in \eta \) if and only if \( \alpha_1 \psi = \alpha_2 \psi \). Hence \( \eta = \ker(\psi) \) and so \( \Gamma_r(H) = T_r(H)/\eta \equiv (G, o) \) as groups.

Since \( U(A/(p^{n-i})) \cong U(\text{GR}(p^{n-i}, p^{(n-i)m})) \), we have \( |U(A/(p^{n-i}))| = |U(\text{GR}(p^{n-i}, p^{(n-i)m}))| = (p^m - 1)p^{(n-i-1)m} \). But \( |(p^i)| = p^{(n-i)m} \), and so we have \( |H^{(i, \omega)}| = |U(A/(p^{n-i}))| \times |(p^i)| \equiv |U(A/(p^{n-i}))| \times |(p^i)| = (p^m - 1)p^{(2n-2i-1)m} \) by Lemma 2.2.

\[\square\]

Acknowledgments

This research is supported in part by the NSF of Shandong Province, China, under Grant 2003ZX13 and the NSF of Shandong University of Technology, under Grant 2005KJM13.

References


Yonglin Cao: Institute of Applied Mathematics, School of Mathematics and Information, Shandong University of Technology, Zibo, Shandong 255091, China

E-mail address: ylcao@sdut.edu.cn