Quasigroups and Related Systems **20** (2012), 275 − 281

Polyadic groups and automorphisms of cyclic extensions

Mohammad Shahryari

Abstract. We show that for any n-ary group (G,f), the group $Aut(G,f)$ can be embedded in $Aut(\mathbb{Z}_{n-1}\ltimes G)$ and so we can obtain a class of interesting automorphisms of cyclic extensions.

1. Introduction

Our notations in this article are standard and can be find in [2], for example.

Let (G,f) be an n-ary group. We know that, there is a binary operation "$\cdot$" on G, such that $(G,\cdot)$ is an ordinary group, and further, there is a $\theta\in Aut(G,\cdot)$ with an element $b\in G$, such that

(i) $\theta(b)=b$, and $\theta^{n-1}(x)=bxb^{-1}$ for all $x\in G$,

(ii) $f(x_1^n)=x_1\theta(x_2)\cdots\theta^{n-1}(x_n)b$.

So, some times, we denote (G,f) by the notation $der_{\theta,b}(G,\cdot)$. If $b=e$, the identity element of $(G,\cdot)$, then we use the notation $der_\theta(G,\cdot)$.

We associate another binary group to (G,f) which is called the *universal covering group* or *Post's cover* of (G,f). Let a be an arbitrary element of G and suppose $G_a^*=\mathbb{Z}_{n-1}\times G$. Define a binary operation on this set by

$$(i,x)*(j,y)=(i+j+1,f_*(x,\overset{(i)}{a},y,\overset{(j)}{a},\overline{a},\overset{(i,j)}{a})).$$

Here of course, $i+j+1$ is computed modulo $n-1$, and $(i,j)=n-i-j-3$ modulo $n-1$. The symbol f_* indicates that f applies one or two times depending on the values of i and j and $\overline{a}$ denotes the skew element of a. It is proved that (see [4]), G_a^* is a binary group and the subset

$$R=\{(n-2,x):x\in G\}$$

is a normal subgroup such that $G_a^*/R\cong\mathbb{Z}_{n-1}$. Further, if we identify G by the subset

$$\{(0,x):x\in G\},$$

2010 Mathematics Subject Classification: 20N15
Keywords: Polyadic group, covering group, semi-direct product, cyclic extensions.

then G is a coset of R and it generates G_a^*. We also have

$$f(x_1^n) = x_1 * x_2 * \cdots * x_n.$$

It is not hard to see that for all $a, b \in G$, we have $G_a^* \cong G_b^*$, so for simplicity, we always, assume that $a = e$, the identity element of $(G, \cdot)$.

Through this article, we assume that $(G, f) = der_\theta(G, \cdot)$. So, we have $\theta^{n-1} = id$ and

$$f(x_1^n) = x_1\theta(x_2)\cdots\theta^{n-2}(x_{n-1})x_n.$$

We also assume that e is the identity element of $(G, \cdot)$. We will prove first the following theorem on the structure of the Post's cover.

Theorem 1.1. *$(der_\theta(G, \cdot))_e^* \cong \mathbb{Z}_{n-1} \ltimes G$, where $\mathbb{Z}_{n-1}$ acts on $(G, \cdot)$ by $i.x = \theta^i(x)$.*

Note that, we used a special case of this theorem in [6], to investigate representations of polyadic groups. The main idea of this article is almost the same as in [6]. Our second goal is to obtain an embedding from $Aut(G, f)$ to $Aut(G_e^*)$. The method we employ is the same as in [6]. For any $i \in \mathbb{Z}_{n-1}$ and $u \in G$, suppose $\delta(i, u) = \theta(u)\theta^2(u)\ldots\theta^i(u)$. We prove

Theorem 1.2. *Let $\Lambda \in Aut(G, f)$ and define $\Lambda^* : G_e^* \to G_e^*$ by*

$$\Lambda^*(i, x) = (i, \Lambda(x)\delta(i, u)),$$

where $u = \Lambda(e)$. Then the map $\Lambda \mapsto \Lambda^*$ is an embedding.

In [3], the structure of automorphisms of (G, f) is determined. If $\Lambda \in Aut(G, f)$, then we have $\Lambda = R_u\varphi$, where u is an idempotent element, i.e. $f(\overset{(n)}{u}) = u$, R_u is the right translation by u and φ is an ordinary automorphism of $(G, \cdot)$ with the property $[\varphi, \theta] = I_u$, (the bracket denotes the commutator $\varphi\theta\varphi^{-1}\theta^{-1}$ and I_u is the inner automorphism corresponding to u). The converse is also true; if u and φ satisfy above conditions, the $\Lambda = R_u\varphi$ is an automorphism of the polyadic group (G, f). We will use this fact frequently through this article. The interested reader should see [3] for a full description of homomorphisms between polyadic groups.

Combining Theorems 1.1 and 1.2, we obtain an embedding of $Aut(G, f)$ into $Aut(\mathbb{Z}_{n-1} \ltimes G)$. More precisely, we prove the following.

Theorem 1.3. *Let $\hat{G} = A \ltimes G$, with $A = \langle a \rangle$ cyclic of order $n-1$ and let $\theta(x) = axa^{-1}$. Then for any $\varphi \in Aut(G)$ and $u \in G$, the hypotheses $[\varphi, \theta] = I_u$ and $(au)^{n-1} = 1$ imply that the map*

$$(a^i, x) \mapsto (a^i, u^{-1}\varphi(x)u(au)^i a^{-i})$$

is an automorphism of $\hat{G}$ and these automorphisms are mutually distinct.

2. Proofs

Proof of Theorem 1.1. Note that in G_e^*, we have

$$\begin{aligned}(i,x)*(j,y) &= (i+j+1, f_*(x, \overset{(i)}{e}, y, \overset{(j)}{e}, \overline{e}, \overset{(i,j)}{e}))\\ &= (i+j+1, x\theta(e)\cdots\theta^i(e)\theta^{i+1}(y)\theta^{i+2}(e)\\ &\qquad\qquad \cdots\theta^{i+j+2}(e)\theta^{i+j+3}(\overline{e})\cdots\theta^{n-2}(e))\\ &= (i+j+1, x\theta^{i+1}(y)\theta^{i+j+3}(\overline{e})),\end{aligned}$$

but, since $\overline{e}=e$, so

$$(i,x)*(j,y) = (i+j+1, x\theta^{i+1}(y)) = (i,x)(1,e)(j,y),$$

where the right hand side product is done in $\mathbb{Z}_{n-1}\ltimes G$. Note that in general, if $(A,\cdot)$ is a group and $a\in A$, then we can define a new binary operation on A by $x\circ y = xay$ and together with this new operation, A is a group too, and so we denote it by $A_a=(A,\circ)$. We have $A\cong A_a$ and the isomorphism is given by $\varphi(x)=a^{-1}x$. Now, by this notation, we have

$$(der_\theta(G,\cdot))_e^* = G_e^* = (\mathbb{Z}_{n-1}\ltimes G)_{(1,e)},$$

and hence $(der_\theta(G,\cdot))_e^* \cong \mathbb{Z}_{n-1}\ltimes G$. □

Now, let $\Lambda\in Aut(G,f)$ and $u=\Lambda(e)$. Define $\Lambda_e^*: G_e^*\to G_u^*$ by $\Lambda_e^*(i,x) = (i,\Lambda(x))$.

Lemma 2.1. *Λ_e^* is an isomorphism.*

Proof. Note that

$$\Lambda_e^*((i,x)*(j,y)) = \Lambda_e^*(i+j+1, x\theta^{i+1}(y)) = (i+j+1, \Lambda(x\theta^{i+1}(y))).$$

On the other hand,

$$\begin{aligned}\Lambda_e^*(i,x)*\Lambda_e^*(j,y) &= (i,\Lambda(x))*(j,\Lambda(y))\\ &= (i+j+1, f_*(\Lambda(x), \overset{(i)}{u}, \Lambda(y), \overset{(j)}{u}, \overline{u}, \overset{(i,j)}{u})).\end{aligned}$$

But $f(\overline{u}, \overset{(n-1)}{u}) = u$, so $\Lambda(f(v, \overset{(n-1)}{e})) = \Lambda(e)$, where $\Lambda(v)=\overline{u}$. Therefore $f(v, \overset{(n-1)}{e}) = e$ and so $v=e$ and hence $\overline{u}=\Lambda(e)=u$. Now, we have

$$\begin{aligned}\Lambda_e^*(i,x)*\Lambda_e^*(j,y) &= (i+j+1, \Lambda(f_*(x, \overset{(i)}{e}, y, \overset{(j)}{e}, e, \overset{(i,j)}{e}))) = (i+j+1, \Lambda(x\theta^{i+1}(y)))\\ &= \Lambda_e^*((i,x)*(j,y)).\end{aligned}$$

This shows that Λ_e^* is an isomorphism. □

An element $u \in G$ is said to be *idempotent* if $f(\overset{(n)}{u}) = u$. For an arbitrary element $u \in G$, we remember that the *right translation map* R_u is defined by $R_u(x) = xu$. In [3], it is proved that every element of $Aut(G, f)$ can be uniquely represented as $R_u\varphi$ with u an idempotent and $\varphi \in Aut(G, \cdot)$ satisfies $[\varphi, \theta] = I_u$, where I_u is the inner automorphism of G, corresponding to u. The converse is also true and so we have a complete description of automorphisms of $Aut(G, f)$ in terms of automorphisms of $(G, \cdot)$ and idempotents. Now, for any idempotent u and $i \in \mathbb{Z}_{n-1}$, define

$$\delta(i, u) = \theta(u)\theta^2(u)\cdots\theta^i(u).$$

Note that for the case $i = 0$, we have $\delta(0, u) = \delta(n-1, u) = e$. If $\Lambda \in Aut(G, f)$ and $u = \Lambda(e)$, then we define a map $q_u : G^*_u \to G^*_e$ by $q_u(i, x) = (i, x\delta(i, u))$.

Lemma 2.2. *The map q_u is an isomorphism.*

Proof. We first assume that $i, j \neq 0$. Note that in G^*_u, we have

$$\begin{aligned}(i, x) * (j, y) &= (i + j + 1, f_*(x, \overset{(i)}{u}, y, \overset{(j)}{u}, \overline{u}, \overset{(i,j)}{u}))\\ &= (i + j + 1, \Lambda(f_*(\Lambda^{-1}(x), \overset{(i)}{e}, \Lambda^{-1}(y), \overset{(j)}{e}, e, \overset{(i,j)}{e})))\\ &= (i + j + 1, \Lambda(\Lambda^{-1}(x)\theta^{i+1}(\Lambda^{-1}(y)))).\end{aligned}$$

Now, as we said before, $\Lambda = R_u\varphi$ such that $\varphi \in Aut(G)$ and $[\varphi, \theta] = I_u$. Therefore

$$\begin{aligned}(i, x) * (j, y) &= (i + j + 1, R_u\varphi(\varphi^{-1}R_u^{-1}(x)\theta^{i+1}(\varphi^{-1}R_u^{-1}(y))))\\ &= (i + j + 1, R_u((xu^{-1})\varphi\theta^{i+1}\varphi(yu^{-1}))).\end{aligned}$$

Since $[\varphi, \theta] = I_u$, so we have $\varphi\theta^{i+1}\varphi^{-1} = (I_u\theta)^{i+1}$. But

$$\begin{aligned}(I_u\theta)^{i+1}(z) &= u\theta(u)\cdots\theta^i(u)\theta^{i+1}(z)\theta(u)^{-1}\cdots\theta(u)^{-1}u^{-1}\\ &= u\delta(i, u)\theta^{i+1}(z)\delta(i, u)^{-1}u^{-1}.\end{aligned}$$

Hence, we have

$$\begin{aligned}(i, x) * (j, y) &= (i + j + 1, R_u(xu^{-1}u\delta(i, u)\theta^{i+1}(yu^{-1})\delta(i, u)^{-1}u^{-1}))\\ &= (i + j + 1, x\delta(i, u)\theta^{i+1}(yu^{-1})\delta(i, u)^{-1}).\end{aligned}$$

Now, we are ready to show that q_u is a homomorphism. First, note that

$$\begin{aligned}q_u((i, x) * (j, y)) &= q_u(i + j + 1, x\delta(i, u)\theta^{i+1}(yu^{-1})\delta(i, u)^{-1})\\ &= (i + j + 1, x\delta(i, u)\theta^{i+1}(yu^{-1})\delta(i, u)^{-1}\delta(i + j + 1, u)).\end{aligned}$$

On the other hand

$$\begin{aligned}q_u(i, x) * q_u(j, y) &= (i, x\delta(i, u)) * (j, y\delta(j, u))\\ &= (i + j + 1, x\delta(i, u)\theta^{i+1}(y\delta(j, u)))\\ &= (i + j + 1, x\delta(i, u)\theta^{i+1}(y)\theta^{i+1}(\delta(j, u))).\end{aligned}$$

Hence, q_u is a homomorphism, if and only if we have

$$\theta^{i+1}(\delta(j,u)) = \theta^{i+1}(u^{-1})\delta(i,u)^{-1}\delta(i+j+1,u).$$

But, we have,

$$\theta^{i+1}(u^{-1})\delta(i,u)^{-1}\delta(i+j+1,u) = \theta^{i+2}(u)\cdots\theta^{i+j+1}(u) = \theta^{i+1}(\delta(j,u)).$$

The case $i=0$ can be verified similarly, so q_u is a homomorphism. It is easy to see that also q_u is a bijection and so we proved the lemma. □

Combining two isomorphisms q_u and Λ_e^*, we obtain an automorphism $\Lambda^* = q_u \circ \Lambda_e^* \in Aut(G_e^*)$. Note that, we have

$$\Lambda^*(i,x) = (i, \Lambda(x)\delta(i,u)) = (0,\Lambda(x)) * (0,u)^i.$$

Lemma 2.3. *The map $\Lambda \mapsto \Lambda^*$ is an embedding from $Aut(G,f)$ into $Aut(G_e^*)$.*

Proof. Let $\Lambda_1, \Lambda_2 \in Aut(G,f)$ and $u = \Lambda_1(e)$ and $v = \Lambda_2(e)$. Suppose also $w = \Lambda_1(v) = (\Lambda_1 \circ \Lambda_2)(e)$. We have

$$(\Lambda_1 \circ \Lambda_2)^*(i,x) = (i, \Lambda_1(\Lambda_2(x))\delta(i,w)).$$

On the other hand

$$\Lambda_1^*(\Lambda_2^*(i,x)) = \Lambda_1^*(i,\Lambda_2(x)\delta(i,v)) = (i, \Lambda_1(\Lambda_2(x)\delta(i,v))\delta(i,u)).$$

But we have

$$\begin{aligned}
\Lambda_1(\Lambda_2(x)\delta(i,v)) &= \Lambda_1(\Lambda_2(x)\theta(v)\cdots\theta^i(v)\theta^{i+1}(e)\cdots\theta^{n-2}(e)e) \\
&= \Lambda_1(f(\Lambda_2(x), \overset{(i)}{v}, \overset{(n-i-2)}{e}, e)) \\
&= f(\Lambda_1(\Lambda_2(x)), \overset{(i)}{w}, \overset{(n-i-2)}{u}, \Lambda_1(e)) \\
&= \Lambda_1(\Lambda_2(x))\delta(i,w)\theta^{i+1}(u)\cdots\theta^{n-2}(u)\Lambda_1(e).
\end{aligned}$$

Note that we have

$$\theta^{i+1}\cdots\theta^{n-2}\Lambda_1(e)\delta(i,u) = \theta^{i+1}(u)\cdots\theta^{n-2}(u)u\theta(u)\cdots\theta^i(u) = e,$$

because,

$$\theta(u)\cdots\theta^i(u)\theta^{i+1}(u)\cdots\theta^{n-2}(u)\Lambda_1(e) = u^{-1}\Lambda_1(f(\overset{(n)}{e})) = u^{-1}\Lambda_1(e) = e.$$

Therefore we obtain

$$\Lambda_1^*(\Lambda_2^*(i,x)) = (i, \Lambda_1(\Lambda_2(x))\delta(i,w)),$$

and this shows that the map $\Lambda \mapsto \Lambda^*$ is a homomorphism. Now suppose $\Lambda^* = id$. Then $\Lambda(x)\delta(i,u) = x$ for all x and i, so if we put $x = e$, then $\delta(i,u) = u^{-1}$ for all i. Assuming $i=1$, we get $\theta(u) = u^{-1}$ and so assuming $i=2$, we obtain $u^{-1}u = u^{-1}$, hence $u = e$ and consequently $\Lambda = id$. This completes the proof of the lemma. □

Remember that we proved

$$G_e^* = (\mathbb{Z}_{n-1} \ltimes G)_{(1,e)} \cong \mathbb{Z}_{n-1} \ltimes G,$$

and this isomorphism is given by $\varphi(i,x) = (1,e)^{-1}(i,x)$. So,

$$\varphi(i,x) = (n-2,e)(i,x) = (n+i-2, \theta^{n-2}(x)) = (i-1, \theta^{n-2}(x)).$$

Now, for any $\Lambda \in Aut(G,f)$, define

$$\alpha(\Lambda) = \varphi^{-1} \circ \Lambda^* \circ \varphi.$$

Therefore $\alpha(\Lambda)$ is an automorphism of $\mathbb{Z}_{n-1} \ltimes G$ and the map $\Lambda \mapsto \alpha(\Lambda)$ is an embedding. We have

$$\begin{aligned}\alpha(\Lambda)(i,x) &= \varphi^{-1}(i-1, \Lambda(\theta^{-1}(x))\delta(i-1,u)) \\ &= (1,e)(i-1, \Lambda(\theta^{-1}(x))\delta(i-1,u)) \\ &= (i, (\theta\Lambda\theta^{-1})(x)\theta(u^{-1})\delta(i,u)).\end{aligned}$$

Since $\Lambda = R_u\varphi$, so $(\theta\Lambda\theta^{-1})(x) = (\theta\varphi\theta^{-1})(x)\theta(u)$. Hence

$$\alpha(\Lambda)(i,x) = (i, (\theta\varphi\theta^{-1})(x)\delta(i,u)).$$

On the other hand $\theta\varphi\theta^{-1} = I_u^{-1}\varphi$ and hence

$$\alpha(\Lambda)(i,x) = (i, u^{-1}\varphi(x)u\delta(i,u)).$$

Summarizing, we obtain the following corollary:

Corollary 2.4. *There is an embedding* $\alpha : Aut(G,f) \to Aut(\mathbb{Z}_{n-1} \ltimes G)$*, such that*

$$\alpha(\Lambda)(i,x) = (i, u^{-1}\varphi(x)u\delta(i,u)).$$

Now, we are ready to prove Theorem 1.3.

Proof of Theorem 1.3. Suppose $\hat{G} = A \ltimes G$ where $A = \langle a \rangle$ is a cyclic of order $n-1$. Define an automorphism of G by $\theta(x) = axa^{-1}$, so $\theta^{n-1} = id$. Let

$$(G,f) = der_\theta(G,\cdot).$$

So, there is an embedding $\alpha : Aut(G,f) \to Aut(\hat{G})$ such that

$$\alpha(\Lambda)(a^i,x) = (a^i, u^{-1}\varphi(x)u\delta(i,u)).$$

Since u is an idempotent, so $f(\overset{(n)}{u}) = u$, and therefore

$$u\theta(u)\cdots\theta^{n-1}(u) = u,$$

which implies that

$$aua^{-1}a^2ua^{-2}\cdots a^{n-2}ua^{-(n-2)}u = e.$$

Hence $(au)^{n-1} = 1$. Similarly, $\delta(i,u) = (au)^i a^{-i}$, so for any $\varphi \in Aut(G)$ and for any $u \in G$, the hypotheses

$$(au)^{n-1} = 1, \quad [\varphi, \theta] = I_u$$

imply that the map

$$(a^i, x) \mapsto (a^i, u^{-1}\varphi(x)u(au)^i a^{-i})$$

is an automorphism of $\hat{G}$. Clearly this is an embedding and hence the theorem is proved. $\square$

Example 2.5. Let $E = GF(q)$ be the Galois field of order q and $m \geqslant 1$. Let $G = (E^m, +)$ and suppose $\alpha : E^m \to E^m$ is a linear map of order $n-1$. Then $A = \langle \alpha \rangle$ acts naturally on G, so $\hat{G} = A \ltimes G \cong \mathbb{Z}_{n-1} \ltimes E^m$. In this case $\theta = \alpha^{-1}$ and for any $u \in \ker(1 + \alpha + \cdots + \alpha^{n-2})$ and any

$$\varphi \in C_{GL_m(q)}(\alpha)$$

we have $[\theta, \varphi] = 1 = I_u$. Note that we have $u \in \ker(1 + \alpha + \cdots + \alpha^{n-2})$, iff $u = \alpha(v) - v$ for some $v \in E^m$. This shows that for any such v and φ, the map

$$(\alpha^i, x) \mapsto (\alpha^i, \varphi(x) + (\alpha^{i-1} - \alpha^{-1})(v))$$

is an automorphism of $\mathbb{Z}_{n-1} \ltimes E^m$.

References

[1] **W.A. Dudek and K. Glazek**, *Around the Hosszú-Gluskin Theorem for n-ary groups*, Discrete Math. **308** (2008), 4861 – 4876.

[2] **W.A. Dudek and M. Shahryari**, *Representation theory of polyadic groups*, Algebras and Representation Theory **15** (2012), 29 – 51.

[3] **H. Khodabandeh and M. Shahryari**, *On the Automorphisms and representations of polyadic groups*, Commun. Algebra **40** (2012), 2199 – 2212.

[4] **J. Michalski**, *Covering k-groups of n-groups*, Archivum Math. (Brno) **17** (1981), 207 – 226.

[5] **E.L. Post**, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208 – 350.

[6] **M. Shahryari**, *Representations of finite polyadic groups*, Commun. Algebra **40** (2012), 1625 – 1631.

Received June 7, 2012

Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Tabriz, Tabriz, Iran
E-mail: mshahryari@tabrizu.ac.ir