Quasigroups and related systems, vol. 1, no. 1(1), 1994

ON LINEAR ISOTOPES OF CYCLIC GROUPS

Sokhatskyj Fedir, Syvakivskyj Petro

Abstract

A description of all cyclic group n-ary linear isotopes is found to within isomorphism. Some results on their automorphism group and endomorphism semigroup are given.

An operative *(G;f)* will be called a multiplace isotope of the group *(Q;+)* iff there exists a sequence $(\gamma_1,...,\gamma_n,\gamma)$, named isotopy, of one-to-one mappings from G onto Q such that

$$f(x_1,x_2,...,x_n)=\gamma^{-1}(\gamma_1x_1+\gamma_2x_2+...+\gamma_nx_n)$$

holds for all $x_1,x_2,...,x_n$ in G. If all isotopy components are linear transformations of the group, then it will be called linear one. (Here and henceforth a linear transformation α of a group *(Q;+)* is a mapping from Q into Q such that $\alpha x=\theta x+c$, where θ is an automorphism and c is an arbitrary element of the group). According to **Albert's theorem** isomorphism of group isotopes implies isomorphism of the corresponding groups. So, it is enough to find an isomorphical test for isotopes of the same arbitrary fixed group. In this article we do it for a cyclic group, describe all its linear isotopes up to isomorphism, consider their automorphism groups and endomorphism semigroups. In the next works we shall consider the general case, but the main results one may find in [1].

Let Z be the integer ring and C=Z or $C=Z_m=Z/mZ$. It is easy to verify that any n-ary linear isotope of a cyclic group is isomorphic to *(C;f)* defined by the equality

$$f(x_1,x_2,...,x_n)=h_1x_1+h_2x_2+...+h_nx_n+a, \qquad (1)$$

where $h_1,h_2,...,h_n$ are invertible elements in the ring C (denote by C^* the group of ones). In this case the elements $h_1,h_2,...,h_n$ will be called *coefficients of (C;f)* and a will be its free member. Let *(C;g)* be defined by equality

$$g(x_1,x_2,...,x_n)=k_1x_1+k_2x_2+...+k_nx_n+b \qquad (2)$$

and α be a homomorphism from *(C;g)* into *(Q;f)*, i.e. the equality

$$\alpha(k_1x_1+k_2x_2+\ldots+k_nx_n+b)=h_1\alpha x_1+h_2\alpha x_2+\ldots+h_n\alpha x_n+a \tag{3}$$

holds for all $x_1,x_2,\ldots,x_n$ in C. In particular, replacing $x_3,\ldots,x_n$ by 0 and x_1,x_2 by the suitable expressions we have the equality

$$\alpha(x+y)=\beta x+\gamma y$$

for some transformations β,γ of the set C. Applying **Lemma 2.5** from [2] we get

$$\alpha x=kx+c$$

for some k,c of the set C. It is clear the element k is invertible together with the transformation α, i.e. when these isotopes are isomorphic. The relationship (3) with $x_1=x_2=\ldots=x_n=0$ gives the dependence

$$kb=(h_1+h_2+\ldots+h_n-1)c+a \tag{4}$$

and with $x_j=0$ for all $j\neq i$ and $x_i=1$ it gives

$$kk_i=h_ik,\quad i=1,\ldots,n, \tag{5}$$

in the ring C. The last equalities in the infinite ring for homomorphic isotopes mean that the corresponding sequenses of the coeffitients coincide. If the ring C is finite the relation (5) is equivalent to congruence

$$k_i\equiv h_i(\mathrm{mod}\,\frac{m}{s}),\quad i=1,\ldots,n,$$

i.e.

$$k_i\in\frac{m}{s}Z_m+h_i,\quad i=1,\ldots,n, \tag{6}$$

where $s=GCD(k,m)$. Hence, we can make the following conclusions.

Lemma 1. *A transformation α of the set Z_m is a homomorphism of the isotope $(Z_m;g)$ into $(Z_m;f)$ defined by (2) and (1) respectively if and only if there exist elements k,c in Z_m such that*

$$\alpha x=kx+c$$

and the relationships (4) and (6) hold.

Lemma 2. *A transposition α of the set Z is a homomorphic mapping from the isotope (Z;g) into (Z;f) defined by (2) and (1) if and only if there exist elements k,c such that the equalities*

$$\alpha x=kx+c,\quad k_i=h_i,\quad i=1,\ldots,n,$$

and (4) hold.

Corollary. *Different sequences of invertible elements of the ring C define nonisomorphic linear isotopes of the cyclic group (C,+).*

Lemma 3. *Let $(C;f)$ and $(C;g)$ be linear isotopes defined by the equalities* (1) *and*

$$g(x_1,x_2,\ldots,x_n)=h_1x_1+h_2x_2+\ldots+h_nx_n+b.$$

Then a substitution α of the set C will be an isomorphism between them if and only if

$$\alpha x=kx+c \quad \text{and} \quad kb=\mu c+a$$

for some element c and invertible element k of the ring C, where

$$\mu=h_1+h_2+\ldots+h_n-1.$$

To establish an isomorphical test for the linear isotopes we need the following.

Lemma 4. *For every integer a there exists a number r which is relatively prime to m and*

$$d\equiv ra(\operatorname{mod} m),$$

where $d=GCD(a,m)$.

Proof. Let a_1 and m_1 be integers defined by the equalities $a=a_1d$ and $m=m_1d$, and t be a product of all prime integers having the same exponent in the factorizations a and b into prime numbers. We can take r such that

$$(a_1-tm_1)r\equiv 1(\operatorname{mod} m).$$

Theorem 1. *Any linear isotope $(Z_m;f)$ defined by* (1) *is isomorphic to the isotope $(Z_m;g)$ defined by the following equality*

$$g(x_1,x_2,\ldots,x_n)=h_1x_1+h_2x_2+\ldots+h_nx_n+d, \tag{7}$$

where $d=GCD(\mu,m,a)$ and $\mu=h_1+h_2+\ldots+h_n-1$.

Proof. We adopt the notations $a_0=GCD(a,m)$, $\mu_0=GCD(\mu,m)$, then $d=GCD(a_0,\mu_0)$ and the **lemma 4** implies the existence of a number x which is relatively prime to μ_0 and

$$d\equiv xa_0(\operatorname{mod}\mu_0). \tag{8}$$

Let us denote by z the product of all prime divisors of the number m not dividing the number x. Since every prime divisor of the integer m divides exactly one of the numbers $x,\mu_0,z,$ then the integers $r=x+\mu_0z$ and m are relatively prime. **Lemma 4** implies the existence of numbers r_1 and r_2 which are relatively prime to m and

$$a_0\equiv ar_1(\operatorname{mod} m),$$
$$\mu_0\equiv \mu r_2(\operatorname{mod} m),$$

and the relationship (8) implies the equality

$$d=a_0x+\mu_0y$$

for some integer y. For this reason

$$d = a_0(x+\mu_0 z-\mu_0 z)+\mu_0 y = a_0 r-\mu_0(a_0 z-y)\equiv$$
$$\equiv (ar_1 r-\mu r_2(a_0 z-y))(\bmod m).$$

So, after the notations $k = r_1 r$ and $c = r_2(a_0 z-y)$ we get the relationship

$$ka \equiv (\mu c+d)(\bmod m),$$

which completes the proof according to **lemma 3**.

Theorem 2. *Any linear isotope of a cyclic m order group is isomorphic to exactly one isotope* $(Z_m;g)$ *defined by the equality* (7), *where* $h_1,h_2,\ldots,h_n$ *is a sequence of invertible elements of the ring* Z_m *and d is a common divisor of* $\mu = h_1+h_2+\ldots+h_n-1$ *and m.*

Proof. Any linear isotope of a cyclic group G is isomorphic to a linear isotope of the group Z_m. According to **theorem 1**, it is isomorphic to the isotope $(Z_m;g)$ satisfying to the conditions of this theorem. Let us consider two different isotopes $(Z_m;g_1)$ and $(Z_m;g_2)$. If they have the different sequences of their coefficients, then by the **corollary** of **lemma 1** these isotopes are not isomorphic. When the isotopes differ from each other only by their free members named a,b and taken $a<b$, then by **lemma 3** the existence of an isomorphism of the isotopes is equivalent to the existence of numbers k,c such that

$$kb \equiv \mu c+a(\bmod m)$$

holds. Under the conditions of the theorem the numbers a,b are common divisors of the integers μ,m and k is relatively prime to a, so b is divided by a. A contradiction.

If we consider group isotopes of a prime order, we can give more exact information following from the **theorem 2**.

Corollary 1. *Any n-ary linear group isotope of the prime order p is isomorphic:*

1) *one to the other, if the sum of the coeffitients is not the identity transformation;*

2) *to exactly one of the isotopes* (Z_p,g_0) *or* (Z_p,g_1) *defined by* (1) *with* $a=0$ *and* $a=1$, *respectively, in contrary case.*

Define $F(n,m)$ as the number of all pairwise nonisomorphic n-ary linear isotopes of the m order cyclic groups. According to **theorem 2**, $F(n,m)$ is the cardinal number of the set

$$\{(h_1,h_2,\ldots,h_n,d)|h_1,h_2,\ldots,h_n \in Z_m^{**}, d\in D(h_1+h_2+\ldots+h_n-1,m)\},$$

where Z_m^{**} denotes a set of all pairwise noncongruent by modulo m integers, which are relatively prime to m and $D(k,m)$ is the set of all common divisors of the integers k and m. We put the following problem:

what is the analytical expression of the number function F(n,m)?

Here we shall give a solution of this problem for prime m.

Corollary 2. *There exist exactly*

$$F(n,p) = \frac{(p+1)(p-1)^n + (-1)^{n+1}}{p}$$

n-ary linear group isotopes of a prime order p up to isomorphism.

Proof. Let us denote by $k_{n,j}$ the number of all sequences $(h_1, h_2, \dots, h_n)$ with

$$h_1 + h_2 + \dots + h_n \equiv i \pmod{p}$$

and

$$0 < h_1, h_2, \dots, h_n < p.$$

It is easy to see that

$$k_{n,0} + k_{n,1} + \dots + k_{n,p-1} = (p-1)^n, \tag{9}$$

Let

$$h_1 + h_2 + \dots + h_n \equiv j \pmod{p},$$

then there exists exactly one number h_{n+1} with conditions

$$h_1 + h_2 + \dots + h_n + h_{n+1} \equiv i \pmod{p},$$
$$0 < h_{n+1} < p$$

if and only if $j \neq i$. So, the equalities

$$k_{n+1,j} = (p-1)^n - k_{n,j}, \quad i = 0, 1, \dots, n,$$

hold. Since $k_{1,0} = 0$ and

$$k_{1,1} = k_{1,2} = \dots = k_{1,p-1} = 1,$$

then

$$k_{n,1} = k_{n,2} = \dots = k_{n,p-1} = k_{n,0} - (-1)^n$$

for every $n = 1, 2, \dots$. From (9) we have

$$k_{n,1} + (-1)^n + (p-1)k_{n,1} = (p-1)^n,$$

and

$$k_{n,1} = \frac{(p-1)^n - (-1)^n}{p}.$$

Hence, by **corollary 1** we get

$$F(n,p) = \frac{(p-1)^n - (-1)^n}{p} + (p-1)^n = \frac{(p+1)(p-1)^n + (-1)^{n+1}}{p}.$$

A description of all linear isotopes of infinite cyclic groups is given by the following theorem.

Theorem 3. *Any linear isotope of an infinite cyclic group is isomorphic to exactly one linear isotope (Z;f) defined by* (1), *where*

1) $a = 0,1,2,\dots,$ *if* $\mu = 0$;

2) $a = 0,$ *if* $\mu = -1,1$;

3) $a = 0,1,\dots,[|\frac{\mu}{2}|],$ *if* $\mu \neq -1,0,1,$

where $\mu = h_1 + h_2 + \dots + h_n - 1.$

Proof. An isomorphical test of such isotopes is given by **lemma 2** and is expressed by the relationship (4). Since in this case k=1 or k=-1, then the isomorphism of the isotopes means that one of the equalities

$$b = \mu c + a \quad \text{or} \quad -b = \mu c + a \tag{10}$$

is true. Let $\mu = 0$, then the isomorphism is possible iff $b = \pm a$. Hence all isotopes with $a > 0$ are pairwise nonisomorphic. If $\mu = \pm 1$, then $c = b \pm a$ give an isomorphism of any pair of linear isotopes with the same coeffitient sequence. Finally, let $\mu \neq -1,0,1$, then the equalities (10) mean that

$$b \equiv a (\operatorname{mod} \mu).$$

So, in this case any linear isotope is isomorphic to exactly one isotope defined by (1) with $a = 0,1,\dots,[|\frac{\mu}{2}|]$. The proof has been completed.

The immediate corollary of the lemmas **1,2** is

Lemma 5. *A transformation* α *of the set* C *is an endomorphism of the isotope (C;f) defined by* (1) *if and only if there exist elements* k *and* c *of* C *such that*

$$\alpha x = kx + c, \quad (k-1)a = \mu c,$$

where $\mu = h_1 + h_2 + \dots + h_n - 1.$

The next statements is obvious (we denote the semidirect product by "♦").

Corollary. *If the isotope (C;f) is defined by* (1) *and* $a = 0$, *then the relations*

$$End(C;f) \cong Ker\mu \blacklozenge C, \quad Aut(C;f) \cong Ker\mu \blacklozenge C$$

hold. In particular, $End(C;f)$ *is a subnearing of the linear transformation nearing of the group (C;+).*

Theorem 3, lemma 5 and its **corollary** permit to calculate the endomorphism semigroup and the automorphism group of the arbitrary linear isotope of the infinite cyclic group. We shall express these results in the following theorem.

Theorem 4. *Let (Z;f) be an arbitrary isotope of the infinite cyclic group (Z;+), where Z is the ring of integers, and* (1) *be its decomposition. If we denote* $\mu = h_1 + h_2 + \ldots + h_n - 1$ *and* $d = GCD(a,\mu)$, *then the following conditions are fulfilled:*

1) $End(Z;f) \cong Z \blacklozenge Z, Aut(Z;f) \cong Z_2 \blacklozenge Z,$ *when* $a = \mu = 0$;

2) $End(Z;f) \cong Z, Aut(Z;f) \cong Z_2,$ *when* $a = 0$ *and* $\mu \neq 0$;

3) $End(Z;f) \cong Aut(Z;f) \cong (Z;+),$ *when* $a \neq 0$ *and* $\mu = 0$;

4) $End(Z;f) \cong (Z;\cdot), Aut(Z;f) \cong Z_2,$ *when* $a \neq 0$ *and* $\mu = \pm 1$;

5) $End(Z;f) \cong (\frac{\mu}{d}Z + 1;\cdot), Aut(Z;f) \cong Z_2,$ *when* $a \neq 0$ *and* $\mu = \pm 2a$;

6) $End(Z;f) \cong (\frac{\mu}{d}Z + 1;\cdot), Aut(Z;f) \cong \{1\},$ *when* $a \neq 0$ *and* $\mu \neq 0, \pm 1, \pm 2a$.

Proof. We consider the case $\mu \neq 0, \pm 1$, $a \neq 0$ only because other ones are obvious. By the **lemma 5** we have the equality

$$(k-1)\frac{a}{d} = \frac{\mu}{d}c.$$

It implies the existence of an integer t such that

$$k - 1 = \frac{\mu}{d}t \quad \text{and} \quad c = \frac{a}{d}t,$$

i.e. any endomorphism has the expression

$$\alpha(x) = (\frac{\mu}{d}t + 1)x + \frac{a}{d}t$$

for some integer t. It is easy to see that the converse statement is true as well. Thus, we have established an one-to-one correspondence between semigroups

$$End(Q;f) \quad \text{and} \quad (\frac{\mu}{d}Z + 1).$$

It is easy to verify that it is an isomorphism. In particular, the group of all invertible elements of the semigroup $(\frac{\mu}{d}Z+1)$ is isomorphic to the automorphism group of the linear isotope *(Z;f)*. If an integer is invertible, then it belongs to {-1,1}. Let

$$\frac{\mu}{d}t+1=-1,$$

i.e. $\frac{\mu}{d}t=-2$. Then $t=\pm1,\pm2$ and the numbers t,μ have different signs. Since $a\leq[|\frac{\mu}{2}|]$, then $d\leq a<|\mu|$, so *t*=1 if $\mu<0$ and *t*=-1 if $\mu>0$. Moreover, the relationships both $|\mu|=2d$ and $d\leq a<|\mu|$ hold only if *a*=*d*.

A problem of description of endomorphism semigroup and automorphism group of a finite linear isotope is still open. We shall single out some relationships only.

Denote by $M(f)$ $(M^*(f))$ the set of all coefficients of endomorphisms (respectively isomorphisms), i.e.

$$M(f)=\{k|(\exists c)\alpha\in End(Q;f),\text{ where }\alpha x=kx+c\},$$
$$M^*(f)=\{k|(\exists c)\alpha\in Aut(Q;f),\text{ where }\alpha x=kx+c\},$$

It is easy to verify that $(M(f);\cdot)$ is a monoid and $(M^*(f);\cdot)$ is a subgroup of all its invertible elements. The **lemma 5** implies

Corollary. *A transformation* α *of the set* Z_m *is an endomorphism of the isotope* $(Z_m;f)$ *defined by* (1) *if and only if* $\alpha x=kx+c$ *and*

$$(k-1)c=\mu c(\text{mod}\,m), \qquad (11)$$

where $\mu=h_1+h_2+\ldots+h_n-1$.

After the **theorem 2** and the corollary of the **lemma 5** we shall only consider the case

$$a\not\equiv0(\text{mod}\,m)$$

and *a* is a common divisor of μ and *m*. The relationship (11) means that

$$k\equiv\frac{\mu}{a}c+1(\text{mod}\frac{m}{a}),$$

i.e.

$$k \equiv \frac{m}{a} t + \frac{\mu}{a} c + 1 (\mathrm{mod}\, m)$$

for some integer t. So,

$$k \in \frac{m}{a} Z_m + \frac{\mu}{a} Z_m + 1.$$

It is easy to verify that the converse statement is true as well. Thus

$$M(f) = \frac{m}{a} Z_m + \frac{\mu}{a} Z_m + 1$$

and

$$M^*(f) = Z_m^* \cap (\frac{m}{a} Z_m + \frac{\mu}{a} Z_m + 1). \tag{12}$$

It is easy to make sure that

1) the transformations α and β defined by

$$\alpha x \equiv kx + c (\mathrm{mod}\, m),$$
$$\beta x \equiv k_1 x + c (\mathrm{mod}\, m)$$

are endomorphisms of $(Z_m; f)$ if and only if

$$k_1 \in \frac{m}{a} Z_m + k.$$

2) the transformations α and β defined by

$$\alpha x \equiv kx + c (\mathrm{mod}\, m),$$
$$\beta x \equiv kx + c_1 (\mathrm{mod}\, m)$$

are endomorphisms of $(Z_m; f)$ if and only if

$$c_1 \in \frac{m}{d} Z_m + c,$$

where $d = GCD(\mu, m)$.

These assertions imply the following relationships for the sets $End(Z_m; f)$ and $Aut(Z_m; f)$:

$$End(Z_m; f) = \bigcup_{c \in Z_m} (\frac{m}{a} Z_m + \frac{\mu}{a} c + 1) \times (\frac{m}{d} Z_m + c), \tag{13}$$

$$End(Z_m; f) = \bigcup_{k \in M(f)} (\frac{m}{a} Z_m + k) \times (\frac{m}{d} Z_m + (\frac{\mu}{d})^{\varphi(\frac{\mu}{d})-1} \frac{(k-a)}{d}),$$

$$Aut(Z_m;f) = \bigcup_{c\in Z_m} ((\frac{m}{a}Z_m + \frac{\mu}{a}c+1)\cap Z_m^*)\times(\frac{m}{d}Z_m + c), \tag{14}$$

$$Aut(Z_m;f) = \bigcup_{k\in M^*(f)} ((\frac{m}{a}Z_m + k)\cap Z_m)\times((\frac{m}{d}Z_m + (\frac{m}{d})^{\varphi(\frac{\mu}{d})-1}\frac{(k-1)a}{d}),$$

where φ is the *Euler's phi-function.* From (13) and (14) it follows

Proposition 1. *In the linear isotope* $(Z_m;f)$ *defined by* (1) *with*

$$h_1+h_2+\ldots+h_n \equiv 1(\mathrm{mod}\, m)$$

the following relationships

$$End(Z_m;f) \cong Z_m \times (\frac{m}{a}Z_m + 1),$$

$$Aut(Z_m;f) \cong Z_m \times ((\frac{m}{a}Z_m + 1)\cap Z_m^*)$$

hold. If in addition $a=1$, *then the endomorphism semigroup coincides with the automorphism group and is isomorphic to* Z_m.

Proposition 2. *An automorphism group of a linear isotope of prime order* p *is isomorphic to* $Z_p, HolZ_p$ *or* Z_{p-1}.

References

1. *Sokhatskii F.N.* About isomorphism of linear quasigroups., International algebraic conference, Barnaul, 20-25 august 1991, p.138.

2. *Belousov V.D.* Foundations of the theory of quasigroups and loops.(Russian), Moscow, "Nauka", 1967.

3. *Sokhatskii F.N.* About the *M*-associative operatives. (Russian), Third All-union symposium on semigroup theory (Sverdlovsk), 1988, p.88.

4. *Sokhatskii F.N., Sivakovskii P.V.* Quasigroups which are linear on a cyclic group. International algebraic conference, Barnaul, 20-25 august 1991, p.140.

5. *Izbash V.I.* About quasigroups which are group isotopes. (Russian), IM VC AN MSSR, Kishinev, 1989, 21p., Dep. VINITI 29.06.89, N 4298-B89.

Sokhatskyj Fedir **Ph.D.**
Syvakivskyj Petro
department of algebra,
Vinnytsa State Pedagogical Institute,
32, Chervonopraporna str.,
Vinnytsa, 287100,
Ukraine.

Received August 15, 1993