Journal of the Nigerian Mathematical Society
Vol. 32, pp. 317-329, 2013

ON THE ISOTOPY STRUCTURE OF ELEMENTS OF THE GROUP $\mathcal{P}_p(\mathbb{Z}_n)$

T. G. JAÍYÉỌLÁ[1], E. ILỌJIDE AND B. A. POPOOLA

IN HONOUR OF PROFESSOR CHINUA ACHEBE (1930-2013)
TO PROFESSOR ADENIRAN OLUSHOLA JOHN

ABSTRACT. In this study, some linear-bivariate polynomials $p(x, y) = a + bx + cy$ that generate quasigroups over the ring $\mathbb{Z}_n$ and which forms a group $\mathcal{P}_p(\mathbb{Z}_n)$ which is a subgroup of a monoid $H_p(\mathbb{Z}_n)$ are studied. Their isotopy structure (isotopism, autotopism, isomorphism, automorphism) are also studied. Some sufficient conditions based on a, b, c, for the isomorphism, isotopism and equivalence of the generated quasigroups are also deduced.

Keywords and phrases: quasigroups, parastrophes, linear bivariate polynomials
2010 Mathematical Subject Classification: 20N02, 20N05

1. INTRODUCTION

Let G be a non-empty set. Define a binary operation $(\cdot)$ on G. $(G, \cdot)$ is called a groupoid if G is closed under the binary operation $(\cdot)$. A groupoid $(G, \cdot)$ is called a quasigroup if the equations $a \cdot x = b$ and $y \cdot c = d$ have unique solutions for x and y for all $a, b, c, d \in G$. A quasigroup $(G, \cdot)$ is called a loop if there exists a unique element $e \in G$ called the identity element such that $x \cdot e = e \cdot x = x$ for all $x \in G$.

A function $f : S \times S \to S$ on a finite set S of size $n > 0$ is said to be a Latin square (of order n) if for any value $a \in S$ both functions $f(a, \cdot)$ and $f(\cdot, a)$ are permutations of S. That is, a Latin square is a square matrix with n^2 entries of n different elements, none of them occurring more than once within any row or column of the matrix.

Received by the editors December 13, 2012; Revised: April 15, 2013; Accepted: April 25, 2013
[1]Corresponding author

Definition 1: A pair of Latin squares $f_1(\cdot,\cdot)$ and $f_2(\cdot,\cdot)$ is said to be orthogonal if the pairs $\big(f_1(x,y), f_2(x,y)\big)$ are all distinct, as x and y vary.

For every quasigroup $(G,\cdot)$, there exists five other corresponding quasigroups.

Definition 2: (Parastrophes) Let (G,θ) be a quasigroup. The five parastrophes of (G,θ) are (G,θ^*), (G,θ^{-1}), $(G,{}^{-1}\theta)$, $\Big(G,(\theta^{-1})^*\Big)$ and $\Big(G,({}^{-1}\theta)^*\Big)$ whose binary operations θ^*, θ^{-1}, ${}^{-1}\theta$, $(\theta^{-1})^*$ and $({}^{-1}\theta)^*$ defined on G satisfy the conditions :

(a): $y\theta^* x = z \Leftrightarrow x\theta y = z \ \forall\ x,y,z \in G$;
(b): $x\theta^{-1} z = y \Leftrightarrow x\theta y = z \ \forall x,y,z \in G$;,
(c): $z\ {}^{-1}\theta y = x \Leftrightarrow x\theta y = z \ \forall x,y,z \in G$;
(d): $z(\theta^{-1})^* x = y \Leftrightarrow x\theta y = z \ \forall x,y,z \in G$; and
(e): $y({}^{-1}\theta)^* z = x \Leftrightarrow x\theta y = z \ \forall\ x,y,z \in G$.

A quasigroup which is equivalent to all its parastrophes is called a totally symmetric quasigroup while its loop is called a Steiner loop.

Definition 3: Let $(G,\cdot)$ be a groupoid or quasigroup. The triple (A,B,C) where $A,B,C \ : \ G \longrightarrow G$ are bijections is called an autotopism of $(G,\cdot)$ if

$$xA \cdot yB = (x \cdot y)C \text{ for all } x,y \in G.$$

The group of all autotopisms of $(G,\cdot)$ is denoted by $AUT(G,\cdot)$.

Definition 4: Let $(G,\cdot)$ be a groupoid or quasigroup. A triple $(A,A,A) \in AUT(G,\cdot)$ is called an automorphism of $(G,\cdot)$ and is written simply as A. The group of all automorphisms of $(G,\cdot)$ is denoted by $AUM(G,\cdot)$.

Remark 1: Note that $AUM(G,\cdot) \leq AUT(G,\cdot)$.

Definition 5: Let $(G,\cdot)$ and $(H,\circ)$ be two groupoids. let $\alpha,\beta,\gamma : G \longrightarrow H$ be bijections. The triple (α,β,γ) is called an isotopism from $(G,\cdot)$ onto $(H,\circ)$ if

$$x\alpha \circ y\beta = (x \cdot y)\gamma \text{ for all } x,y \in G.$$

This will be expressed in the form $(G,\cdot) \xrightarrow[\text{Isotopism}]{(\alpha,\beta,\gamma)} (H,\circ)$. $(G,\cdot)$ and $(H,\circ)$ are said to be isotopic and are referred to as isotopes of each other.

Definition 6: Let $(G,\cdot) \xrightarrow[\text{Isotopism}]{(\alpha,\beta,I)} (G,\circ)$. Then, the triple (α,β,I) is called a principal isotopism from $(G,\cdot)$ onto $(G,\circ)$. $(G,\cdot)$ and $(G,\circ)$ are called principal isotopes.

Definition 7: Let $(G,\cdot) \xrightarrow[\text{Isotopism}]{(\alpha,\alpha,\alpha)} (H,\circ)$. Then, the triple (α,α,α) is called an isomorphism from $(G,\cdot)$ onto $(G,\circ)$. $(G,\cdot)$ and $(G,\circ)$ are called isomorphes and are said to be isomorphic under α which will be expressed as $(G,\cdot) \overset{\alpha}{\cong} (G,\circ)$.

The basic text books on quasigroups, loops are Pflugfelder [10], Bruck [1], Chein, Pflugfelder and Smith [2], Dene and Keedwell [3], Goodaire, Jespers and Milies [4], Sabinin [14], Smith [15], Jaíyéọlá [6] and Vasantha Kandasamy [17].

Definition 8: (Bivariate Polynomial) A bivariate polynomial is a polynomial in two variables, x and y of the form $P(x,y) = \Sigma_{i,j} a_{ij} x^i y^j$.

Definition 9: (Bivariate Polynomial Representing a Latin Square) A bivariate polynomial $P(x,y)$ over $\mathbb{Z}_n$ is said to represent (or generate) a Latin square if $(\mathbb{Z}_n,*)$ is a quasigroup where $* : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ is defined by $x * y = P(x,y)$ for all $x,y \in \mathbb{Z}_n$.

In 2001, Rivest [11] studied permutation polynomials over the ring $(\mathbb{Z}_n,+,\cdot)$ where n is a power of 2: $n = 2^w$. This is based on the fact that modern computers perform computations modulo 2^w efficiently (where $w = 2, 8, 16, 32$ or 64 is the word size of the machine), and so it was of interest to study PPs modulo a power of 2. Below are some important results from his work.

Theorem 1: (Rivest [11]) A bivariate polynomial $P(x,y) = \Sigma_{i,j} a_{ij} x^i y^j$ represents a Latin square modulo $n = 2^w$, where $w \geq 2$, if and only if the four univariate polynomials $P(x,0)$, $P(x,1)$, $P(0,y)$, and $P(1,y)$ are all permutation polynomial modulo n.

Theorem 2: (Rivest [11]) There are no two polynomials $P_1(x,y)$, $P_2(x,y)$ modulo 2^w for $w \geq 1$ that form a pair of orthogonal Latin squares.

In 2009, Vadiraja and Shankar [16] motivated by the work of Rivest continued the study of permutation polynomials over the ring $(\mathbb{Z}_n,+,\cdot)$ by studying Latin squares represented by linear and quadratic bivariate polynomials over $\mathbb{Z}_n$ when $n \neq 2^w$ with the characterization of some PPs. Some of the main results they got are stated below.

Theorem 3: (Vadiraja and Shankar [16]) A bivariate linear polynomial $a+bx+cy$ represents a Latin square over $\mathbb{Z}_n$, $n \neq 2^w$ if and only if one of the following equivalent conditions is satisfied:

(i): both b and c are coprime with n.

(ii): $a+bx$, $a+cy$, $(a+c)+bx$ and $(a+b)+cy$ are all permutation polynomials modulo n.

(iii): b and c are invertible in $(\mathbb{Z}, \times)$.

Theorem 4: (Vadiraja and Shankar [16]) If $P(x, y)$ is a bivariate polynomial having no cross term, then $P(x, y)$ gives a Latin square if and only if $P(x, 0)$ and $P(0, y)$ are permutation polynomials.

Theorem 5: (Vadiraja and Shankar [16]) Let n be even and $P(x, y) = f(x) + g(y) + xy$ be a bivariate quadratic polynomial, where $f(x)$ and $g(y)$ are permutation polynomials modulo n. Then $P(x, y)$ does not give a Latin square.

The authors were able to establish the fact that Rivest's result for a bivariate polynomial over $\mathbb{Z}_n$ when $n = 2^w$ is true for a linear-bivariate polynomial over $\mathbb{Z}_n$ when $n \neq 2^w$. Although the result of Rivest was found not to be true for quadratic-bivariate polynomials over $\mathbb{Z}_n$ when $n \neq 2^w$ with the help of counter examples, nevertheless some of such squares can be forced to be Latin squares by deleting some equal numbers of rows and columns.

Furthermore, Vadiraja and Shanhar [16] were able to find examples of pairs of orthogonal Latin squares generated by bivariate polynomials over $\mathbb{Z}_n$ when $n \neq 2^w$ which was found impossible by Rivest for bivariate polynomials over $\mathbb{Z}_n$ when $n = 2^w$.

Theorem 6: (Jaiyéọlá and Ilojide [7]) Let $P_1(x, y) = P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that b and c are invertible in $\mathbb{Z}_n$. Let $P_i(x, y)$, $i = 2, 3, 4, 5, 6$ denote the linear-bivariate polynomials that represent the parastrophes of $(G, \theta) = (G, P_1)$: $(G, \theta^*) = (G, P_2)$, $(G, \theta^{-1}) = (G, P_3)$, $(G, {}^{-1}\theta) = (G, P_5)$, $\left(G, (\theta^{-1})^*\right) = (G, P_4)$ and $\left(G, ({}^{-1}\theta)^*\right) = (G, P_6)$. Then,

(i): $P_2(x, y) = a + cx + by$;
(ii): $P_3(x, y) = -ac^{-1} - bc^{-1}x + c^{-1}y$;
(iii): $P_4(x, y) = -ac^{-1} + c^{-1}x - bc^{-1}y$;
(iv): $P_5(x, y) = -ab^{-1} + b^{-1}x - cb^{-1}y$;
(v): $P_6(x, y) = -ab^{-1} - cb^{-1}x + b^{-1}y$.

Theorem 7: (Jaiyéọlá and Ilojide [7]) Let $P_1(x, y) = P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ and let

$$\mathcal{H}_P(\mathbb{Z}_n) = \{P_f(x, y) = f_1(a, b, c) + f_2(a, b, c)x + f_3(a, b, c)y \mid$$

$$f_1, f_2, f_3 \ : \ \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n\}.$$

For all $P_f, P_g \in \mathcal{H}_P(\mathbb{Z}_n)$, where $P_f(x, y) = f_1(a, b, c) + f_2(a, b, c)x + f_3(a, b, c)y$ and $P_g(x, y) = g_1(a, b, c) + g_2(a, b, c)x + g_3(a, b, c)y$, define

$*$ on $\mathcal{H}_P(\mathbb{Z}_n)$ as follows:

$$\begin{aligned} P_f * P_g = (P_f)_g = g_1\Big(f_1(a,b,c), f_2(a,b,c), f_3(a,b,c)\Big) \\ + g_2\Big(f_1(a,b,c), f_2(a,b,c), f_3(a,b,c)\Big)x \\ + g_3\Big(f_1(a,b,c), f_2(a,b,c), f_3(a,b,c)\Big)y. \end{aligned}$$

$\Big(\mathcal{H}_P(\mathbb{Z}_n), *\Big)$ is a monoid.

Theorem 8: (Jaiyéọlá and Ilojide [7]) Let $P_1(x,y) = P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ and let $\mathcal{P}_P(\mathbb{Z}_n) = \{P_1, P_2, P_3, P_4, P_5, P_6\}$. Then, $\Big(\mathcal{P}_P(\mathbb{Z}_n), *\Big)$ is a subgroup of $\Big(\mathcal{H}_P(\mathbb{Z}_n), *\Big)$.

The objective of the present work is to study the isotopic structure of elements of the group $\mathcal{P}_P(\mathbb{Z}_n) \leq \mathcal{H}_P(\mathbb{Z}_n)$. Some linear-bivariate polynomials $P(x,y) = a + bx + cy$ that generate quasigroups over the ring $\mathbb{Z}_n$ and which forms a group $\mathcal{P}_P(\mathbb{Z}_n)$ which is a subgroup of a monoid $H_P(\mathbb{Z}_n)$ are investigated. Their isotopy structure (isotopism, autotopism, isomorphism, automorphism) are studied. Some sufficient conditions based on a, b, c, for the isomorphism, isotopism and equivalence of the generated quasigroups are also deduced.

2. MAIN RESULTS

Theorem 9: Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Let $P_f(x,y) = f_1(a,b,c) + f_2(a,b,c)x + f_3(a,b,c)y = f_1 + f_2x + f_3y \in \mathcal{H}_P(\mathbb{Z}_n)$ such that f_1, f_2 and f_3 are invertible. Then

(a): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{ba^{-1}f_1f_2^{-1}}, R^{\times}_{ca^{-1}f_1f_3^{-1}}, R^{\times}_{a^{-1}f_1}\right)} (\mathbb{Z}_n, P_f)$.

(b): $(\mathbb{Z}_n, P) \overset{R^{\times}_{a^{-1}}R^{\times}_{f_1}}{\cong} (\mathbb{Z}_n, P_f) \Longleftrightarrow (\mathbb{Z}_n, P_f) \xrightarrow[\text{autotopism}]{\left(R^{\times}_{bf_2^{-1}}, R^{\times}_{cf_3^{-1}}, I\right)} (\mathbb{Z}_n, P_f)$.

(c): $R^{\times}_{a^{-1}}R^{\times}_{f_1} \in AUM(\mathbb{Z}_n, P) \Longleftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{bf_2^{-1}}, R^{\times}_{cf_3^{-1}}, I\right)} (\mathbb{Z}_n, P_f)$.

Proof:

$$\text{Now, } P_f(x,y) = f_1(a,b,c) + f_2(a,b,c)x + f_3(a,b,c)y = f_1 + f_2x + f_3y = (a + af_1^{-1}f_2x + af_1^{-1}f_3y)a^{-1}f_1 = [a + b(b^{-1}af_1^{-1}f_2x) + c(c^{-1}af_1^{-1}f_3y)]a^{-1}f_1.$$

$$\text{This implies, } P_f(x,y) = \big(P(b^{-1}af_1^{-1}f_2x, c^{-1}af_1^{-1}f_3y)\big)a^{-1}f_1 \Longrightarrow P_f(ba^{-1}f_1f_2^{-1}x, ca^{-1}f_1f_3^{-1}y) = [P(x,y)]a^{-1}f_1$$
$$\Longrightarrow P_f(xR^{\times}_{ba^{-1}f_1f_2^{-1}}, yR^{\times}_{ca^{-1}f_1f_3^{-1}}) = P(x,y)R^{\times}_{a^{-1}f_1}.$$

The conclusions of the theorem can be deduced from this.

Remark 2: Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R_b^{\times}R^{\times}_{a^{-1}}R_a^{\times}R^{\times}_{c^{-1}}, R_c^{\times}R^{\times}_{a^{-1}}R_a^{\times}R^{\times}_{b^{-1}}, R^{\times}_{a^{-1}}R_a^{\times}\right)} (\mathbb{Z}_n, P_2)$.

(b): $(\mathbb{Z}_n, P) \overset{R^{\times}_{a^{-1}}R_a^{\times}}{\cong} (\mathbb{Z}_n, P_2) \Longleftrightarrow (R^{\times}_{bc^{-1}}, R^{\times}_{cb^{-1}}, I) \in AUT(\mathbb{Z}_n, P_2) \Longleftrightarrow b = c.$

(c): $(\mathbb{Z}_n, P) \overset{R_a^{\times}}{\cong} (\mathbb{Z}_n, P_2) \Leftrightarrow (R^{\times}_{a^{-1}}R^{\times}_{bc^{-1}}, R^{\times}_{a^{-1}}R^{\times}_{cb^{-1}}, R^{\times}_{a^{-1}}) \in AUT(\mathbb{Z}_n, P_2)$.

(d): $R^{\times}_{a^{-1}}R_a^{\times} \in AUM(\mathbb{Z}_n, P) \Longleftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{(R^{\times}_{bc^{-1}}, R^{\times}_{cb^{-1}}, I)} (\mathbb{Z}_n, P_2)$.

(e): $R_a^{\times} \in AUM(\mathbb{Z}_n, P) \Longleftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R_b^{\times}R^{\times}_{a^{-1}}R^{\times}_{c^{-1}}, R_c^{\times}R^{\times}_{a^{-1}}R^{\times}_{b^{-1}}, R^{\times}_{a^{-1}}\right)} \big(\mathbb{Z}_n, P_2\big)$.

Proof: These follow from Theorem 9 with the following substitutions:

$P_2(x,y) = a + cx + by$. So, $f_1 = a, f_2 = c, f_3 = b$.

Remark 3: Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R_b^{\times}R^{\times}_{a^{-1}}R^{\times}_{-ac^{-1}}R^{\times}_{-cb^{-1}}, R_c^{\times}R^{\times}_{a^{-1}}R^{\times}_{-ac^{-1}}R_c^{\times}, R^{\times}_{a^{-1}}R^{\times}_{-ac^{-1}}\right)} (\mathbb{Z}_n, P_3)$.

(b): $(\mathbb{Z}_n, P) \overset{R^{\times}_{-c^{-1}}}{\cong} (\mathbb{Z}_n, P_3) \Longleftrightarrow (R^{\times}_{-c}, R^{\times}_{c^2}, I) \in AUT(\mathbb{Z}_n, P_3)$.

(c): $(\mathbb{Z}_n, P) \overset{R^{\times -1}_a}{\cong} (\mathbb{Z}_n, P_3) \Leftrightarrow (R_a^{\times}, R^{\times}_{-ac}, R^{\times}_{-ac^{-1}}) \in AUT(\mathbb{Z}_n, P_3)$.

(d): $R^{\times}_{-c^{-1}} \in AUM(\mathbb{Z}_n, P) \Longleftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{(R^{\times}_{-c}, R^{\times}_{c^2}, I)} (\mathbb{Z}_n, P_3)$.

(e): $R_a^{\times -1} \in AUM(\mathbb{Z}_n, P) \Leftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R_a^{\times}, R^{\times}_{-ac}, R^{\times}_{-ac^{-1}}\right)} \big(\mathbb{Z}_n, P_3\big)$.

Proof: These follow from Theorem 9 with the following substitutions:

$P_3(x,y) = -ac^{-1} - bc^{-1}x + c^{-1}y$. So, $f_1 = -ac^{-1}, f_2 = -bc^{-1}, f_3 = c^{-1}$.

Remark 4: Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R_b^{\times} R_{a^{-1}}^{\times} R_{-ac^{-1}}^{\times} R_c^{\times}, R_c^{\times} R_{a^{-1}}^{\times} R_{-ac^{-1}}^{\times} R_{-cb^{-1}}^{\times}, R_{a^{-1}}^{\times} R_{-ac^{-1}}^{\times}\right)} (\mathbb{Z}_n, P_4).$

(b): $(\mathbb{Z}_n, P) \overset{R_{-c^{-1}}^{\times}}{\cong} (\mathbb{Z}_n, P_4) \Longleftrightarrow (R_{bc}^{\times}, R_{-c^2b^{-1}}^{\times}, I) \in AUT(\mathbb{Z}_n, P_4).$

(c): $(\mathbb{Z}_n, P) \overset{R_a^{\times -1}}{\cong} (\mathbb{Z}_n, P_4) \Longleftrightarrow (R_{-ab}^{\times}, R_{acb^{-1}}^{\times}, R_{-ac^{-1}}^{\times}) \in AUT(\mathbb{Z}_n, P_4).$

(d): $R_{-c^{-1}}^{\times} \in AUM(\mathbb{Z}_n, P) \Longleftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{(R_{bc}^{\times}, R_{c^2b^{-1}}^{\times}, I)} (\mathbb{Z}_n, P_4).$

(e): $R_a^{\times -1} \in AUM(\mathbb{Z}_n, P) \Longleftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R_{-ab}^{\times}, R_{-acb^{-1}}^{\times}, R_{-ac^{-1}}^{\times}\right)} (\mathbb{Z}_n, P_4)\big).$

Proof: These follow from Theorem 9 with the following substitution:

$P_4(x,y) = -ac^{-1} + c^{-1}x - bc^{-1}y$. So, $f_1 = -ac^{-1}, f_2 = c^{-1}, f_3 = -bc^{-1}$.

Remark 5: Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R_{ba^{-1}}^{\times} R_{-ab^{-1}}^{\times} R_b^{\times}, R_{ca^{-1}}^{\times} R_{-ab^{-1}}^{\times} R_{-bc^{-1}}^{\times}, R_{a^{-1}}^{\times} R_{-ab^{-1}}^{\times}\right)} (\mathbb{Z}_n, P_5).$

(b): $(\mathbb{Z}_n, P) \overset{R_{-b^{-1}}^{\times}}{\cong} (\mathbb{Z}_n, P_5) \Longleftrightarrow (R_{b^2}^{\times}, R_{-b}^{\times}, I) \in AUT(\mathbb{Z}_n, P_5).$

(c): $(\mathbb{Z}_n, P) \overset{R_a^{\times -1}}{\cong} (\mathbb{Z}_n, P_5) \Longleftrightarrow (R_{-ab}^{\times}, R_a^{\times}, R_{-ab^{-1}}^{\times}) \in AUT(\mathbb{Z}_n, P_5).$

(d): $R_{-b^{-1}}^{\times} \in AUM(\mathbb{Z}_n, P) \Longleftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{(R_{b^2}^{\times}, R_{-b}^{\times}, I)} (\mathbb{Z}_n, P_5).$

(e): $R_a^{\times -1} \in AUM(\mathbb{Z}_n, P) \Longleftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R_{-ab}^{\times}, R_a^{\times}, R_{-ab^{-1}}^{\times}\right)} (\mathbb{Z}_n, P_5)\big).$

Proof: These follow from Theorem 9 with the following substitutions:

$P_5(x,y) = -ab^{-1} + b^{-1}x - cb^{-1}y$. So, $f_1 = -ab^{-1}, f_2 = b^{-1}, f_3 = -cb^{-1}$.

Remark 6: Let $P(x,y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{ba^{-1}}R^{\times}_{-ab^{-1}}R^{\times}_{-bc^{-1}}, R^{\times}_{ca^{-1}}R^{\times}_{-ab^{-1}}R^{\times}_{b}, R^{\times}_{a^{-1}}R^{\times}_{-ab^{-1}}\right)} (\mathbb{Z}_n, P_6)$.

(b): $(\mathbb{Z}_n, P) \overset{R^{\times}_{-b^{-1}}}{\cong} (\mathbb{Z}_n, P_6) \iff (R^{\times}_{b^2c^{-1}}, R^{\times}_{cb}, I) \in AUT(\mathbb{Z}_n, P_6)$.

(c): $(\mathbb{Z}_n, P) \overset{R^{\times -1}_{a}}{\cong} (\mathbb{Z}_n, P_6) \Leftrightarrow (R^{\times}_{-abc^{-1}}, R^{\times}_{-ac}, R^{\times}_{-ab^{-1}}) \in AUT(\mathbb{Z}_n, P_6)$.

(d): $R^{\times}_{-b^{-1}} \in AUM(\mathbb{Z}_n, P) \iff (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{(R^{\times}_{b^2c^{-1}}, R^{\times}_{cb}, I)} (\mathbb{Z}_n, P_6)$.

(e): $R^{\times -1}_{a} \in AUM(\mathbb{Z}_n, P) \Leftrightarrow (\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{-abc^{-1}}, R^{\times}_{-ac}, R^{\times}_{-ab^{-1}}\right)} (\mathbb{Z}_n, P_6)\big)$.

Proof: These follow from Theorem 9 with the following substitutions:

$P_6(x, y) = -ab^{-1} - b^{-1}cx + b^{-1}y$. So, $f_1 = -ab^{-1}$, $f_2 = -b^{-1}c$, $f_3 = b^{-1}$.

Corollary 1: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(R^{\times}_{bc^{-1}}, R^{\times}_{cb^{-1}}, I) \in AUT(\mathbb{Z}_n, P_2) \iff (\mathbb{Z}_n, P) \cong (\mathbb{Z}_n, P_2) \iff P_2(bx, cy) = P_2(cx, by) \iff (b - c)[cx - by] = 0 \iff b = c \iff P_1(x, y) = P_2(x, y)$.

(b): $(R^{\times}_{a^{-1}}R^{\times}_{bc^{-1}}, R^{\times}_{a^{-1}}R^{\times}_{cb^{-1}}, R^{\times}_{a^{-1}}) \in AUT(\mathbb{Z}_n, P_2) \iff aP_2(bx, cy) = P_2(acx, aby) \iff a[(a - 1) + (b - c)(cx - by)] = 0 \iff aP(x, y) = P_2(ax, ay)$.

(c): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{bc^{-1}}, R^{\times}_{cb^{-1}}, I\right)} (\mathbb{Z}_n, P_2)\big)$.

(d): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{b}R^{\times}_{a^{-1}}R^{\times}_{c^{-1}}, R^{\times}_{c}R^{\times}_{a^{-1}}R^{\times}_{b^{-1}}, R^{\times}_{a^{-1}}\right)} (\mathbb{Z}_n, P_2)\big) \iff P(x, y)a = P(ax, ay) \iff a = 1$.

Proof: These follow from Remark 2.

(a): This is obtained from (b) of Remark 2.
(b): This is obtained from (c) of Remark 2.
(c): This is obtained from (d) of Remark 2.
(d): This is obtained from (e) of Remark 2.

Corollary 2: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $(\mathbb{Z}_n, \times)$. Then

(a): $b = c \iff (\mathbb{Z}_n, P_2) \equiv (\mathbb{Z}_n, P_1)$.
(b): $aP_1(x, y) = P_2(ax, ay) \iff aP_2(bx, cy) = P_2(acx, aby)$.

Proof: These are gotten from (a) of Corollary 1.

Corollary 3: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(R^{\times}_{-c}, R^{\times}_{c^2}, I) \in AUT(\mathbb{Z}_n, P_3) \iff P_3(-cx, c^2y) = P_3(x, y) \iff -cP_3(x, y) = P(-cx, -cy)$.

(b): $(R^{\times}_{a}, R^{\times}_{-ac}, R^{\times}_{-ac^{-1}}) \in AUT(\mathbb{Z}_n, P_3) \iff cP_3(ax, -acy) = -aP_3(x, y) \iff P(ax, ay) = aP_3(x, y)$.

(c): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{-c}, R^{\times}_{c^2}, I\right)} (\mathbb{Z}_n, P_3) \iff P_3(-cx, c^2y) = P_3(x, y) \iff -P(cx, cy) = cP(-x, -y) \iff c = -1 \iff (\mathbb{Z}_n, P_1) \equiv (\mathbb{Z}_n, P_3)$.

(d): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{a}, R^{\times}_{-ac}, R^{\times}_{-ac^{-1}}\right)} (\mathbb{Z}_n, P_3) \iff cP_3(ax, -acy) = -aP(x, y) \iff P(ax, ay) = aP(x, y)$.

Proof: These follow from Remark 3.

(a): This is obtained from (b) of Remark 3.
(b): This is obtained from (c) of Remark 3.
(c): This is obtained from (d) of Remark 3.
(d): This is obtained from (e) of Remark 3.

Corollary 4: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $(\mathbb{Z}_n, \times)$. Then $c = -1 \iff (\mathbb{Z}_n, P_3) \equiv (\mathbb{Z}_n, P_1)$.

Proof: This is obtained from (a) of Corollary 3.

Corollary 5: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(R^{\times}_{bc}, R^{\times}_{-c^2b^{-1}}, I) \in AUT(\mathbb{Z}_n, P_4) \iff P_4(bcx, -c^2y) = P_4(x, by) \iff -P(cx, cy) = cP_4(-x, -y)$.

(b): $(R^{\times}_{-ab}, R^{\times}_{acb^{-1}}, R^{\times}_{-ac^{-1}}) \in AUT(\mathbb{Z}_n, P_4) \iff P(ax, ay) = aP_4(x, y) \iff cP_4(-abx, acy) = -aP_4(x, by)$.

(c): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{bc}, R^{\times}_{-c^2b^{-1}}, I\right)} (\mathbb{Z}_n, P_4) \iff P_4(bcx, -c^2y) = P(x, by) \iff -P(cx, cy) = cP(-x, -y) \iff c = -1$.

(d): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{-ab}, R^{\times}_{acb^{-1}}, R^{\times}_{-ac^{-1}}\right)} (\mathbb{Z}_n, P_4) \iff cP_4(-abx, acy) = -aP(x, by) \iff P(ax, ay) = aP(x, y) \iff a = 1$.

Proof: These follow from Remark 4.

(a): This is obtained from (b) of Remark 4.
(b): This is obtained from (c) of Remark 4.
(c): This is obtained from (d) of Remark 4.
(d): This is obtained from (e) of Remark 4.

Corollary 6: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $(\mathbb{Z}_n, \times)$. Then

(a): if $bc = 1$ and $c^3 = -1$, then $-P(cx, cy) = cP_4(-x, -y)$;
(b): if $bc = 1$, $c^3 = -1$ and $a + c = 0$, then $P(ax, ay) = aP_4(x, y)$;
(c): if $bc = 1$ and $c^3 = -1$, then $b = -1$ and $(\mathbb{Z}_n, P_4) \equiv (\mathbb{Z}_n, P)$;
(d): if $bc = 1$, $c^3 = -1$ and $a + c = 0$, then $b = c = -1$ and $(\mathbb{Z}_n, P_4) \equiv (\mathbb{Z}_n, P)$.

Proof: These follow from Corollary 5.

(a): This is obtained from (a) of Corollary 5.
(b): This is obtained from (b) of Corollary 5.
(c): This is obtained from (c) of Corollary 5.
(d): This is obtained from (d) of Corollary 5.

Corollary 7: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(R^{\times}_{b^2}, R^{\times}_{-b}, I) \in AUT(\mathbb{Z}_n, P_5) \Longleftrightarrow -P(bx, by) = bP_5(-x, -y)$.
(b): $(R^{\times}_{-ab}, R^{\times}_{a}, R^{\times}_{-ab^{-1}}) \in AUT(\mathbb{Z}_n, P_5) \Longleftrightarrow P(ax, ay) = aP_5(x, y)$.
(c): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{b^2}, R^{\times}_{-b}, I\right)} (\mathbb{Z}_n, P_5) \Longleftrightarrow -P(bx, by) = bP(-x, -y)$.
(d): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{-ab}, R^{\times}_{a}, R^{\times}_{-ab^{-1}}\right)} (\mathbb{Z}_n, P_5) \Longleftrightarrow P(ax, ay) = aP(x, y)$.

Proof: These follow from Remark 5.

(a): This is obtained from (b) of Remark 5.
(b): This is obtained from (c) of Remark 5.
(c): This is obtained from (d) of Remark 5.
(d): This is obtained from (e) of Remark 5.

Corollary 8: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $(\mathbb{Z}_n, \times)$. Then

(a): if $b = -1$, then $(\mathbb{Z}_n, P_5) \equiv (\mathbb{Z}_n, P)$;
(b): if $a = 1$, then $(\mathbb{Z}_n, P_5) \equiv (\mathbb{Z}_n, P)$.

Proof: These follow from Corollary 7.

(a): This gotten from (a) of Corollary 7.
(b): This is obtained from (b) of Corollary 7.

Corollary 9: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n$. Then

(a): $(R^{\times}_{b^2c^{-1}}, R^{\times}_{cb}, I) \in AUT(\mathbb{Z}_n, P_6) \Longleftrightarrow -P(bx, by) = bP_6(-x, -y)$.
(b): $(R^{\times}_{-abc^{-1}}, R^{\times}_{-ac}, R^{\times}_{-ab^{-1}}) \in AUT(\mathbb{Z}_n, P_6) \Longleftrightarrow P(ax, ay) = aP_6(x, y)$.
(c): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{b^2c^{-1}}, R^{\times}_{cb}, I\right)} (\mathbb{Z}_n, P_6) \Longleftrightarrow -P(bx, by) = bP(-x, -y)$.

(d): $(\mathbb{Z}_n, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{-abc^{-1}}, R^{\times}_{-ac}, R^{\times}_{-ab^{-1}}\right)} (\mathbb{Z}_n, P_6) \iff P(ax, ay) = aP(x, y)$.

Proof: These follow from Remark 6.

(a): This is obtained from (b) of Remark 6.
(b): This is obtained from (c) of Remark 6.
(c): This is obtained from (d) of Remark 6.
(d): This is obtained from (e) of Remark 6.

Corollary 10: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $\mathbb{Z}_n, \times$. Then

(a): if $b = -1$, then $(\mathbb{Z}_n, P_6) \equiv (\mathbb{Z}_n, P)$;
(b): if $a = 1$, then $(\mathbb{Z}_n, P_6) \equiv (\mathbb{Z}_n, P)$.

Proof: These follow from Corollary 9.

(a): This is obtained from (a) of Corollary 9.
(b): This is obtained from (b) of Corollary 9.

Remark 7: Let $P(x, y) = a + bx + cy$ represent a quasigroup over $\mathbb{Z}_n$ such that a is invertible in $(\mathbb{Z}_n, \times)$. Then

(a): $(\mathbb{Z}_n, P_2) \xrightarrow[\text{Isotopism}]{(R^{\times}_{cb^{-1}}, R^{\times}_{-b}, R^{\times}_{-c^{-1}})} (\mathbb{Z}_n, P_3)$.

(b): $(\mathbb{Z}_n, P_2) \xrightarrow[\text{Isotopism}]{(R^{\times}_{-c}, I, R^{\times}_{-c^{-1}})} (\mathbb{Z}_n, P_4)$.

(c): $(\mathbb{Z}_n, P_2) \xrightarrow[\text{Isotopism}]{(R^{\times}_{-c}, R^{\times}_{bc^{-1}}, R^{\times}_{-b^{-1}})} (\mathbb{Z}_n, P_5)$.

(d): $(\mathbb{Z}_n, P_2) \xrightarrow[\text{Isotopism}]{(I, R^{\times}_{-b}, R^{\times}_{-b^{-1}})} (\mathbb{Z}_n, P_6)$.

(e): $(\mathbb{Z}_n, P_3) \xrightarrow[\text{Isotopism}]{(R^{\times}_{-b}, R^{\times}_{-b^{-1}}, I)} (\mathbb{Z}_n, P_4)$.

(f): $(\mathbb{Z}_n, P_3) \xrightarrow[\text{Isotopism}]{(R^{\times}_{-b}, R^{\times}_{-c^{-1}}, R^{\times}_{cb^{-1}})} (\mathbb{Z}_n, P_5)$.

(g): $(\mathbb{Z}_n, P_3) \xrightarrow[\text{Isotopism}]{(R^{\times}_{bc^{-1}}, I, R^{\times}_{cb^{-1}})} (\mathbb{Z}_n, P_6)$.

(h): $(\mathbb{Z}_n, P_4) \xrightarrow[\text{Isotopism}]{(I, R^{\times}_{bc^{-1}}, R^{\times}_{cb^{-1}})} (\mathbb{Z}_n, P_5)$.

(i): $(\mathbb{Z}_n, P_4) \xrightarrow[\text{Isotopism}]{(R^{\times}_{-c^{-1}}, R^{\times}_{-b}, R^{\times}_{cb^{-1}})} (\mathbb{Z}_n, P_6)$.

(j): $(\mathbb{Z}_n, P_5) \xrightarrow[\text{Isotopism}]{(R^{\times}_{-c^{-1}}, R^{\times}_{-c}, I)} (\mathbb{Z}_n, P_6)$.

Proof: These follow from Remark 2, Remark 3, Remark 4, Remark 5 and Remark 6 by multiplying the isotopisms appropriately.

3. CONCLUSION

Some results in Ilojide et. al. [5] on the characterization of groupoids and quasigroups generated by linear-bivariate polynomials $P(x, y) = a+bx+cy$ over $\mathbb{Z}_n$ in conjunction with the isotopic characterization of $P(x, y)$ and some other elements group $\mathcal{P}_P(\mathbb{Z}_n)$ in this present work are applicable to cryptography. This will be of double advantage since the theory of numbers and quasigroups have been found useful for cryptography.
n-T-quasigroups have been found applicable in coding theory according to Mullen and Scherbakov [9]. Hence some of the results of this work will be found useful for the determination of error detection capabilities of the quasigroups generated by linear bivariate polynomials.

REFERENCES

[1] R. H. Bruck, *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1966.
[2] O. Chein, H. O. Pflugfelder and J. D. H. Smith, *Quasigroups and loops : Theory and applications*, Heldermann Verlag, 1990.
[3] J. Dene and A. D. Keedwell, *Latin squares and their applications*, the English University press Lts, 1974.
[4] E. G. Goodaire, E. Jespers and C. P. Milies, *Alternative loop rings*, NHMS(184), Elsevier, 1996.
[5] E. Ilojide, T. G. Jaiyeola and O. O. Owojori, *Varieties of groupoids and quasigroups generated by linear-bivariate polynomials over the ring* $\mathbb{Z}_n$, International Journal of Mathematical Combinatorics, **2**, 79–97, 2011.
[6] T. G. Jaiyeola, *A study of new concepts in smarandache quasigroups and loops*, ProQuest Information and Learning(ILQ), Ann Arbor, USA, 2009.
[7] T. G. Jaiyeola and E. Ilojide, *On a group of linear-bivariate polynomials that generate quasigroups over the ring* $\mathbb{Z}_n$, Analele Universitatii De Vest Din Timisoara, Seria Matematica-Informatica, **50**(2), 45-53, 2012.
[8] R. A. Mollin, C. Small, *On permutation polynomials over finite fields*, Internat. J. Math. and Math. Sci. **10**(3), 535–544, 1987.
[9] G. L. Mullen, V. A. Shcherbakov, *n-T-quasigroups codes with one check symbol and their error detection capabilities*, Commentationes Mathematicae Universitatis Carolinae, **45**(2), 321–340, 2004.
[10] H. O. Pflugfelder, *Quasigroups and loops : Introduction*, Sigma series in Pure Math. 7, Heldermann Verlag, Berlin, 1990.
[11] R. L. Rivest, *Permutation polynomials Modulo* 2^w, Finite Fields and Their Applications **7**, 287–292, 2001.
[12] L. Rudolf, G. L. Mullen, *When does a polynomial over a finite field Permute the elements of the field?*,The American Mathematical Monthly, **95**(3), 243–246, 1988.

[13] L. Rudolf, G. L. Mullen, *When does a polynomial over a finite field Permute the elements of the field? II*, The American Mathematical Monthly, **100**(1), 71–74, 1993.
[14] L. V. Sabinin, *Smooth quasigroups and loops*, Kluver Academic Publishers, Dordrecht, 1999.
[15] J. D. H. Smith, *An introduction to quasigroups and their representations*, Taylor and Francis Group, LLC, 2007.
[16] G. R. Vadiraja Bhatta and B. R. Shankar, *Permutation Polynomials modulo n, $n \neq 2^w$ and Latin Squares*, International J. Math. Combin. **2**, 58–65, 2009.
[17] W. B. Vasantha Kandasamy, *Smarandache loops*, Department of Mathematics, Indian Institute of Technology, Madras, India, 2002.

DEPARTMENT OF MATHEMATICS, OBAFEMI AWOLOWO UNIVERSITY, ILE - IFE, 220005, NIGERIA.
E-mail address: jaiyeolatemitope@yahoo.com and tjayeola@oauife.edu.ng

DEPARTMENT OF MATHEMATICS, FEDERAL UNIVERSITY OF AGRICULTURE, ABEOKUTA 110101, NIGERIA.
E-mail address: emmailojide@yahoo.com, ilojidee@unaab.edu.ng

DEPARTMENT OF MATHEMATICS, FEDERAL COLLEGE OF EDUCATION, OSIELE, ABEOKUTA 110101, NIGERIA.
E-mail address: bolajipopoola2002@yahoo.com