Journal of the Nigerian Mathematical Society
Vol. 31, pp. 107-118, 2012
©Nigerian Mathematical Society

ON THE RIGHT, LEFT AND MIDDLE LINEAR-BIVARIATE POLYNOMIALS OF A LINEAR-BIVARIATE POLYNOMIAL THAT GENERATES A QUASIGROUP OVER THE RING $\mathbb{Z}_n$

E. ILỌJIDE, T. G. JAÍYÉỌLÁ[1] AND S. A. AKÍNLẸ́YẸ

ON THE 50TH ANNIVERSARY OF OBAFEMI AWOLOWO UNIVERSITY

ABSTRACT. In this work, the right, left and middle linear-bivariate polynomials of a given linear-bivariate polynomials $P(x, y)$ are derived and the isotopy structure (isotopism, autotopism, isomorphism, automorphism) of quasigroups generated by them are also studied. Some sufficient conditions for the isomorphism, isotopism and equivalence of the generated quasigroups are also deduced.

Keywords and phrases: quasigroups, 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.

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.

Received by the editors March 27, 2012; Revised: June 20, 2012; Accepted: June 20, 2012

[1]Corresponding author

Definition 2: 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 3: 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 4: 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 5: 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 of each other.

Definition 6: 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 of each other and are said to be isomorphic under α which will be expressed as $(G, \cdot) \overset{\alpha}{\cong} (G, \circ)$.
Definition 7: Let $(G, \cdot)$ be a quasigroup. The left, right and middle inner mappings of $(G, \cdot)$ are:

$L_{(x,y)} = L_x L_y L_{yx}^{-1}$, $R_{(x,y)} = R_x R_y R_{xy}^{-1}$ and $T_{(x)} = R_x L_x^{-1}$ for all $x, y \in G$ respectively. R_x and L_x are respectively the right and left translation maps of $x \in G$.
Remark 2: Actually, the mappings $L_{(x,y)}$, $R_{(x,y)}$ and $T_{(x)}$ are well defined in a loop $(G, \cdot)$ with identity element e because $eL_{(x,y)} = eR_{(x,y)} = eT_{(x)} = e$. But in this study, the requirement that the inner mappings fix the identity element is not required since we are considering a quasigroup.

The basic text books on quasigroups, loops are Pflugfelder [6], Bruck [1], Chein, Pflugfelder and Smith [2], Dene and Keedwell [3],

Goodaire, Jespers and Milies [4], Sabinin [8], Smith [9], Jaíyéọlá [5] and Vasantha Kandasamy [11].

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 [7] studied permutation polynomials (PPs) 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 [7])

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 [7])

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 [10] 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 [10])

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.

Theorem 4: (Vadiraja and Shankar [10])

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 [10])

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.

Remark 3: In $(\mathbb{Z}_n, +, \cdot)$, the right translation map of $x \in \mathbb{Z}_n$ in $(\mathbb{Z}_n, \cdot)$ will be represented by $R_x^{\times}$ while the right translation map of $x \in \mathbb{Z}_n$ in $(\mathbb{Z}_n, +)$ will be represented by R_x^{+}. Note that if $n \in \mathbb{N}$ is prime, then we shall write $\mathbb{Z}_p$ for $\mathbb{Z}_n$.

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 [10] 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 $n = 2^w$.

In this present study, the right, left and middle linear-bivariate polynomials of a given linear-bivariate polynomials $P(x,y)$ are derived and the isotopy structure (isotopism, autotopism, isomorphism, automorphism) of quasigroups generated by them are also 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

2.1 DERIVATION OF THE LEFT, RIGHT AND MIDDLE BIVARIATE POLYNOMIALS OF $P(x,y)$

Theorem 6: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $zR_{(x,y)} = b^{-1}a(b-c) + bz + b^{-1}c(1-c)y$.
(b): $zT_{(x)} = bc^{-1}z + x(1 - bc^{-1})$.
(c): $zL_{(x,y)} = a(1 - bc^{-1}) + bc^{-1}(1-b)y + cz$.

Proof: Now, $xR_y = a + bx + cy$, $yL_x = a + bx + cy, xR_y^{-1} = b^{-1}(x - a - cy)$, $yL_x^{-1} = c^{-1}(y - a - bx)$.

(a): Consider $R_{(x,y)} = R_x R_y R_{xy}^{-1}$. So, $zR_{(x,y)} = zR_xR_yR_{P(x,y)}^{-1}$
$= (a + bz + cx)R_yR_{P(x,y)}^{-1} = [a + b(a + bz + cx) + cy]R_{P(x,y)}^{-1}$
$= (a + ab + b^2z + bcx + cy)R_{a+bx+cy}^{-1} = b^{-1}[a + ab + b^2z + bcx$
$+cy - a - c(a + bx + cy)] = b^{-1}a(b - c) + bz + b^{-1}c(1 - c)y$
as required.

(b): Consider $T_{(x)} = R_xL_x^{-1}$. So, $zR_xL_x^{-1} = (a + bz + cx)L_x^{-1}$
$= c^{-1}[a + bz + cx - a - bx] = bc^{-1}z + x(1 - bc^{-1})$
as required.

(c): Consider $L_{(x,y)} = L_xL_yL_{yx}^{-1}$. So, $zL_{(x,y)} = zL_xL_yL_{yx}^{-1}$
$= (a + bx + cz)L_yL_{yx}^{-1} = [a + by + c(a + bx + cz)]L_{yx}^{-1} =$
$(a + by + ac + bcx + c^2z)L_{a+by+cx}^{-1} = c^{-1}[a + by + ac + bcx + c^2z$
$-a - b(a + by + cx)] = a(1 - bc^{-1}) + bc^{-1}(1 - b)y + cz$
as required.

Theorem 7: Let $P(x, y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then
(a): $zR_{(x,y)} = b^{-1}(b - c)P\big[zb(b - c)^{-1}, y(1 - c)(b - c)^{-1}\big]$;
(b): $zT_{(x)} = P\big[c^{-1}z, c^{-1}(1 - bc^{-1})x\big] - a$;
(c): $zL_{(x,y)} = c^{-1}(c - b)P\big[(1 - b)(c - b)^{-1}y, c(c - b)^{-1}z\big]$.

Proof:

(a): Now, $zR_{(x,y)} = b^{-1}a(b-c)+bz+b^{-1}c(1-c)y$. Also, $P(x, y) = a + bx + cy$. Multiplying both sides of the last equation by $b^{-1}(b - c)$ gives
$b^{-1}(b - c)P(x, y) = ab^{-1}(b - c) + (b - c)x + b^{-1}(b - c)cy =$
$ab^{-1}(b - c) + b[b^{-1}(b - c)x] + b^{-1}c(1 - c)[(1 - c)^{-1}(b - c)y]$.
Let $x' = b^{-1}(b-c)x$ and $y' = (1-c)^{-1}(b-c)y$. This implies
$x = x'(1 - b^{-1}c)^{-1} = x'b(b - c)^{-1}$ and $y = y'[(1 - c)^{-1}(b - c)]^{-1} =$
$y'(1 - c)(b - c)^{-1} \Longrightarrow b^{-1}(b - c)P[x'b(b - c)^{-1}, y'(1 - c)(b - c)^{-1}]$
$= ab^{-1}(b - c) + bx + b^{-1}c(1 - c)y \Longrightarrow$
$zR_{(x,y)} = b^{-1}(b - c)P\big[zb(b - c)^{-1}, y(1 - c)(b - c)^{-1}\big]$
as required.

(b): Now, $zT_{(x)} = bc^{-1}z+x(1-bc^{-1})$. So, $zT_{(x)} = b[c^{-1}z]+c[c^{-1}(1-bc^{-1})x]$ and
$a+zT_{(x)} = a+b(c^{-1}z)+c[c^{-1}(1-bc^{-1})x] = P[c^{-1}z, c^{-1}(1-bc^{-1})x]$.

Therefore, $zT_{(x)} = P\big[c^{-1}z, c^{-1}(1-bc^{-1})x\big] - a$ as required.

(c): Now, $zL_{(x,y)} = a(1-bc^{-1}) + bc^{-1}(1-b)y + cz$. Also, $P(x,y) = a + bx + cy$. Multiplying both sides of the last equation by $(1-bc^{-1})$ gives

$$(1-bc^{-1})P(x,y) = a(1-bc^{-1}) + b(1-bc^{-1})x + c(1-bc^{-1})y =$$

$$a(1-bc^{-1}) + bc^{-1}(c-b)x + c(1-bc^{-1})y \Longleftrightarrow (1-bc^{-1})P(x,y) =$$

$$a(1-bc^{-1}) + bc^{-1}(1-b)[(1-b)^{-1}(c-b)x] + c[(1-bc^{-1})y].$$

Let $x' = [(1-b)^{-1}(c-b)x]$ and $y' = [(1-bc^{-1})y] = [c^{-1}(c-b)y]$. This implies $x = x'(1-b)(c-b)^{-1}$ and $y = y'c(c-b)^{-1}$. By substituting these variables, we have

$$c^{-1}(c-b)P[(1-b)(c-b)^{-1}x', c(c-b)^{-1}y'] = a(1-bc^{-1}) + bc^{-1}x'$$

$$+cy' \Longrightarrow zL_{(x,y)} = c^{-1}(c-b)P\big[(1-b)(c-b)^{-1}y, c(c-b)^{-1}z\big]$$

as required.

Theorem 8: Let $P(x,y) = a+bx+cy$ represent a groupoid over $\mathbb{Z}_p$. The corresponding left, right and middle inner bivariate polynomial of P are respectively given by:

(a): $P_\lambda(x,y) = a(1-bc^{-1}) + cx + bc^{-1}(1-b)y$,
(b): $P_\rho(x,y) = b^{-1}a(b-c) + bx + b^{-1}c(1-c)y$ and
(c): $P_\mu(x,y) = (1-bc^{-1})x + bc^{-1}y$.

Proof: These are proved by using Theorem 6 with the following argument.

(a): By writing (c) of Theorem 6 in our polynomial form, with the substitution of z with x, we obtain (a) of Theorem 8.

(b): Similarly, by writing (a) of Theorem 6 in our polynomial form, with the substitution of z with x, we obtain (b) of Theorem 8.

(c): And, by writing (b) of Theorem 6 in our polynomial form, with the substitution of z with y, we obtain (c) of Theorem 8.

2.2 ISOTOPY OF $P_\lambda(x,y)$, $P_\rho(x,y)$ AND $P_\mu(x,y)$

Theorem 9: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(\left(R^{\times}_{[b(b-c)^{-1}]}\right)^{-1}, \left(R^{\times}_{[(1-c)(b-c)^{-1}]}\right)^{-1}, R^{\times}_{[b^{-1}(b-c)]}\right)} (\mathbb{Z}_p, P_\rho)$.

(b): $(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(\left(R^{\times}_{[(1-b)(c-b)^{-1}]}\right)^{-1}, \left(R^{\times}_{[c(c-b)^{-1}]}\right)^{-1}, R^{\times}_{[c^{-1}(c-b)]}\right)} (\mathbb{Z}_p, P_\lambda)$.

(c): $(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(\left(R^{\times}_{c^{-1}}\right)^{-1}, \left(R^{\times}_{[c^{-1}(1-bc^{-1})]}\right)^{-1}, R^{+}_{(-a)}\right)} (\mathbb{Z}_p, P_\mu)$.

Proof: These are proved by using Theorem 7 and Theorem 8 as follow.

(a): From (a) of Theorem 7 and (b) of Theorem 8,

$$P_\rho(z,y) = b^{-1}(b-c)P\big[zb(b-c)^{-1}, y(1-c)(b-c)^{-1}\big]$$

which we can write as

$$P_\rho(z,y) = P\big[zR^{\times}_{[b(b-c)^{-1}]}, yR^{\times}_{[(1-c)(b-c)^{-1}]}\big]R^{\times}_{[b^{-1}(b-c)]} \Longrightarrow$$

$$P(z,y)R^{\times}_{[b^{-1}(b-c)]} = P_\rho\Big(z\big[R^{\times}_{[b(b-c)^{-1}]}\big]^{-1}, y\big[R^{\times}_{[(1-c)(b-c)^{-1}]}\big]^{-1}\Big) \Longrightarrow$$

$$(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(\left(R^{\times}_{[b(b-c)^{-1}]}\right)^{-1}, \left(R^{\times}_{[(1-c)(b-c)^{-1}]}\right)^{-1}, R^{\times}_{[b^{-1}(b-c)]}\right)} (\mathbb{Z}_p, P_\rho)$$

as required.

(b): From (c) of Theorem 7 and (a) of Theorem 8,

$$P_\lambda(y,z) = c^{-1}(c-b)P\big[(1-b)(c-b)^{-1}y, c(c-b)^{-1}z\big]$$

which we can write as

$$P_\lambda(y,z) = P\big[yR^{\times}_{(1-b)(c-b)^{-1}}, zR^{\times}_{c(c-b)^{-1}}\big]R^{\times}_{c^{-1}(c-b)} \Longrightarrow$$

$$P(y,z)R^{\times}_{c^{-1}(c-b)} = P_\lambda\Big(y\big[R^{\times}_{(1-b)(c-b)^{-1}}\big]^{-1}, z\Big[R^{\times}_{c(c-b)^{-1}}\Big]^{-1}\Big) \Longrightarrow$$

$$(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(\left(R^{\times}_{[(1-b)(c-b)^{-1}]}\right)^{-1}, \left(R^{\times}_{[c(c-b)^{-1}]}\right)^{-1}, R^{\times}_{[c^{-1}(c-b)]}\right)} (\mathbb{Z}_p, P_\lambda)$$

as required.

(c): From (b) of Theorem 7 and (c) of Theorem 8,

$$P_\mu(z,x) = P\big[c^{-1}z, c^{-1}(1-bc^{-1})x\big] - a$$

which we can write as

$$P_\mu(z,x) = P\big[zR^{\times}_{c^{-1}}, xR^{\times}_{c^{-1}(1-bc^{-1})}\big]R^{+}_{(-a)} \Longrightarrow$$

$$P(z,x)R^{+}_{(-a)} = P_\mu\Big(z\big[R^{\times}_{c^{-1}}\big]^{-1}, x\big[R^{\times}_{c^{-1}(1-bc^{-1})}\big]^{-1}\Big) \Longrightarrow$$

$$(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(\left(R^{\times}_{c^{-1}}\right)^{-1}, \left(R^{\times}_{[c^{-1}(1-bc^{-1})]}\right)^{-1}, R^{+}_{(-a)}\right)} (\mathbb{Z}_p, P_\mu)$$

as required.

Theorem 10: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P) \overset{R^{\times}_{b-c}}{\cong} (\mathbb{Z}_p, P_\rho) \iff (R^{\times}_b, R^{\times}_{1-c}, R^{\times}_b) \in AUT(\mathbb{Z}_p, P_\rho) \iff [a(b-c)](b^{-1}-1) + [c(1-c)y](b^{-1}(1-c)-1) = 0.$

(b): $(\mathbb{Z}_p, P) \overset{R^{\times}_{b-c}}{\cong} (\mathbb{Z}_p, P_\rho) \Longleftrightarrow (R^{\times}_{b^{-1}}, R^{\times}_{(1-c)^{-1}}, R^{\times}_{b^{-1}}) \in AUT(\mathbb{Z}_p, P_\rho)$
$\Longleftrightarrow [b^{-1}a(b-c)](1-b^{-1}) + [b^{-1}cy(1-b^{-1}(1-c))] = 0.$

(c): $R^{\times}_{b-c} \in AUM(\mathbb{Z}_p, P) \Longleftrightarrow b = 1 + c \Longleftrightarrow$
$(\mathbb{Z}_p, P_\rho) \xrightarrow[\text{Isotopism}]{(R^{\times}_b, R^{\times}_{1-c}, R^{\times}_b)} (\mathbb{Z}_p, P).$

Proof: These follow from (a) of Theorem 9.

Corollary 1: Let $P(x, y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$.

(a): If $a = 0$ and $b + c = 1$, then $(\mathbb{Z}_p, P) \overset{R^{\times}_{2b-1}}{\cong} (\mathbb{Z}_p, P_\rho)$;

(b): if $b = 1 + c$, then $(\mathbb{Z}_p, P_\rho) \xrightarrow[\text{Isotopism}]{(R^{\times}_{1+c}, R^{\times}_{1-c}, R^{\times}_{1+c})} (\mathbb{Z}_p, P)$.

Proof: These follow from Theorem 10.

Theorem 11: Let $P(x, y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P) \overset{R^{\times}_{c-b}}{\cong} (\mathbb{Z}_p, P_\lambda) \Longleftrightarrow (R^{\times}_{1-b}, R^{\times}_c, R^{\times}_c) \in AUT(\mathbb{Z}_p, P_\lambda) \Longleftrightarrow$
$[a(1 - bc^{-1})(1 - c)] + cx[(1 - b) - c] = 0.$

(b): $(\mathbb{Z}_p, P) \overset{R^{\times}_{c-b}}{\cong} (\mathbb{Z}_p, P_\lambda) \Longleftrightarrow (R^{\times}_{(1-b)^{-1}}, R^{\times}_{c^{-1}}, R^{\times}_{c^{-1}}) \in AUT$
$(\mathbb{Z}_p, P_\lambda) \Longleftrightarrow [a(1 - bc^{-1})(1 - c^{-1})] + x[c(1 - b)^{-1} - 1] = 0.$

(c): $R^{\times}_{c-b} \in AUM(\mathbb{Z}_p, P) \Longleftrightarrow c = 1 + b \Longleftrightarrow$
$(\mathbb{Z}_p, P_\lambda) \xrightarrow[\text{Isotopism}]{(R^{\times}_{1-b}, R^{\times}_c, R^{\times}_c)} (\mathbb{Z}_p, P).$

Proof: These follow from (b) of Theorem 9.

Corollary 2: Let $P(x, y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$.

(a): If $a = 0$ and $c + b = 1$, then $(\mathbb{Z}_p, P) \overset{R^{\times}_{2c-1}}{\cong} (\mathbb{Z}_p, P_\lambda)$;

(b): if $c = 1 + b$, then $(\mathbb{Z}_p, P_\lambda) \xrightarrow[\text{Isotopism}]{(R^{\times}_{1-b}, R^{\times}_{1+b}, R^{\times}_{1+b})} (\mathbb{Z}_p, P)$.

Proof: These follow from Theorem 11.

Theorem 12: Let $P(x, y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P) \overset{R^{\times}_c}{\cong} (\mathbb{Z}_p, P_\mu) \Longleftrightarrow (R^{\times}_1, R^{\times}_{(1-bc^{-1})^{-1}}, R^{\times}_{c^{-1}} R^{+}_{-a}) \in AUT$
$(\mathbb{Z}_p, P_\mu) \Longleftrightarrow [(1 - bc^{-1})(1 - c^{-1})]x + [bc^{-1}][(1 - bc^{-1})^{-1} - c^{-1}]y + a = 0.$

(b): $(\mathbb{Z}_p, P) \overset{R^{\times}_c}{\cong} (\mathbb{Z}_p, P_\mu) \Longleftrightarrow (R^{\times}_1, R^{\times}_{1-bc^{-1}}, R^{+}_a R^{\times}_c) \in AUT(\mathbb{Z}_p, P_\mu)$
$\Longleftrightarrow [(1 - bc^{-1})(1 - c)]x + b[c^{-1}(1 - bc^{-1}) - 1]y - ac = 0.$

(c): $R^{\times}_c \in AUM(\mathbb{Z}_p, P) \Longleftrightarrow c = 1 \Longleftrightarrow$

$$(\mathbb{Z}_p, P_\mu) \xrightarrow[\text{Isotopism}]{(R_1^\times, R_{(1-bc^{-1})}^\times, R_a^+ R_c^\times)} (\mathbb{Z}_p, P).$$

Proof: These follow from (c) of Theorem 9.

Corollary 3: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. If $c = 1$, then $(\mathbb{Z}_p, P_\mu) \xrightarrow[\text{Isotopism}]{(R_1^\times, R_{1-b}^\times, R_a^+)} (\mathbb{Z}_p, P)$.

Proof: Theses follow from Theorem 12.

Theorem 13: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P_\rho) \overset{R_{-1}^\times}{\cong} (\mathbb{Z}_p, P) \Longleftrightarrow$

$$(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(R_b^\times R_{(1-b)^{-1}}^\times, R_{c^{-1}}^\times R_{1-c}^\times, R_b^\times R_{c^{-1}}^\times\right)} (\mathbb{Z}_p, P_\lambda).$$

(b): $R_{-1}^\times \in AUM(\mathbb{Z}_p, P_\rho) \Longleftrightarrow$

$$(\mathbb{Z}_p, P_\rho) \xrightarrow[\text{Isotopism}]{\left(R_b^\times R_{(1-b)^{-1}}^\times, R_{c^{-1}}^\times R_{1-c}^\times, R_b^\times R_{c^{-1}}^\times\right)} (\mathbb{Z}_p, P_\lambda).$$

(c): $(\mathbb{Z}_p, P_\rho) \overset{R_{-1}^\times}{\cong} (\mathbb{Z}_p, P_\lambda) \Longleftrightarrow$

$$(\mathbb{Z}_p, P_\lambda) \xrightarrow[\text{autotopism}]{\left(R_b^\times R_{(1-b)^{-1}}^\times, R_{c^{-1}}^\times R_{1-c}^\times, R_b^\times R_{c^{-1}}^\times\right)} (\mathbb{Z}_p, P_\lambda).$$

Proof: These follow from (a) and (b) of Theorem 9.

Theorem 14: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P_\rho) \overset{R_{-1}^\times}{\cong} (\mathbb{Z}_p, P) \Longleftrightarrow P(-x,-y) = -P_\rho(x,y)(b-c) \Longleftrightarrow a(2b-c) + c[(1-c)-b]y = 0$.

(b): $R_{-1}^\times \in AUM(\mathbb{Z}_p, P_\rho) \Longleftrightarrow P_\rho(-x,-y) = -P_\rho(x,y) \Longleftrightarrow 2ab(b-c) = 0$.

(c): $(\mathbb{Z}_p, P_\rho) \overset{R_{-1}^\times}{\cong} (\mathbb{Z}_p, P_\lambda) \Longleftrightarrow -P_\rho(x,y) = P_\lambda(-x,-y) \Longleftrightarrow acb(b-c)^2 + bc(c-b)x + [b^2(1-b) - c^2(1-c)]y = 0$.

Proof: These follow from Theorem 13.

Corollary 4: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$.

(a): If $a = 0$ or $2b = c$ and $b + c = 1$, then $P(-x,-y) = -P_\rho(x,y)$ and $(\mathbb{Z}_p, P_\rho) \cong (\mathbb{Z}_p, P)$;

(b): if $a = 0$ or $b = c$, then $P_\rho(-x,-y) = -P_\rho(x,y)$ and $R_{-1}^\times \in AUM(\mathbb{Z}_p, P_\rho)$;

(c): if $b = c$, then $-P(x,y) = P_\lambda(-x,-y)$ and $(\mathbb{Z}_p, P_\rho) \cong (\mathbb{Z}_p, P_\lambda)$;

(d): if $a = 0$, $b = c$ and $b + c = 1$, then $(\mathbb{Z}_p, P) \equiv (\mathbb{Z}_p, P_\rho) \equiv (\mathbb{Z}_p, P_\lambda)$.

Proof: These follow from Theorem 13.

Theorem 15: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P_\rho) \overset{R^{\times}_{(b-c)^{-1}}}{\cong} (\mathbb{Z}_p, P) \Longleftrightarrow$

$$(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(R_b^{\times}R_c^{\times}, R_{1-c}^{\times}R_c^{\times}R^{\times}_{(1-bc^{-1})^{-1}}, R_b^{\times}R^{+}_{-a}\right)} (\mathbb{Z}_p, P_\mu).$$

(b): $R^{\times}_{(b-c)^{-1}} \in AUM(\mathbb{Z}_p, P_\rho) \Longleftrightarrow$

$$(\mathbb{Z}_p, P_\rho) \xrightarrow[\text{Isotopism}]{\left(R_b^{\times}R_c^{\times}, R_{1-c}^{\times}R_c^{\times}R^{\times}_{(1-bc^{-1})^{-1}}, R_b^{\times}R^{+}_{-a}\right)} (\mathbb{Z}_p, P_\mu).$$

(c): $(\mathbb{Z}_p, P_\rho) \overset{R^{\times}_{(b-c)^{-1}}}{\cong} (\mathbb{Z}_p, P_\mu) \Longleftrightarrow$

$$(\mathbb{Z}_p, P_\mu) \xrightarrow[\text{autotopism}]{\left(R_b^{\times}R_c^{\times}, R_{1-c}^{\times}R_c^{\times}R^{\times}_{(1-bc^{-1})^{-1}}, R_b^{\times}R^{+}_{-a}\right)} (\mathbb{Z}_p, P_\mu).$$

Proof: These follow from (a) and (c) of Theorem 9.

Theorem 16: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P_\rho) \overset{R^{\times}_{(b-c)^{-1}}}{\cong} (\mathbb{Z}_p, P) \Longleftrightarrow P_\rho[(b-c)x, (b-c)y] = P(x,y)(b-c) \Longleftrightarrow [a(b-c)(1-b)] + [c(b-c)(1-c) - b]y = 0.$

(b): $R^{\times}_{(b-c)^{-1}} \in AUM(\mathbb{Z}_p, P_\rho) \Longleftrightarrow P_\rho[(b-c)x, (b-c)y] = P_\rho(x,y)(b-c) \Longleftrightarrow [a(b-c)(1-b+c)] = 0.$

(c): $(\mathbb{Z}_p, P_\rho) \overset{R^{\times}_{(b-c)^{-1}}}{\cong} (\mathbb{Z}_p, P) \Longleftrightarrow P_\rho[(b-c)x, (b-c)y] = [P_\mu(x,y)](b-c) \Longleftrightarrow ac(b-c) + b(b-c)[bc-c+b]x + (b-c)[c^2(1-c) - b^2]y = 0.$

Proof: These follow from Theorem 15.

Corollary 5: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$.

(a): If $a = 0$, and $c(b-c)(1-c) = b$, then $P_\rho[(b-c)x, (b-c)y] = P(x,y)(b-c)$ and $(\mathbb{Z}_p, P_\rho) \cong (\mathbb{Z}_p, P)$;

(b): if $a = 0$, $b = 1$, and $c(1-c)^2 = 1$, then $P_\rho[(1-c)x, (1-c)y] = P(x,y)(1-c)$ and $(\mathbb{Z}_p, P_\rho) \cong (\mathbb{Z}_p, P)$;

(c): if $a = 0$ or $b = c$ or $b = 1 + c$, then $R^{\times}_{(b-c)^{-1}} \in AUM(\mathbb{Z}_p, P_\rho)$ and $P_\rho[(b-c)x, (b-c)y] = P_\rho(x,y)(b-c)$;

(d): if $a = 0$, $bc = c - b$ and $c^2(1-c) = b^2$, then $P_\rho[(b-c)x, (b-c)y] = [P_\mu(x,y)](b-c)$, and $(\mathbb{Z}_p, P_\rho) \cong (\mathbb{Z}_p, P_\mu)$;

(e): if $a = 0$ and $c(b-c)(1-c) = b$, then and $c^2(1-c) = b^2$, then $(\mathbb{Z}_p, P) \equiv (\mathbb{Z}_p, P_\rho) \equiv (\mathbb{Z}_p, P_\mu)$.

Proof: These follow from Theorem 16.

Theorem 17: Let $P(x,y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P_\lambda) \overset{R^{\times}_{c(c-b)^{-1}}}{\cong} (\mathbb{Z}_p, P) \Longleftrightarrow$

$$(\mathbb{Z}_p, P) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{1-b}, R^{\times}_{c} R^{\times}_{(1-bc^{-1})^{-1}}, R^{+}_{-a}\right)} (\mathbb{Z}_p, P_\mu).$$

(b): $R^{\times}_{c(c-b)^{-1}} \in AUM(\mathbb{Z}_p, P_\lambda) \Longleftrightarrow$

$$(\mathbb{Z}_p, P_\lambda) \xrightarrow[\text{Isotopism}]{\left(R^{\times}_{1-b}, R^{\times}_{c} R^{\times}_{(1-bc^{-1})^{-1}}, R^{+}_{-a}\right)} (\mathbb{Z}_p, P_\mu).$$

(c): $(\mathbb{Z}_p, P_\lambda) \overset{R^{\times}_{c(c-b)^{-1}}}{\cong} (\mathbb{Z}_p, P_\mu) \Longleftrightarrow$

$$(\mathbb{Z}_p, P_\mu) \xrightarrow[\text{autotopism}]{\left(R^{\times}_{1-b}, R^{\times}_{c} R^{\times}_{(1-bc^{-1})^{-1}}, R^{+}_{-a}\right)} (\mathbb{Z}_p, P_\mu).$$

Proof: These follow from (b) and (c) of Theorem 9.

Theorem 18: Let $P(x, y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$. Then

(a): $(\mathbb{Z}_p, P_\lambda) \overset{R^{\times}_{c(c-b)^{-1}}}{\cong} (\mathbb{Z}_p, P) \Longleftrightarrow [P(x, y)]c^{-1}(c-b) = P_\lambda[c^{-1}(c-b)x, c^{-1}(c-b)y] \Longleftrightarrow c(c-b)(b-c)x+(c-b)[c^2-b(1-b)]y = 0.$

(b): $R^{\times}_{c(c-b)^{-1}} \in AUM(\mathbb{Z}_p, P_\lambda) \Longleftrightarrow [P_\lambda(x, y)]c^{-1}(c-b) = P_\lambda[c^{-1}(c-b)x, c^{-1}(c-b)y] \Longleftrightarrow a(c-b)[(c-b)-c]+b(1-b)(c-b)(1-c^2)y = 0.$

(c): $(\mathbb{Z}_p, P_\lambda) \overset{R^{\times}_{c(c-b)^{-1}}}{\cong} (\mathbb{Z}_p, P_\mu) \Longleftrightarrow [P_\mu(x, y)]c^{-1}(c-b) = P_\lambda[c^{-1}(c-b)x, c^{-1}(c-b)y] \Longleftrightarrow ac(c-b) + (c-b)[c^2-(c-b)]x + b(c-b)[(1-b)-1]y = 0.$

Proof: These follow from Theorem 17.

Corollary 6: Let $P(x, y) = a + bx + cy$ represent a groupoid over $\mathbb{Z}_p$.

(a): If $b = c$, then $[P(x, y)]c^{-1}(c-b) = P_\lambda[c^{-1}(c-b)x, c^{-1}(c-b)y]$ and $(\mathbb{Z}_n, P_\lambda) \cong (\mathbb{Z}_n, P)$;

(b): if $b = c$, then $[P_\lambda(x, y)]c^{-1}(c-b) = P_\lambda[c^{-1}(c-b)x, c^{-1}(c-b)y]$ and $R^{\times}_{c(c-b)^{-1}} \in AUM(\mathbb{Z}_n, P_\lambda)$;

(c): if $a = 0$ and $b = 1$, then $R^{\times}_{c(c-1)^{-1}} \in AUM(\mathbb{Z}_p, P_\lambda)$;

(d): if $a = 0$ and $c^2 = 1$, then $R^{\times}_{c(c-b)^{-1}} \in AUM(\mathbb{Z}_p, P_\lambda)$;

(e): if $a = 0$ and $b = c$, then $[P_\mu(x, y)]c^{-1}(c-b) = P_\lambda[c^{-1}(c-b)x, c^{-1}(c-b)y]$ and $(\mathbb{Z}_n, P_\lambda) \cong (\mathbb{Z}_n, P_\mu)$;

(f): if $a = 0$ and $b = c$, then $(\mathbb{Z}_p, P) \equiv (\mathbb{Z}_p, P_\lambda) \equiv (\mathbb{Z}_p, P_\mu)$.

Proof: These follow from Theorem 18.

REFERENCES

[1] R. H. Bruck (1966), *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen - Heidelberg, 185pp.

[2] O. Chein, H. O. Pflugfelder and J. D. H. Smith (1990), *Quasigroups and loops : Theory and applications*, Heldermann Verlag, 568pp.
[3] J. Dene and A. D. Keedwell (1974), *Latin squares and their applications*, the English University press Lts, 549pp.
[4] E. G. Goodaire, E. Jespers and C. P. Milies (1996), *Alternative loop rings*, NHMS (184), Elsevier, 387pp.
[5] T. G. Jaíyéọlá (2009), *A study of new concepts in smarandache quasigroups and loops*, ProQuest Information and Learning(ILQ), Ann Arbor, USA, 127pp.
[6] H. O. Pflugfelder (1990), *Quasigroups and loops : Introduction*, Sigma series in Pure Math. 7, Heldermann Verlag, Berlin, 147pp.
[7] R. L. Rivest (2001), *Permutation polynomials Modulo* 2^w, Finite Fields and Their Applications 7, 287–292.
[8] L. V. Sabinin (1999), *Smooth quasigroups and loops*, Kluver Academic Publishers, Dordrecht, 249pp.
[9] J. D. H. Smith (2007), *An introduction to quasigroups and their representations*, Taylor and Francis Group, LLC.
[10] G. R. Vadiraja Bhatta and B. R. Shankar (2009), *Permutation Polynomials modulo* n, $n \neq 2^w$ *and Latin Squares*, International J. Math. Combin. 2, 58–65.
[11] W. B. Vasantha Kandasamy (2002), *Smarandache loops*, Department of Mathematics, Indian Institute of Technology, Madras, India, 128pp.

Department of Mathematics, Federal University of Agriculture, Abeokuta 110101, Nigeria.
E-mail addresses: emmailojide@yahoo.com, ilojidee@unaab.edu.ng
Department of Mathematics, Obafemi Awolowo University, Ile Ife 220005, Nigeria.
E-mail addresses: jaiyeolatemitope@yahoo.com ,tjayeola@oauife.edu.ng
Department of Mathematics, Federal University of Agriculture, Abeokuta 110101, Nigeria.
E-mail addresses: akinleye_sa@yahoo.com, saakinleye@unaab.edu.ng