



On Isomorphism Classes of Right Loops

Sushmita Kushwaha¹, A. C. Yadav²

^{1,2}Department of Mathematics

Faculty of Science and Technology

Mahatma Gandhi Kashi Vidyapith

Varanasi, 221002, INDIA

ARTICLE INFO

Published Online:
13 May 2025

Corresponding Author:
Sushmita Kushwaha

ABSTRACT

In this article, we find formula for non-isomorphic right loops of order n by operation \circ will be termed as the deformation of \circ through the map $g: S \rightarrow \text{Sym}(S)$ with $g(e) = I$.

KEYWORDS: Right loops, Group Torsion, Isomorphic classes, Deformation of operation.

I. INTRODUCTION

In 1937, Quasigroup was introduced by D. Hilbert and theory extended in 1940's by R. Moufang and other algebraists prompt that a set with a binary operation division is always possible. In 1950's, Quasigroup studied by R. H. Bruck and L. J. Paige. In time duration 1960 to 1970, connections established between right loops and other algebraic structures. M. Kinyon research on the structure of finite right loops. Petr. vojtechovsky research on computational study of right loops.

Let H be a subgroup of a finite group G . Let S be a right transversal to a subgroup H in G which is obtained by selecting one and only one element from each right coset Hx in G including identity element $e \in H$. Then operation induces a binary operation \circ on S given by $\{a \circ b\} = S \cap H_{ab}$ so that (S, \circ) is a right loop. Indeed, R. Lal observed that it determines a new algebraic structure (S, H, σ, f) termed as c -groupoid and conversely each c -groupoid (S, H, σ, f) determines a group $G = H \times S$ which contains H as a subgroup and S as a right transversal to H in G [9], Theorem 2.2]. The group operation on $G = H \times S$ is given by

$$(a, x)(b, y) = (a \sigma_x(b) f(x \theta b, y), x \theta b \circ y).$$

He also proved that each right loop (S, \circ) determines a group

$$G^s = \text{Sym}(S/\{e\}) S$$

which contains S as a right transversal to its subgroup $\text{Sym}(S/\{e\})$, where $\text{Sym}(S/\{e\}) = \{h \in \text{Sym}(S) : h(e) = e\}$ [9], Theorem 3.4]. This establishes a connection between groups and right loops.

Some special types of right loops which are called as gyrogroup play a crucial role in physics and geometry [10], [3]. There are several article [12] and [13] in which number

of isomorphism classes of transversals are discussed but we give the total number of isomorphism class by the operation \circ_g will be termed as the deformation of \circ through the map $g: S \rightarrow \text{Sym}(S/\{e\})$ with $g(e) = I$. The study of right loops and quasigroups continuous to evolve with researchers exploring new connections to other algebraic structures and potential applications recent advancements in computational techniques have enabled more comprehensive investigations into the properties and classification of finite right loops. As the field progresses, there is growing interest in understanding the role of right loops and quasigroups in abstract algebra, geometry theoretical computer science and cryptography. As research in this field continuous to progress, new applications and connections to other areas of mathematics and computer science are likely to emerge, further expanding the importance of right loops and quasigroups in theoretical and applied mathematics. This motivates us to find non-isomorphic right loops of given order.

In this article, In second section we gave basic terminology of right loops and operation \circ_g . In third section we gave isomorphic property of right loops and in fourth section we gave the total number of non-isomorphic class of right loops of finite order.

II. PRELIMINARIES

In this section, we given basic concept related to right loops and their properties.

Let G be a group, H a subgroup of the group G and S a right transversal of H in G containing identity of G . Let $x, y \in S$ and $h \in H$. Then $xy, xh \in G = HS$ and so

$$x \circ y = f(x, y) (x \circ y)$$

and

$$x \circ h = \sigma_x(h) \circ x \theta h$$

for unique $f(x, y)$, $\sigma_x(h) \in H$ and $x \circ y, x \theta h \in S$. Since $xe = x$, $(xy)h = x(yh)$, $(xy)z = x(yz)$, $e \circ h = h \circ e = h$ and $x(h_1 h_2) = (x h_1) h_2$. Indeed, it determines a new structure known as c -groupoid [8]. It is observed that for a given c -groupoid (S, H, σ, f) there is a group G containing H as a subgroup and S as a right transversal of H in G such that the corresponding c -groupoid is (S, H, σ, f) [[8], Theorem2.2].

The group operation \cdot on $G = H \times S$ is given by

$$(a, x) \cdot (b, y) = (a \sigma_x(b) f(x \theta b, y), x \theta b \circ y) \dots (1)$$

It is also observed that (S, \circ) is a right loop.

Next, let (S, \circ) be a right loop and $y, z \in S$. Then uniqueness of solution to equation $X \circ (y \circ z) = (x \circ y) \circ z$, $x \in S$ determines a map $f_s(y, z) : S \rightarrow S$ given by $f_s(y, z)(x) \circ (y \circ z) = (x \circ y) \circ z$. Indeed, $f_s(y, z) \in \text{Sym } S$ and $f_s(y, z)(e) = e$, $f(x, e) = f(e, x) = I_S$ for each $x \in S$. The subgroup of generated by $\{f_s(y, z) : y, z \in S\}$ of $\text{Sym } S$ is called the group torsion of S and is denoted by G_S [8]. Further, let $h \in \text{Sym}(S)$ and $y \in S$. Then for each $y \in S$, the uniqueness of solution to the equation $X \circ h(y) = h(x \circ y)$ determines a map $\sigma_y(h) : S \rightarrow S$ given by $h(x \circ y) = \sigma_y(h)(x) \circ h(y)$.

where $x \in S$. Clearly $\sigma_e(x) = x$, $\forall x \in S$. One may easily observe that $G^S = H \times S$ forms a group w.r.t. operation given by equation (2) where σ is natural action of H on S , where $H = \text{Sym}(S/\{e\}) \subset \text{Sym}(S)$.

Indeed, we have the following:

Theorem 2.1 ([8], Theorem 2.6). Let S be a right loops. Then there exists a group G^S containing S as a right transversal such that if there is any group G containing S as a right transversal then there is a unique homomorphism from G to G^S which is the identity map on S .

Take $H = \text{Sym}(S/\{e\}) \subset \text{Sym}(S)$ and $g : S \rightarrow H$ such that $g(e) = I_S$ (identity map on symbol S) then it determines an operation \circ_g on S given by $x \circ_g y = x \theta g(y) \circ y$ such that (S, \circ_g) is a right loop [10].

It is observed that every right transversal of a subgroup H in the group G determines and is determined uniquely by a map $g : S \rightarrow H$ s.t. $g(e) = I$. The operation \circ_g will be termed as the deformation of \circ through the map $g : S \rightarrow H$ with $g(e) = I$ [10]. Computation of operation \circ_g described in section IV.

III. ISOMORPHISM OF RIGHT LOOPS

In this section, we explain homomorphic and isomorphic properties of right loops.

Definition 3.2. Let (Q, \cdot) and (H, \circ) be any two right loops. Then a function $f : Q \rightarrow H$ is called a homomorphism if

$$h(x_1 \cdot x_2) = h(x_1) \circ h(x_2).$$

If h is bijective homomorphism then h is called an isomorphism.

Proposition 3.3. Let (Q, \cdot) and (H, \circ) be any two right loops. Let $h : Q \rightarrow H$ be a right loop homomorphism. Then homomorphic image $h(Q)$ is a right loop.

Proof. Let h be a homomorphism from (Q, \cdot) into (H, \circ) . Let $h(a), h(b) \in h(Q)$ and consider the equation $X \circ h(a) = h(b)$, where X is unknown.

Let c be the solution of $x \cdot a = b$ then $h(c) \circ h(a) = h(b)$, i.e; $h(c) \in h(Q)$ is a solution to the equation $X \circ h(a) = h(b)$.

Uniqueness follows immediately. Clearly $h(e_1) \in h(Q) \subset H$ is the identity of $h(Q)$.

Proposition 3.4. Let S_1 and S_2 be two right loops. If h is a isomorphism map from S_1 to S_2 then G_{S_1} isomorphic to G_{S_2} , where G_{S_i} is the group torsion of S_i .

Proof. Let S_1 and S_2 be any two right loops and $h : S_1 \rightarrow S_2$ be an isomorphism map. Let $y, z \in S_1$

$$f^{S_1}(y, z)(x) \circ (y \circ z) = (x \circ y) \circ z.$$

Applying h on both side, we get

$$\begin{aligned} h(f^{S_1}(y, z)(x) \circ (y \circ z)) &= h((x \circ y) \circ z) \\ h(f^{S_1}(y, z)(x)) \circ (h(y) \circ h(z)) &= (h(x) \circ h(y)) \circ h(z) \\ &= h(x) \theta f^{S_2}(h(y), h(z)) \circ (h(y) \circ h(z)) \end{aligned}$$

(by uniqueness of solution)

$$h(f^{S_1}(y, z)(x)) = h(x) \theta f^{S_2}(h(y), h(z))$$

$$h(f^{S_1}(y, z)(x)) = f^{S_2}(h(y), h(z)) (h(x))$$

$$h \circ f^{S_1}(y, z) = f^{S_2}(h(y), h(z)) \circ h$$

$$f^{S_2}(h(y), h(z)) = h \circ f^{S_1}(y, z) \circ h^{-1}$$

Define a map $\overline{h} : G_{S_1} \rightarrow G_{S_2}$ by

$$\overline{h}(f(y, z)) = h \circ f(y, z) \circ h^{-1} = f^{S_2}(h(y), h(z))$$

Clearly it is bijective. Now

$$\begin{aligned} \overline{h}(f^{S_1}(y_1, z_1) \circ f^{S_1}(y_2, z_2)) &= h(f^{S_1}(y_1, z_1) \circ f^{S_1}(y_2, z_2)) h^{-1} \\ &= \overline{h}(f^{S_1}(y_1, z_1)) \circ \overline{h}(f^{S_1}(y_2, z_2)) \end{aligned}$$

for all $f^{S_1}(y_1, z_1), f^{S_1}(y_2, z_2) \in G_{S_1}$.

Since $\{f^{S_1}(y, z) : y, z \in S_1\}$ generates G_{S_1} . Thus, \overline{h} is an isomorphism.

Remark 3.5. Converse need not be true. Take $S_1 = Z_4$ and $S_2 = Z_2 \times Z_2$ then $G_{S_1} \sim G_{S_2} = I$ but S_1 is not isomorphic to S_2 .

IV. NON-ISOMORPHISM CLASS OF RIGHT LOOPS

In this section, we given the non-isomorphic class of right loops of any order.

Let (S, \circ) be a finite loop of order n .

Proposition 4.6. Let (S, \circ) be any right loop of order n . Then a right loop (S, \circ_1) of order n determines unique and is uniquely determined by a map $g : S \rightarrow \text{Sym}(S/\{e\})$ such that $x \circ_g y = g(y)(x) \circ y \forall x, y \in S$.

Proof. Let (S, \circ_1) be another right loop of order n , where $e \circ_1 x = x \circ_1 e = x$, $\forall x \in S$ and e is identity of (S, \circ) . Let $x, y \in S$, by uniqueness of solution of right loop (S, \circ_1) then \exists unique element $ux \in S$ s.t. $ux \circ_1 y = x \circ_1 y$ for each $x \in S$. Clearly $e \circ_1 y = y = e \circ_1 y$ i.e; $ue = e$.

Now, for $y \in S$, define a map $g(y) : S \rightarrow S$ given by $g(y)(x) = ux$ where $ux \circ_1 y = x \circ_1 y$. By uniqueness of $ux \in S$ for each $x \in S$, $g(y)$ is bijective and $g(y)(e) = ue = e$ i.e; $g(y) \in \text{Sym}(S/\{e\})$. Clearly, $g(e) = I_S$. This determines a map $g : S \rightarrow \text{Sym}(S/\{e\})$ given by $g(y)(x) \circ y = x \circ_1 y$. Conversely each $g : S \rightarrow \text{Sym}(S/\{e\})$ determines a right loop (S, \circ_g) , where $x \circ_g y = g(y)(x) \circ y$ [10].

For convenience, we denote $g(y)(x)$ by $x \theta g(y)$.

Remark 4.7. The total no. of right loop of order n is $(n - 1)!(n - 1)$

Consider $S = \{1, 2, 3, 4\}$ be a right loop and corresponding composition table is

o	1	2	3	4
1	1	2	3	4
2	2	1	2	3
3	3	4	1	2
4	4	3	4	1

Let g be a map s.t. $g(1) = g(2) = g(3) = I, g(4) = (23)$ and the right loop structure (S, \circ_g) is given by the composition table:

(S, \circ_g)	1 2 3 4
1	1 2 3 4
2	2 1 2 2
3	3 4 1 3
4	4 3 4 1

Similarly, we calculate all right loops of order 4. Total number of right loops of order 4 is 216. The next proposition explores information when two right loops (S, \circ_{g_1}) and (S, \circ_{g_2}) are isomorphic.

Proposition 4.8. Two right loops are isomorphic if $g_1(y) = \phi^{-1}(g_2(\phi(y))\phi)$, where $\phi \in Sym(S/\{e\})$.

Proof. Let (S, \circ_{g_1}) and (S, \circ_{g_2}) are two right loops. To show that if $g_1(y) = \phi^{-1}(g_2(\phi(y))\phi)$ then (S, \circ_{g_1}) is isomorphic to (S, \circ_{g_2}) . We have

$$\begin{aligned} g_1(y) &= \phi^{-1}(g_2(\phi(y))\phi) \\ \phi(g_1(y)) &= g_2(\phi(y))\phi \\ \phi(g_1(y))x &= g_2(\phi(y))\phi(x) \\ \phi(g_1(y)x) \circ \phi(y) &= g_2(\phi(y))\phi(x) \circ \phi(y) \\ \phi(x\theta_{g_1}(y) \circ y) &= \phi(x)\theta_{g_2}(\phi(y)) \circ \phi(y) \\ \phi(x\theta_{g_1}(y) \circ y) &= \phi(x) \circ_{g_2} \phi(y) \\ \phi(x \circ_{g_1} y) &= \phi(x) \circ_{g_2} \phi(y) \end{aligned}$$

hence, (S, \circ_{g_1}) is isomorphic to (S, \circ_{g_2}) .

Proposition 4.9. Any two element ϕ_1 and ϕ_2 give unique g iff $g(\phi_1(y))\phi_1\phi_2^{-1} = \phi_1\phi_2^{-1}g(\phi_2(y))$ for all S .

Proof. Let if possible there exist g_1 and g_2 s.t.

$$\begin{aligned} g_1(y) &= \phi_1^{-1} (g(\phi_1(y)))\phi_1 \\ g_2(y) &= \phi_2^{-1} (g(\phi_2(y)))\phi_2 \end{aligned}$$

we have

$$\begin{aligned} g(\phi_1(y))\phi_1\phi_2^{-1} &= \phi_1\phi_2^{-1}g(\phi_2(y)) \\ \phi_1^{-1}g(\phi_1(y))\phi_1 &= \phi_2^{-1}g(\phi_2(y))\phi_2 \\ g_1(y) &= g_2(y) \end{aligned}$$

hence

$$g_1 = g_2$$

Conversely, suppose that

$$g(y) = \phi_1^{-1} (g(\phi_1(y)))\phi_1$$

and

$$g(y) = \phi_2^{-1} (g(\phi_2(y)))\phi_2$$

then

$$\phi_1^{-1}g(\phi_1(y))\phi_1 = \phi_2^{-1}g(\phi_2(y))\phi_2$$

hence

$$g(\phi_1(y))\phi_1\phi_2^{-1} = \phi_1\phi_2^{-1}g(\phi_2(y)).$$

In the next proposition, we calculate how many isomorphism classes of right loops of order n . From proposition [4.8] and [4.9] it is clear that number of isomorphism class is equal to no. of orbits.

Proposition 4.10. The number of isomorphism classes of right loop of order n is

$$\sum_t N_t \prod_i^{n-1} (C(t))^{n_i} / (n-1)!$$

where t run over the structure of cycle in P_{n-1} (permutation group on $n-1$ symbols), N_t is total number of element of t type in P_{n-1} , $C(t^i)$ is centralizer of t_i in P_{n-1} and n_i no. of i -length cycle in t .

Proof. By Burnside theorem, we have

$$\text{no. of orbit} = \sum (\text{Fix}(\sigma)) / (n-1)!$$

$\text{Fix}(\sigma)$ depends only on σ and two conjugate permutations have the same cycle structure. Thus, we can write

$$\text{no. of isomorphism class} = \sum_t N_t (\text{Fix}(\sigma_t)) / (n-1)!$$

$$\text{no. of isomorphism class} = \sum_t N_t \prod_i^{n-1} (C(t^i))^{n_i} / (n-1)!$$

Example 4.11. Let S be a right loop of order 4 then it has non- isomorphic class is 44.

ACKNOWLEDGEMENTS

The first author thanks to my co-author and GAP form members.

REFERENCES

- [1] A. A. Albert, “Quasigroup I”, Trans. Amer. Math. Soc., 54(1943), 507-519.
- [2] A. A. Albert, “Quasigroup II”, Trans. Amer. Math. Soc., 55(1944),401-419.
- [3] A. A. Ungar, “Weakly Associative Groups”, Resultes in Mathematics,17(1990), 150 – 168.
- [4] A. C. Yadav and V. Kakkar, “Public key exchange using right transversals and right loops”, Journal of Discrete Mathematical Sciences and Cryptography, 20. 5(2017), 1207 – 1215.
- [5] GAP Software 4.11.1.
- [6] R. Baer, “Nets and groups”, Trans. Amer. Soc., 46(1939), 110-141.
- [7] R. H. Bruck, “Contributions to the theory of Loops”, Trans. Amer. Math. Soc., 60(1946), 245-354.
- [8] R. Lal, “Transversals in groups”, Journal of algebra, 181(1996), 70 – 81.
- [9] R. Lal and A. C. Yadav, “Twisted Automorphisms and Twisted Right Gyrogroups”, Communications in Algebra, 43:8(2015), 3442-3458.
- [10] R. Lal and A. C. Yadav, “Topological Right Gyrogroups and Gyrotransversals”, Communications in Algebra, 41:9(2013), 3559 – 3575.
- [11] V. Kakkar and R. P. Shukla, “On the number of isomorphism classes of transversals”, Proc. Indian Acad. Sci. (Math. Sci.), 123(2012), 345 – 359.
- [12] V. K. Jain and R. P. Shukla, “On the Isomorphism Classes of Transversals-II”, Communications in Algebra, 39:6(2011), 2024-2036.