

On the finite Loop Algebra of the smallest Moufang loop $M(S_3, 2)$

S. Sidana and R. K. Sharma
Indian Institute of Technology Delhi

Abstract. Let $F[L]$ be a loop algebra of a loop L over a field F . In this paper, we obtain the unit loop of the loop algebra $F[L]$, where L is the smallest Moufang loop $M(S_3, 2)$ and F is a finite field of characteristic different from 3.

Key Words: Loop Algebra, Smallest Moufang Loop, Zorn's Algebra, Unit Loop.

Mathematics Subject Classification 2010: 20N05, 17D05.

1 Introduction

An alternative ring is a ring in which $x(xy) = x^2y$ and $(yx)x = yx^2$ are identities. A loop L whose loop ring $R[L]$ over some commutative, associative ring R with unity and of characteristic different from 2 is alternative, but not associative is called a RA (Ring Alternative) loop. $RA2$ loop is the loop whose loop ring is alternative only when characteristic of R is 2. Let G be a non-abelian group, $g_0 \in \mathcal{Z}(G)$ and $g \mapsto g^*$ be an involution of G such that $g_0^* = g_0$ and $gg^* \in \mathcal{Z}(G)$ for every $g \in G$. For an indeterminate u , let $L = G \dot{\cup} Gu$. Extend the multiplication in G to L by the rules

$$g(hu) = (hg)u, \quad (gu)h = (gh^*)u, \quad (gu)(hu) = g_0h^*g, \quad \text{for all } g, h \in G.$$

The loop L so constructed is a Moufang loop and is denoted by $M(G, *, g_0)$. When the involution is the inverse map and $g_0 = 1$, the identity element of G , then $M(G, -1, 1)$ is denoted as $M(G, 2)$.

The problem of determining the structure of the unit group of a group ring has always been a challenge. Associative loops are groups and not much work has been done in the direction of loop rings. So, the study of the unit loop of loop ring is equally important.

Authors [5, 6, 7] determined the structure of the unit loops of finite loop algebras of RA loops of order 32, 64 and in general of seven non-isomorphic

classes of indecomposable RA loops. FERRAZ, GOODAIRE and MILIES [2] studied the semisimple loop algebras of RA loops. But the structure of the unit loops of loop algebras of $RA2$ loops is still not known. Note that $M(S_3, 2)$ is $RA2$ loop and is the smallest Moufang loop. In this paper, we characterize the structure of the unit loop of the loop algebra $F[L]$, when L is $M(S_3, 2)$ and F is a finite field of characteristic different from 3.

The paper is organized as follows: In Section 2, we give some notations and discuss some preliminary results which will be used to prove our main results. In Section 3, we give the structure of the unit loop of $F[L]$ when the characteristic of F is 2 (Theorem 3.1) and determine the structure of the unit loop of $F[L]$ when the characteristic of F is different from 2, 3 (Theorem 3.2).

2 Preliminaries

In this section, we discuss some results which will be used further.

CHEIN and PFLUGFELDER [1] determined the smallest Moufang Loop, denoted by $M(S_3, 2)$. VOJTĚCHOVSKÝ [8] gave the presentation of $M(S_3, 2)$ as

$$M(S_3, 2) = S_3 \dot{\cup} S_3u \cong \langle a, b, u \mid a^3, b^2, u^2, abab, (au)^2, (bu)^2, (ab.u)^2 \rangle,$$

which is obtained from $S_3 \cong \langle a, b \mid a^3, b^2, abab \rangle$, the symmetric group of degree 3.

For a normal subloop N of L , the canonical map $\epsilon : L \rightarrow L/N$ lifts to an R -linear ring epimorphism $\epsilon_N : R[L] \rightarrow R[L/N]$ defined as $\epsilon_N \left(\sum_{l \in L} \alpha_l l \right) = \sum_{l \in L} \alpha_l \epsilon(l)$. We denote the kernel of ϵ_N by $\Delta_R(L, N)$.

Proposition 2.1 [3, Ch. VI, Lemma 1.2] *Let $F[L]$ be the loop algebra of a Moufang loop L and N be a finite subloop of L such that $|N|$ is invertible in F . Then $\tilde{N} = \frac{1}{|N|} \sum_{n \in N} n$ is an idempotent in $F[L]$. Moreover if N is normal in L , then*

$$(a) \quad F[L] = (F[L])\tilde{N} \oplus F[L](1 - \tilde{N})$$

$$(b) \quad (F[L])\tilde{N} \cong F[L/N] \text{ and } F[L](1 - \tilde{N}) = \Delta_F(L, N).$$

We shall use the following notations:

Table 1: Multiplication table of $M(S_3, 2)$.

\cdot	1	a	a^2	b	ab	a^2b	u	au	a^2u	bu	abu	a^2bu
1	1	a	a^2	b	ab	a^2b	u	au	a^2u	bu	abu	a^2bu
a	a	a^2	1	ab	a^2b	b	au	a^2u	u	a^2bu	bu	abu
a^2	a^2	1	a	a^2b	b	ab	a^2u	u	au	abu	a^2bu	bu
b	b	a^2b	ab	1	a^2	a	bu	abu	a^2bu	u	au	a^2u
ab	ab	b	a^2b	a	1	a^2	abu	a^2bu	bu	a^2u	u	au
a^2b	a^2b	ab	b	a^2	a	1	a^2bu	bu	abu	au	a^2u	u
u	u	a^2u	au	bu	abu	a^2bu	1	a^2	a	b	ab	a^2b
au	au	u	a^2u	abu	a^2bu	bu	a	1	a^2	a^2b	b	ab
a^2u	a^2u	au	u	a^2bu	bu	abu	a^2	a	1	ab	a^2b	b
bu	bu	abu	a^2bu	u	a^2u	au	b	a^2b	ab	1	a	a^2
abu	abu	a^2bu	bu	au	u	a^2u	ab	b	a^2b	a^2	1	a
a^2bu	a^2bu	bu	abu	a^2u	au	u	a^2b	ab	b	a	a^2	1

L'	the commutator-associator subloop of the loop L
G'	the commutator subgroup of the group G
C_n	cyclic group of order n
$M(2, F)$	ring of all 2×2 matrices over the field F
F^*	$F \setminus \{0\}$
$\mathfrak{Z}(R)$	Zorn's vector matrix algebra over a commutative and associative ring R (with unity)
$GLL(2, R)$	General Linear Loop of degree 2 over R
$J(F[L])$	Jacobson radical of alternative loop algebra $F[L]$

For more definitions and terminologies, we refer the reader to [3].

3 The Unit Loop of $F[L]$

In this section, we determine the structure of the unit loop of a finite loop algebra of $L = M(S_3, 2)$.

When $\text{char } F = 2$, we prove the following result.

Theorem 3.1 *Let F be a finite field such that $|F| = 2^n$, $L = M(S_3, 2)$. Then*

$$\mathcal{U}(F[L]/J(F[L])) \cong F^* \times GLL(2, F)$$

and $1 + J(F[L]) \cong C_2^{3n}$, an elementary abelian 2-group of order 2^{3n} .

Proof. Since $\text{char } F = 2$, $F[L]$ is an alternative loop algebra. From [4, Th 2.1], the matrix representation of S_3 is

$$\theta : S_3 \rightarrow F^* \times GL(2, F)$$

given by

$$a \mapsto \left(1, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right),$$

$$b \mapsto \left(1, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right).$$

Then the matrix representation of L as

$$\phi : L \rightarrow F^* \times GLL(2, F)$$

defined by

$$a \mapsto \left(1, \begin{bmatrix} 0 & (0, 1, 0) \\ (0, 1, 0) & 1 \end{bmatrix} \right)$$

$$b \mapsto \left(1, \begin{bmatrix} 1 & (0, 1, 0) \\ (0, 0, 0) & 1 \end{bmatrix} \right)$$

and

$$u \mapsto \left(1, \begin{bmatrix} 0 & (0, 0, 1) \\ (0, 0, 1) & 0 \end{bmatrix} \right)$$

It can be easily checked that ϕ is a well defined loop homomorphism. Thus ϕ can be extended to an F -algebra homomorphism

$$\phi^* : F[L] \rightarrow F \oplus \mathfrak{3}(F).$$

Let $X = \alpha_1 1 + \alpha_2 a + \alpha_3 a^2 + \alpha_4 b + \alpha_5 ab + \alpha_6 a^2 b + \alpha_7 u + \alpha_8 au + \alpha_9 a^2 u + \alpha_{10} bu + \alpha_{11} abu + \alpha_{12} a^2 bu \in \text{Ker } \phi^*$, where $\alpha_i \in F$.

Therefore $\phi^*(X) = 0$ gives the following system of equations

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 + \alpha_7 + \alpha_8 + \alpha_9 + \alpha_{10} + \alpha_{11} + \alpha_{12} = 0$$

$$\alpha_1 + \alpha_3 + \alpha_4 + \alpha_6 = 0$$

$$\alpha_8 + \alpha_9 + \alpha_{11} + \alpha_{12} = 0$$

$$\alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = 0$$

$$\alpha_7 + \alpha_9 + \alpha_{10} + \alpha_{12} = 0$$

$$\alpha_8 + \alpha_9 + \alpha_{10} + \alpha_{11} = 0$$

$$\alpha_2 + \alpha_3 + \alpha_5 + \alpha_6 = 0$$

$$\alpha_7 + \alpha_8 + \alpha_{10} + \alpha_{12} = 0$$

$$\alpha_1 + \alpha_2 + \alpha_4 + \alpha_6 = 0$$

By solving this system of equations, we get

$$\alpha_1 = \alpha_2 = \alpha_3,$$

$$\alpha_4 = \alpha_5 = \alpha_6,$$

$$\alpha_7 = \alpha_8 = \alpha_9,$$

$$\alpha_{10} = \alpha_{11} = \alpha_{12} \text{ and}$$

$$\alpha_1 = \alpha_4 + \alpha_7 + \alpha_{10}.$$

Thus,

$$\begin{aligned} X &= \alpha_4(1 + a + a^2 + b + ab + a^2b) + \alpha_7(1 + a + a^2 + u + au + a^2u) \\ &+ \alpha_{10}(1 + a + a^2 + bu + abu + a^2bu). \\ &= \alpha_4e_1 + \alpha_7e_2 + \alpha_{10}e_3. \end{aligned}$$

Also, it can be verified that the set $S = \{e_1, e_2, e_3\}$ is linearly independent over F . Thus S forms a basis of $\text{Ker } \phi^*$ as a vector space over F . Since characteristic of F is 2, therefore $e_1^2 = 0$, $e_2^2 = 0$ and $e_3^2 = 0$. Note that

$$e_i.e_j = 1 + a + a^2 + b + ab + a^2b + u + au + a^2u + bu + abu + a^2bu$$

for all $i, j = 1, 2, 3$. It follows that each element of $\text{Ker } \phi^*$ is quasiregular with quasi-inverse as itself which implies that $\text{Ker } \phi^*$ is a quasiregular ideal of $F[L]$, which implies that $\text{Ker } \phi^* \subset J(F[L])$. Table 2 implies that ϕ^* is onto, so we have $\phi^*(J(F[L])) \subset J(F \oplus \mathfrak{Z}(F)) = 0$ and hence $J(F[L]) \subset \text{Ker } \phi^*$. This gives $J(F[L]) = \text{Ker } \phi^*$. Hence, $F[L]/J(F[L]) \cong F \oplus \mathfrak{Z}(F)$.

Considering $V_1 = 1 + J(F[L])$, an element h of V_1 is of the form $h = 1 + a_1.e_1 + a_2.e_2 + a_3.e_3$, where $a_i's \in F$. Note that

$$(e_i.e_j).e_k = e_i.(e_j.e_k) = 0 \quad \text{for all } i, j, k = 1, 2, 3.$$

Thus V_1 is an abelian group and $h^2 = 1$ for all $h \in V_1$, which gives $V_1 \cong (C_2 \times C_2 \times C_2)^n$. \square

The following theorem gives the structure of the unit loop of $F[L]$, when the characteristic of field F is different from 2, 3.

Theorem 3.2 *Let F be a finite field of characteristic different from 2, 3 and $L = M(S_3, 2)$. Then*

$$\mathcal{U}(F[L]) \cong 4F^* \times \mathcal{U}(\mathcal{A}),$$

where \mathcal{A} is a nonassociative simple algebra of dimension 8 over the field F .

Proof. We know that $L' = G' = \{1, a, a^2\} = \langle a \rangle$.

Therefore $\tilde{L}' = \frac{1 + a + a^2}{3}$ is an idempotent in $F[L]$.

From Theorem 2.1,

$$F[L] = F[L/L'] \oplus (F[L])f,$$

where $f = 1 - \tilde{L}'$.

Now

$$\begin{aligned} L/L' &= \langle a, b, u \mid a, a^3, b^2, u^2, abab, (au)^2, (bu)^2, (ab.u)^2 \rangle \\ &= \langle b, u \mid b^2, u^2, (bu)^2 \rangle \\ &\cong C_2 \times C_2. \end{aligned}$$

Table 2: Ontones of ϕ^* .

Basis element of $F \oplus \mathfrak{3}(F)$	Preimage under ϕ^*
$\left(1, \begin{pmatrix} 0 & (0, 0, 0) \\ (0, 0, 0) & 0 \end{pmatrix}\right)$	$1 + a + a^2$
$\left(0, \begin{pmatrix} 1 & (0, 0, 0) \\ (0, 0, 0) & 0 \end{pmatrix}\right)$	$a^2 + ab$
$\left(0, \begin{pmatrix} 0 & (1, 0, 0) \\ (0, 0, 0) & 0 \end{pmatrix}\right)$	$u + a^2bu$
$\left(0, \begin{pmatrix} 0 & (0, 1, 0) \\ (0, 0, 0) & 0 \end{pmatrix}\right)$	$1 + b$
$\left(0, \begin{pmatrix} 0 & (0, 0, 1) \\ (0, 0, 0) & 0 \end{pmatrix}\right)$	$a^2u + abu$
$\left(0, \begin{pmatrix} 0 & (0, 0, 0) \\ (1, 0, 0) & 0 \end{pmatrix}\right)$	$u + bu$
$\left(0, \begin{pmatrix} 0 & (0, 0, 0) \\ (0, 1, 0) & 0 \end{pmatrix}\right)$	$1 + a^2b$
$\left(0, \begin{pmatrix} 0 & (0, 0, 0) \\ (0, 0, 1) & 0 \end{pmatrix}\right)$	$au + abu$
$\left(0, \begin{pmatrix} 0 & (0, 0, 0) \\ (0, 0, 0) & 1 \end{pmatrix}\right)$	$a + ab$

Thus $F[L/L'] \cong 4F$.

Next we have to determine $(F[L])f$. We know from [4](Theorem 2.3),

$$F[S_3] = F[S_3/S'_3] \oplus (F[S_3])f \cong 2F \oplus M(2, F).$$

We first determine the isomorphism between $(F[S_3])f$ and $M(2, F)$. An element of $(F[S_3])f$ is of the form,

$$\begin{aligned} & (\alpha_1.1 + \alpha_2.a + \alpha_3.a^2 + \alpha_4.b + \alpha_5.ab + \alpha_6.a^2b) \left(\frac{2 - a - a^2}{3} \right) \\ &= \beta_1 \frac{2 - a - a^2 + 2b - a^2b - ab}{6} + \beta_2 \frac{a - a^2 - ab + a^2b}{2} \\ & \quad + \beta_3 \frac{-a + a^2 - ab + a^2b}{6} + \beta_4 \frac{2 - a - a^2 - 2b + ab + a^2b}{6} \quad (1) \end{aligned}$$

where

$$\beta_1 = \frac{2\alpha_1 - \alpha_2 - \alpha_3 + 2\alpha_4 - \alpha_5 - \alpha_6}{2}, \quad \beta_2 = \frac{\alpha_2 - \alpha_3 - \alpha_5 + \alpha_6}{2},$$

$$\beta_3 = \frac{-3\alpha_2 + 3\alpha_3 - 3\alpha_5 + 3\alpha_6}{2}, \quad \text{and } \beta_4 = \frac{2\alpha_1 - \alpha_2 - \alpha_3 - 2\alpha_4 + \alpha_5 + \alpha_6}{2}.$$

It can be easily checked that the set

$$\mathcal{B} = \left\{ E_1 = \frac{2 - a - a^2 + 2b - a^2b - ab}{6}, E_2 = \frac{a - a^2 - ab + a^2b}{2}, \right.$$

$$\left. E_3 = \frac{-a + a^2 - ab + a^2b}{6}, E_4 = \frac{2 - a - a^2 - 2b + ab + a^2b}{6} \right\}$$

is linearly independent over F .

So, \mathcal{B} forms a basis of $(F[S_3])f$ over F .

Thus $M(2, F)$ is isomorphic to $(F[S_3])f$ by defining

$$\begin{aligned} e_{11} &\mapsto E_1 \\ e_{12} &\mapsto E_2 \\ e_{21} &\mapsto E_3 \\ e_{22} &\mapsto E_4 \end{aligned}$$

where e_{ij} denotes the 2×2 matrix whose ij -th entry is 1, and all other entries are 0.

Consider the set

$$\mathcal{B}_1 = \{E'_1 = E_1 + E_4, E'_2 = E_2 - E_3, E'_3 = E_2 + E_3, E'_4 = E_1 - E_4\}.$$

Clearly \mathcal{B}_1 forms a basis of $(F[S_3])f$ over F . So, $(F[S_3])f$ is a vector space with basis \mathcal{B}_1 over the field F .

Table 3: Multiplication table of the basis elements of $(F[S_3])f$.

\cdot	E'_1	E'_2	E'_3	E'_4
E'_1	E'_1	E'_2	E'_3	E'_4
E'_2	E'_2	$-E'_1$	E'_4	$-E'_3$
E'_3	E'_3	$-E'_4$	E'_1	$-E'_2$
E'_4	E'_4	E'_3	E'_2	E'_1

Thus $(F[S_3])f$ is an associative simple algebra over the field F with identity element as E'_1 .

Now $\dim_F F[L] = 12$ and $\dim_F F[L/L'] = 4$, this implies $\dim_F (F[L])f = 8$.

We have

$$\begin{aligned} (F[L])f &\cong (F[S_3] \oplus F[S_3]u)f \\ &\cong (F[S_3])f \oplus (F[S_3])fu \\ &\cong M(2, F) \oplus (M(2, F)u) \\ &\cong \mathcal{A}. \end{aligned}$$

\mathcal{A} is an 8-dimensional non associative algebra with the basis $\{E'_1, E'_2, E'_3, E'_4, E'_5, E'_6, E'_7, E'_8\}$ and identity element as E'_1 . Here $E'_5 = E'_1u, E'_6 = E'_2u, E'_7 = E'_3u, E'_8 = E'_4u$.

Table 4: Multiplication table of the basis elements of $(F[L])f \cong \mathcal{A}$.

\cdot	E'_1	E'_2	E'_3	E'_4	E'_5	E'_6	E'_7	E'_8
E'_1	E'_1	E'_2	E'_3	E'_4	E'_5	E'_6	E'_7	E'_8
E'_2	E'_2	$-E'_1$	E'_4	$-E'_3$	E'_6	$-E'_5$	$-E'_8$	E'_7
E'_3	E'_3	$-E'_4$	E'_1	$-E'_2$	E'_7	E'_8	E'_5	E'_6
E'_4	E'_4	E'_3	E'_2	E'_1	E'_8	$-E'_7$	$-E'_6$	E'_5
E'_5	E'_5	$-E'_6$	E'_7	E'_8	E'_1	$-E'_2$	E'_3	E'_4
E'_6	E'_6	E'_5	E'_8	$-E'_7$	E'_2	E'_1	$-E'_4$	E'_3
E'_7	E'_7	E'_8	E'_5	$-E'_6$	E'_3	$-E'_4$	E'_1	E'_2
E'_8	E'_8	$-E'_7$	E'_6	E'_5	E'_4	E'_3	$-E'_2$	E'_1

We claim that \mathcal{A} is a simple algebra. So we just have to prove that f is a primitive idempotent of $F[L]$.

Let $f = x + yu$ be the central element of $F[L]$.

$$\begin{aligned}
\text{This implies} & & gf = fg & & \forall g \in S_3 \\
\Rightarrow & & g(x + yu) = (x + yu)g & & \forall g \in S_3 \\
\Rightarrow & & gx + yg.u = xg + yg^{-1}.u & & \forall g \in S_3 \\
\Rightarrow & & yg = yg^{-1} & & \forall g \in S_3 \\
\Rightarrow & & yg^2 = y & & \forall g \in S_3 \quad (*)
\end{aligned}$$

For $g = a, a^2$, $(*)$ gives $ya^2 = y, ya = y$. Thus $ya + ya^2 = 2y$ implies $yf = 0$. If possible, suppose f is not primitive in $F[L]$. That is, $f = f_1 + f_2$, where $f_1 = x_1 + y_1u$ and $f_2 = x_2 + y_2u$. Then $f_i = f_i f = (x_i + y_iu)f = x_i f \in F[S_3]$. But f is primitive in $F[S_3]$. So either $f_1 = 0$ or $f_2 = 0$. This implies f is a primitive idempotent in $F[L]$. Hence $F[L] \cong 4F \oplus \mathcal{A}$. \square

Acknowledgments.

The first author was supported by Council of Scientific and Industrial Research (CSIR), India.

References

- [1] O. Chein, H.O. Pflugfelder: The smallest Moufang loop, *Arch. Math. (Basel)* **22** (1971), 573-576.
- [2] R.A. Ferraz, E.G. Goodaire, C.P. Milies: Some classes of semisimple group (and loop) algebras over finite fields, *J. Algebra* **324** (2010), 3457-3469.
- [3] E.G. Goodaire, E. Jespers, C.P. Milies: *Alternative Loop Rings*, North-Holland Math. Stud., Vol. 184, Elsevier, Amsterdam, 1996.
- [4] R. K. Sharma, J. B. Srivastava, Manju Khan: The unit group of FS_3 , *Acta Math. Acad. Paedagog. Nyházi. (N.S.)* **23**(2) (2007), 129-142.
- [5] S. Sidana, R.K. Sharma: The unit loop of finite loop algebras of loops of order 32, *Beitr Algebra Geom*, **56** (2015), 339-349.
- [6] S. Sidana, R.K. Sharma: Finite loop algebras of RA loops of order 64, *Acta Mathematica Academiae Paedagogicae Nyíregyháziensis*, **30** (2014), 27-42.
- [7] S. Sidana, R.K. Sharma: Finite semisimple loop algebras of indecomposable RA loops, *Canad. Math. Bull.*, **58**(2) (2015), 363-373.
- [8] P. Vojtěchovský: The smallest Moufang loop revisited. *Results Math.*, **44**(1-2) (2003), 189-193.

S. Sidana* and R. K. Sharma**
Institute of Mechanics of NAS Armenia
24b Marshal Baghramian Ave.
Yerevan 0019, Armenia
*swatisidana@gmail.com
**rksharmaiitd@gmail.com

Please, cite to this paper as published in
Armen. J. Math., V. **8**, N. 1(2016), pp. 68-76