Canad. J. Math. Vol. **44** (**5**) 1992, pp. 951–973.

SIX MOUFANG LOOPS OF UNITS

EDGAR G. GOODAIRE

ABSTRACT. We compute the loops of units in the integral alternative loop rings of six Moufang loops. Four of these are subloops of the loop of matrices of determinant one in Zorn's vector matrix algebra over a ring of integers while the remaining two are closely related to this interesting algebra. This paper thus serves, in part, to highlight a Moufang analogue of SL(2, **Z**) which the author suggests is worthy of further study.

1. **Introduction.** For many people, the group of units (invertible elements) in the integral group ring **Z**G of a finite group G holds great fascination. Certainly the elements of G (together with their negatives) are units, but, as Higman showed in 1940 [8], it is rare that these are all. So how can one construct other units? Can one perhaps describe the full group of units in some specific cases? These are the sorts of questions which intrigue people and to which many have put considerable effort with, by and large, spotty progress. The unit groups of **Z**S_3 and **Z**D_4 (S_3, the symmetric group on three letters and D_4, the dihedral group of order 8) were the first to be discovered [9, 13]. Lately, Allen and Hobby have described completely the units in the integral group rings of the alternating and symmetric groups on four letters [1, 2]. In a remarkable paper not yet in print [10] Jespers and Leal have found the units in the group rings of whole families of 2-groups. In another direction, in cases where the full group of units is illusive, Sehgal and others hunt for subgroups of finite index [16].

In recent years, Chein and the author have introduced the notion of an *alternative loop ring*. Here, one starts with a loop L (an algebraic structure with a single operation; it's like a group without the requirement of associativity) and, in a manner identical to the construction of an integral group ring, constructs the *loop ring* **Z**L which is sometimes alternative. An *alternative ring* is a ring which satisfies the two laws

$$(yx)x = yx^2 \text{ and } x(xy) = x^2y.$$

An associative ring is alternative, hence a group ring is an alternative loop ring, but the interest, for some, lies in the "not associative" situation for here one can hope to generalize or prove analogues of theorems already known for group rings. In particular, the loop of units in an alternative loop ring is a natural place to look for such results. In 1986, Parmenter and the author generalized the afore-mentioned Higman result by proving that except for abelian groups of certain small exponents and for *Hamiltonian*

Research supported in part by the Natural Sciences and Engineering Research Council of Canada, Grant No. A9087

Received by the editors September 24, 1990.

AMS subject classification: Primary: 20N05, 17D05; secondary: 16A25.

https://doi.org/10.4153/CJM-1992-059-7 Published online by Cambridge University Press

Moufang 2-loops, the loop of units in the alternative loop ring of a periodic loop L consists of more than just the so-called *trivial units*, $\pm\ell$, $\ell \in L$ [6]. In this paper, we determine the full loop of units in the integral alternative (not associative) loop rings of the six smallest order loops where it is known that the loop rings have non-trivial units.

I want to acknowledge with gratitude the encouragement of my good friend, M. M. Parmenter, whose paper [15] relating the unit groups of D_4 and $16\Gamma_2 c_2$ motivated this work.

2. **Zorn's vector matrix algebra.** Since any alternative ring satisfies the three (equivalent) *Moufang identities*

$$\big((xy)z\big)y = x\big(y(zy)\big); \ \big((xy)x\big)z = x\big(y(xz)\big); \ (xy)(zx) = \big(x(yz)\big)x$$

it follows that if $\mathbf{Z}L$ is alternative, then the loop L as well as the full unit loop in $\mathbf{Z}L$ will satisfy these identities; hence, by definition, these are *Moufang* loops.

Since our object here is to describe six Moufang unit loops, we begin by explaining the form these descriptions will take. The experience with group rings has been often to represent a unit group as a certain subgroup of the special linear group $\mathrm{SL}(2,\mathbf{Z})$. It is particularly pleasing that there is a Moufang matrix loop available which plays the role of $\mathrm{SL}(2,\mathbf{Z})$ in the not associative context. In fact, each of the unit loops we determine in this paper is closely related to this matrix loop, whose origins go back to Max Zorn.

As in [19, p. 46], for any commutative and associative ring R with identity, we let R^3 denote the set of ordered triples over R and consider the set of 2×2 matrices of the form

$$\begin{bmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{bmatrix}, \quad a, b \in R, \ \mathbf{x}, \mathbf{y} \in R^3$$

Such matrices are to be added entrywise, but multiplied according to the following modification of the usual rule:

$$\begin{bmatrix} a_1 & \mathbf{x}_1 \\ \mathbf{y}_1 & b_1 \end{bmatrix}\begin{bmatrix} a_2 & \mathbf{x}_2 \\ \mathbf{y}_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + \mathbf{x}_1\cdot\mathbf{y}_2 & a_1\mathbf{x}_2 + b_2\mathbf{x}_1 - \mathbf{y}_1\times\mathbf{y}_2 \\ a_2\mathbf{y}_1 + b_1\mathbf{y}_2 + \mathbf{x}_1\times\mathbf{x}_2 & b_1b_2 + \mathbf{y}_1\cdot\mathbf{x}_2 \end{bmatrix}$$

where $\cdot$ and $\times$ denote the dot and cross products respectively in R^3. By this construction, we obtain an alternative algebra over R which we denote $\mathfrak{Z}(R)$ in honour of Zorn who used such an algebra to represent the Cayley numbers, taking R to be the field of real numbers. Of significance is the fact that there is a (multiplicative) determinant function in $\mathfrak{Z}(R)$:

$$\det\begin{bmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{bmatrix} = ab - \mathbf{x}\cdot\mathbf{y}$$

For many years, it has been fashionable to use a process due to Dickson to construct simple alternative algebras (see, for example, [19, pp. 28–33 and Corollary 1, p. 151]); consequently, Zorn's algebra is less known than perhaps it should be. This paper highlights the loop of invertible matrices in $\mathfrak{Z}(\mathbf{Z})$, a Moufang loop obviously analogous to

GL(2, **Z**), and with an interesting subloop, $\mathfrak{Z}_1(\mathbf{Z})$, like SL(2, **Z**), consisting of integral matrices of determinant 1.

$$\mathfrak{Z}_1(\mathbf{Z}) = \{A \in \mathfrak{Z}(\mathbf{Z}) \mid \det A = 1\}$$

In our view, these Moufang loops deserve to be studied further. It is worth remarking in this connection that the units in $\mathfrak{Z}(F)$, F a finite field, turned out to be crucial in the classification of simple Moufang loops [14, 12].

3. **The loops of interest.** Our goal is to find the loop of units in the integral loop rings of six loops which we label $L_0, L_1, \ldots, L_5$ and whose significance is this: except for the omission of the so-called *Cayley loop* of order 16 and the direct product of this loop with the cyclic group C_2 of order 2 (in whose integral loop rings all units are trivial [6, Theorem 7]), these are all the Moufang loops of order $n \leq 32$ with loop rings over **Z** which are alternative: the loop L_0 has order 16, the remaining five loops have order 32.

$$\begin{aligned}
L_0 &= M_{16}(\mathbf{Q}, 2) = \langle a, b, u \mid a^4 = b^2 = 1, u^2 = (a,b) = (a,u) = (b,u) = (a,b,u) = a^2 \rangle \\
L_1 &= M_{32}(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_2^{\sharp}, 16\Gamma_2 c_2^{\sharp}) \\
&= \langle a, b, u \mid a^4 = b^4 = 1, u^2 = (a,b) = (a,u) = (b,u) = (a,b,u) = a^2 \rangle \\
L_2 &= M_{32}(\mathbf{Q} \times C_2, 2) \\
&= \langle a, b, c, u \mid a^4 = b^2 = c^2 = 1,\ u^2 = (a,b) = (a,u) = (b,u) = (a,b,u) = a^2, \\
&\qquad (a,c) = (b,c) = (c,u) = (a,b,c) = (a,c,u) = (b,c,u) = 1 \rangle \\
L_3 &= M_{32}(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_1, 16\Gamma_2 c_1) \\
&= \langle a, b, u \mid a^4 = b^4 = 1, u^2 = a^2 b^2, (a,b) = (a,u) = (b,u) = (a,b,u) = a^2 \rangle \\
L_4 &= M_{32}(E_i, 16) \\
&= \langle a, b, c, u \mid a^4 = 1,\ (a,c) = (b,c) = (a,b,c) = (a,c,u) = (b,c,u) = 1, \\
&\qquad b^2 = c^2 = u^2 = (a,b) = (a,u) = (b,u) = (c,u) = (a,b,u) = a^2 \rangle \\
L_5 &= M_{32}(5,5,5,2,2,4) \\
&= \langle a, b, u \mid a^8 = b^2 = 1, u^2 = a^2, (a,b) = (a,u) = (b,u) = (a,b,u) = a^4 \rangle
\end{aligned}$$

We use (a,b) and (a,b,c) to denote the commutator of a and b and the associator of a, b and c, respectively. The names of these loops are due to Chein [3] as are the above presentations, except for a couple of notational changes. Where Chein uses u_1, u_2, u_3 or u_1, u_2, u_3, u_4 for generators, we adopt a, b, u and a, b, c, u, respectively. In L_4, we have interchanged u_1 and u_3; that is, Chein's u_1, u_2, u_3 are our c, b, a. In L_5, we have replaced Chein's u_2 with the product u_1u_2 so as to obtain an element of order 2; thus Chein's u_1, u_1u_2, u_3 are our a, b, c. In each loop, there is a unique commutator ($\neq 1$) and a unique associator ($\neq 1$) and these are equal. This element, which we generally denote e, is the element a^2 in the presentation of each of the above loops except L_5, where $e = a^4$. Note that, in every loop, e is central and of order 2. Also, in each loop L, the given set of generators excluding u generates a group G of index 2 (as a subloop of L). Specifically, and using Hall and Senior notation (see also [18])

- in L_0, $G = \langle a, b\rangle \cong D_4$;
- in L_1, $G = \langle a, b\rangle \cong 16\Gamma_2 c_2$;
- in L_2, $G = \langle a, b, c\rangle \cong D_4 \times C_2$;
- in L_3, $G = \langle a, b\rangle \cong 16\Gamma_2 c_2$;
- in L_4, $G = \langle a, b, c\rangle \cong 16\Gamma_2 b$;
- in L_5, $G = \langle a, b\rangle \cong 16\Gamma_2 d$;

Thus each of our six loops L is the disjoint union of G and Gu. Moreover, in each case, the map

$$g \longmapsto g^* = \begin{cases} g & g \text{ central} \\ 3g & \text{otherwise} \end{cases}$$

is an *involution* (an anti-automorphism of period 2) such that gg^* is central, for any $g \in G$, and multiplication in $L = G \cup Gu$ is given by

$$g(hu) = (hg)u$$
$$(gu)h = (gh^*)u$$
$$(gu)(hu) = g_0 h^* g$$

for $g, h \in G$, where $u^2 = g_0$ is central in G and $g_0^* = g_0$. It follows that every element in the loop ring $\mathbf{Z}L$ can be expressed in the form $x + yu$, $x, y \in \mathbf{Z}G$, and that multiplication in $\mathbf{Z}L$ is given by

$$(x + yu)(a + bu) = (xa + g_0 b^* y) + (bx + ya^*)u$$

where, for $x = \sum \alpha_i g_i \in \mathbf{Z}G$, x^* means $\sum \alpha_i g_i^*$. The involution extends from G to L by defining $(gu)^* = e(gu)$ and then to $\mathbf{Z}L$ by the rule $(x+yu)^* = x^* + eyu$. We refer the reader to [4], [7] and [6] where this material is explained in greater detail.

4. **General results.** If L is any loop and $x \in L$, we denote as usual the left and right translations $L(x), R(x)\colon L \longrightarrow L$ by

$$L(x)\colon a \longmapsto xa, \quad R(x)\colon a \longmapsto ax$$

for $a \in L$. In general loop theory, a subloop H of L is, by definition, *normal* if and only if for all $x, y \in L$, $HT(x)$, $HR(x, y)$ and $HL(x, y)$ are subsets of H. Here, $T(x)$, $R(x, y)$ and $L(x, y)$ are the maps $L \longrightarrow L$ defined by

$$T(x) = L(x)^{-1} R(x)$$
$$R(x, y) = R(x)R(y)R(xy)^{-1}$$
$$L(x, y) = L(x)L(y)L(yx)^{-1}$$

Observe that if x and y are units in an alternative loop ring $\mathbf{Z}L$, then each of $T(x)$, $R(x, y)$ and $L(x, y)$ extends, by linearity, to a function $\mathbf{Z}L \longrightarrow \mathbf{Z}L$ which we denote with the same symbolism.

In any group or loop ring, the *augmentation* map ϵ, which is defined by $\epsilon(\sum \alpha_g g) = \sum \alpha_g$, is easily seen to be a ring homomorphism. As a consequence, the augmentation of a unit is ± 1 and, more importantly, the maps $T(x)$, $R(x, y)$ and $L(x, y)$ preserve augmentation. For example, if $t = sR(x, y)$, then $t(xy) = (sx)y$, so $\epsilon(t)\epsilon(x)\epsilon(y) = \epsilon(s)\epsilon(x)\epsilon(y)$ and, because neither $\epsilon(x)$ nor $\epsilon(y)$ is 0, we get $\epsilon(t) = \epsilon(s)$.

The next theorem was established for L_0 by Jespers and Leal [10].

THEOREM 4.1. *Let $L = \langle G, u\rangle$ be any of the six loops $L_0, \ldots, L_5$ defined in Section 3, with u and G as specified there. Let e denote the unique non-identity commutator (associator) in L. Let $\mathcal{U} = \mathcal{U}(\mathbf{Z}L)$ denote the unit loop of the integral loop ring of L. Then $\mathcal{U} = \pm L\mathcal{V}$ where*

$$\mathcal{V} = \{r \in \mathcal{U} \mid r = 1 + (1 - e)(x + yu), x, y \in \mathbf{Z}G, \epsilon(x + yu) \text{ even}\}$$

is a subloop of $\mathcal{U}$, a torsion-free normal complement for L.

PROOF. The centre $\mathcal{Z}(L)$ of L has order 4 and contains the associator-commutator subloop $L' = \{1, e\}$. Since the square of any element of L is central, the quotient L/L' is an abelian group of exponent 2 or 4 [8] (see also [17, p. 57]). So all units in $\mathbf{Z}(L/L')$ are trivial. By Proposition 4[1] of [6] there are two possibilities for the shape of a unit r in $\mathcal{U}$. Either

$$r = \pm[g + (1 - e)x] + [(1 - e)y]u = \pm g\{1 + (1 - e)[g^{-1}x + yg^{-1}u]\}$$

or

$$r = \pm[(1 - e)x] + [g + (1 - e)y]u = \pm gu\{1 + (1 - e)[(g^{-1}y)^* + (g_0^{-1}xg^{-1})^* u]\}$$

where x and y are in the group ring $\mathbf{Z}G$. In either case, r is in the form $\pm g[1+(1-e)(x+yu)]$, $g \in L$, and hence in $\pm L\mathcal{V}$ whenever $\epsilon(x + yu)$ is even, but also if $\epsilon(x + yu)$ is odd, as we see by the equation

$$g[1 + (1 - e)(x + yu)] = eg[1 + (1 - e)(e - x - yu)]$$

The calculation

$$\begin{aligned}[1 + (1 - e)(x + yu)]&[1 + (1 - e)(a + bu)] \\ &= 1 + (1 - e)\{[x + a + 2(xa + g_0 b^* y)] + [y + b + 2(bx + ya^*)]u\}\end{aligned}$$

shows that $\mathcal{V}$ is closed under multiplication.

To show that $\mathcal{V}$ contains the inverse of each of its elements we note that for $r = 1 + (1 - e)(x + yu)$, $r^* = 1 + (1 - e)(x^* + eyu) = 1 + (1 - e)(x^* - yu)$ and

$$rr^* = 1 + (1 - e)[x + x^* + 2(xx^* - g_0 yy^*)] \tag{4.1}$$

[1] Note the error in the statement of this proposition. The phrase "in the group ring $\mathbf{Z}G$ of a group determining L" should quite obviously (in light of the preamble) read "in the group ring $\mathbf{Z}(L/L')$".

Now rr^* is a central unit, but, since both L/L' and $Z(L)$ are abelian groups of exponent 2 or 4, $\mathbf{Z}L$ has only trivial central units [6]. Thus $rr^* = \pm a$ for some central a. In fact, $rr^* = a$ because its augmentation is positive and $a = 1$ because $(1-e)[x + x^* + 2(xx^* - g_0yy^*)]$ can be written as $(1-e)2t$, $t \in \mathbf{Z}G$. This follows by writing

$$x = x_1 + x_2,\ x_1 = \sum_{\alpha_g \in Z(G)} \alpha_g g,\ x_2 = \sum_{\alpha_g \notin Z(G)} \alpha_g g$$

and observing that $x + x^* = 2x_1 + (1+e)x_2$. We have shown that if $r = 1 + (1-e)(x+yu) \in \mathcal{V}$, then $r^{-1} = r^* = 1 + (1-e)(x^* - yu)$. Since x and x^* have the same augmentation, $r^{-1} \in \mathcal{V}$, so $\mathcal{V}$ is a subloop of $\mathcal{U}$. Normality follows from remarks at the beginning of this section: if $r = 1 + (1-e)(x+yu) \in \mathcal{V}$, if a and b are arbitrary elements of $\mathcal{U}$ and if θ is any of $T(a)$, $R(a,b)$, $L(a,b)$, then $1\theta = 1$ and $e\theta = e$, so $r\theta = 1 + (1-e)[(x+yu)\theta]$ and $\epsilon(x+yu)$ even implies $\epsilon\big((x+yu)\theta\big)$ even as well.

Finally, we must prove that every $r = 1 + (1-e)(x+yu) \in \mathcal{V}$, $r \neq 1$, has infinite order (from which $L \cap \mathcal{V} = \{1\}$ also follows). For this, note that the coefficient of the identity in r is $m = 1 + \alpha_1 - \alpha_e$ while the coefficient of e is $n = \alpha_e - \alpha_1$, where α_1 and α_e are the coefficients of 1 and e in x. Since it is impossible for both m and n to be 0, some coefficient of a central element in r is non-zero. Thus, if r has finite order, $r = \pm a$ for some central a [5, Corollary 2.2], $r = +a$ because it has positive augmentation and $a = 1$ because the augmentation of $x + yu$ is even, as in our previous argument about rr^*. ∎

Because of this theorem, our search for units in the integral loop ring of any of the loops in question can be restricted to a hunt for units of the form $1 + (1-e)(x+yu)$. In the work which follows, our achievement for each L_i will be to represent $\mathcal{V}$ either as a subloop of the invertible matrices in Zorn's vector matrix algebra over the rational or Gaussian integers or else as a subloop of the direct product of $\mathfrak{Z}_1(\mathbf{Z})$ with itself. Our method, in every case, makes use of an observation implicit in the proof of the theorem.

COROLLARY 4.2. *Let $r = 1 + (1-e)(x+yu)$, $x, y \in \mathbf{Z}G$, be an element of the loop ring $\mathbf{Z}L$. Write $x = \sum_{\alpha_g \in G} \alpha_g g$ and define x_1 by $x_1 = \sum_{\alpha_g \in Z(G)} \alpha_g g$. Then r is a unit if and only if $(1-e)(x_1 + xx^* - g_0yy^*) = 0$.*

PROOF. Equation (4.1) made it clear that r is a unit if and only if $(1-e)[x + x^* + 2(xx^* - g_0yy^*)] = 0$. The proof of the theorem shows that $(1-e)(x+x^*) = (1-e)2x_1$. Therefore r is a unit if and only if $2(1-e)(x_1 + xx^* - g_0yy^*) = 0$ and the result follows. ∎

5. $M_{16}(\mathbf{Q}, 2)$. The unit loop of $\mathbf{Z}M_{16}(\mathbf{Q}, 2)$ has been determined recently by Jespers and Leal [10]. We find it again here (in a slightly different form) because it provides a simple illustration of our general approach and because this particular unit loop reappears later.

We present $L_0 = M_{16}(\mathbf{Q}, 2)$ as in Section 3; that is,

$$L_0 = \langle a, b, u \mid a^4 = b^2 = 1, u^2 = (a,b) = (a,u) = (b,u) = (a,b,u) = a^2 \rangle$$

Recall that $G = \langle a, b\rangle \cong D_4$, $e = a^2$ and $g_0 = u^2 = e$. Any element of $\mathbf{Z}G$ is a linear combination of $1, a, b, ab$ and the product of these elements with $a^2 = e$. Since $(1-e)e = -(1-e)$ and

$$(1-e)[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + e(\alpha_4 + \alpha_5 a + \alpha_6 b + \alpha_7 ab)]$$
$$= (1-e)[(\alpha_0 - \alpha_4) + (\alpha_1 - \alpha_5)a + (\alpha_2 - \alpha_6)b + (\alpha_3 - \alpha_7)ab],$$

for any $x \in \mathbf{Z}G$, $(1-e)x$ is a linear combination of just 1, a, b and ab. Therefore, if an element r in $\mathbf{Z}L$ has the form $r = 1 + (1-e)(x + yu)$, we may assume that

$$x = \alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab \text{ and}$$
$$y = \beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab$$

Recalling the definition of * and noting that $\mathcal{Z}(G) = \{1, e\}$,

$$x^* = \alpha_0 + e(\alpha_1 a + \alpha_2 b + \alpha_3 ab) \text{ and}$$
$$y^* = \beta_0 + e(\beta_1 a + \beta_2 b + \beta_3 ab)$$

With x_1 defined as in Corollary 4.2, here we have $x_1 = \alpha_0$ and it is easy to see that

$$xx^* = (\alpha_0^2 + \alpha_1^2) + e(\alpha_2^2 + \alpha_3^2) + (1+e)s \text{ and}$$
$$yy^* = (\beta_0^2 + \beta_1^2) + e(\beta_2^2 + \beta_3^2) + (1+e)t$$

for certain $s, t \in \mathbf{Z}G$. Since $g_0 = u^2 = e$,

$$(1-e)(x_1 + xx^* - g_0 yy^*) = (1-e)(x_1 + xx^* + yy^*)$$
$$= (1-e)[\alpha_0 + (\alpha_0^2 + \alpha_1^2) - (\alpha_2^2 + \alpha_3^2) + (\beta_0^2 + \beta_1^2) - (\beta_2^2 + \beta_3^2)]$$

Let m be the integer

$$m = \alpha_0 + \alpha_0^2 + \alpha_1^2 - \alpha_2^2 - \alpha_3^2 + \beta_0^2 + \beta_1^2 - \beta_2^2 - \beta_3^2.$$

By Corollary 4.2, r is a unit if and only if $(1-e)m = 0$, hence if and only if $m = 0$, or equivalently, if and only if

(5.1)
$$(1 + 2\alpha_0)^2 + (2\alpha_1)^2 - (2\alpha_2)^2 - (2\alpha_3)^2 + (2\beta_0)^2 + (2\beta_1)^2 - (2\beta_2)^2 - (2\beta_3)^2 = 1$$

Note that $\epsilon(x + yu)$ is even if and only if α_0 is even since $0 = m \equiv \alpha_0 + \big(\sum(\alpha_i + \beta_i)\big)^2 \pmod 2 \equiv \alpha_0 + \sum(\alpha_i + \beta_i) \pmod 2 = \alpha_0 + \epsilon(x + yu)$.

The trick now is to observe that (5.1) is equivalent to

$$\det \begin{bmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{bmatrix} = 1$$

in Zorn's algebra $\mathfrak{Z}(\mathbf{Z})$ where

$$\begin{aligned} a &= 1 + 2(\alpha_0 + \alpha_3) \\ b &= 1 + 2(\alpha_0 - \alpha_3) \\ \mathbf{x} &= 2(\alpha_2 + \alpha_1, \beta_3 + \beta_0, \beta_2 - \beta_1) \\ \mathbf{y} &= 2(\alpha_2 - \alpha_1, \beta_3 - \beta_0, \beta_2 + \beta_1) \end{aligned}$$

and then to verify that the map which this matrix suggests,

$$\varphi: r \longrightarrow \begin{bmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{bmatrix}$$

is a loop homomorphism into $\mathfrak{Z}_1(\mathbf{Z})$. It's clearly one-to-one and its range is easily determined. So we obtain the following theorem.

THEOREM 5.1. *Let*

$$L_0 = M_{16}(\mathbf{Q}, 2) = \langle a, b, u \mid a^4 = b^2 = 1, u^2 = (a, b) = (a, c) = (b, c) = (a, b, u) = a^2 \rangle.$$

Then the unit loop of the integral loop ring $\mathbf{Z}L_0$ is $\pm L_0 \mathcal{V}$ where $\mathcal{V}$ is a torsion-free normal complement of L_0 consisting of elements of the form

$$r = 1 + (1 - a^2)[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab)u]$$

with α_0 even and

$$(1 + 2\alpha_0)^2 + (2\alpha_1)^2 - (2\alpha_2)^2 - (2\alpha_3)^2 + (2\beta_0)^2 + (2\beta_1)^2 - (2\beta_2)^2 - (2\beta_3)^2 = 1$$

Furthermore,

$$\mathcal{V} \cong \left\{ \begin{bmatrix} 1 + 2a & 2\mathbf{x} \\ 2\mathbf{y} & 1 + 2b \end{bmatrix} \in \mathfrak{Z}_1(\mathbf{Z}) \mid a + b \in 2\mathbf{Z}, \mathbf{x} + \mathbf{y} \in (2\mathbf{Z}, 2\mathbf{Z}, 2\mathbf{Z}) \right\}$$

the isomorphism being given by

$$r \longmapsto \begin{bmatrix} 1 + 2(\alpha_0 + \alpha_3) & 2(\alpha_2 + \alpha_1, \beta_3 + \beta_0, \beta_2 - \beta_1) \\ 2(\alpha_2 - \alpha_1, \beta_3 - \beta_0, \beta_2 + \beta_1) & 1 + 2(\alpha_0 - \alpha_3) \end{bmatrix}$$

6. $M_{32}(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_2{}^\sharp, 16\Gamma_2 c_2{}^\sharp)$. We present this loop ($L_1$) as in Section 3:

$$L_1 = \langle a, b, u \mid a^4 = b^4 = 1, u^2 = (a, b) = (a, u) = (b, u) = (a, b, u) = a^2 \rangle$$

As with L_0, $G = \langle a, b \rangle$, $e = a^2$ and $g_0 = u^2 = e$. The centre of G is $\mathcal{Z}(G) = \{1, e, b^2, eb^2\} \cong C_2 \times C_2$. Any $x \in \mathbf{Z}G$ is a linear combination of $1, a, b, b^2, b^3, ab, ab^2, ab^3$ and the product of these elements with $a^2 = e$. It follows that $(1 - e)x$ is a linear combination of just 1, a,

b, b^2, b^3, ab, ab^2 and ab^3. So for an element $r \in \mathbf{Z}L_1$ of the form $r = 1 + (1-e)(x+yu)$, $x, y \in \mathbf{Z}G$, we may assume

$$x = (\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + b^2(\alpha_0' + \alpha_1' a + \alpha_2' b + \alpha_3' ab) \text{ and}$$
$$y = (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + b^2(\beta_0' + \beta_1' a + \beta_2' b + \beta_3' ab)$$

We have

$$x^* = (\alpha_0 + b^2\alpha_0') + e[(\alpha_1 a + \alpha_2 b + \alpha_3 ab) + b^2(\alpha_1' a + \alpha_2' b + \alpha_3' ab)]$$

and there's a similar expression for y^*. With x_1 defined as in Corollary 4.2, we have $x_1 = \alpha_0 + b^2\alpha_0'$,

$$(6.1) \qquad xx^* = (\alpha_0^2 + {\alpha_0'}^2 + \alpha_1^2 + {\alpha_1'}^2) + e(2\alpha_2\alpha_2' + 2\alpha_3\alpha_3') + b^2[(2\alpha_0\alpha_0' + 2\alpha_1\alpha_1') + e(\alpha_2^2 + {\alpha_2'}^2 + \alpha_3^2 + {\alpha_3'}^2)] + (1+e)s$$

for some $s \in \mathbf{Z}G$, and a similar expression for yy^*.

It may be of help to the reader to indicate how we calculate these expressions quickly. (Exactly the same procedure works when dealing with the loop rings of each of the remaining loops.) We write $x = (\alpha_0 + b^2\alpha_0') + (p + b^2 q)$ where $p = \alpha_1 a + \alpha_2 b + \alpha_3 ab$ and $q = \alpha_1' b + \alpha_2' b + \alpha_3' ab$. Then $x^* = (\alpha_0 + b^2\alpha_0') + e(p + b^2 q)$ and $xx^* = (\alpha_0 + b^2\alpha_0')^2 + e(p + b^2 q)^2$ plus another term containing $1+e$ as a factor (which is of no concern since it is $(1-e)xx^*$ in which we are actually interested). Since no two of a, b, ab commute, $gh + hg = (1+e)gh$ for $g \neq h \in \{a, b, ab\}$ and therefore, modulo more terms containing the factor $1+e$,

$$p^2 = \alpha_1^2 a^2 + \alpha_2^2 b^2 + \alpha_3^2 b^2$$
$$q^2 = {\alpha_1'}^2 a^2 + {\alpha_2'}^2 b^2 + {\alpha_3'}^2 b^2$$
$$pq + qp = 2\alpha_1\alpha_1' a^2 + 2\alpha_2\alpha_2' b^2 + 2\alpha_3\alpha_3' b^2$$

So, modulo $(1+e)\mathbf{Z}G$,

$$\begin{aligned} xx^* &= (\alpha_0 + b^2\alpha_0')^2 + e(p + b^2 q)^2 \\ &= (\alpha_0^2 + 2b^2\alpha_0\alpha_0' + {\alpha_0'}^2) + ep^2 + eb^2(pq + qp) + eq^2 \\ &= \alpha_0^2 + 2b^2\alpha_0\alpha_0' + {\alpha_0'}^2 + \alpha_1^2 + eb^2(\alpha_2^2 + \alpha_3^2) \\ &\quad + 2\alpha_1\alpha_1' b^2 + 2e\alpha_2\alpha_2' + 2e\alpha_3\alpha_3' + {\alpha_1'}^2 + eb^2({\alpha_2'}^2 + {\alpha_3'}^2) \end{aligned}$$

which gives (6). Now we return to our central line of reasoning.

Since $g_0 = e$, we have $(1-e)(x_1 + xx^* - g_0 yy^*) = (1-e)(x_1 + xx^* + yy^*) = (1-e)(m + nb^2)$ where m and n are the integers

$$\begin{aligned} m &= \alpha_0 + \alpha_0^2 + {\alpha_0'}^2 + \alpha_1^2 + {\alpha_1'}^2 - 2\alpha_2\alpha_2' - 2\alpha_3\alpha_3' \\ &\quad + \beta_0^2 + {\beta_0'}^2 + \beta_1^2 + {\beta_1'}^2 - 2\beta_2\beta_2' - 2\beta_3\beta_3' \\ n &= \alpha_0' - \alpha_2^2 - {\alpha_2'}^2 - \alpha_3^2 - {\alpha_3'}^2 + 2\alpha_0\alpha_0' + 2\alpha_1\alpha_1' \\ &\quad - \beta_2^2 - {\beta_2'}^2 - \beta_3^2 - {\beta_3'}^2 + 2\beta_0\beta_0' + 2\beta_1\beta_1'. \end{aligned}$$

https://doi.org/10.4153/CJM-1992-059-7 Published online by Cambridge University Press

By Corollary 4.2, $r = 1 + (1-e)(x+yu)$ is a unit if and only if $(1-e)(m+nb^2) = 0$ and so, because 1, e, b^2 and eb^2 are linearly independent over $\mathbf{Z}$, if and only if $m = n = 0$. Subtracting the above expressions for m and n, then multiplying by 4 and adding 1, the conditions $m = n = 0$ imply

$$[1+2(\alpha_0-\alpha_0')]^2 + [2(\alpha_1-\alpha_1')]^2 + [2(\alpha_2-\alpha_2')]^2 + [2(\alpha_3-\alpha_3')]^2 \\ + [2(\beta_0-\beta_0')]^2 + [2(\beta_1-\beta_1')]^2 + [2(\beta_2-\beta_2')]^2 + [2(\beta_3-\beta_3')]^2 = 1$$

to which there are two solutions. In each of these, $\alpha_i = \alpha_i'$, $i = 1,2,3$ and $\beta_i = \beta_i'$, $i = 0,1,2,3$. In addition, in one case we have $\alpha_0 = \alpha_0'$ and, in the other, $\alpha_0' = 1 + \alpha_0$.

CASE i. $\alpha_0 = \alpha_0'$.
In this case,

(6.2)
$$x = (1+b^2)(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) \\ y = (1+b^2)(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab)$$

and $m = n = \alpha_0 + 2\alpha_0{}^2 + 2\alpha_1^2 - 2\alpha_2^2 - 2\alpha_3^2 + 2\beta_0^2 + 2\beta_1^2 - 2\beta_2^2 - 2\beta_3^2$. The condition $m = n = 0$ is conveniently expressed as

(6.3)
$$(1+4\alpha_0)^2 + (4\alpha_1)^2 - (4\alpha_2)^2 - (4\alpha_3)^2 + (4\beta_0)^2 + (4\beta_1)^2 - (4\beta_2)^2 - (4\beta_3)^2 = 1$$

CASE ii. $\alpha_0' = 1 + \alpha_0$
This time

$$x = b^2 + (1+b^2)(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) \text{ and} \\ y = (1+b^2)(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab)$$

with

$$0 = m = n = \alpha_0 + \alpha_0^2 + (1+\alpha_0)^2 + 2\alpha_1^2 - 2\alpha_2^2 - 2\alpha_3^2 + 2\beta_0^2 + 2\beta_1^2 - 2\beta_2^2 - 2\beta_3^2 \\ = -(1+\alpha_0) + 2[-(1+\alpha_0)]^2 + 2(-\alpha_1)^2 - 2(-\alpha_2^2) - 2(\alpha_3)^2 \\ + 2(-\beta_0)^2 + 2(-\beta_1)^2 - 2(-\beta_2)^2 - 2(-\beta_3)^2.$$

So

$$r = 1 + (1-e)(x+yu) = 1 - e + e + (1-e)(x+yu) \\ = e + (1-e)(1+x+yu) = e[1 + (1-e)(-1-x-yu)] \\ = e[1 + (1-e)(x_1 + y_1 u)]$$

where

$$x_1 = -1 - x = (1+b^2)[-(1+\alpha_0) - \alpha_1 a - \alpha_2 b - \alpha_3 ab] \text{ and} \\ y_1 = -y = (1+b^2)[-\beta_0 - \beta_1 a - \beta_2 b - \beta_3 ab].$$

https://doi.org/10.4153/CJM-1992-059-7 Published online by Cambridge University Press

In other words, $r = er_1$ where r_1 is a unit of the type discovered in Case i.

Summarizing, we have shown that $r = 1 + (1 - e)(x + yu)$ is a unit if and only if x and y in $\mathbf{Z}G$ have the form (6), their coefficients satisfying (6.3). Note that this time, the condition which puts $r \in \mathcal{V}$—augmentation of $x + yu$ even—is automatically satisfied. We are now in a position to characterize the loop of units in $\mathbf{Z}L_1$.

THEOREM 6.1. *Let* $L_1 = M_{32}(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_2^\sharp, 16\Gamma_2 c_2^\sharp)$ *be the loop*

$$\langle a, b, u \mid a^4 = b^4 = 1, u^2 = (a, b) = (a, u) = (b, u) = (a, b, u) = a^2 \rangle$$

Then the unit loop of the loop ring $\mathbf{Z}L_1$ *is* $\pm L_1\mathcal{V}$ *where* $\mathcal{V}$ *is a torsion-free normal complement for* L_1 *consisting of elements of the form*

$$r = 1 + (1 - a^2)(1 + b^2)[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab)u]$$

whose coefficients satisfy

$$(1 + 4\alpha_0)^2 + (4\alpha_1)^2 - (4\alpha_2)^2 - (4\alpha_3)^2 + (4\beta_0)^2 + (4\beta_1)^2 - (4\beta_2)^2 - (4\beta_3)^2 = 1.$$

Furthermore, the subloop $\mathcal{V}$ *is isomorphic to*

$$\left\{ \begin{bmatrix} 1 + 4a & 4\mathbf{x} \\ 4\mathbf{y} & 1 + 4b \end{bmatrix} \in \mathfrak{Z}_1(\mathbf{Z}) \mid a + b \in 2\mathbf{Z}, \mathbf{x} + \mathbf{y} \in (2\mathbf{Z}, 2\mathbf{Z}, 2\mathbf{Z}) \right\}$$

the isomorphism being given by

$$r \quad \longmapsto \quad \begin{bmatrix} 1 + 4(\alpha_0 + \alpha_3) & 4(\alpha_2 + \alpha_1, \beta_3 + \beta_0, \beta_2 - \beta_1) \\ 4(\alpha_2 - \alpha_1, \beta_3 - \beta_0, \beta_2 + \beta_1) & 1 + 4(\alpha_0 - \alpha_3) \end{bmatrix}.$$

PROOF. Let $\mathcal{U}_0 = \pm L_0\mathcal{V}_0$ be the loop of units of $\mathbf{Z}L_0$ where $\mathcal{V}_0$ is the loop $\mathcal{V}$ specified in Theorem 5.1. We have determined already that the loop of units of $\mathbf{Z}L_1$ is $\mathcal{U}_1 = \pm L_1\mathcal{V}_1$ where $\mathcal{V}_1$ is the subloop of $\mathcal{U}_1$ consisting of units of the form $r = 1 + (1 - a^2)(x + yu)$,

$$x = (1 + b^2)(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab)$$
$$y = (1 + b^2)(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab)$$

the coefficients here satisfying (6.3). Rather than viewing (6.3) as a statement about a certain determinant (as we did at this point in the previous section), we proceed in a manner which avoids the tedium of checking that a certain map is a homomorphism.

Let $\mathcal{W}_0$ be the subloop of $\mathcal{V}_0$ generated by units of the form $1 + 2(1 - a^2)(x + yu)$, where

$$x = \alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab$$
$$y = \beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab$$

The map $\psi: L_1 \longrightarrow L_0$ defined by $b^2 \longmapsto 1$ extends to a one-to-one loop homomorphism $\mathcal{V}_1 \longrightarrow \mathcal{W}_0$ which (surprisingly?) is also onto. To see this, just note that any unit $s = 1 + 2(1 - a^2)(x + yu) \in \mathcal{W}_0$ is $\psi(r)$ for $r = 1 + (1 - a^2)(1 + b^2)(x + yu)$, the coefficients of x and y in such r satisfying (6.3) because the coefficients of $2x$ and $2y$ satisfy (5.1); *i.e.*, $r \in \mathcal{V}_1$. Finally, we obtain the isomorphism specified in the statement of the theorem by composing ψ with the isomorphism of Theorem 5.1. ∎

7. $M_{32}(\mathbf{Q}\times C_2,2)$. We present $L_2 = M_{32}(\mathbf{Q}\times C_2, 2)$ as in Section 3:

$$L_2 = \langle a,b,c,u \,|a^4 = b^2 = c^2 = 1, u^2 = (a,b) = (a,u) = (b,u) = (a,b,u) = a^2,$$
$$(a,c) = (b,c) = (c,u) = (a,b,c) = (a,c,u) = (b,c,u) = 1\rangle$$

We have $G = \langle a,b,c\rangle \cong D_4\times C_2$, $\mathcal{Z}(G) = \{1,e,c,ec\} \cong C_2\times C_2$, $e = a^2$ and $g_0 = u^2 = e$.

Any $x \in \mathbf{Z}G$ is a linear combination of $1,a,b,ab,c,ca,cb,cab$ and the product of these elements with $a^2 = e$ so $(1-e)x$ is a linear combination of just 1, a, b, ab, c, ca, cb and cab. For $r = 1 + (1-e)(x+yu)$, we may therefore assume that

$$x = (\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + c(\alpha_0' + \alpha_1' a + \alpha_2' b + \alpha_3' ab) \text{ and}$$
$$y = (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + c(\beta_0' + \beta_1' a + \beta_2' b + \beta_3' ab)$$

This time, we have

$$x^* = (\alpha_0 + c\alpha_0') + e[(\alpha_1 a + \alpha_2 b + \alpha_3 ab) + c(\alpha_1' a + \alpha_2' b + \alpha_3' ab)]$$

and there's a similar expression for y^*. Also, $x_1 = \alpha_0 + c\alpha_0'$,

$$xx^* = [(\alpha_0^2 + {\alpha_0'}^2 + \alpha_1^2 + {\alpha_1'}^2) + c(2\alpha_0\alpha_0' + 2\alpha_1\alpha_1')]$$
$$+ e[(\alpha_2^2 + {\alpha_2'}^2 + \alpha_3^2 + {\alpha_3'}^2) + c(2\alpha_2\alpha_2' + 2\alpha_3\alpha_3')] + (1+e)s$$

for some $s \in \mathbf{Z}G$, and there's a similar expression for yy^*. Since $g_0 = e$,

$$\begin{aligned}
&(1-e)(x_1 + xx^* - g_0 yy^*)\\
&\quad = (1-e)(x_1 + xx^* + yy^*)\\
&\quad = (1-e)\big\{\alpha_0 + c\alpha_0' + (\alpha_0^2 + {\alpha_0'}^2 + \alpha_1^2 + {\alpha_1'}^2 - \alpha_2^2 - {\alpha_2'}^2 - \alpha_3^2 - {\alpha_3'}^2)\\
&\qquad + 2c(\alpha_0\alpha_0' + \alpha_1\alpha_1' - \alpha_2\alpha_2' - \alpha_3\alpha_3')\\
&\qquad + (\beta_0^2 + {\beta_0'}^2 + \beta_1^2 + {\beta_1'}^2 - \beta_2^2 - {\beta_2'}^2 - \beta_3^2 - {\beta_3'}^2)\\
&\qquad + 2c(\beta_0\beta_0' + \beta_1\beta_1' - \beta_2\beta_2' - \beta_3\beta_3')\big\}
\end{aligned}$$

which is of the form $(1-e)(m+cn)$ where m and n are the integers

$$\begin{aligned}
m &= \alpha_0 + \alpha_0^2 + {\alpha_0'}^2 + \alpha_1^2 + {\alpha_1'}^2 - \alpha_2^2 - {\alpha_2'}^2 - \alpha_3^2 - {\alpha_3'}^2\\
&\quad + \beta_0^2 + {\beta_0'}^2 + \beta_1^2 + {\beta_1'}^2 - \beta_2^2 - {\beta_2'}^2 - \beta_3^2 - {\beta_3'}^2\\
n &= \alpha_0' + 2(\alpha_0\alpha_0' + \alpha_1\alpha_1' - \alpha_2\alpha_2' - \alpha_3\alpha_3'\\
&\quad + \beta_0\beta_0' + \beta_1\beta_1' - \beta_2\beta_2' - \beta_3\beta_3')
\end{aligned}$$

By Corollary 4.2, $r = 1+(1-e)(x+yu)$ is a unit if and only if $(1-e)(m+cn) = 0$, hence, if and only if $m = n = 0$. (Note that here, $\epsilon(x+yu)$ even is equivalent to $\alpha_0 \equiv \alpha_0' \equiv 0$ (mod 2).) First adding and then subtracting the above expressions for m and n, it is convenient to observe that the equations $m = n = 0$ are equivalent to

$$(\alpha_0+\alpha_0')+(\alpha_0+\alpha_0')^2+(\alpha_1+\alpha_1')^2-(\alpha_2+\alpha_2')^2-(\alpha_3+\alpha_3')^2 \\ +(\beta_0+\beta_0')^2+(\beta_1+\beta_1')^2-(\beta_2+\beta_2')^2-(\beta_3+\beta_3')^2=0 \text{ and}$$

$$(\alpha_0-\alpha_0')+(\alpha_0-\alpha_0')^2+(\alpha_1-\alpha_1')^2-(\alpha_2-\alpha_2')^2-(\alpha_3-\alpha_3')^2 \\ +(\beta_0-\beta_0')^2+(\beta_1-\beta_1')^2-(\beta_2-\beta_2')^2-(\beta_3-\beta_3')^2=0$$

and hence to

$$[(1+2(\alpha_0\pm\alpha_0')]^2+[2(\alpha_1\pm\alpha_1')]^2-[2(\alpha_2\pm\alpha_2')]^2-[2(\alpha_3\pm\alpha_3')]^2 \\ +[2(\beta_0\pm\beta_0')]^2+[2(\beta_1\pm\beta_1')]^2-[2(\beta_2\pm\beta_2')]^2-[2(\beta_3\pm\beta_3')]^2=1. \tag{7.1}$$

Now the map $L_2 \longrightarrow L_0$ which sends c to 1 extends to a ring homomorphism $\mathbf{Z}L_2 \longrightarrow \mathbf{Z}L_0$ which induces a loop homomorphism $\varphi\colon \mathcal{U}(\mathbf{Z}L_2) \longrightarrow \mathcal{U}(\mathbf{Z}L_0)$ with kernel

$$\ker\varphi = \{1+(1-e)(1-c)(x+yu) \mid x,y \in \mathbf{Z}G\}$$

and, similarly, the map $L_2 \longrightarrow L_0$ which sends c to $e = a^2$ induces a loop homomorphism $\psi\colon \mathcal{U}(\mathbf{Z}L_2) \longrightarrow \mathcal{U}(\mathbf{Z}L_0)$ with kernel

$$\ker\psi = \{1+(1-e)(1+c)(x+yu) \mid x,y \in \mathbf{Z}G\}$$

Since $(1+c)(1-c)=0$, $\ker\varphi\cap\ker\psi=\{1\}$ and thus $r\longmapsto\big(\varphi(r),\psi(r)\big)$ is a one-to-map homomorphism into $\mathcal{U}(\mathbf{Z}L_0)\times\mathcal{U}(\mathbf{Z}L_0)$. We claim that its range is

$$\begin{aligned}\{(s_1,s_2) \mid\ & s_1 = 1+(1-e)[(\alpha_0+\alpha_1 a+\alpha_2 b+\alpha_3 ab)+(\beta_0+\beta_1 a+\beta_2 b+\beta_3 ab)u] \\ & s_2 = 1+(1-e)[(\gamma_0+\gamma_1 a+\gamma_2 b+\gamma_3 ab)+(\delta_0+\delta_1 a+\delta_2 b+\delta_3 ab)u] \\ & \text{where } (\alpha_i+\gamma_i) \text{ and } (\beta_i+\delta_i) \text{ are even, for all } i, \\ & (1+2\alpha_0)^2+(2\alpha_1)^2-(2\alpha_2)^2-(2\alpha_3)^2 \\ & \qquad +(2\beta_0)^2+(2\beta_1)^2-(2\beta_2)^2-(2\beta_3)^2=1 \text{ and} \\ & (1+2\gamma_0)^2+(2\gamma_1)^2-(2\gamma_2)^2-(2\gamma_3)^2 \\ & \qquad +(2\delta_0)^2+(2\delta_1)^2-(2\delta_2)^2-(2\delta_3)^2=1\}\end{aligned} \tag{7.2}$$

the conditions on the coefficients appearing because, as units of $\mathbf{Z}L_0$, s_1 and s_2 must satisfy (5.1).

To justify our claim, let s_1 and s_2 be as above. Then, letting

$$\rho_i=\tfrac{1}{2}(\alpha_i+\gamma_i),\quad \rho_i'=\tfrac{1}{2}(\alpha_i-\gamma_i)$$
$$\tau_i=\tfrac{1}{2}(\beta_i+\delta_i),\quad \tau_i'=\tfrac{1}{2}(\beta_i-\delta_i)$$

the element $r = 1+(1-e)(x+yu)$ with

$$x=(\rho_0+\rho_1 a+\rho_2 b+\rho_3 ab)+c(\rho_0'+\rho_1' a+\rho_2' b+\rho_3' ab)$$
$$y=(\tau_0+\tau_1 a+\tau_2 b+\tau_3 ab)+c(\tau_0'+\tau_1' a+\tau_2' b+\tau_3' ab)$$

satisfies $\big(\varphi(r),\psi(r)\big)=(s_1,s_2)$ and is a unit in $\mathbf{Z}L_2$ *because* the equations (7) hold, these being exactly the two equations (7.2) which say that s_1 and s_2 are units in $\mathbf{Z}L_0$. Thus we obtain the following characterization of the units in $\mathbf{Z}L_2$.

https://doi.org/10.4153/CJM-1992-059-7 Published online by Cambridge University Press

THEOREM 7.1. *Let $L_2 = M_{32}(\mathbf{Q} \times C_2, 2)$ be the Moufang loop with presentation*

$$\langle a, b, c, u \mid a^4 = b^2 = c^2 = 1, u^2 = (a,b) = (a,u) = (b,u) = (a,b,u) = a^2, \\ (a,c) = (b,c) = (c,u) = (a,b,c) = (a,c,u) = (b,c,u) = 1\rangle$$

Then the unit loop of $\mathbf{Z}L_2$ is $\pm L_2\mathcal{V}$ where $\mathcal{V}$ is a torsion-free normal complement of L_2 consisting of elements of the form

$$r = 1 + (1-a^2)\big\{[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + c(\alpha_0' + \alpha_1' a + \alpha_2' b + \alpha_3' ab)] \\ + [(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + c(\beta_0' + \beta_1' a + \beta_2' b + \beta_3' ab)]u\big\}$$

with $\alpha_0 \equiv \alpha_0' \equiv 0 \pmod 2$ and

$$[(1 + 2(\alpha_0 \pm \alpha_0')]^2 + [2(\alpha_1 \pm \alpha_1')]^2 - [2(\alpha_2 \pm \alpha_2')]^2 - [2(\alpha_3 \pm \alpha_3')]^2 \\ + [2(\beta_0 \pm \beta_0')]^2 + [2(\beta_1 \pm \beta_1')]^2 - [2(\beta_2 \pm \beta_2')]^2 - [2(\beta_3 \pm \beta_3')]^2 = 1$$

Furthermore,

$$\mathcal{V} \cong \big\{(A_1, A_2) \in \mathfrak{Z}_1(\mathbf{Z}) \times \mathfrak{Z}_1(\mathbf{Z}) \mid \\ A_1 = \begin{bmatrix} 1+2a_1 & 2\mathbf{x}_1 \\ 2\mathbf{y}_1 & 1+2b_1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1+2a_2 & 2\mathbf{x}_2 \\ 2\mathbf{y}_2 & 1+2b_2 \end{bmatrix} \\ a_1 + a_2, b_1 + b_2 \text{ and } a_i + b_i \in 2\mathbf{Z}, \quad i = 1,2, \\ \mathbf{x}_1 + \mathbf{x}_2, \mathbf{y}_1 + \mathbf{y}_2 \text{ and } \mathbf{x}_i + \mathbf{y}_i \in (2\mathbf{Z}, 2\mathbf{Z}, 2\mathbf{Z}), \quad i = 1,2, \\ a_1 + a_2 + b_1 + b_2 \text{ and } x_{1i} + y_{1i} + x_{2i} + y_{2i} \in 4\mathbf{Z}, \quad i = 1,2\big\} \tag{7.3}$$

where $\mathbf{x}_i = (x_{i1}, x_{i2}, x_{i3})$ and $\mathbf{y}_i = (y_{i1}, y_{i2}, y_{i3})$, $i = 1, 2$, the isomorphism being given by $r \longmapsto (A_1, A_2)$ where

$$A_1 = \begin{bmatrix} 1+2a_1 & 2\mathbf{x}_1 \\ 2\mathbf{y}_1 & 1+2b_1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1+2a_2 & 2\mathbf{x}_2 \\ 2\mathbf{y}_2 & 1+2b_2 \end{bmatrix}$$

$$a_1 = \alpha_0 + \alpha_0' + \alpha_3 + \alpha_3'$$
$$b_1 = \alpha_0 + \alpha_0' - \alpha_3 - \alpha_3'$$
$$\mathbf{x}_1 = (\alpha_2 + \alpha_2' + \alpha_1 + \alpha_1', \beta_3 + \beta_3' + \beta_0 + \beta_0', \beta_2 + \beta_2' - \beta_1 - \beta_1')$$
$$\mathbf{y}_1 = (\alpha_2 + \alpha_2' - \alpha_1 - \alpha_1', \beta_3 + \beta_3' - \beta_0 - \beta_0', \beta_2 + \beta_2' + \beta_1 + \beta_1')$$
$$a_2 = \alpha_0 - \alpha_0' + \alpha_3 - \alpha_3'$$
$$b_2 = \alpha_0 - \alpha_0' - \alpha_3 + \alpha_3'$$
$$\mathbf{x}_2 = (\alpha_2 - \alpha_2' + \alpha_1 - \alpha_1', \beta_3 - \beta_3' + \beta_0 - \beta_0', \beta_2 - \beta_2' - \beta_1 + \beta_1')$$
$$\mathbf{y}_2 = (\alpha_2 - \alpha_2' - \alpha_1 + \alpha_1', \beta_3 - \beta_3' - \beta_0 + \beta_0', \beta_2 - \beta_2' + \beta_1 - \beta_1')$$

PROOF. The isomorphism is the composition of the map $r \longmapsto \big(\varphi(r), \psi(r)\big)$ and applications in each coordinate of the isomorphism exhibited in Theorem 5.1. The conditions on the entries of the matrices A_1 and A_2 are obtained by noting that a pair

https://doi.org/10.4153/CJM-1992-059-7 Published online by Cambridge University Press

(A_1, A_2) of matrices with A_i as in (7.3) is in the range of the homomorphism if and only if the following systems have integral solutions:

$$\begin{aligned}\alpha_0 + \alpha_0' + \alpha_3 + \alpha_3' &= a_1\\ \alpha_0 + \alpha_0' - \alpha_3 - \alpha_3' &= b_1\\ \alpha_0 - \alpha_0' + \alpha_3 - \alpha_3' &= a_2\\ \alpha_0 - \alpha_0' - \alpha_3 + \alpha_3' &= b_2\end{aligned}$$

$$\begin{aligned}\alpha_2 + \alpha_2' + \alpha_1 + \alpha_1' &= x_{11}\\ \alpha_2 + \alpha_2' - \alpha_1 - \alpha_1' &= y_{11}\\ \alpha_2 - \alpha_2' + \alpha_1 - \alpha_1' &= x_{21}\\ \alpha_2 - \alpha_2' - \alpha_1 + \alpha_1' &= y_{21}\end{aligned}$$

$$\begin{aligned}\beta_3 + \beta_3' + \beta_0 + \beta_0' &= x_{12}\\ \beta_3 + \beta_3' - \beta_0 - \beta_0' &= y_{12}\\ \beta_3 - \beta_3' + \beta_0 - \beta_0' &= x_{22}\\ \beta_3 - \beta_3' - \beta_0 + \beta_0' &= y_{22}\end{aligned}$$

$$\begin{aligned}\beta_2 + \beta_2' + \beta_1 + \beta_1' &= y_{13}\\ \beta_2 + \beta_2' - \beta_1 - \beta_1' &= x_{13}\\ \beta_2 - \beta_2' + \beta_1 - \beta_1' &= y_{23}\\ \beta_2 - \beta_2' - \beta_1 + \beta_1' &= x_{23}\end{aligned}$$

Each of these systems has the same matrix of coefficients. Over $\mathbf{Z}$ the first reduces to

$$\left[\begin{array}{cccc|l} 1 & 1 & 1 & 1 & a_1 \\ 2 & 0 & 2 & 0 & a_1 + a_2 \\ 2 & 2 & 0 & 0 & a_1 + b_1 \\ 4 & 0 & 0 & 0 & a_1 + b_1 + a_2 + b_2 \end{array}\right]$$

which implies that $4 \mid (a_1 + b_1 + a_2 + b_2)$, $2 \mid (a_1 + a_2)$ and $2 \mid (a_1 + b_1)$. Conversely, assuming these three conditions, the elements

$$\begin{aligned}\alpha_0 &= \tfrac{1}{4}(a_1 + b_1 + a_2 + b_2)\\ \alpha_0' &= \tfrac{1}{2}(a_1 + b_1) - \alpha_0\\ \alpha_3 &= \tfrac{1}{2}(a_1 + a_2) - \alpha_0\\ \alpha_3' &= a_1 - \alpha_0 - \alpha_0' - \alpha_3\end{aligned}$$

satisfy the first system. The solution to the other three systems is similar and it is apparent that the range of our homomorphism is as given. ∎

8. $M_{32}(16\Gamma_2c_2, 16\Gamma_2c_2, 16\Gamma_2c_1, 16\Gamma_2c_1)$. This loop is L_3, which was presented in Section 3 as:

$$L_3 = \langle a, b, u \mid a^4 = b^4 = 1, u^2 = a^2b^2, (a, b) = (a, u) = (b, u) = (a, b, u) = a^2 \rangle$$

The group $G = \langle a, b \rangle$ has centre $Z(G) = \{1, e, b^2, eb^2\} \cong C_2 \times C_2$; moreover, $e = a^2$ and $g_0 = u^2 = a^2b^2$.

Any $x \in \mathbf{Z}G$ is a linear combination of 1, a, b, b^2, b^3, ab, ab^2, ab^3 and the product of these elements with $a^2 = e$ and so $(1 - e)x$ is a linear combination of just the eight elements just listed. Thus, for $r = 1 + (1 - e)(x + yu)$, we may assume

$$\begin{aligned} x &= (\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + b^2(\alpha_0' + \alpha_1' a + \alpha_2' b + \alpha_3' ab) \\ y &= (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + b^2(\beta_0' + \beta_1' a + \beta_2' b + \beta_3' ab). \end{aligned} \tag{8.1}$$

We have

$$x^* = (\alpha_0 + b^2\alpha_0') + e[(\alpha_1 a + \alpha_2 b + \alpha_3 ab) + b^2(\alpha_1' a + \alpha_2' b + \alpha_3' ab)]$$

and a similar expression for y^*, $x_1 = \alpha_0 + b^2\alpha_0'$,

$$\begin{aligned} xx^* = {} & [(\alpha_0^2 + {\alpha_0'}^2 + \alpha_1^2 + {\alpha_1'}^2) + b^2(2\alpha_1\alpha_1' + 2\alpha_0\alpha_0')] \\ & + e[(2\alpha_2\alpha_2' + 2\alpha_3\alpha_3') + b^2(\alpha_2^2 + {\alpha_2'}^2 + \alpha_3^2 + {\alpha_3'}^2] + (1 + e)s \end{aligned}$$

for some $s \in \mathbf{Z}G$, and a similar expression for yy^*. Since $g_0 = eb^2$, $g_0(1 - e) = -(1 - e)b^2$ and $(1 - e)(x_1 + xx^* - g_0yy^*) = (1 - e)(x_1 + xx^* + b^2yy^*) = (1 - e)(m + nb^2)$ where m and n are the integers

$$\begin{aligned} m &= \alpha_0 + \alpha_0^2 + {\alpha_0'}^2 + \alpha_1^2 + {\alpha_1'}^2 - \beta_2^2 - {\beta_2'}^2 - \beta_3^2 - {\beta_3'}^2 \\ &\quad - 2\alpha_2\alpha_2' - 2\alpha_3\alpha_3' + 2\beta_0\beta_0' + 2\beta_1\beta_1' \\ n &= \alpha_0' - \alpha_2^2 - {\alpha_2'}^2 - \alpha_3^2 - {\alpha_3'}^2 + \beta_0^2 + {\beta_0'}^2 + \beta_1^2 + {\beta_1'}^2 \\ &\quad + 2\alpha_0\alpha_0' + 2\alpha_1\alpha_1' - 2\beta_2\beta_2' - 2\beta_3\beta_3' \end{aligned}$$

By the linear independence of $1, e, b^2, eb^2$ over $\mathbf{Z}$ and Corollary 4.2, $r = 1 + (1 - e)(x + yu)$ is a unit if and only if $m = n = 0$; *i.e.*, if and only if

$$\begin{aligned} & (\alpha_0 + \alpha_0') + (\alpha_0 + \alpha_0')^2 + (\alpha_1 + \alpha_1')^2 - (\alpha_2 + \alpha_2')^2 - (\alpha_3 + \alpha_3')^2 \\ & \qquad + (\beta_0 + \beta_0')^2 + (\beta_1 + \beta_1')^2 - (\beta_2 + \beta_2')^2 - (\beta_3 + \beta_3')^2 = 0 \text{ and} \\ & (\alpha_0 - \alpha_0') + (\alpha_0 - \alpha_0')^2 + (\alpha_1 - \alpha_1')^2 + (\alpha_2 - \alpha_2')^2 + (\alpha_3 - \alpha_3')^2 \\ & \qquad - (\beta_0 - \beta_0')^2 - (\beta_1 - \beta_1')^2 - (\beta_2 - \beta_2')^2 - (\beta_3 - \beta_3')^2 = 0 \end{aligned}$$

which is to say, if and only if

$$\begin{aligned} & [1 + 2(\alpha_0 + \alpha_0')]^2 + [2(\alpha_1 + \alpha_1')]^2 - [2(\alpha_2 + \alpha_2')]^2 - [2(\alpha_3 + \alpha_3')]^2 \\ & \qquad + [2(\beta_0 + \beta_0')]^2 + [2(\beta_1 + \beta_1')]^2 - [2(\beta_2 + \beta_2')]^2 - [2(\beta_3 + \beta_3')]^2 = 1 \text{ and} \\ & [1 + 2(\alpha_0 - \alpha_0')]^2 + [2(\alpha_1 - \alpha_1')]^2 - [2(\beta_0 - \beta_0')]^2 - [2(\beta_1 - \beta_1')]^2 \\ & \qquad + [2(\alpha_2 - \alpha_2')]^2 + [2(\alpha_3 - \alpha_3')]^2 - [2(\beta_2 - \beta_2')]^2 - [2(\beta_3 - \beta_3')]^2 = 1 \end{aligned} \tag{8.2}$$

https://doi.org/10.4153/CJM-1992-059-7 Published online by Cambridge University Press

(Note that here we must have $\alpha_0 \equiv \alpha_0' \pmod 2$.) Now we proceed as in the previous section. We observe that the maps φ and ψ: $L_3 \longrightarrow L_0$ which send b^2 to 1 and b^2 to $a^2 = e$ respectively induce loop homomorphisms $\mathcal{U}(\mathbf{Z}L_3) \longrightarrow \mathcal{U}(\mathbf{Z}L_0)$ with kernels

$$\ker\varphi = \{1 + (1-e)(1-b^2)(x+yu) \mid x, y \in \mathbf{Z}G\}$$
$$\ker\psi = \{1 + (1-e)(1+b^2)(x+yu) \mid x, y \in \mathbf{Z}G\}$$

Again, $\ker\varphi \cap \ker\psi = \{1\}$ and $r \longmapsto \big(\varphi(r), \psi(r)\big)$ is a one-to-one homomorphism into $\mathcal{U}(\mathbf{Z}L_0) \times \mathcal{U}(\mathbf{Z}L_0)$.

At this point, we note a subtle difference between what is happening here and what happened at a similar stage of the previous section. While φ maps the generators a, b, u of L_3 to the generators a, b, u of L_0, respectively (as both φ and ψ did in Section 7), here the map ψ interchanges b and u; that is, ψ sends a, b, u of L_3 to a, u, b of L_0, respectively. Thus, for x and y as in (8) and $r = 1 + (1-e)(x+yu)$,

$$\begin{aligned}\psi(r) = 1 + (1-e)\big\{&[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + e(\alpha_0' + \alpha_1' a + \alpha_2' b + \alpha_3' ab)]\\ &+ [(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + e(\beta_0' + \beta_1' a + \beta_2' b + \beta_3' ab)]u\big\}\\ = 1 + (1-e)\big\{&[(\alpha_0 - \alpha_0') + (\alpha_1 - \alpha_1')a + (\alpha_2 - \alpha_2')b + (\alpha_3 - \alpha_3')ab]\\ &+ [(\beta_0 - \beta_0') + (\beta_1 - \beta_1')a + (\beta_2 - \beta_2')b + (\beta_3 - \beta_3')ab]u\big\}\end{aligned}$$

and so, using $bu = eub$ and $(ab)u = e(au)b$, we see that the way to write $\psi(r)$ as an element of $\mathcal{V}_0$, the torsion-free complement of L_0 in $\mathcal{U}(\mathbf{Z}L_0)$, when the generators of L_0 are a, u, b is

$$\begin{aligned}\psi(r) = 1 + (1-e)\big\{&[(\alpha_0 - \alpha_0') + (\alpha_1 - \alpha_1')a + (\beta_0 - \beta_0')u + (\beta_1 - \beta_1')au]\\ &+ [(\alpha_2 - \alpha_2') + (\alpha_3 - \alpha_3')a - (\beta_2 - \beta_2')u - (\beta_3 - \beta_3')au]bbigr\}\end{aligned}$$

Notice that the second equation of (8), together with the fact that $\alpha_0 - \alpha_0' \equiv 0 \pmod 2$, are precisely the conditions of Theorem 5.1 which say that $\psi(r)$ is in $\mathcal{V}_0$ (just as $\alpha_0 + \alpha_0' \equiv 0 \pmod 2$ and the first equation of (8) are the conditions that put $\varphi(r)$ in $\mathcal{V}_0$).

We claim that the range of the map $r \longmapsto \big(\varphi(r), \psi(r)\big)$ is

$$\begin{aligned}\big\{(s_1, s_2) \mid s_1 &= 1 + (1-e)[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab)u]\\ s_2 &= 1 + (1-e)[(\gamma_0 + \gamma_1 a + \gamma_2 u + \gamma_3 au) + (\delta_0 + \delta_1 a + \delta_2 u + \gamma_3 au)b]\\ &\quad \alpha_0 + \gamma_0, \alpha_1 + \gamma_1, \alpha_2 + \delta_0,\\ &\quad \alpha_3 + \delta_1, \beta_0 + \gamma_2, \beta_1 + \gamma_3, \beta_2 + \delta_2, \beta_3 + \delta_3 \text{ even},\\ &\quad (1 + 2\alpha_0)^2 + (2\alpha_1)^2 - (2\alpha_2)^2 - (2\alpha_3)^2 + (2\beta_0)^2 + (2\beta_1)^2\\ &\quad - (2\beta_2)^2 - (2\beta_3)^2 = 1,\\ &\quad (1 + 2\gamma_0)^2 + (2\gamma_1)^2 - (2\gamma_2)^2 - (2\gamma_3)^2\\ &\quad + (2\delta_0)^2 + (2\delta_1)^2 - (2\delta_2)^2 - (2\delta_3)^2 = 1\big\}\end{aligned} \tag{8.3}$$

https://doi.org/10.4153/CJM-1992-059-7 Published online by Cambridge University Press

Equations (8.4) follow from the fact that, as units of $\mathbf{Z}L_0$, s_1 and s_2 must satisfy (5.1). Our claim is justified by observing that given s_1, s_2 as described and letting

$$\begin{aligned}
\rho_0(\rho_0') &= \tfrac{1}{2}(\alpha_0 \pm \gamma_0), & \rho_1(\rho_1') &= \tfrac{1}{2}(\alpha_1 \pm \gamma_1)\\
\rho_2(\rho_2') &= \tfrac{1}{2}(\alpha_2 \pm \delta_0), & \rho_3(\rho_3') &= \tfrac{1}{2}(\alpha_3 \pm \delta_1)\\
\tau_0(\tau_0') &= \tfrac{1}{2}(\beta_0 \pm \gamma_2), & \tau_1(\tau_1') &= \tfrac{1}{2}(\beta_1 \pm \gamma_3)\\
\tau_2(\tau_2') &= \tfrac{1}{2}(\beta_2 \mp \delta_2), & \tau_3(\tau_3') &= \tfrac{1}{2}(\beta_3 \mp \delta_3),
\end{aligned}$$

the element $r = 1 + (1-e)(x + yu)$ with

$$\begin{aligned}
x &= (\rho_0 + \rho_1 a + \rho_2 b + \rho_3 ab) + b^2(\rho_0' + \rho_1' a + \rho_2' b + \rho_3' ab)\\
y &= (\tau_0 + \tau_1 a + \tau_2 b + \tau_3 ab) + b^2(\tau_0' + \tau_1' a + \tau_2' b + \tau_3' ab)
\end{aligned}$$

satisfies $\big(\varphi(r), \psi(r)\big) = (s_1, s_2)$ and is a unit in $\mathbf{Z}L_3$ because the coefficients of x and y satisfy (8), these being exactly the equations (8.4) which say that s_1 and s_2 are units in $\mathbf{Z}L_0$. Thus we obtain the following characterization of the units in $\mathbf{Z}L_3$.

THEOREM 8.1. *Let*

$$\begin{aligned}
L_3 &= M_{32}(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_1, 16\Gamma_2 c_1)\\
&= \langle a, b, u \mid a^4 = b^4 = 1, u^2 = a^2b^2, (a,b) = (a,u) = (b,u) = (a,b,u) = a^2 \rangle
\end{aligned}$$

Then the unit loop of $\mathbf{Z}L_3$ *is* $\pm L_3\mathcal{V}$ *where* $\mathcal{V}$ *is a torsion-free normal complement of* L_3 *consisting of elements*

$$\begin{aligned}
r = 1 + (1-a^2)\big\{&[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + b^2(\alpha_0' + \alpha_1' a + \alpha_2' b + \alpha_3' ab)]\\
&+ [(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + b^2(\beta_0' + \beta_1' a + \beta_2' b + \beta_3' ab)]u\big\}
\end{aligned}$$

with $\alpha_0 \equiv \alpha_0' \pmod 2$,

$$\begin{aligned}
&[1 + 2(\alpha_0 + \alpha_0')]^2 + [2(\alpha_1 + \alpha_1')]^2 - [2(\alpha_2 + \alpha_2')]^2 - [2(\alpha_3 + \alpha_3')]^2\\
&\quad + [2(\beta_0 + \beta_0')]^2 + [2(\beta_1 + \beta_1')]^2 - [2(\beta_2 + \beta_2')]^2 - [2(\beta_3 + \beta_3')]^2 = 1 \text{ and}\\
&[1 + 2(\alpha_0 - \alpha_0')]^2 + [2(\alpha_1 - \alpha_1')]^2 - [2(\beta_0 - \beta_0')]^2 - [2(\beta_1 - \beta_1')]^2\\
&\quad + [2(\alpha_2 - \alpha_2')]^2 + [2(\alpha_3 - \alpha_3')]^2 - [2(\beta_2 - \beta_2')]^2 - [2(\beta_3 - \beta_3')]^2 = 1
\end{aligned}$$

Furthermore,

$$\mathcal{V} \cong \Big\{(A_1, A_2) \in \mathfrak{Z}_1(\mathbf{Z}) \times \mathfrak{Z}_1(\mathbf{Z}) \mid$$

(8.4)
$$A_1 = \begin{bmatrix} 1 + 2a_1 & 2\mathbf{x}_1 \\ 2\mathbf{y}_1 & 1 + 2b_1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 + 2a_2 & 2\mathbf{x}_2 \\ 2\mathbf{y}_2 & 1 + 2b_2 \end{bmatrix}$$

$a_i + b_i \in 2\mathbf{Z}$, $\mathbf{x}_i + \mathbf{y}_i \in (2\mathbf{Z}, 2\mathbf{Z}, 2\mathbf{Z})$, $i = 1, 2$

and each of the following in $4\mathbf{Z}$

$$\begin{aligned}
&a_1 + b_1 + a_2 + b_2, && x_{13} + y_{13} + x_{23} + y_{23},\\
&a_1 - b_1 + x_{23} - y_{23}, && a_2 - b_2 + x_{13} - y_{13},\\
&x_{11} - y_{11} + x_{21} - y_{21}, && x_{11} + y_{11} + x_{22} - y_{22},\\
&x_{12} - y_{12} + x_{21} + y_{21}, && x_{12} + y_{12} + x_{22} + y_{22}\Big\}
\end{aligned}$$

where $\mathbf{x}_i = (x_{i1}, x_{i2}, x_{i3})$ *and* $\mathbf{y}_i = (y_{i1}, y_{i2}, y_{i3})$, $i = 1, 2$, *the isomorphism being given by* $r \longmapsto (A_1, A_2)$ *where*

$$A_1 = \begin{bmatrix} 1+2a_1 & 2\mathbf{x}_1 \\ 2\mathbf{y}_1 & 1+2b_1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1+2a_2 & 2\mathbf{x}_2 \\ 2\mathbf{y}_2 & 1+2b_2 \end{bmatrix}$$

$$a_1 = \alpha_0 + \alpha_0' + \alpha_3 + \alpha_3'$$

$$b_1 = \alpha_0 + \alpha_0' - \alpha_3 - \alpha_3'$$

$$\mathbf{x}_1 = (\alpha_2 + \alpha_2' + \alpha_1 + \alpha_1', \beta_3 + \beta_3' + \beta_0 + \beta_0', \beta_2 + \beta_2' - \beta_1 - \beta_1')$$

$$\mathbf{y}_1 = (\alpha_2 + \alpha_2' - \alpha_1 - \alpha_1', \beta_3 + \beta_3' - \beta_0 - \beta_0', \beta_2 + \beta_2' + \beta_1 + \beta_1')$$

$$a_2 = \alpha_0 - \alpha_0' + \beta_1 - \beta_1'$$

$$b_2 = \alpha_0 - \alpha_0' - \beta_1 + \beta_1'$$

$$\mathbf{x}_2 = (\beta_0 - \beta_0' + \alpha_1 - \alpha_1', \beta_3' - \beta_3 + \alpha_2 - \alpha_2', \beta_2' - \beta_2 - \alpha_3 + \alpha_3')$$

$$\mathbf{y}_2 = (\beta_0 - \beta_0' - \alpha_1 + \alpha_1', \beta_3' - \beta_3 - \alpha_2 + \alpha_2', \beta_2' - \beta_2 + \alpha_3 - \alpha_3')$$

PROOF. The isomorphism is the composition of the maps $r \longmapsto \big(\varphi(r), \psi(r)\big)$ and two applications of the isomorphism given in Theorem 5.1. The conditions on the entries of the matrices A_1 and A_2 are obtained by noting that a pair (A_1, A_2) of matrices with A_i as in (8.4) is in the image of the homomorphism if and only if

$$\begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\
0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0
\end{bmatrix}
\begin{bmatrix} \alpha_0 \\ \alpha_0' \\ \alpha_1 \\ \alpha_1' \\ \alpha_2 \\ \alpha_2' \\ \alpha_3 \\ \alpha_3' \\ \beta_0 \\ \beta_0' \\ \beta_1 \\ \beta_1' \\ \beta_2 \\ \beta_2' \\ \beta_3 \\ \beta_3' \end{bmatrix}
=
\begin{bmatrix} a_1 \\ b_1 \\ x_{11} \\ y_{11} \\ x_{12} \\ y_{12} \\ x_{31} \\ y_{31} \\ a_2 \\ b_2 \\ x_{21} \\ y_{21} \\ x_{22} \\ y_{22} \\ x_{23} \\ y_{23} \end{bmatrix}$$

has an integral solution, and this occurs if and only if the following sixteen integers are congruent to 0 (mod 4):

$$a_1 + a_2 + b_1 + b_2,\ x_{11} - y_{11} + x_{21} - y_{21},\ x_{11} + y_{11} + x_{22} - y_{22},\ a_1 - b_1 + x_{23} - y_{23},$$

$$a_1 - a_2 + b_1 - b_2,\ x_{11} - x_{21} - y_{11} + y_{21},\ x_{11} + y_{11} - x_{22} + y_{22},\ -a_1 + b_1 + x_{23} - y_{23},$$

$$x_{12} - y_{12} + x_{21} + y_{21},\ a_2 - b_2 + x_{13} - y_{13},\ x_{13} + y_{13} + x_{23} + y_{23},\ x_{12} + y_{12} + x_{22} + y_{22},$$

$$x_{12} - y_{12} - x_{21} - y_{21},\ a_2 - b_2 - x_{13} + y_{13},\ x_{13} + y_{13} - x_{23} - y_{23},\ x_{12} + y_{12} - x_{22} - y_{22}$$

The second and fourth rows are consequences of the first and third because $a_i + b_i$ as well as $x_{ij} + y_{ij}$ are all even. The first and third rows are those specified in the statement of the theorem. ∎

9. $M_{32}(E_i, 16)$. As in Section 3,

$$M_{32}(E_i, 16) = L_4 = \langle a,b,c,u \mid a^4 = 1, (a,c) = (b,c) = (a,b,c) = (a,c,u) = (b,c,u) = 1,\\ b^2 = c^2 = u^2 = (a,b) = (a,u) = (b,u) = (c,u) = (a,b,u) = a^2\rangle$$

In this case, $G = \langle a,b,c\rangle$ has centre $\mathcal{Z}(G) = \{1, c, e, ce\} \cong C_4$ and $g_0 = u^2 = a^2 = e$. Any $x \in \mathbf{Z}G$ is a linear combination of 1, a, b, ab, c, ac, bc, abc and the product of these elements with e so, for $r = 1 + (1-e)(x+yu) \in \mathbf{Z}L_4$, we may assume that

$$(9.1) \qquad \begin{aligned} x &= (\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + c(\alpha_0' + \alpha_1' a + \alpha_2' b + \alpha_3' ab) \text{ and}\\ y &= (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + c(\beta_0' + \beta_1' a + \beta_2' b + \beta_3' ab)\end{aligned}$$

We have

$$x^* = (\alpha_0 + c\alpha_0') + e[(\alpha_1 a + \alpha_2 b + \alpha_3 ab) + c(\alpha_1' a + \alpha_2' b + \alpha_3' ab)]$$

with a similar expression for y^*, $x_1 = \alpha_0 + c\alpha_0'$,

$$xx^* = [(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2) + c(2(\alpha_0\alpha_0' + 2\alpha_1\alpha_1' + 2\alpha_2\alpha_2' + 2\alpha_3\alpha_3')]\\ + e[\alpha_0'^2 + \alpha_1'^2 + \alpha_2'^2 + \alpha_3'^2] + (1+e)s$$

for some $s \in \mathbf{Z}G$, and a similar expression for yy^*. Therefore, $(1-e)(x_1 + xx^* - g_0 yy^*) = (1-e)(x_1 + xx^* + yy^*) = (1-e)(m+nc)$ where m and n are the integers

$$\begin{aligned} m &= \alpha_0 + \alpha_0^2 - \alpha_0'^2 + \alpha_1^2 - \alpha_1'^2 + \alpha_2^2 - \alpha_2'^2 + \alpha_3^2 - \alpha_3'^2\\ &\quad + \beta_0^2 - \beta_0'^2 + \beta_1^2 - \beta_1'^2 + \beta_2^2 - \beta_2'^2 + \beta_3^2 - \beta_3'^2\\ n &= \alpha_0' + 2(\alpha_0\alpha_0' + \alpha_1\alpha_1' + \alpha_2\alpha_2' + \alpha_3\alpha_3' + \beta_0\beta_0' + \beta_1\beta_1' + \beta_2\beta_2' + \beta_3\beta_3')\end{aligned}$$

Since 1, e, a, and ea are linearly independent over $\mathbf{Z}$, $r = 1 + (1-e)(x+yu)$ is a unit if and only if $m = n = 0$; equivalently, if and only if $m + ni = 0$, $i = \sqrt{-1}$, a condition in turn equivalent to

$$[1 + 2(\alpha_0 + i\alpha_0')]^2 + [2(\alpha_1 + i\alpha_1')]^2 + [2(\alpha_2 + i\alpha_2')]^2 + [2(\alpha_3 + i\alpha_3')]^2\\ + [2(\beta_0 + i\beta_0')]^2 + [2(\beta_1 + i\beta_1')]^2 + [2(\beta_2 + i\beta_2')]^2 + [2(\beta_3 + i\beta_3')]^2 = 1$$

If we let $z_k = \alpha_k + i\alpha_k'$ and $w_k = \beta_k + i\beta_k'$, for $k = 0, 1, 2, 3$, this becomes

$$(1+2z_0)^2 + (2z_1)^2 + (2z_2)^2 + (2z_3)^2 + (2w_0)^2 + (2w_1)^2 + (2w_2)^2 + (2w_3)^2 = 1$$

which we recognize as $\det A = 1$, where $A \in \mathfrak{Z}(\mathbf{Z}[i])$ is the matrix

$$\begin{bmatrix} 1 + 2(z_0 + iz_1) & 2(iz_2 - z_3, iw_0 - w_1, w_2 - iw_3)\\ 2(iz_2 + z_3, iw_0 + w_1, -w_2 - iw_3) & 1 + 2(z_0 - iz_1)\end{bmatrix}$$

Just as with L_0, the idea is now to prove (admittedly, with some labour) that the map $r = 1 + (1-e)(x+yu) \mapsto A$ (x and y as in (9)) is a homomorphism into $\mathfrak{Z}_1(\mathbf{Z}[i])$. Its range is readily determined and so we obtain the following characterization of the unit loop of $\mathbf{Z}L_4$.

https://doi.org/10.4153/CJM-1992-059-7 Published online by Cambridge University Press

THEOREM 9.1. *Let L_4 denote the loop*

$$M_{32}(E_i, 16) = \langle a, b, c, u \mid a^4 = 1, (a,c) = (b,c) = (a,b,c) = (a,c,u) = (b,c,u) = 1, \\ b^2 = c^2 = u^2 = (a,b) = (a,u) = (b,u) = (c,u) = (a,b,u) = a^2 \rangle.$$

Then the unit loop of $\mathbf{Z}L_4$ is $\pm L_4\mathcal{V}$ where $\mathcal{V}$ is a torsion-free normal complement of L_4 consisting of elements of the form

$$r = 1 + (1-a^2)\big\{[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + c(\alpha'_0 + \alpha'_1 a + \alpha'_2 b + \alpha'_3 ab)] \\ + [(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + c(\beta'_0 + \beta'_1 a + \beta'_2 b + \beta'_3 ab)]u\big\}$$

with $\alpha_0 \equiv \alpha'_0 \equiv 0 \pmod 2$ and

$$[1 + 2(\alpha_0 + i\alpha'_0)]^2 + [2(\alpha_1 + i\alpha'_1)]^2 + [2(\alpha_2 + i\alpha'_2)]^2 + [2(\alpha_3 + i\alpha'_3)]^2 \\ + [2(\beta_0 + i\beta'_0)]^2 + [2(\beta_1 + i\beta'_1)]^2 + [2(\beta_2 + i\beta'_2)]^2 + [2(\beta_3 + i\beta'_3)]^2 = 1.$$

Furthermore,

$$\mathcal{V} \cong \left\{ \begin{bmatrix} 1+2a & 2\mathbf{x} \\ 2\mathbf{y} & 1+2b \end{bmatrix} \in \mathfrak{Z}_1(\mathbf{Z}[i]) \mid a+b \in 2\mathbf{Z}[i], \mathbf{x}+\mathbf{y} \in (2\mathbf{Z}[i], 2\mathbf{Z}[i], 2\mathbf{Z}[i]) \right\}$$

the isomorphism being given by

$$r \mapsto \begin{bmatrix} 1 + 2(\alpha_0 + i\alpha'_0 + i\alpha_1 - \alpha'_1) & \begin{matrix} 2(i\alpha_2 - \alpha'_2 - \alpha_3 - i\alpha'_3, \\ i\beta_0 - \beta'_0 - \beta_1 - i\beta'_1, \\ \beta_2 + i\beta'_2 - i\beta_3 + \beta'_3) \end{matrix} \\ \begin{matrix} 2(i\alpha_2 - \alpha'_2 + \alpha_3 + i\alpha'_3, \\ i\beta_0 - \beta'_0 + \beta_1 + i\beta'_1, \\ -\beta_2 - i\beta'_2 - i\beta_3 + \beta'_3) \end{matrix} & 1 + 2(\alpha_0 + i\alpha'_0 - i\alpha_1 + \alpha'_1) \end{bmatrix}$$

10. **$M_{32}(5,5,5,2,2,4)$.** We present $L_5 = M_{32}(5,5,5,2,2,4)$ as in Section 3:

$$L_5 = \langle a, b, u \mid a^8 = b^2 = 1, a^2 = u^2, (a,b) = (a,u) = (b,u) = (a,b,u) = a^4 \rangle.$$

Here $G = \langle a, b \rangle \cong 16\Gamma_2 d$, $\mathcal{Z}(G) = \{1, a^2, e, ea^2\} \cong C_4$, $e = a^4$ and $g_0 = a^2$. Any $x \in \mathbf{Z}G$ is a linear combination of 1, a, a^2, a^3, b, ab, a^2b, a^3b, and the product of these elements with e, so for $r = 1 + (1-e)(x + yu) \in \mathbf{Z}L_5$, we may assume that

$$x = (\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + a^2(\alpha'_0 + \alpha'_1 a + \alpha'_2 b + \alpha'_3 ab) \\ y = (\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + a^2(\beta'_0 + \beta'_1 a + \beta'_2 b + \beta'_3 ab). \tag{10.1}$$

Here we have

$$x^* = (\alpha_0 + a^2\alpha'_0) + e[(\alpha_1 a + \alpha_2 b + \alpha_3 ab) + a^2(\alpha'_1 a + \alpha'_2 b + \alpha'_3 ab)]$$

with a similar expression for y^*, $x_1 = \alpha_0 + a^2\alpha'_0$,

$$xx^* = (\alpha_0^2 + {\alpha'_2}^2 + 2\alpha_1\alpha'_1) + a^2(2\alpha_0\alpha'_0 + {\alpha'_1}^2 + \alpha_3^2) \\ + e[({\alpha'_0}^2 + \alpha_2^2 + 2\alpha_3\alpha'_3) + a^2(\alpha_1^2 + {\alpha'_3}^2 + 2\alpha_2\alpha'_2)] + (1+e)s$$

for some $s \in \mathbf{Z}G$, and a similar expression for yy^*. Also, $(1-e)(x_1 + xx^* - g_0yy^*) = (1-e)(m + na^2)$ where m and n are the integers

$$\begin{aligned} m &= \alpha_0 + \alpha_0^2 - {\alpha_0'}^2 - \alpha_2^2 + {\alpha_2'}^2 + 2\alpha_1\alpha_1' - 2\alpha_3\alpha_3' \\ &\quad - \beta_1^2 + {\beta_1'}^2 + \beta_3^2 - {\beta_3'}^2 + 2\beta_0\beta_0' - 2\beta_2\beta_2' \\ n &= \alpha_0' - \alpha_1^2 + {\alpha_1'}^2 + \alpha_3^2 - {\alpha_3'}^2 + 2\alpha_0\alpha_0' - 2\alpha_2\alpha_2' \\ &\quad - \beta_0^2 + {\beta_0'}^2 + \beta_2^2 - {\beta_2'}^2 - 2\beta_1\beta_1' + 2\beta_3\beta_3' \end{aligned}$$

so, just as in the previous section, we discover that $r = 1 + (1-e)(x + yu)$ is a unit (x and y as in (10)) if and only if $m + ni = 0$, a condition which can be expressed as

$$\begin{aligned} &[1 + 2(\alpha_0 + i\alpha_0')]^2 - i[2(\alpha_1 + i\alpha_1')]^2 - [2(\alpha_2 + i\alpha_2')]^2 + i[2(\alpha_3 + i\alpha_3')]^2 \\ &\qquad - i[2(\beta_0 + i\beta_0')]^2 - [2(\beta_1 + i\beta_1')]^2 + i[2(\beta_2 + i\beta_2')]^2 + [2(\beta_3 + i\beta_3')]^2 = 1 \end{aligned}$$

or, equivalently,

$$\det \begin{bmatrix} 1 + 2(z_0 + z_2) & 2(i(z_1 - z_3), w_1 + w_3, i(w_0 + w_2)) \\ 2(z_1 + z_3, w_1 - w_3, w_0 - w_2) & 1 + 2(z_0 - z_2) \end{bmatrix} = 1$$

where $z_k = \alpha_k + i\alpha_k'$ and $w_k = \beta_k + i\beta_k'$ for $k = 0, 1, 2, 3$. The matrix here suggests a map into $\mathfrak{Z}_1(\mathbf{Z}[i])$ which turns out to be a loop homomorphism.

THEOREM 10.1. *Let L_5 denote the loop*

$$M_{32}(5,5,5,2,2,4) = \langle a, b, u \mid a^8 = b^2 = 1, u^2 = a^2, \\ (a,b) = (a,u) = (b,u) = (a,b,u) = a^4 \rangle.$$

Then the unit loop of $\mathbf{Z}L_5$ is $\pm L_5 \mathcal{V}$ where $\mathcal{V}$ is a torsion-free normal complement of L_5 consisting of elements of the form

$$\begin{aligned} r = 1 + (1 - a^4)\big\{&[(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) + a^2(\alpha_0' + \alpha_1' a + \alpha_2' b + \alpha_3' ab)] \\ &+ [(\beta_0 + \beta_1 a + \beta_2 b + \beta_3 ab) + a^2(\beta_0' + \beta_1' a + \beta_2' b + \beta_3' ab)]u\big\} \end{aligned}$$

with $\alpha_0 \equiv \alpha_0' \pmod 2$ and

$$\begin{aligned} &[1 + 2(\alpha_0 + i\alpha_0')]^2 - i[2(\alpha_1 + i\alpha_1')]^2 - [2(\alpha_2 + i\alpha_2')]^2 + i[2(\alpha_3 + i\alpha_3')]^2 \\ &\qquad - i[2(\beta_0 + i\beta_0')]^2 - [2(\beta_1 + i\beta_1')]^2 + i[2(\beta_2 + i\beta_2')]^2 + [2(\beta_3 + i\beta_3')]^2 = 1. \end{aligned}$$

Furthermore,

$$\mathcal{V} \cong \left\{ \begin{bmatrix} 1 + 2a & 2\mathbf{x} \\ 2\mathbf{y} & 1 + 2b \end{bmatrix} \in \mathfrak{Z}_1(\mathbf{Z}[i]) \mid a + b, x_2 + y_2, x_1 + iy_1, x_3 + iy_3 \in 2\mathbf{Z}[i] \right\}$$

the isomorphism being given by

$$r \longmapsto \begin{bmatrix} 1 + 2(\alpha_0 + i\alpha_0' + \alpha_2 + i\alpha_2') & \begin{matrix} 2(i\alpha_1 - \alpha_1' - i\alpha_3 + \alpha_3', \\ \beta_1 + i\beta_1' + \beta_3 + i\beta_3', \\ i\beta_0 - \beta_0' + i\beta_2 - \beta_2') \end{matrix} \\ \begin{matrix} 2(\alpha_1 + i\alpha_1' + \alpha_3 + i\alpha_3', \\ \beta_1 + i\beta_1' - \beta_3 - i\beta_3', \\ \beta_0 + i\beta_0' - \beta_2 - i\beta_2') \end{matrix} & 1 + 2(\alpha_0 + i\alpha_0' - \alpha_2 - i\alpha_2') \end{bmatrix}$$

References

1. P. J. Allen and C. Hobby, *A characterization of units in* $\mathbf{Z}[A_4]$, J. Algebra **66**(1980), 534–543.
2. ———, *A characterization of units in* $\mathbf{Z}[S_4]$, Comm. Algebra (7) **16** (1988), 1479–1505.
3. Orin Chein, *Moufang loops of small order*, Mem. Amer. Math. Soc. (13) **197**(1978).
4. Orin Chein and Edgar G. Goodaire, *Loops whose loop rings are alternative*, Comm. Algebra **14**(1986), 293–310.
5. Edgar G. Goodaire and César Polcino Milies, *Torsion units in alternative loop rings*, Proc. Amer. Math. Soc. **107**(1989), 7–15.
6. Edgar G. Goodaire and M. M. Parmenter, *Units in alternative loop rings*, Israel J. Math. (2) **53**(1986), 209–216.
7. ———, *Semi-simplicity of alternative loop rings*, Acta Math. Hungar. (3–4) **50**(1987), 241–247.
8. Graham Higman, *The units of group rings*, Proc. London Math. Soc. (2) **46**(1940), 231–248.
9. I. Hughes and K. R. Pearson, *The group of units of the integral group ring* $\mathbf{Z}S_3$, Canad. Math. Bull. **15**(1972), 529–534.
10. Eric Jespers and Guilherme Leal, *A characterization of the unit loop of the integral loop ring* $\mathbf{Z}M_{16}(\mathbf{Q}, 2)$, to appear in J. Alg.
11. ———, *Describing units of integral group rings of some 2-groups*, Comm. Algebra (6) **19**(1991), 1809–1827.
12. Martin W. Liebeck, *The classification of finite simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **102**(1987), 33–47.
13. C. S. Polcino Milies, *The group of units of the integral group ring* $\mathbf{Z}D_4$, Bol. Soc. Brasil. Mat. (2) **4**(1973), 85–92.
14. Lowell J. Paige, *A class of simple Moufang loops*, Proc. Amer. Math. Soc. **7**(1956), 471–482.
15. M. M. Parmenter, *Torsion-free normal complements in unit groups of integral group rings*, C.R. Math. Rep. Acad. Sci. Canada (4) **XII**(1990), 113–118.
16. Jürgen Ritter and Sudarshan K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. (2) **324**(1991), 603–621.
17. S. K. Sehgal, *Topics in group rings*, Marcel Dekker, New York, 1978.
18. A. D. Thomas and G. V. Wood, *Group tables*, Shiva Publishing, Orpington, 1980.
19. K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov and A. I. Shirshov, *Rings that are nearly associative*, Academic Press, New York, 1982, Translated by Harry F. Smith.

Memorial University of Newfoundland
St. John's, Newfoundland
A1C 5S7
Email: edgar@morgan.ucs.mun.ca