ISRAEL JOURNAL OF MATHEMATICS, Vol. 53, No. 2, 1986

UNITS IN ALTERNATIVE LOOP RINGS[†]

BY

EDGAR G. GOODAIRE AND M. M. PARMENTER

Department of Mathematics and Statistics,
Memorial University of Newfoundland, St. John's, Newfoundland, Canada A1C 5S7

ABSTRACT

In this paper, we show that certain well known theorems concerning units in integral group rings hold more generally for integral loop rings which are alternative.

0. Introduction

The determination of the group of units in a group ring is a subject of continuing interest to many people. In any integral group ring $\mathbf{Z}G$, the elements of $\pm G$ are obviously units: such units are called *trivial*. Several of the early results about units in group rings give conditions under which certain types of units are trivial. For example, when G is abelian it is known that all the units of finite order in $\mathbf{Z}G$ are trivial. In 1940, Graham Higman [6] found necessary and sufficient conditions for all the units in an integral group ring of a periodic group to be trivial; later, Berman [1] proved a similar theorem for finite groups for the units of finite order. In 1965, Cohn and Livingstone [3] proved that all the central units of finite order in an integral group ring are trivial.

An alternative ring is one in which the *associator* $(x, y, z) := (xy)z - x(yz)$ is a skew-symmetric function of its arguments. One of the most useful properties of an alternative ring was established by Artin: the subring generated by any pair of elements is associative. This fact will be used implicitly throughout our paper. We refer the reader to Chapter 3 of Schafer [8] where the properties of alternative rings which we require here are discussed. The variety of alternative rings not only includes that of associative rings, but resembles it in many ways. Many theorems in associative ring theory hold also in the wider variety. In this

[†] This research was supported in part by the Natural Sciences and Engineering Research Council, Grants No. A9087 and A8775.

Received May 2, 1985 and in revised form October 15, 1985

spirit, we prove here that the theorems about units which we have mentioned above hold more generally for alternative *loop* rings over the integers. (We assume throughout this paper that the coefficient ring is the ring $\mathbf{Z}$ of integers.) In addition, for loop rings which are alternative but not associative we prove an interesting theorem which is not true for group rings: all central units in $\mathbf{Z}L$ are trivial if and only if the centre of L and the quotient of L by its commutator subloop are abelian groups of exponent 2, 3, 4 or 6.

By a *loop* we just mean a set L and a closed binary operation $(a,b)\rightarrow ab$ on L relative to which there is a two-sided identity element and which has the property that the right and left multiplication maps defined by any element of L are bijections. If the integral loop ring $\mathbf{Z}L$ is alternative, then one of the many identities which hold in the ring (and hence in L) is $(xy)(zx)=[x(yz)]x$ [8]. This identity defines what is known as a *Moufang loop*. Clearly then L is such a loop; it's a group of course if $\mathbf{Z}L$ is associative, but otherwise has special properties which have been established elsewhere [2, 4, 5].

THEOREM 1. *Suppose $\mathbf{Z}L$ is an alternative ring which is not associative.*

(i) *The centre, $Z(L)$, and nucleus, $N(L)$, coincide.*

(ii) *$g^2\in Z(L)$ for any $g\in L$.*

(iii) *There exists an element $e\in Z(L)$ of order 2 such that for every g and h in L, either $hg=gh$ or $hg=egh$, and for every g, h and k in L either $g(hk)=(gh)k$ or $g(hk)=e(gh)k$.*

(iv) *If g and h are any two elements of L which do not commute, then the subloop G of L generated by g, h and $Z(L)$ is a subgroup of index 2 with $Z(G)=Z(L)$.*

Later, the structure of the alternative rings which appear as loop rings of Moufang loops was investigated. What we need is summarized below:

THEOREM 2. [5] *Suppose $\mathbf{Z}L$ is an alternative ring which is not associative and G is any subgroup of index 2 in L. Then*

(i) *The map $*: G\rightarrow G$ defined by*

$$g^*=\begin{cases} g, & g\in Z(G)\\ eg, & g\notin Z(G)\end{cases}$$

is an involution on G which extends to an involution on the group ring $\mathbf{Z}G$ as follows:

$$\Big(\sum_{g\in G}\alpha_g g\Big)^*=\sum \alpha_g g^*.$$

(ii) *Every element in* $\mathbf{Z}L$ *can be written in the form* $x + yu$ *where* $x, y \in \mathbf{Z}G$. *Multiplication in* $\mathbf{Z}L$ *is given by*

$$(x + yu)(z + wu) = (xz + g_0 w^* y) + (wx + yz^*)u,$$

where $x, y, z, w \in \mathbf{Z}G$ *and* g_0 *is an element in* $Z(G)$.

(iii) *The map* $* : \mathbf{Z}L \to \mathbf{Z}L$ *defined by* $(x + yu)^* = x^* + eyu$ *is an involution on* $\mathbf{Z}L$ *extending the one on* $\mathbf{Z}G$ *given in* (i). *An element* $\alpha \in \mathbf{Z}L$ *is central* $\Leftrightarrow$ $\alpha^* = \alpha$.

(iv) *The centre and nucleus of the ring* $\mathbf{Z}L$ *coincide and are equal to*

$$\{x + yu \mid x, y \in Z(RG), ey = y\} = \{x + yu \mid x \in Z(RG) \text{ and } ey = y\}.$$

1. Units

Suppose now that L is a loop whose loop ring is alternative, but not associative. Fix arbitrarily any subgroup G of index 2 in L. If $x + yu$, $x, y \in \mathbf{Z}G$ is a unit in the alternative ring $\mathbf{Z}L$, then for some $z + wu \in \mathbf{Z}L$,

$$(x + yu)(z + wu) = (z + wu)(x + yu) = 1.$$

Therefore, $xz + g_0 w^* y = zx + g_0 y^* w = 1$ and $wx + yz^* = yz + wx^* = 0$. It follows immediately that $x^* - yu$ is invertible too, since

$$\begin{aligned}(x^* - yu)(z^* - wu) &= (x^* z^* + g_0 w^* y) + (-wx^* - yz)u \\ &= (zx + g_0 y^* w)^* = 1^* = 1,\end{aligned}$$

and similarly, $(z^* - wu)(x^* - yu) = 1$. Since the product of invertible elements in an alternative ring is invertible, it follows that $(x + yu)(x^* - yu) = xx^* - g_0 yy^*$ is also invertible. On the other hand, if x and $y \in \mathbf{Z}G$ are such that $xx^* - g_0 yy^*$ is invertible (with inverse a, say), then $x + yu$ is invertible, with inverse $ax^* - ayu$. Furthermore, the map $\theta : \mathbf{Z}L \to \mathbf{Z}L$ defined by $(x + yu)\theta = x^* - yu$ is easily verified to be an involution on $\mathbf{Z}L$. Since $r \in \mathbf{Z}L$ and $r\theta$ commute, if r has finite order, so does $r(r\theta) = xx^* - g_0 yy^*$. The following Proposition is now apparent:

PROPOSITION 3. *An element* $x + yu$ *is a unit in* $\mathbf{Z}L$ *if and only if* $xx^* - g_0 yy^*$ *is a central unit in* $\mathbf{Z}G$. *If* $x + yu$ *has finite order, so does* $xx^* - g_0 yy^*$.

We will frequently wish to pass from the alternative ring $\mathbf{Z}L$ to the abelian group ring $\mathbf{Z}(L/L')$, where $L' = \{1, e\}$ is the commutator subloop of L. We use $\bar{r}$ to denote the image of r in $\mathbf{Z}(L/L')$. Since the kernel of the homomorphism

$r \to \bar{r}$ is the ideal of $\mathbf{Z}L$ generated by $1-e$, if $r = x + yu$ and $\bar{r} = \bar{0}$, then $(1+e)r = 0$ and so $(1+e)x = (1+e)y = 0$; i.e. $x, y \in (1-e)\mathbf{Z}G$. Suppose that $\bar{r}$ is a trivial unit in the group ring $\mathbf{Z}(L/L')$; i.e., $\bar{r} = \pm \bar{g}$ or $\pm \overline{gu}$ for some $g \in G$. (Recall that $L = G \cup Gu$.) In the first case, $(\bar{x} \mp \bar{g}) + \overline{yu} = \bar{0}$ implies that both $x \mp g$ and y are in $(1-e)\mathbf{Z}G$. In the second case both x and $y \mp g$ are in $(1-e)\mathbf{Z}G$. We have therefore established the following useful result:

PROPOSITION 4. *Suppose r is a unit in an alternative loop ring $\mathbf{Z}L$ such that $\bar{r}$ is a trivial unit in the group ring $\mathbf{Z}G$ of a group determining L. Then either*

$$x = \pm g + (1-e)x_1, \qquad y = (1-e)y_1 \tag{1}$$

for certain elements x_1 and y_1 in the group ring $\mathbf{Z}G$, or

$$x = (1-e)x_1, \qquad y = \pm g + (1-e)y_1 \tag{2}$$

for some $x_1, y_1 \in \mathbf{Z}G$.

COROLLARY 5. *Suppose r is a central unit in an alternative loop ring $\mathbf{Z}L$ such that $\bar{r}$ is trivial. Then r is in the group ring $\mathbf{Z}G$.*

PROOF. Since r is central, $ey = y$ (Theorem 2) and since $\bar{r}$ is trivial, either (1) or (2) hold. In the event of (2), $ey = y \Rightarrow \pm eg - (1-e)y_1 = \pm g + (1-e)y_1 \Rightarrow 2(1-e)y_1 = \pm eg \mp g$; the coefficients on the left are even and on the right odd. This contradiction says that (1) must be the case. This time $ey = -y = y \Rightarrow y = 0$ and so $r = x$ is in the group ring $\mathbf{Z}G$. ∎

If r is a central unit of finite order in an alternative loop ring, then $\bar{r}$ is a unit of finite order in an abelian group ring and so is trivial. The corollary says r is in the group ring. Therefore r is trivial because central units of finite order in a group ring are trivial. We have now established this result more generally for alternative loop rings.

THEOREM 6. *Central units of finite order in an alternative loop ring are trivial.*

The next theorem extends that of Higman from associative group rings to alternative loop rings.

THEOREM 7. *Suppose L is a periodic loop. Then $\mathbf{Z}L$ is an alternative ring in which all units are trivial if and only if L is an abelian group of exponent* 2, 3, 4 *or* 6 *or a Hamiltonian Moufang 2-loop.*

PROOF. Suppose that either L is an abelian group of one of the cited exponents or a Hamiltonian Moufang 2-loop. Higman's theorem then says that

all the units are trivial if the loop ring is associative. To deal with the non-associative case, we note that Norton [7] has proved that L is the direct product of the Cayley loop with an abelian group of exponent 2; the loop ring of such a loop is known to be alternative [4]. The Cayley loop occurs as the (Moufang) loop of units in the Cayley numbers just as the quaternion group is the group of units in the real quaternions.[†] With L the direct product of the Cayley loop and an elementary abelian 2-group, L/L' is clearly an elementary abelian 2-group and Higman's result shows that the units of the integral group ring of such a group are trivial. Thus, by Proposition 4, if $r = x + yu$ is any unit in $\mathbf{Z}L$, $yx \in (1-e)\mathbf{Z}G$ and so

$$rr^* = (xx^* + g_0 eyy^*) + (1+e)yx \cdot u = xx^* + yy^*$$

(because $g_0 = e$ and $e^2 = 1$). Moreover, rr^* is a unit in $\mathbf{Z}Q$ because r and r^* commute. But $\mathbf{Z}Q$ has only trivial units and so $xx^* + yy^* = \pm g$ for some $g \in Q$. In particular, the element $xx^* + yy^*$ has finite order. Now if $x = \sum_{g \in Q} \alpha_g g$ and $y = \sum_{g \in Q} \beta_g g$, then the coefficient of 1 in $xx^* + yy^*$ is a positive integer; namely, $\sum \alpha_g^2 + \sum \beta_g^2$ ($*$ is induced by $g \to g^{-1}$). It now follows that $xx^* + yy^*$ is just a multiple of 1 [9, Cor. 1.3, p. 45] and since it's invertible, it has to be $+1$. This quickly implies that a unique α_g or β_g is ± 1 while all other α's and β's are 0; i.e. r is trivial. For the converse, suppose that $\mathbf{Z}L$ is an alternative loop ring in which all units are trivial. If L is abelian, then it must be associative and Higman's result says L has exponent 2, 3, 4 or 6. So we assume that L is not abelian and prove that all subloops are normal. Precisely as in Sehgal [9, p. 57] we can prove that $\mathbf{Z}L$ has no nilpotent elements and then, as in [9, p. 51], that for any g and h in L, $g^{-1}hg$ is a power of h. Hence,

$$Hg = gH \tag{3}$$

for any subloop H of L and $g \in L$. Unlike the associative situation, this condition does not by itself imply the normality of H. It must also be established that

$$Hg \cdot k = H \cdot gk \quad \text{and} \quad k \cdot gH = kg \cdot H \tag{4}$$

for all $g, k \in L$. These conditions, however, are assured by Theorem 1 (iii) since $\mathbf{Z}L$ is alternative. They are trivially satisfied if H is central (since $Z(L) = N(L)$). On the other hand, if H is not central then for some $h \in H$ and $g \in G$, $g^{-1}hg = eh$, but $g^{-1}hg$ is also a power of h, as we have observed, and so in this

[†] Its elements are those of $Q \cup Qu$, Q the group of quaternions. Multiplication is given by the rules $g \cdot hu = hg \cdot u$, $gu \cdot h = gh^* \cdot u$, $gu \cdot hu = g_0 h^* g$ for $g, h \in Q$ where g_0 is the generator of the centre of Q and $*$ is $g \to g^{-1}$.

situation, $e \in H$. Therefore, any associator (h,g,k) is in H and again the conditions (4) hold. We see then that L is Hamiltonian, and since it is also Moufang, Norton's result guarantees that L is the direct product $C \times A \times B$ where C is the Cayley loop, A is abelian of exponent 2 and B abelian with all elements of finite odd order. If the factor B is actually present, then the loop assuredly contains an abelian group of exponent outside the set $\{2,3,4,6\}$ and the group ring of such a group, which is contained in the loop ring, contains non-trivial units. It follows that the loop is just $C \times A$ and the theorem is complete. ■

We next settle the question, for finite loops, of when just the torsion units are trivial. The theorem for alternative rings is the obvious extension of that of Berman for group rings.

THEOREM 8. *Let L be a finite loop. Then $\mathbf{Z}L$ is an alternative loop ring in which all torsion units are trivial if and only if L is an abelian group or a Hamiltonian Moufang 2-loop.*

PROOF. Berman's Theorem and Theorem 7 give the result in one direction. Conversely, suppose that $\mathbf{Z}L$ is an alternative loop ring in which all the torsion units are trivial. If r is any unit in $\mathbf{Z}L$ and a is any element in L, then $r^{-1}ar$ is a torsion unit, hence of the form $\pm g$ for some $g \in L$. Since the augmentation of $r^{-1}ar = 1$, this element is actually in L. This implies that $r^{-i}ar^i \in L$ for all integers $i \geqq 0$. Since L is finite, we see first that some power of r must commute with a and then that r^n must be in the centre of $\mathbf{Z}L$ for some positive integer n. Now since all the torsion units in $\mathbf{Z}L$ are trivial, the same holds true for the group ring $\mathbf{Z}G$, where G is any group determining L in the sense of Theorem 2. It is known that such G has to be the direct product of the quaternions and an abelian group of exponent 2. Thus $Z(G) = Z(L)$ has exponent 2. Since $g^2 \in Z(L)$ for any $g \in L$, L has exponent 4 and L/L' exponent 2 or 4. In particular, all units in $\mathbf{Z}(L/L')$ are trivial. Thus $\overline{r^n}$ is trivial and so by Corollary 5 it belongs to $\mathbf{Z}G$. Since all units in $\mathbf{Z}G$ have finite order, r^n, and hence r itself, have finite order. The hypothesis then says that r is trivial. ■

2. Central units

The authors are unaware of any published result which gives necessary and sufficient conditions for all the central units in a group ring to be trivial. We are able, however, to find rather nice conditions in the non-associative case because of the rather special nature of the Moufang loops which determine alternative

loop rings. In order to do this, we require the fact that if all the central units in the group ring $\mathbf{Z}G$ of a finite group G are trivial, then all the units in the abelian group ring $\mathbf{Z}(G/G')$ are trivial. Here, briefly, is a way to see this. In the rational group algebra, $\mathbf{Q}G$, the group algebra of G/G' is a direct summand. Any unit α in $\mathbf{Z}(G/G')$ can be thought of as a central unit in $\mathbf{Q}G$. If it has finite order, then of course it is trivial. Now $\mathbf{Q}(G/G')$ is the direct sum $\oplus\Sigma\mathbf{Q}(\xi_i)$ of cyclotomic fields and since α is an algebraic integer, we know that $\alpha \in \oplus\Sigma\mathbf{Z}[\xi_i]$. Call this ring R. A result of Sehgal [9, p. 49] says that the unit group of $\mathbf{Z}G$ is of finite index in the unit group of R. Thus some power of α, say α^n, is in $\mathbf{Z}G$. By assumption all central units in this ring are trivial, so, because G is finite, $(\alpha^n)^k = 1$ for some k; i.e. α has finite order.

THEOREM 9. *Suppose L is a periodic Moufang loop and $\mathbf{Z}L$ is an alternative loop ring which is not associative. Let A denote the centre of L. Then the central units in $\mathbf{Z}L$ are trivial $\Leftrightarrow$ all units in $\mathbf{Z}A$ and $\mathbf{Z}(L/L')$ are trivial; i.e. $\Leftrightarrow$ both A and L/L' are abelian groups of exponent 2, 3, 4 or 6.*

PROOF. The last equivalence obviously is a consequence of Theorem 7. To establish the first equivalence, suppose initially that both $\mathbf{Z}A$ and $\mathbf{Z}(L/L')$ have only trivial units. If r is any central unit in $\mathbf{Z}L$, then it follows by Corollary 5 that r is in the group ring $\mathbf{Z}G$. Write $r = r_1 + r_2$ where $r_1 \in \mathbf{Z}A$ and $r_2 = \sum_{g \notin A} \alpha_g g$. Since r is central, $r = r^*$, hence $r_2 = er_2$. On the other hand, since $\bar{r}$ is a trivial unit in $\mathbf{Z}(G/G')$, for some $g \in G$, we have $r \pm g \in (1-e)\mathbf{Z}G$ and hence $e(r \pm g) = -(r \pm g)$. Remembering that $er_2 = r_2$, we obtain $(1+e)r_1 + 2r_2 \pm (1+e)g = 0$; whence $r_2 = 0$. Therefore $r \in \mathbf{Z}A$ and, by assumption, all units in this ring are trivial. Now we attack the converse. Certainly if all the central units in $\mathbf{Z}L$ are trivial then all units in $\mathbf{Z}A$ are trivial. Thus A has exponent 2, 3, 4 or 6 and since $g^2 \in A$ for any $g \in L$, L/L' has exponent 4, 6, 8 or 12. If it has exponent 4 or 6, then all units are trivial by Theorem 7 and the theorem is proved. We rule out the possibilities of exponent 8 or 12. Suppose for the moment that L/L' has exponent 8. Thus for some $g \in L$, g^8, but no lower power, is in L'. Remember that $L' = \{1, e\}$. If $g^8 = e$, g^2 would be a central element of order 8 in a group of exponent 2, 3, 4 or 6. This can't be, so g has order 8. It follows then that g can't be central; hence by Theorem 1, it's an element in some group G contained within L with $Z(G) = A$. Easily $G' = L'$, so the element $\bar{g} \in G/G'$ has order 8. But all the central units in $\mathbf{Z}G$ are trivial, so by our discussion above, all units $\mathbf{Z}(G/G')$ are trivial and so G/G' has exponent 2, 3, 4 or 6. The contradiction implies that L/L' cannot have exponent 8. Similarly it cannot have exponent 12. ∎

ACKNOWLEDGEMENTS

Most of the work contained in this article was accomplished while the authors were guests of Professor S. K. Sehgal at the University of Alberta. We thank Professor Sehgal for his gracious hospitality and Professors Sehgal and G. H. Cliff for their interest and helpful discussions.

REFERENCES

1. S. D. Berman, *On the equation $x^m = 1$ in an integral group ring*, Ukrain. Mat. Z. **7** (1955), 253–261.

2. Orin Chein and Edgar G. Goodaire, *Loops whose loop rings are alternative*, Comm. Algebra, to appear.

3. J. A. Cohn and D. Livingstone, *On the structure of group algebras*, Can J. Math. **17** (1965), 583–593.

4. Edgar G. Goodaire, *Alternative loop rings*, Publ. Math. Deb. **30** (1983), 31–38.

5. Edgar G. Goodaire and M. M. Parmenter, *Semi-simplicity of alternative loop rings*, Acta Math. Hungar., to appear.

6. Graham Higman, *The units of group-rings*, Proc. London Math. Soc (2), **46** (1940), 231–248.

7. D. A. Norton, *Hamiltonian loops*, Proc. Amer. Math. Soc. **3** (1952), 56–65.

8. Richard D. Schafer, *An Introduction to Nonassociative Algebras*, Academic Press, New York, 1966.

9. Sudarshan K. Sehgal, *Topics in Group Rings*, Marcel Dekker, New York and Basel, 1978.