JOURNAL OF ALGEBRA **181,** 593–600 (1996)
ARTICLE NO. 0136

Matrix-Isomorphic Maximal Z-Orders

A. W. Chatters

University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom

Communicated by A. W. Goldie

We construct many pairwise non-isomorphic maximal Z-orders A and B which have isomorphic n by n matrix rings for every positive integer $n \neq 1$. In most cases A also has the property that every one-sided ideal of $M_2(A)$ is principal but not every one-sided ideal of A is principal.

1. INTRODUCTION

Maximal Z-orders are some of the most natural and well behaved of all non-commutative rings. Yet even for these rings the isomorphism type of $M_2(A)$ does not determine that of A. Examples are already known of non-isomorphic orders A and B in a finite-dimensional central simple algebra such that $M_2(A) \cong M_2(B)$ [2, 3, 10]. But the examples in [2] and [3], although numerous, are not maximal orders; those in [10] are maximal orders but they are relatively complicated and the underlying commutative ring is the ring of integers of a four-dimensional algebraic number field.

As in [8] we say that rings A and B are matrix-isomorphic if $M_n(A) \cong M_n(B)$ for every positive integer $n \neq 1$. We shall show that, given a positive integer r, there are r matrix-isomorphic pairwise non-isomorphic maximal Z-orders (Theorem 4.4). The most difficult part of such constructions is usually that of showing that the rings are not isomorphic, but in this case there is a sufficient condition which is easy to check numerically (Theorem 4.3). The same construction gives an infinite family of maximal Z-orders A such that every one-sided ideal of $M_2(A)$ is principal but not every one-sided ideal of A is principal; a slightly different construction gives infinitely many such A with a stably free non-free two-sided ideal (Section 6).

0021-8693/96 $18.00

2. CONSTRUCTION OF THE MAXIMAL Z-ORDER S

The ring S which we shall construct is a maximal Z-order in a division algebra of generalised rational quaternions. We shall show that S has the additional property that every two-sided ideal is principal, and this will be useful when we consider in Section 3 the question of determining when the endomorphism rings of two maximal right ideals of S are isomorphic. We shall use Z and Q to denote respectively the ring of rational integers and the field of rational numbers.

Throughout the rest of this paper, w will denote the prime number with $w \equiv 3 \bmod(4)$. Let D be the rational division algebra of generalised quaternions with basis $1, i, j, ij$ where $i^2 = -1$, $j^2 = -w$, and $ij = -ji$. Set $k = ij$. A typical element x of D has the form $x = a + bi + cj + dk$ for unique elements a, b, c, d of Q. The conjugate x^*, trace $\mathrm{Tr}(x)$, and norm $N(x)$ of x are defined by $x^* = a - bi - cj - dk$, $\mathrm{Tr}(x) = x + x^* = 2a$, and $N(x) = xx^* = x^*x = a^2 + b^2 + w(c^2 + d^2)$.

Set $u = (1 + j)/2$. Then $u^2 = \mathrm{Tr}(u)u - N(u) = u - (1 + w)/4$ where $(1 + w)/4 \in Z$. Set $S = Z[i, u]$, i.e., S is the subring of D generated by i and u. It is easy to check that the additive group of S is free Abelian of rank 4 with Z-basis $1, i, u, iu$. It is routine to check that the discriminant $D(S)$ of S has the value $D(S) = -w^2$; one way of doing this is to use the formula $D(S) = \det(\mathrm{Tr}(x_i x_j))$ where x_1, x_2, x_3, x_4 form a Z-basis for S. It is well known that S is a maximal Z order in D (see for instance Section 105 of [5]), but this is also a consequence of the following more precise result.

THEOREM 2.1. *Let S be as above and let I be a non-zero ideal of S. Then either $I = zS$ or $I = zjS$ for some non-zero $z \in Z$.*

Proof. Let p be a prime number with $p \neq w$. Then p does not divide $D(S)$, so that S/pS is a semi-simple Z/pZ-algebra. Also $j \notin pS$, so that $iu - ui = ij \notin pS$. Thus S/pS is a semi-simple four-dimensional Z/pZ-algebra which is not commutative. Therefore $S/pS \cong M_2(Z/pZ)$. In particular, pS is the unique maximal ideal of S containing p.

Now let P be any maximal ideal of S which contains w; we shall show that $P = jS$. We have $j^{-1}ij = -i$ and $j^{-1}kj = -k$, from which it follows readily that $j^{-1}Sj = S$. Thus $jS = Sj$ and $(jS)^2 = wS$. Therefore $jS \subseteq P$. We have $2u - 1 = j$. Hence $u - (1 + w)/2 \in jS$. Therefore $S/jS = (Z/wZ)[x]$, where x is the image of i in S/jS. But $x^2 = -1$ and -1 is not a square in Z/wZ. Therefore $(Z/wZ)[x]$ is a field. Hence jS is a maximal ideal of S and $P = jS$.

This shows that the maximal ideals of S are jS and pS for all primes $p \neq w$, and for such p we have $S/pS \cong M_2(Z/pZ)$. The result now follows by a standard argument.

3. ENDOMORPHISM RINGS OF MAXIMAL RIGHT IDEALS OF S

Throughout this section w and S will be as in Section 2, and p and q will denote prime numbers with $p \neq w \neq q$. Note that we do allow $p = q$, and also that we allow $p = 2$ or $q = 2$. Let K and L be maximal right ideals of S containing p and q respectively. We shall show that we always have $M_2(\mathrm{End}_S(K)) \cong M_2(S) \cong M_2(\mathrm{End}_S(L))$, and that it is almost true that $\mathrm{End}_S(K) \cong \mathrm{End}_S(L)$ as rings if and only if $K \cong L$ as right S-modules (see 3.6 for the precise result).

THEOREM 3.1. *Let p be a prime number with $p \neq w$ and let K be a maximal right ideal of S which contains p. Set $A = \mathrm{End}_S(K)$. Then $M_2(A) \cong M_2(S)$.*

Proof. Recall from the proof of 2.1 that $S/pS \cong M_2(Z/pZ)$. Thus both S/K and K/pS are simple right S/pS-modules so that $S/K \cong K/pS$. But S is a maximal Z-order and so is hereditary (see for instance [1, Theorem 2.9] or [9, Theorem 21.4]). Hence K is projective and Schanuel's lemma gives $K \oplus K \cong S \oplus pS \cong S \oplus S$. Therefore $M_2(A) = M_2(\mathrm{End}(K)) \cong M_2(\mathrm{End}(S)) \cong M_2(S)$ as rings.

Remark 3.2. By using more sophisticated methods it can be shown that, with the notation of 3.1, we have $M_n(A) \cong M_n(S)$ for every positive integer $n \neq 1$; thus A and S are matrix-isomorphic as defined in [8]. One way of doing this is to apply Eichler's theorem [9, Theorem 34.9] to the ring $M_2(S)$ to show that every maximal right ideal of $M_2(S)$ is principal, and hence that $K \oplus S \cong S \oplus S$. Of course 3.1 is trivial if $A \cong S$, but we shall show that this is not always the case.

COROLLARY 3.3. *A is a maximal Z-order.*

Proof. Because K is a non-zero right ideal of the integral domain S, we can identify $\mathrm{Hom}_S(K, S)$ with $K^* = \{d \in D : dK \subseteq S\}$. Also because K is projective, we have $KK^* = \{d \in D : dK \subseteq K\}$. We shall identify A with KK^*. Thus A is a Z-order in D, and its maximality follows readily from the fact that $M_2(A) \cong M_2(S)$.

From now on we shall identify $\mathrm{Hom}_S(K, S)$ with K^* and A with KK^* as in the proof of 3.3.

PROPOSITION 3.4. *With the notation of* 3.1 *we have $A \cong S$ if and only if the maximal right ideal K is principal.*

Proof. If $K = xS$ for some x then $x \neq 0$ and $x^{-1}Ax = S$.

Conversely, suppose that $f\colon S \to A$ is an isomorphism of rings. Because D is the quotient ring of both S and A, we can extend f to an automorphism g of D. But g acts as the identity function on the centre Q of D. It follows from the Skolem–Noether theorem that there is a non-zero element x of D such that $g(d) = x^{-1}dx$ for all $d \in D$. Because D can be formed from S by inverting the non-zero elements of Z, we can suppose without loss of generality that $x \in S$. We have $A = g(S) = x^{-1}Sx$. Hence $K = AK = x^{-1}SxK$, i.e., $xK = SxK$, i.e., xK is a two-sided ideal of S. Therefore by 3.1 we have $xK = aS$ for some a and hence K is principal.

Notation 3.5. p and q are prime numbers with $p \neq w \neq q$; K and L are maximal right ideals of S containing p and q respectively; $K^* = \{d \in D : dK \subseteq S\}$; $L^* = \{d \in D : dL \subseteq S\}$; $A = KK^*$; $B = LL^*$. Recall that, as in the proof of 3.3, we can identify A with $\mathrm{End}_S(K)$ and B with $\mathrm{End}_S(L)$.

THEOREM 3.6. *With the notation of* 3.5 *we have* $A \cong B$ *as rings if and only if* K *is isomorphic as a right* S*-module to either* L *or* $j^{-1}Lj$.

Proof. Note that conjugation by j induces an automorphism of S. Thus the "if" part of the statement is easy to prove.

Suppose that $f : A \to B$ is an isomorphism of rings. As in the proof of 3.4, there is a non-zero element x of S such that $f(a) = x^{-1}ax$ for all $a \in A$. Hence $B = x^{-1}Ax$, so that $L = BL = x^{-1}AxL$. Thus $AxL = xL$. Suppose that xL is not contained in K. Then $K + xL = S$. But $AK = K$ and $AxL = xL$. Therefore $AS = S$, i.e., $A \subseteq S$. But A is a maximal Z-order, by 3.3. Therefore $A = S$, so that $K = AK = SK$. This is a contradiction because K is not a two-sided ideal of S.

This shows that $xL \subseteq K$. Hence $K^*xL \subseteq S$ so that K^*xL is a non-zero two-sided ideal of S. We apply Theorem 2.1 and have two cases to consider. Suppose first that $K^*xL = zS$ for some non-zero $z \in Z$. Then $KK^*xL = KzS = zK$, i.e., $zK = AxL = xL$. Therefore $K \cong L$ as right S-modules. Second, suppose that $K^*xL = zjS$ for some non-zero $z \in Z$. Then $xL = AxL = KK^*xL = KzjS = zKSj = zKj = zjj^{-1}Kj$, so that $L \cong j^{-1}Kj$ and $K \cong j^{-1}Lj$.

4. A SIMPLE NUMERICAL TEST

In Section 3 we showed that, with the notation of 3.5, we have $M_n(\mathrm{End}(K)) \cong M_n(\mathrm{End}(L))$ for all positive integers $n \neq 1$; and a necessary and sufficient condition for $\mathrm{End}(K) \cong \mathrm{End}(L)$ was given in 3.6. However, the condition in 3.6 is not easy to check in practice. The main aim of this section is to use 3.6 to derive a simple numerical condition which guarantees in particular cases that $\mathrm{End}(K)$ is not isomorphic to $\mathrm{End}(L)$ (but which is far from being a necessary condition).

The next result is well known, but for the reader's convenience we shall sketch a proof in the particular case which we need.

LEMMA 4.1. *Let x be a non-zero element of S. Then S/xS has $(N(x))^2$ elements.*

Proof. Because the additive group of S is free Abelian of rank 4, we can fix Z-bases $u_1, \dots, u_4$ for S and $v_1, \dots, v_4$ for xS such that for all t we have $v_t = r_t u_t$ for some positive integer r_t. Set $r = r_1 r_2 r_3 r_4$. Then S/xS has r elements. Let C be the 4 by 4 diagonal matrix with diagonal entries r_1, r_2, r_3, r_4. Then $\det(C) = r$. We can think of C as being the matrix corresponding to the mapping $c : S \to S$ given by $c(u_t) = v_t$ for all t. Let B be the matrix corresponding to the mapping $b : S \to S$ defined by $b(s) = xs$ for all $s \in S$. Then $b^{-1}c$ is an automorphism of the additive group S, so that the determinant of the corresponding matrix is a unit of Z. Therefore $\pm\det(B) = \det(C) = r$. But $\det(B)$ is the determinant of the image of x under the regular representation of D in $M_4(Q)$, and $N(x)$ is the determinant of the image of x under the reduced representation of D in $M_2(Q(i))$. Therefore $\det(B) = (N(x))^2$, so that $(N(x))^2 = \det(C) = r$.

LEMMA 4.2. *With the notation of* 3.5 *suppose that $f : K \to L$ is an isomorphism of right S-modules, and let x be a non-zero element of K. Then $N(x)/p = N(f(x))/Q$.*

Proof. We shall use $|X|$ to denote the number of elements in a set X. Because S/K is a simple S/pS-module with $S/pS \cong M_2(Z/pZ)$, we have $|S/K| = p^2$. Hence by 4.1 we have $(N(x)/p)^2 = |S/xS|/p^2 = |S/K| \cdot |K/xS|/p^2 = |K/xS| = |f(K)/f(xS)| = |L/f(x)S| = |S/L|$. $|L/f(x)S|/q^2 = |S/f(x)S|/q^2 = (N(f(x))/q)^2$.

THEOREM 4.3. *With the notation of* 3.5 *suppose that S has no element of norm pq. Then A is not isomorphic to B.*

Proof. Suppose that $A \cong B$. Then by 3.6 we know that K is isomorphic to either L or $j^{-1}Lj$. Without loss of generality we may suppose that there is a right S-module isomorphism $f : K \to L$. Taking $x = p$ in 4.2 gives $p = N(p)/p = N(f(p))/q$, i.e., $N(f(p)) = pq$; this is the desired contradiction.

THEOREM 4.4. *Let n be any positive integer. Then there is a division algebra D of generalised rational quaternions and n pairwise non-isomorphic maximal Z-orders $A_1, \dots, A_n$ in D such that $M_r(A_s) \cong M_r(A_t)$ for all s and t and for all positive integers $r \neq 1$.*

Proof. Let $p_1, \dots, p_n$ be, in increasing order, the first n primes which are congruent to $3 \bmod(4)$. We fix a prime number w such that $w \equiv 3 \bmod(4)$ and $w \geq 4p_n^2$. With this choice of w, let S be as in Section 2. By

4.3 it is enough to show that if $s \neq t$ then S has no element of norm $p_s p_t$. Suppose to the contrary that there is an element x of S such that $N(x) = p_s p_t$ with $s \neq t$. We have $x = (a + bi + cj + dk)/2$ for some $a, b, c, d \in Z$. Then $N(x) = (a^2 + b^2 + w(c^2 + d^2))/4$. Thus $a^2 + b^2 + w(c^2 + d^2) = 4N(x) = 4p_s p_t < 4p_n^2$. Hence $a^2 + b^2 + w(c^2 + d^2) < w$, so that $c = d = 0$. This gives $4p_s p_t = a^2 + b^2$, which is a contradiction because $4p_s p_t$ is not the sum of two squares.

5. TWO EXAMPLES

We know that every two-sided ideal of S is principal. We shall now give two examples in each of which we construct a second maximal Z-order A with $M_2(A) \cong M_2(S)$ and A not isomorphic to S; in the first example every ideal of A is principal, but in the second example A has a non-principal ideal.

EXAMPLE 5.1. Take $w = 23$ and let S be as in Section 2. Set $x = (1 + j)/2$ and $K = 3S + xS$. We have $N(x) = 6$ and $x \notin 3S$. Because $S/3S \cong M_2(Z/3Z)$ it follows that K is a maximal right ideal of S. As in the proof of 3.3 set $A = KK^*$. Then $M_2(A) \cong M_2(S)$ by 3.1. No element of S has norm 3, so that K is not principal. Hence A is not isomorphic to S (3.4).

It remains to show that every ideal of A is principal, and it is enough to do this for the maximal ideals of A. The maximal ideals of S are pS for primes $p \neq w$, together with jS where $(jS)^2 = wS$. Because $M_2(A) \cong M_2(S)$ it follows that the maximal ideals of A are pA for primes $p \neq w$, together with a unique maximal ideal M such that $M^2 = wA$. But $jK = Kj \subseteq K$ so that $j \in A$. Also $j^{-1}AjK = j^{-1}AKj = j^{-1}Kj = j^{-1}jK = K$, so that $j^{-1}Aj \subseteq A$. It follows that $jA = Aj$. Thus jA is a two-sided ideal of A with $(jA)^2 = wA$. Therefore $M = jA$.

EXAMPLE 5.2. Take $w = 43$ and let S be as in Section 2. Set $x = (1 + 2i + j)/2$, $K = 3S + xS$, and $A = K/K^*$. As in 5.1 we find that K is a maximal right ideal of S and that $M_2(A) \cong M_2(S)$. Also as in 5.1 there is a maximal ideal M of A such that $M^2 = wA$. But this time we shall show that M is not principal.

With the aim of obtaining a contradiction we suppose that $M = vA$ for some $v \in A$. The isomorphism between $M_2(A)$ and $M_2(S)$ induces an isomorphism between $M_2(A/M)$ and $M_2(S/jS)$. Hence A/M has the same number of elements as S/jS, namely w^2. Because $M = vA$ it follows that $N(v) = w$. But $vK \subseteq K$ so that $3v \in S$. Hence $3v = (a + bi + cj + dk)/2$ for some $a, b, c, d \in Z$. Therefore $a^2 + b^2 + w(c^2 + d^2) = 4N(3v) = 36w$ where $w = 43$. Thus 43 divides $a^2 + b^2$. Because -1 is not a square in $Z/43Z$ it follows that 43 divides both a and b. But $a^2 + b^2 \leq$

36.43. Hence $a = b = 0$. We have $c^2 + d^2 = 36$, so that either $c^2 = 36$ and $d = 0$ or $c = 0$ and $d^2 = 36$. Hence without loss of generality we have either $v = j$ or $v = k$. Note that K contains vx, xj, and xk. Also, $3 \in K$, so that the norm of every element of K is divisible by 3. If $v = j$ then K contains $xj - jx = 2k$, which is a contradiction because $N(2k) = 172$. If $v = k$ then K contains $kx + xk = k$, which is again a contradiction.

6. CONNECTION WITH GOLDIE'S QUESTION

In [7, Theorem B], Goldie showed that if R is a prime ring in which every one-sided ideal is principal then $R \cong M_n(S)$ for some positive integer n and some integral domain S, and the question arose naturally as to whether every one-sided ideal of S has to be principal. It has been known for a long time that the answer is "No": the best-known examples are due to Swan [10] where the ring S is a maximal order over the ring of integers of a four-dimensional extension of Q, and to Webber [11] where S is the first Weyl algebra.

The construction in Section 2 gives a further infinite family of examples all of which are maximal Z-orders. Let w and S be as in Section 2. Because S is a maximal Z-order it follows from Eichler's theorem [9, Theorem 34.9] that every one-sided ideal of $M_2(S)$ is principal. But every one-sided ideal of S is principal if and only if $w = 3$ or $w = 7$; this follows immediately from Hey's formula for the class number of S (see [6]). Without using Hey's formula it is easy to show directly that, if $w \geq 11$, then the only elements of S which have norm 2 are $1 + i$, $1 - i$, and their negatives; hence $(1 + i)S$ is the only principal maximal right ideal of S which contains 2, and the other two maximal right ideals of S which contain 2 are therefore not principal.

Perhaps an even more interesting infinite family of examples among maximal Z-orders is the following. Let p and q be distinct odd primes which are congruent to 3 mod(4); set $i^2 = -1$ and $j^2 = -pq$; and let T be the ring of all generalised quaternions of the form $(a + bi + cj + dk)/2$ where a, b, c, d are integers which are either all even or all odd. Then T is a maximal Z-order (see for instance [5, Sect. 105]). As in the last paragraph, every one-sided ideal of $M_2(T)$ is principal. Set $P = pT + jT$. It is easy to check that $jT = Tj$, so that P is a two-sided ideal of T. Also P^2 contains both p^2 and $j^2 = -pq$, from which it follows that $P^2 = pT$. Hence if $P = xT$ for some x then $N(x) = p$; but T has no elements of norm p. Therefore P is a non-principal two-sided ideal of T. Because

$$\begin{pmatrix} P & P \\ T & T \end{pmatrix}$$

is a principal right ideal of $M_2(T)$ it is isomorphic to $M_2(T)$. It follows that $P \oplus T \cong T \oplus T$ as right T-modules, so that P is a stably free non-free two-sided ideal of T. The case in which $p = 3$ and $q = 7$ was studied by more elementary methods in Section 3 of [4].

ACKNOWLEDGMENT

Part of this work was done while the author was a visitor at Rutgers University, and he expresses his thanks for the hospitality and facilities provided by the Rutgers Mathematics Department.

REFERENCES

[1] M. Auslander and O. Goldman, Maximal orders, *Trans. Amer. Math. Soc.* **97** (1960), 1–24.
[2] A. W. Chatters, Matrices, idealisers, and integer quaternions, *J. Algebra* **150** (1992), 45–56.
[3] A. W. Chatters, Non-isomorphic rings with isomorphic matrix rings, *Proc. Edinburgh Math. Soc.* **36** (1993), 339–348.
[4] A. W. Chatters and M. M. Parmenter, Stably free modules over rings of generalized integer quaternions, *Canad. Math. Bull.* **38** (1995), 408–411.
[5] L. E. Dickson, ''Algebras and Their Arithmetics,'' Stechert, New York, 1938.
[6] M. Eichler, Uber die Idealklassenzahl total definiter Quaternionenalgebren, *Math. Z.* **43** (1938), 102–109.
[7] A. W. Goldie, Non-commutative principal ideal rings, *Arch. Math.* **13** (1962), 214–221.
[8] T. Y. Lam, A lifting theorem, and rings with isomorphic matrix rings, *in* ''Five Decades as a Mathematician and Educator—On the 80th Birthday of Prof. Y. C. Wong,'' World Sci. Press, Singapore, 1994.
[9] I. Reiner, ''Maximal Orders,'' Academic Press, New York, 1975.
[10] R. G. Swan, Projective modules over group rings and maximal orders, *Ann. of Math.* **76** (1962), 55–61.
[11] D. B. Webber, Ideals and modules of simple Noetherian hereditary rings, *J. Algebra* **16** (1970), 239–242.