Canad. Math. Bull. Vol. **43** (4), 2000 pp. 413–417

Non-Isomorphic Maximal Orders with Isomorphic Matrix Rings

A. W. Chatters

Abstract. We construct a countably infinite family of pairwise non-isomorphic maximal $\mathbb{Q}[X]$-orders such that the full 2 by 2 matrix rings over these orders are all isomorphic.

1 Introduction

Many examples are now known of non-isomorphic prime Noetherian rings S and T such that the corresponding full 2 by 2 matrix rings $M_2(S)$ and $M_2(T)$ are isomorphic (for instance, an uncountably infinite family of such examples was given in [1]). This phenomenon illustrates the difficulty of distinguishing between closely related but non-isomorphic rings even when they satisfy additional natural conditions. Until recently only a few examples were known of such rings S and T which are also maximal orders (see for instance [3] and [4]). In [2] it was shown how to construct arbitrarily large finite families of such examples among maximal $\mathbb{Z}$-orders, but the method used there cannot give infinite families. In this note we switch from the ring $\mathbb{Z}$ of integers to the rational polynomial ring $\mathbb{Q}[X]$, and we construct a countably infinite family of pairwise non-isomorphic maximal $\mathbb{Q}[X]$-orders in the same division algebra such that the corresponding 2 by 2 matrix rings are all isomorphic. Whatever method is used to construct such examples, the hard part is usually the problem of finding a way to distinguish the non-isomorphic rings. The way used here is probably more simple-minded and elementary than in earlier constructions.

2 The Examples

Let $\mathbb{Q}$ be the field of rational numbers and set $A = \mathbb{Q}[X]$ where X is a central indeterminate. Throughout this section R will denote the ring of quaternions over A on i and j with $i^2 = -1$ and $j^2 = w$ where $w = X^{25} + 4$. Set $k = ij$. Thus a typical element of R has the form $a + bi + cj + dk$ for unique elements a, b, c, d of A, and the norm of this element is $a^2 + b^2 - (c^2 + d^2)w$. It is easy to show, using degree considerations in $A = \mathbb{Q}[X]$, that the above norm-value is 0 if and only if $a = b = c = d = 0$. From this it is routine to show that R is an integral domain which has a quotient division ring D.

Lemma 2.1 *w is an irreducible element of A.*

Proof Recall that $w = X^{25} + 4$ and that $A = \mathbb{Q}[X]$. We can use the change of variable $X = Y + 1$, and then apply the Eisenstein Criterion. ■

Received by the editors October 1, 1998; revised July 29, 1999.
AMS subject classification: Primary: 16S50; secondary: 16H05, 16N60.

Lemma 2.2 *Let f be an irreducible element of A with $fA \neq wA$. Then fR is a maximal ideal of R.*

Proof Set $F = A/fA$ and let u and v denote the images of i and j respectively in R/fR. Then R/fR is quaternions over the field F on u and v with $u^2 = -1$ and $v^2 \neq 0$. It is routine to show that R/fR is a semi-simple F-algebra. Also $ij - ji = 2k \notin fR$, so that R/fR is not commutative. Therefore R/fR is a non-commutative semi-simple 4-dimensional F-algebra, so that either R/fR is a division ring or R/fR is isomorphic to the full 2 by 2 matrix algebra $M_2(F)$. ■

Lemma 2.3 *jR is the unique maximal ideal of R which contains w.*

Proof Clearly jR is a two-sided ideal of R and $(jR)^2 = wR$. Set $E = A/wA$. Because w is irreducible over $\mathbb{Q}$ of odd degree, the field E has odd degree as an extension of $\mathbb{Q}$. Hence E contains no square roots of -1. But $R/jR = E[u]$ where u is the image of i in R/jR. Because $u^2 = -1$ and E contains no square roots of -1, it follows that R/jR is a field. ■

Proposition 2.4 *Every maximal ideal of R is principal (by which we mean that it has the form xR for some element x of R with $xR = Rx$).*

Proof Let M be a maximal ideal of R. Then M contains a non-zero element a of A. Hence M contains an irreducible factor f of a in A. If $fA \neq wA$ then fR is a maximal ideal of R by 2.2, so that $M = fR$. On the other hand, if $fA = wA$ then $M = jR$ by 2.3. ■

Corollary 2.5 *R is a maximal A-order in D.*

Proof Clearly R is a Noetherian A-order in D. In order to show that R is a maximal order, it is enough to show that every non-zero ideal of R is principal (in the sense used in 2.4) and hence is invertible. We know by 2.4 that every maximal ideal of R is principal, and it follows from this by a standard maximal counter-example argument that every non-zero ideal of R is principal. ■

We shall next construct an infinite family of maximal right ideals of R such that the corresponding left orders are pairwise non-isomorphic. These right ideals correspond to prime numbers p, and it will simplify matters to fix the following notation for the rest of the section.

Notation 2.6 Let p be a prime number. Set $f = X^5 - p^2$, $K = fR + (p^5 + 2i + j)R$, and $S = O_\ell(K)$; here $O_\ell(K)$ denotes the set of elements of D which left-multiply K into K.

Lemma 2.7 *f is an irreducible element of A.*

Proof Recall that $f = X^5 - p^2$. If $p = 2$ then we can show that f is irreducible by using the change of variable $X = Y - 1$ and then applying the Eisenstein Criterion. Now suppose that p is odd. Clearly f has no linear factors over $\mathbb{Q}$. Over the integers mod(2) the irreducible factors of f are $X + 1$ and $X^4 + X^3 + X^2 + X + 1$, and from this it follows that f has no quadratic factors over $\mathbb{Q}$. ■

Lemma 2.8 *K is a maximal right ideal of R and is not a two-sided ideal of R.*

Proof By 2.7 and the proof of 2.2 we know that R/fR is either a division ring or a full 2 by 2 matrix ring over a field. Set $x = p^5 + 2i + j$ and $y = p^5 - 2i - j$. Then $K = fR + xR$; x and y do not belong to fR; but $xy = yx = p^{10} + 4 - w = p^{10} - X^{25}$ which is divisible by $p^2 - X^5$. It follows that $fR \neq K \neq R$. Therefore R/fR is a full 2 by 2 matrix ring over a field and K is a maximal right ideal of R containing fR. ■

Proposition 2.9 $M_2(S) \cong M_2(R)$.

Proof Let W denote the endomorphism ring of K as a right R-module. For $s \in S$ define $w_s \in W$ by $w_s(k) = sk$ for all $k \in K$. Because K contains the non-zero central element f of R, it is routine to show that the function which sends s to w_s is an isomorphism from S to W. Thus it is enough to show that $M_2(W) \cong M_2(R)$. We showed in the proof of 2.8 that R/fR is a full 2 by 2 matrix ring over a field and that K is a maximal right ideal of R which contains f. Hence $R/K \cong K/fR$ as right R-modules (in fact R/K and K/fR are both isomorphic to the unique simple right R/fR-module). We can now proceed as in the proof of Theorem 3.1 of [2] to show that $M_2(W) \cong M_2(R)$. ■

Corollary 2.10 *S is a maximal A-order in D.*

Proof Firstly we note that S is a subring of D which contains A. Also $SK \subseteq R$ and $f \in K$, so that $S \subseteq f^{-1}R$. Because R is finitely-generated as an A-module, so also are $f^{-1}R$ and S. Let B be the quotient field of A. Then $RB = D$ and $fB = B$. Also $K \subseteq S$. Hence $D = RB = fRB \subseteq KB \subseteq SB$, so that $SB = D$. Therefore S is an A-order in D. But $M_2(S) \cong M_2(R)$ by 2.9, and we showed in the proof of 2.5 that every non-zero ideal of R is invertible. Hence every non-zero ideal of S is invertible, so that S is a maximal order. Therefore S is a maximal A-order in D. ■

Theorem 2.11 *Let p, f, K, S be as in 2.6. Similarly let q be a prime number and set $g = X^5 - q^2$, $L = gR + (q^5 + 2i + j)R$, and $T = O_\ell(L)$. Then $S \cong T$ if and only if $p = q$.*

Proof Suppose that $e\colon S \to T$ is an isomorphism of rings. Then e can be extended to an automorphism of the quotient division ring D, and we shall also call this automorphism e. Because A is the centre of both S and T, we know that the restriction of e to A is an automorphism of A. Hence e preserves degree in X when applied to elements of $A = \mathbb{Q}[X]$.

We shall determine the values of $e(i)$ and $e(j)$; from these it will follow that e acts as the identity function on A, and that the restriction of e to R is an automorphism of R. Recall that $S = O_\ell(K)$ and $K \supseteq fR$. Hence $fi \in K$ and so $fi \in S$. Thus $e(fi) \in T = O_\ell(L)$ where $L \supseteq gR$. Therefore $e(fi)g \in R$. Set $h = e(f)$. Because f is an irreducible element of A of degree 5, so also is h. We have $\big(e(fi)g\big)^2 = \big(e(i)gh\big)^2 = -g^2h^2$. Thus $e(i)gh$ is an element of R whose square is in A. But $e(i)gh$ is not in A because i is not a central element of D. Therefore

$$e(i)gh = bi + cj + dk \quad \text{for some } b, c, d \in A. \tag{1}$$

Squaring both sides of (1) gives

$$-g^2h^2 = -b^2 + (c^2 + d^2)w. \tag{2}$$

https://doi.org/10.4153/CMB-2000-049-0 Published online by Cambridge University Press

Using "deg" to denote degree in X, we have $\deg(g) = \deg(h) = 5$ and $\deg(w) = 25$. Also because we are working over $\mathbb{Q}$ we have either $c^2 + d^2 = 0$ or $\deg(c^2 + d^2)$ is a non-negative even integer. Thus degree considerations enable us to deduce from (2) that $c^2 + d^2 = 0$, so that $c = d = 0$, and $gh = \pm b$. Therefore from (1) we have $e(i) = \pm i$.

Next we find the possible values of $e(j)$. Proceeding as with $e(i)$, we have

$$e(j)gh = ui + vj + zk \quad \text{for some } u, v, z \in A. \tag{3}$$

But $e(i)e(j) + e(j)e(i) = e(ij + ji) = 0$, and we know that $e(i) = \pm i$. Hence from (3) we have $i(ui + vj + zk) + (ui + vj + zk)i = 0$, so that $u = 0$. Set $a = e(w)$. Then a is an irreducible element of A of degree 25. Also $ag^2h^2 = e(w)g^2h^2 = \big(e(j)\big)^2 g^2h^2 = (ui + vj + zk)^2 = (vj + zk)^2 = (v^2 + z^2)w$. Thus

$$ag^2h^2 = (v^2 + z^2)w. \tag{4}$$

But $\deg(g^2h^2) = 20$, and w is an irreducible element of A of degree 25. It follows from (4) that w divides a in A. But $\deg(a) = \deg(w)$. Therefore $a = tw$ for some non-zero rational number t. Also because e induces an automorphism of $A = \mathbb{Q}[X]$, we have $e(X) = rX + s$ for some $r, s \in \mathbb{Q}$ with $r \neq 0$. We have $(X^{25} + 4)t = tw = a = e(w) = e(X^{25} + 4) = (rX + s)^{25} + 4$, so that

$$(X^{25} + 4)t = (rX + s)^{25} + 4. \tag{5}$$

It follows readily from (5) that $s = 0$, $t = 1$, and $r = 1$. Hence $e(X) = X$, so that e acts as the identity function on A. Also $a = e(w) = w$ and $h = e(f) = f$, so that (4) gives

$$f^2g^2 = v^2 + z^2. \tag{6}$$

But A/fA embeds in the field of real numbers, so that a sum of squares in A/fA is 0 if and only if all the terms are 0. Therefore it follows from (6) that f divides v and z. Because $g^2 = (v/f)^2 + (z/f)^2$, it follows similarly that g divides v/f and z/f. Thus fg divides both v and z, and it follows from (6) that $v = cfg$ and $z = dfg$ for some $c, d \in \mathbb{Q}$ with $c^2 + d^2 = 1$. Going back to equation (3) now gives $e(j) = cj + dk$, so that $e(j) \in R$.

At this point we know that $e(i) = \pm i$ and $e(j) = cj + dk$ for some $c, d \in \mathbb{Q}$ with $c^2 + d^2 = 1$. From this it follows easily that the restriction of e to R is an automorphism of R. Also e acts as the identity function on A. Hence $fR = e(fR) \subseteq e(S) = T$, and clearly $gR \subseteq T$. Therefore $fR + gR \subseteq T$. But $T = O_\ell(L)$ where L is not a left ideal of R, so that R is not contained in T. Hence $fR + gR \neq R$. Therefore $fA + gA \neq A$. But f and g are monic irreducible elements of A. It follows that $f = g$, *i.e.*, $X^5 - p^2 = X^5 - q^2$, *i.e.*, $p = q$. ∎

Corollary 2.12 *For each prime number p let S_p be the maximal $\mathbb{Q}[X]$-order S constructed in 2.6. Then $M_2(S_p) \cong M_2(S_q)$ for all prime numbers p and q, but $S_p \cong S_q$ if and only if $p = q$.*

https://doi.org/10.4153/CMB-2000-049-0 Published online by Cambridge University Press

3 Concluding Remarks

Remark 3.1 With the notation of 2.6 and 2.11, we conjecture that $M_n(S) \cong M_n(T)$ for all positive integers $n \neq 1$.

Remark 3.2 The non-isomorphic rings S and T constructed in Section 2 correspond to maximal right ideals of R lying over different maximal ideals of the centre A of R. It would be elegant if we could do the same sort of thing but using only maximal right ideals of R which contain a fixed irreducible element of A (and then it would be easy to settle the point raised in 3.1), but we have been unable to do this.

Remark 3.3 The construction given in Section 2 relies heavily on special properties of the field $\mathbb{Q}$ of rational numbers. One (but not the only) important property which we have used is that there are polynomials of high degree which are irreducible over $\mathbb{Q}$. It seems unlikely that this approach could be modified to give an uncountably infinite family of such maximal orders S.

Remark 3.4 The strategy for the proof of Theorem 2.11 was to show that only very special automorphisms of the quotient division ring D could induce an isomorphism between the subrings S and T, and it was not obvious in advance that such automorphisms would fix the elements of the centre of D. The same approach could be used to simplify the proofs in [2] concerning maximal $\mathbb{Z}$-orders, and in that case the automorphisms would automatically fix central elements.

References

[1] A. W. Chatters, *Non-isomorphic rings with isomorphic matrix rings.* Proc. Edinburgh Math. Soc. **36**(1993), 339–348.
[2] ———, *Matrix-isomorphic maximal $\mathbb{Z}$-orders.* J. Algebra **181**(1996), 593–600.
[3] R. G. Swan, *Projective modules over group rings and maximal orders.* Ann. of Math. **76**(1962), 55–61.
[4] D. B. Webber, *Ideals and modules of simple Noetherian hereditary rings.* J. Algebra **16**(1970), 239–242.

School of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UK
email: arthur.chatters@bris.ac.uk