RINGS WHICH ARE NEARLY PRINCIPAL IDEAL DOMAINS

by A. W. CHATTERS

(Received 4 November, 1996)

Abstract. We study a class of rings which are closely related to principal ideal domains, and prove in particular that finitely-generated projective modules over such rings are free. Examples include the ring of Lipschitz quaternions; $Z[d^{\frac{1}{2}}]$ with $d = -3$ or $d = -7$; and any subring R of $M_2(Z)$ such that $R \supseteq M_2(pZ)$ for some prime number p and $R/M_2(pZ)$ is a field with p^2 elements.

1. Introduction. Recent work on the recognition of matrix rings has renewed interest in the ring R of Lipschitz quaternions, i.e. $R = Z[i, j]$ with $i^2 = j^2 = -1$ and $ij + ji = 0$ (see for instance [2], [3], [7]). Not every one-sided ideal of R is principal. But R is closely related to the ring S of Hurwitz quaternions, and every one-sided ideal of S is principal. In some sense R seems to be nearly as good a ring as S, and in particular every right ideal of R is either principal or is a right ideal of S. This makes it almost trivial to prove that finitely-generated projective R-modules are free; (see Theorem 5.2 of [3] for an almost trivial proof). The work in this paper arose from an attempt to isolate the special features of the relationship between R and S which make it possible to prove results about R which are nearly as good as those for S. Let M be the largest two-sided ideal of S which is contained in R. Then S/M is the field with four elements, and R/M is the field with two elements. It turns out that what happens in R is controlled by the very small number of R-submodules of S which contain M. In this example every right (left) R-submodule of S which contains M is either principal or is a right (left) ideal of S. We have used this property of these particular rings as the basis for a definition of rings which we regard as being nearly principal ideal domains.

The precise definition which we shall use is given in 3.1, and further examples which satisfy it in Section 5. The property which we are studying, like that of being a principal ideal domain, is very special and so it is not surprising that we can prove strong results from it. For instance, if R is any ring which satisfies definition 3.1, then finitely-generated projective R-modules are free (Theorem 4.1) and, with one exception, every maximal right ideal of R is principal (Proposition 3.17). Examples of such rings include the ring R of Lipschitz quaternions; $R = Z[d^{\frac{1}{2}}]$ where either $d = -3$ or $d = -7$; any subring R of $M_2(Z)$ such that $R \supseteq M_2(pZ)$ for some prime number p and $R/M_2(pZ)$ is a field with p^2 elements; and $R = E + XS$ where $E \subseteq F$ is any quadratic extension of fields and S is the ring of polynomials in X over F twisted by an automorphism of F.

2. Preliminaries. All rings considered here are associative with an identity element, and all modules are unital. We refer to [1] for general background material on ring theory. An element x of a ring R is said to be *normal* if $xR = Rx$, and x is said to be *regular* if x is not a zero-divisor.

Let R be a semi-prime ring and let A be a two-sided ideal of R. It is easy to show that the following conditions are equivalent:

Glasgow Math. J. **40** (1998) 343–351.

A has non-zero intersection with every non-zero right ideal of R;
A has non-zero intersection with every non-zero left ideal of R;
A has non-zero intersection with every non-zero two-sided ideal of R;
The left annihilator of A is zero; the right annihilator of A is zero.

When A satisfies these conditions we shall say that A is an essential ideal of R.

We shall use M_R (resp. ${}_RM$) to indicate that M is being considered as a right (resp. left) R-module. The ring of rational integers and the field of rational numbers will be denoted by Z and Q respectively, and $M_n(R)$ will denote the ring of all n by n matrices over a ring R.

3. Ideal-theory. We shall now give the precise definition of the type of ring R which we shall regard as being nearly a principal ideal domain.

DEFINITION 3.1. A ring R is said to be a near-P.I.D. if

(i) R is an indecomposable ring;
(ii) there is a semi-prime ring S such that every one-sided ideal of S is principal and also S contains R as a proper subring;
(iii) S is finitely-generated as a right R-module and as a left R-module;
(iv) the largest ideal M of S with $M \subseteq R$ is essential as an ideal of S;
(v) any right (left) R-submodule of S containing M is either a right (left) ideal of S or is cyclic as an R-module. It should be noted that R need not be an integral domain.

From now on, unless stated to the contrary, we shall assume tacitly that R, S, M are as in 3.1. We shall also use $Q(S)$ to denote the semi-simple Artinian quotient ring of S. Usually only right-handed results will be stated and proved about such rings R, but of course the corresponding left-handed results will also be true.

It is known that a ring S as in 3.1 is a finite direct sum of matrix rings over integral domains, but it will follow from Theorem 3.12 that in this particular setting S can only be of one of the three following types: S is an integral domain; or S is the direct sum of two integral domains; or $S = M_2(T)$ for some integral domain T (and all three types can occur). In Theorem 3.20 we shall re-formulate Definition 3.1 in a way which will make it easier to check whether particular examples satisfy the definition, and so we will leave a detailed consideration of examples till Section 5.

We shall now prove a sequence of results about the one-sided and two-sided ideals of R, and, not surprisingly, these are strongly linked to corresponding information about the ring S.

LEMMA 3.2. *R is essential as a right R-submodule of S.*

Proof. Let I be a right R-submodule of S with $I \cap R = 0$. Then $IM \subseteq I$ because I is a right R-module, and $IM \subseteq M$ because M is an ideal of S. Hence $IM \subseteq I \cap M \subseteq I \cap R$ so that $IM = 0$. But M is an essential ideal of S. Therefore $I = 0$.

COROLLARY 3.3. *R is a semi-prime Goldie ring with the same quotient ring as S.*

Proof. Let c be a regular element of R. It follows from 3.2 that c is also regular as an element of S and hence is a unit of $Q(S)$. Also M contains a regular element w of S, so that if d is any regular element of S then dw is a regular element of R. It follows easily that if $q \in Q(S)$ then $qc \in R$ for some regular element c of R.

LEMMA 3.4. *S/M is Noetherian as a right R-module.*

Proof. Because S is finitely-generated as a right R-module, so also is every right ideal of S. It now follows immediately from 3.1 that every right R-submodule of S which contains M is finitely-generated.

THEOREM 3.5. *R is right Noetherian.*

Proof. Let I be a right ideal of R. Then IS is a principal right ideal of S so that IS/IM is a cyclic right S/M-module. But $(S/M)_R$ is Noetherian, by 3.4. Hence $(IS/IM)_R$ is Noetherian. Therefore $(I/IM)_R$ is finitely-generated. But S_R is finitely-generated and IM is a right ideal of S, so that $(IM)_R$ is finitely-generated. Therefore I_R is finitely-generated.

PROPOSITION 3.6. *Let L be an essential right ideal of R. Then either L is a principal right ideal of R or L is a right ideal of S.*

Proof. It follows from 3.2 that LS is an essential right ideal of S. Hence $LS = xS$ for some regular element x of S. Note that x has an inverse x^{-1} in $Q(S)$. Set $K = x^{-1}L$. Then K is a right R-submodule of S. Also $K \supseteq KM = KSM = x^{-1}LSM = SM = M$. Therefore, by 3.1, we have either $K = yS$ or $K = yR$ for some $y \in S$. Hence either $L = xyS$ or $L = xyR$.

PROPOSITION 3.7. *R has Krull dimension 1.*

Proof. Let E be an essential right ideal of R. We must show that $(R/E)_R$ is Artinian. Let L be a right ideal of R which contains E. Then either L is a right ideal of S or L is a principal right ideal of R by 3.6. If L is a right ideal of S then $L \supseteq ES$, and it is well-known that $(S/ES)_s$ is Artinian. Therefore it is enough to show that R satisfies the descending chain condition for right ideals L such that $L \supseteq E$ and $L = cR$ for some regular element c of R. But E contains a regular element d of R, so that there is a one-to-one inclusion-reversing correspondence between such right ideals L and some of the cyclic left R-submodules of Rd^{-1} which contain R. But ${}_R(Rd^{-1})$ is Noetherian, by 3.5. Therefore R satisfies the decending chain condition for principal right ideals which contain E.

PROPOSITION 3.8. *Let I be an essential two-sided ideal of R. Then either I is a two-sided ideal of S or $I = xR$ for some regular normal element x of R.*

Proof. Suppose that I is a left ideal of S but not a right ideal of S; we shall obtain a contradiction and then the result will follow easily from 3.6. We could give a proof using the fact that S is a maximal order, but for the reader's convenience we will give a self-contained direct proof. By 3.6 we have $I = cR$ for some regular element c of R. Also IS is an essential two-sided ideal of S by 3.2, so that $IS = aS$ for some regular normal element a of S. We have $SI = I$, i.e. $ScR = cR$, so that $S \subseteq cRc^{-1}$. Also $cRc^{-1}a \subseteq cRc^{-1}aS = cRc^{-1}IS = cRc^{-1}cRS = cS = IS = Sa$. Thus $cRc^{-1}a \subseteq Sa$ so that $cRc^{-1} \subseteq S$. Therefore $cRc^{-1} = S$. Hence $R \cong S$, so that every one-sided ideal of R is principal. In particular $M = dR$ for some regular element d of R. Hence $dR = M = MS = dRS = dS$, which is a contradiction because $R \neq S$.

COROLLARY 3.9. *Let A be a one-sided ideal of S such that $A \subseteq R$. Then $A \subseteq M$.*

Proof. Let W be the sum of all the left ideals of S which are contained in R. Clearly W is a two-sided ideal of R and $M \subseteq W$. Hence W is an essential ideal of R and is a left ideal of S. Therefore W is a two-sided ideal of S by 3.8, so that $W \subseteq M$.

LEMMA 3.10. *Let K be a right R-submodule of S which contains M and suppose that K is not a right ideal of S. Then $K = uR$ for some unit u of S.*

Proof. By 3.1 we have $K = xR$ for some $x \in S$. Because $K \supseteq M$ it follows easily that x is a regular element of S. Thus $yx = 1$ for some $y \in Q(S)$. But $yM \subseteq yxR = R$, and yM is a right S-module. Therefore by 3.9 we have $yM \subseteq M$. Because $M = Sa$ for some regular element a of S, it follows that $ySa \subseteq Sa$, i.e. $y \in S$. Therefore x is a unit of S.

THEOREM 3.11. *R/M is a division ring.*

Proof. Let K be a right ideal of R with $M \subsetneq K$. Then K is not a right ideal of S, by 3.9. Hence by 3.10 we have $K = uR$ for some unit u of S. It follows that every non-zero right ideal of R/M has zero left annihilator in S/M and in particular that R/M is an integral domain. But R/M is Artinian, by 3.7. Therefore R/M is a division ring.

THEOREM 3.12. *Set $D = R/M$. Then S/M is 2-dimensional as a right D-space.*

Proof. Let $'$ denote image in $S' = S/M$, and let "dim" denote dimension as a right D-space. Because $R \neq S$ we have $D \neq S'$, i.e. $\dim(S') \geq 2$. Let $w \in S'$ with $w \notin D$. Set $W = D + wD$. Then $\dim(W) = 2$ and W is not cyclic as a right D-module. Hence the inverse image K of W in S is not a cyclic right R-module. It follows from 3.1 that K is a right ideal of S, i.e. W is a right ideal of S'. But $1 \in W$. Therefore $W = S'$.

COROLLARY 3.13. *S is an integral domain, or the direct sum of two integral domains, or a full 2 by 2 matrix ring over an integral domain.*

Proof. Because S is a semi-prime ring in which every one-sided ideal is principal, there are orthogonal central idempotent elements $e_1, \ldots, e_n$ of S such that $1 = e_1 + \cdots + e_n$ and each e_iS is a matrix ring over an integral domain ([5]). Because $M \subseteq R$ and R is indecomposable, there is no value of i such that $e_i \in M$. Therefore for each i we have $e_iM \neq e_iS$. Hence $S/M \cong e_1S/e_1M \oplus \cdots \oplus e_nS/e_nM$ where each e_iS/e_iM is a matrix ring over a non-zero ring. But it follows from 3.12 that S/M has length at most 2 as a module over itself. Hence $n \leq 2$. If $n = 2$ then $S/M \cong e_1S/e_1M \oplus e_2S/e_2M$, and it follows from 3.12 that each of e_1S/e_1M and e_2S/e_2M is a division ring; hence S is the direct sum of two integral domains. If $n = 1$ then S/M is a full matrix ring which has size at most 2 by 2, so that either S is an integral domain or S is all 2 by 2 matrices over an integral domain.

PROPOSITION 3.14. *Let P be a maximal ideal of R with $P \neq M$. Then $P = xR$ for some regular normal element x of R, and R/P is simple Artinian.*

Proof. We shall show that P is an essential ideal of R; the result will then follow from 3.7 and 3.8. Set $A = \{r \in R : rP = 0\}$. Then A is an ideal of R, and because R is semi-prime we have $A \cap P = 0$. Also R is indecomposable so that we cannot have $R = A + P$. Therefore $A \subseteq P$ and hence $A = 0$. Therefore P is an essential ideal of R.

PROPOSITION 3.15. $\cap_{n=1}^{\infty} M^n = 0$.

Proof. Let e be an indecomposable central idempotent element of S. Then, as in the proof of 3.13, we have $eM \neq eS$. But eS is a prime ring in which every one-sided ideal is principal, so that $\cap(eM)^n = 0$. The result now follows easily from the fact that the identity element of S is a sum of such elements e.

COROLLARY 3.16. *R has no non-trivial idempotents.*

Proof. This follows quickly from 3.15 and 3.11.

PROPOSITION 3.17. *Let I be a right ideal of R which is not contained in M. Then $I = xR$ for some regular element x of R.*

Proof. There is a right ideal B of R such that $I \cap B = 0$ and $I + B$ is an essential right ideal of R. Also $I + B$ is not contained in M, so that $I + B$ is not a right ideal of S (3.9). Hence by 3.6 we have $I + B = xR$ for some $x \in R$, and x is regular because $I + B$ is essential. Thus $xR \cong R$ as right R-modules, and R_R is indecomposable by 3.16. Therefore $(xR)_R$ is indecomposable with $xR = I \oplus B$. But $I \neq 0$. Therefore $B = 0$ and $I = xR$.

PROPOSITION 3.18. *Let $x \in R$. Then either x is regular or $xR = xS$.*

Proof. Set $A = \{s \in S : xs = 0\}$. Because xS is a projective right ideal of S we have $A = eS$ for some idempotent element e. Suppose firstly that $e \in R$. By 3.16 we have either $e = 0$ so that x is regular, or $e = 1$ so that $x = 0$ and trivially $xR = xS$. Now suppose that $e \notin R$. It follows from 3.12 that R is a maximal submodule of S_R. Therefore $S = R + A$ and $xS = xR + xA = xR$.

COROLLARY 3.19. *Let I be a non-essential right ideal of R. Then I is a right ideal of S.*

Proof. This follows immediately from 3.18 and the fact that the elements of I are not regular elements of R.

The next result will make it easier to test whether particular rings satisfy Definition 3.1. In view of Corollary 3.13 we may, without loss of generality, impose the condition that the uniform dimension of S is at most 2.

THEOREM 3.20. *Let S be a semi-prime ring of uniform dimension at most 2 in which every one-sided ideal is principal, and let R be an indecomposable subring of S with $R \neq S$. Suppose that S_R and R_s are finitely-generated, and that R contains an essential ideal of S. Let M be the largest ideal of S with $M \subseteq R$. Then the following two conditions are equivalent.*

1. *R satisfies Definition 3.1 with respect to S and M, i.e. every right (resp. left) R-submodule of S which contains M is either a right (resp. left) ideal of S or is cyclic as an R-module.*

2. *R/M is a division ring, S/M is 2-dimensional as a right and as a left R/M-space, and for every unit u of S/M there is a unit d of R/M such that ud is the image in S/M of a unit of S.*

Proof. Let $'$ denote image in $S' = S/M$ and set $D = R' = R/M$. Suppose that (1) is true. Then D is a division ring and S' is 2-dimensional over D (3.11 and 3.12). Let u be a unit of S'. Then $uD \neq uS'$ so that uD is not a right ideal of S'. Let K be the inverse image of uD in S. Then K is not a right ideal of S, so that $K = vR$ for some unit v of SS (3.10). Therefore $v' = ud$ for some non-zero element d of D, and (2) has been proved.

Conversely suppose that (2) is true. The part of Condition (2) which concerns units does not immediately appear to be right-left symmetric, but in fact it is because of the fact that $(ud)^{-1} = d^{-1}u^{-1}$. Let K be a right R-submodule of S which contains M. Suppose that K is not a right ideal of S; we must show that K_R is cyclic. We have $S \supsetneq K \supsetneq M$, so that K' is a proper right D-subspace of the 2-dimensional space S'. Hence $K' = uD$ for some $u \in S'$. Also $uD \neq uS'$ because $K \neq KS$. Because S'_D is 2-dimensional we must have $uS' = S'$, i.e. u is a unit

https://doi.org/10.1017/S0017089500032699 Published online by Cambridge University Press

of S'. Hence $ud = v'$ for some units d and v of D and S respectively. Therefore $K' = uD = udD = v'D$, i.e. $K = vR + M = vR + vM = vR$.

4. Module-theory. We shall now prove some module-theoretic results for the rings R which satisfy Definition 3.1. In particular we shall show that finitely-generated projective R-modules are free (this need not be true of the corresponding ring S, for instance if S is the direct sum of two integral domains, but every finitely-generated projective S-module is a direct sum of cyclic projective S-modules). We suspect that there is a good structure theorem for finitely-generated torsion-free R-modules, but at present we do not know what it is. It will also be shown that R has injective dimension 1 and infinite global dimension. As in Section 3 we shall assume that R, S, M are as in 3.1

THEOREM 4.1. *Finitely-generated projective R-modules are free.*

Proof. Let P be a non-zero indecomposable projective right R-module; it is enough to show that $P \cong R$. Set $P^* = \mathrm{Hom}_R(P, R)$. Then P^*P is a non-zero idempotent ideal of R. Because $\cap M_n = 0$ (3.15), we know that P^*P is not contained in M. Thus we can fix $f \in P^*$ such that $f(P)$ is not contained in M. By 3.17 we have $f(P) = xR$ for some regular element x of R. In particular $xR \cong R$ and f splits to give $P \cong R$.

COROLLARY 4.2. *S_R is not projective.*

Proof. Suppose that S_R is projective. Then M_R is projective. Hence by 4.1. we have $M = xR$ for some regular element x of R. Thus $xR = M = MS = xS$ so that $R = S$, which is a contradiction.

THEOREM 4.3. *S_R has infinite projective dimension.*

Proof. By 3.12 there is an element a of S such that the images of 1 and a in S/M form a basis for S/M as a right R/M-space. In particular $R + aR = S$. Also if $r \in R$ with $ar \in R$ then $r \in M$. Thus $R \cap aR = aM$. Because M contains a regular element of S, it follows by a result of Robson that so also does the coset $a + M$ (see for instance Corollary 1.20 of [1]). Therefore without loss of generality we can suppose that a is a regular element of S. Thus, working with right R-modules, we have $aR \cong R$ and $R \cap aR = aM \cong M \cong S$. The usual short exact sequence $0 \to (R \cap aR) \to (R \oplus aR) \to (R + aR) \to 0$ induces an exact sequence $0 \to S \to (R \oplus R) \to S \to 0$. But by 4.2 we know that S_R is not projective. It follows that S_R has infinite projective dimension.

THEOREM 4.4. *R has injective dimension* 1.

Proof. Recall from 3.3 that R and S have the same quotient ring $Q(S)$. Set $E = Q(S)/R$. We must show that E_R is injective. By Baer's Criterion we can suppose that $f: K \to E$ is a right R-module homomorphism where K is an essential right ideal of R, and we must show that f extends to an R-module homomorphism $g : R \to E$. This is trivial if $K = xR$ for some regular element x of R.

Therefore by 3.6 we need only consider the following situation: K is an essential right ideal of R with $K = xS$ for some regular element x of S; $f: K \to E$ is a right R-module homomorphism; we must extend f to a homomorphism $g : R \to E$. For the remainder of the

proof we fix $a \in S$ with $a \notin R$. By 3.12 we have $S = R + aR = R + Ra$. In particular $K = xS = xR + xaR$, so that f is determined by the values of $f(x)$ and $f(xa)$. We have $f(x) = w + R$ and $f(xa) = z + R$ for some $w, z \in Q(S)$. Let $m \in M$. Then $am \in R$ so that $wam + R = f(x)am = f(xam) = f(xa)m = zm + R$. It follows that $(wa - z)M \subseteq R$. Set $M^* = \{q \in Q(S) : qM \subseteq R\}$. Then $wa - z \in M^*$. Also M^*M is a right ideal of S which is contained in R, so that $M^*M \subseteq M$ by 3.9. But $M = Sy$ for some regular element y of S. Therefore $M^* \subseteq S$. Hence $wa - z \in S$, i.e. $z = wa + s$ for some $s \in S$. We have $s = u + va$ for some $u, v \in R$. Define $g : R \to E$ by $g(r) = (w + v)x^{-1}r + R$ for all $r \in R$. It is routine to check that $g(x) = f(x)$ and $g(xa) = f(xa)$, so that g is the desired extension of f.

REMARK 4.5. Let T be a torsion-free right R-module. An easy modification of the proof of 3.18 shows that if $t \in T$ then either $tR = tS$ or $tR \cong R$ as right R-modules. We conjecture that if T_R is finitely-generated then T is the direct sum of a free right R-module and a right S-module.

5. Examples. We shall now give some detailed examples of rings which are near P.I.D.'s according to Definition 3.1, and we shall show that all three types of S listed in 3.13 can occur. As might be expected by analogy with the theory of P.I.D.'s, some constructions always give rings of the right sort, while others do so only when some parameter is small.

EXAMPLE 5.1. Let F be the rational division algebra of standard quaternions. Thus the elements of F are uniquely of the form $a + bi + cj + dk$ with $a, b, c, d \in Q$, where $i^2 = j^2 = -1$ and $ij = k = -ji$. Set $S = \{(a + bi + cj + dk)/2 : a, b, c, d$ are integers which are either all even or all odd$\}$; $M = (1 + i)S$; and $R = Z[i, j] = \{a + bi + cj + dk : a, b, c, d \in Z\}$. Then R and S are respectively the rings of Lipshitz and Hurwitz quaternions. It is well-known that S is an order in F and that every one-sided ideal of S is principal. Also M is an ideal of S with $M \subseteq R$, and S/M and R/M are fields with four and two elements, respectively. Set $f(X) = X^2 + X + 1$. Then $f(X)$ is irreducible over R/M. Set $u = (1 + i + J + k)/2$ and let v be the image of u in S/M. Then $u^2 = u - 1$, so that u is a unit of S and $f(v) = 0$. Therefore v is algebraic of degree 2 over R/M. Hence the non-zero elements of S/M are $1, v, v^2$ and clearly these are the images of units of S. Thus Condition (2) of 3.20 is satisfied, and so R is a near-P.I.D.

We conjecture that no further examples of rings R satisfying Definition 3.1 can be found by allowing i^2 and j^2 to be arbitrary negative integers in 5.1.

EXAMPLE 5.2. Let F, M, S, R be as in 5.1 except that this time we take $i^2 = -1$ and $j^2 = p$ where p is a prime number with $p \equiv 3$ mod(4). Then S is a maximal Z-order in F (see for instance Section 105 of [4]}, and it follows from a theorem of Latimer [6] that every one-sided ideal of S is principal. In order to find instances in which R is a near-P.I.D., it is enough, as in 5.1, to fine an element u of S such that $u^2 = au \pm 1$ for some odd integer a. If $p = 3$ we can take $u = (1 + 3i + j + K)/2$; if $p = 7$ we can take $u = (3 + 3i + j + k)/2$; if $p = 11$ we can take $u = (1 + 5i + j + k)/2$; if $p = 19$ we can take $u = (3 + 5i + j + k)/2$; and we suspect that this can be done for any such p.

EXAMPLE 5.3. Let $E \subseteq F$ be any quadratic extension of fields, and let X be an indeterminate. Set $S = F[X]$, $M = XS$, and $R = E + M$. It is clear that the units of S/M are the images of the units of S (namely the non-zero elements of F). Therefore R is a near-P.I.D. The same is true if the multiplication of S is twisted by an automorphism of F.

EXAMPLE 5.4. Let p be a prime number. Set $F = Z/pZ$, $S = Z \oplus Z$, and $M = pS$. We shall identify S/pS with $F \oplus F$. Let D be the diagonal copy of F in $F \oplus F$, and let R be the subring of S such that $R \supseteq pS$ and $R/pS = D$. Then R is a near-P.I.D. if and only if the units of S/M lift to units of S, i.e. if and only if $p = 2$ or $p = 3$. Let R_p and S_p denote respectively the rings formed from R and S by inverting the elements of Z which are not divisible by p. Then S_p is semi-local with Jacobson radical pS_p, and for every prime number p we see that R_p is a near-P.I.D.

EXAMPLE 5.5. Let p be a prime number. Set $S = M_2(Z)$ and $M = pS$. Let R be any subring of S such that $R \supseteq M$ and R/M is a field with p_2 elements. We shall show that R is a near-P.I.D. We shall identify S/M with $M_2(F)$ where $F = Z/pZ$. We note that the field with p^2 elements can be embedded in $M_2(F)$, so that R does exist. We shall identify F with the centre of $M_2(F)$. Set $D = R/M$.

Let u be a unit of $S/M = M_2(F)$. In order to apply Theorem 3.20 we must show that there is a non-zero element d of D and a unit v of S such that ud is the image of v in S/M. We need to consider three cases.

CASE (1). $\det(u) = f^2$ for some $f \in F$. Let d be the 2 by 2 scalar matrix with f^{-1} in the diagonal positions. Then $d \in F$ and hence $d \in D$. We have $\det(ud) = 1$, so that ud is a product of transvections in $M_2(F)$ which lift to transvections in S.

CASE (2). $\det(u) = -f^2$ for some $f \in F$. Let a be a unit of S with $\det(a) = -1$, and let b be the image of a in $M_2(F)$. Then $\det(bu) = f^2$. Thus we can apply Case (1) to bu, and it follows that u lifts to a unit of S.

CASE (3). Suppose that neither of the previous cases applies. Set $a = \det(u)$. Then neither a nor $-a$ is a square in F. It follows that we must have $p \equiv 1 \bmod(4)$. Working in $M_2(F)$ set

$$t = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$$

Then $t^2 = a$, so that $F(t)$ is a subfield of $M_2(F)$ with p^2 elements. But D is also a subfield of $M_2(F)$ with p^2 elements. Therefore $D = w^{-1}F(t)w$ for some unit w of $M_2(F)$. Set $d = w^{-1}tw$. Then $d \in D$ and $\det(d) = \det(t) = -a$. Hence $\det(ud^{-1}) = -1$. But -1 is a square in F because $p \equiv 1 \bmod(4)$. Therefore we can apply Case (1) to ud^{-1}.

EXAMPLE 5.6. Let d be a negative square-free integer with $d \equiv 1 \bmod(4)$, and set $R = Z[d^{\frac{1}{2}}]$. We shall show that R is a near-P.I.D. if and only if $d = -3$ or $d = -7$. Let S be the ring of integers of $Q(d^{\frac{1}{2}})$, i.e. $S = \{(a + b.d^{\frac{1}{2}})/2 : a, b \in Z \text{ with } a + b \text{ even}\}$, and set $M = 2S$. Then M is an ideal of R. Also S/M has four elements, and $R/M \cong Z/2Z$. Clearly M is not a principal ideal of R. It follows from 3.14 that, if R is a near-P.I.D., then the M considered here is the only possibility for M in 3.1 and similarly for S. We shall not need to know all the values of d for which S is a P.I.D., but we remind the reader that these are the numbers -3, -7, -11, -19, -43, -67, -163 (recall that we are assuming that d is negative square-free with $d \equiv 1 \bmod(4)$). We divide the argument into two cases.

CASE (1). $d \equiv 5 \bmod(8)$. Let $s \in S$. Then $s = \left(a + b.d^{\frac{1}{2}}\right)/2$ for some $a, b \in Z$ with $a + b$ even. The norm $N(s)$ of s is given by $N(s) = \left(a^2 - db^2\right)/4$. Then $N(s) \in Z$, and the condition

https://doi.org/10.1017/S0017089500032699 Published online by Cambridge University Press

that $d \equiv 5 \bmod(8)$ implies that if $N(s) \in 2Z$ then $s \in 2S$. Because 4 divides the norm of any element of $2S$, it now follows quite easily that $2S$ is a maximal ideal of S. Therefore S/M is the field with 4 elements. On the other hand the only units of S are 1 and -1 unless $d = -3$. It follows from 3.20 that if $d \neq -3$ then R does not satisfy Definition 3.1. Now suppose that $d = -3$. Set $w = \left(1 + d^{\frac{1}{2}}\right)/2$. Then $w^2 = w - 1$. As in 5.1 it follows that the images of $1, w, w^2$ in S/M are the units of S/M, so that R is a near-P.I.D. by 3.20.

CASE (2). $d \equiv 1 \bmod(8)$. Set $x = \left(1 + d^{\frac{1}{2}}\right)/2$. Then $N(x)$ is even. Set $P = 2S + xS$ and $P^* = 2S + x^*S$, where x^* is the complex conjugate of x. It is routine to check that $PP^* = 2S$ and that $P \neq S \neq P^*$. Also $P \neq P^*$. Hence $S/2S \cong Z/2Z \oplus Z/2Z$, and it is trivial that the units of $S/2S$ lift to units of S. Thus we must determine when S is a P.I.D. This is well-known to be so if $d = -7$ (in fact in this case S is a Euclidean domain). Now suppose that S is a P.I.D. Then $P = uS$ for some $u \in S$. Because $S/P \cong Z/2Z$ we have $N(u) = 2$. But $u = (a + b.d^{\frac{1}{2}})/2$ as above. Therefore $a^2 - db^2 = 8$, and for the sort of d which we are considering this forces $d = -7$.

Now suppose that d is a positive square-free integer with $d \equiv 1 \bmod(4)$, and set $R = Z[d^{\frac{1}{2}}]$. For certain values of d, such as $d = 5$ and $d = 13$, it is possible to show that R is a near-P.I.D., but there seems to be no hope of getting a complete list in this case.

ACKNOWLEDGEMENT. Part of this work was done while the author was visiting the Mathematics Department of Rutgers University, and he wishes to thank the members of that department for their hospitality and the facilities which they provided.

REFERENCES

1. A. W. Chatters and C. R. Hajarnavis, *Rings with chain conditions* (Pitman, 1980).

2. A. W. Chatters, Matrices, idealisers, and integer quaternions, *J. Algebra* **150** (1992), 45–56.

3. A. W. Chatters, Isomorphic subrings of matrix rings over the integer quaternions, *Comm. Algebra* **23** (1995), 783–802.

4. L. E. Dickson, *Algebras and their arithmetics* (G. E. Stechert and Co., 1938).

5. A. W. Goldie, Non-commutative principal ideal rings, *Arch. Math.* **13** (1962), 214–221.

6. C. G. Latimer, On the class number of a quaternion algebra with a negative fundamental number, *Trans. Amer. Math. Soc.* **40** (1936), 318–323.

7. L. S. Levy, J. C. Robson and J. T. Stafford, Hidden matrices, *Proc. London Math. Soc.* **69** (1994), 277–305.

SCHOOL OF MATHEMATICS
UNIVERSITY OF BRISTOL
BRISTOL, BS8 1TW
ENGLAND
E-mail: arthurchatters@bristol.ac.uk