Can. J. Math., Vol. XXIII, No. 1, 1971, pp. 1–11

INVERTIBILITY AND CLASS NUMBER OF ORDERS

HOWARD GORMAN

1. Introduction. This paper continues the work begun in [**5**] and concerns the invertibility of modules in a finite-dimensional, symmetric algebra L with 1 over a field. In particular, we continue the work done in [**5**] which dealt with the connection between invertibility in these algebras and a condition called the Brandt Condition, which is a reformulation by Kaplansky [**6**] of some ideas of Brandt.

We begin by proving some preliminary results on invertibility and some equivalent conditions for the dual of an order to be principal.

Then, we define the class number of an order and reformulate the concept of invertibility in terms of class number. In this terminology, we find some equivalent conditions which ensure that an order in certain algebras L (including commutative, symmetric algebras, and algebras with a strong involution) has class number equal to 1 (i.e., all modules principal), and we characterize a class of Brandt algebras over the quotient fields of valuation rings as those in which all orders have class number less than or equal to 2. Finally, we prove a result, a corollary of which is the fact that if L is a commutative, symmetric algebra or an algebra with a strong involution over the quotient field K of a discrete valuation ring with finite residue class field, then any order in L has finite class number.

2. Basic concepts. By L we shall always mean a finite-dimensional algebra with 1 over the quotient field K of R, a commutative infinite domain with 1.

By a *module*, we shall always mean a finitely generated R-module contained in L which spans L as a vector space over K. If a module is also a ring containing 1, we shall call it an *order*. We note that, because orders are finitely generated, they consist of elements integral over R. If a module merely contains 1 and consists of elements integral over R, we call it a *semi-order*. Since modules are finitely generated and span L over K, it follows that for any modules A and B, there is an $r \in R$ such that $rA \subseteq B$.

If A is a module, we write $A = {}_PA_Q$ to mean that

$$P = \{x \in L |\, xA \subseteq A\} \qquad \text{and} \qquad Q = \{x \in L |\, Ax \subseteq A\}.$$

We call P (Q) the *left* (*right*) *orders* associated with A. It is standard that P and Q are rings containing 1 and that they span L over K. We write

$$A^{-1} = \{x \in L |\, AxA \subseteq A\}.$$

Received April 1, 1969.

https://doi.org/10.4153/CJM-1971-001-1 Published online by Cambridge University Press

We call A^{-1} the *inverse* of A. Then A^{-1} spans L over K. When R is a Prüfer ring (all finitely generated, non-zero ideals invertible), then P, Q, and A^{-1} are finitely generated (see [**4**]). Thus, P and Q are orders and A^{-1} is a module.

We say that A is *right* (*left*) *invertible* if $AA^{-1} = P$ $(A^{-1}A = Q)$, and *invertible* if it is both left and right invertible. We note that if $A = {}_PA_Q$ is invertible, then $A^{-1} = {}_Q(A^{-1})_P$ (see [**4**]).

For any $x \in L$, we define the *norm* of x, written $\mathfrak{N}(x)$, to be the determinant of x in the left regular representation.

For details of the above remarks, see [**4**].

3. The Brandt condition. Suppose that L is a symmetric algebra, i.e., that there is defined on L a symmetric, non-singular, invariant, bilinear form, written (,).

Let A be a module. We define the *dual* of A, written $A^\#$ by

$$A^\# = \{x \in L|\ (x, A) \subseteq R\}.$$

If A is a free module, then $A^\#$ is a module and $(A^\#)^\# = A$ (see [**5**]).

If $a_1, \ldots, a_n$ is a generating set for A over R, then for any $x \in A$, $x = \sum_{i=1}^n x_i a_i$ with $x_i \in R$ for each i. Then

$$\mathfrak{N}(x) = \mathfrak{N}\left(\sum_{i=1}^n x_i a_i\right) = f(x_1, \ldots, x_n),$$

a homogeneous polynomial in $x_1, \ldots, x_n$. We define the *norm* of A, written $\mathfrak{N}(A)$, to be the finitely generated, fractional R-ideal generated by the coefficients of $f(x_1, \ldots, x_n)$. Then $\mathfrak{N}(A)$ is independent of the generating set chosen (see [**5**]). Further, if R is a valuation ring, then $\mathfrak{N}(A)$ will be principal and the norm of a semi-order is R (see [**5**]).

Now, suppose that A is free with basis $a_1, \ldots, a_n$ over R. We define the *discriminant* of A, written $\Delta(A)$, to be the principal R-ideal generated by the determinant of the matrix $((a_i, a_j))$. We remark that for any $x \in L$, $\Delta(xA) = \mathfrak{N}(x)^2\Delta(A)$ and that $\Delta(A^\#) = (\Delta(A))^{-1}$.

We say that a free module A satisfies the *Brandt condition* if

$$\mathfrak{N}(A^\#)\Delta(A) \subseteq R.$$

4. Localization. If A is a module and M is a maximal ideal of R, we write A_M for the localization of A at M. Then, as M runs over the maximal ideals of R, we have:

(1) $A = {}_PA_Q$ if and only if $A_M = {}_{P_M}(A_M)_{Q_M}$ for every maximal ideal M of R;

(2) $(AB)_M = A_M B_M$;

(3) $(A^{-1})_M = (A_M)^{-1}$;

(4) $\mathfrak{N}(A_M) = \mathfrak{N}(A)_M$;

(5) $\Delta(A)_M = \Delta(A_M)$.

Hence, invertibility and the Brandt condition are local concepts. In this spirit, we define a module A to be a *Brandt module* if it satisfies the Brandt condition at every localization at a maximal ideal, and L to be a *Brandt algebra* if a module is invertible if and only if it is a Brandt module.

Finally, we remark that R is a Prüfer ring if and only if R_M is a valuation ring for each maximal ideal M of R. When R is Prüfer, any module is finitely generated and torsion-free, and so, is projective. *If, in addition, R is a valuation ring, a module is free.*

5. Extending the base field. Let R be a valuation ring. By extending the base field, we proved in [**4**] that we may assume the following. If A is a module, then A contains an element of minimal norm, i.e., there is an x in A such that $\mathfrak{N}(x)$ divides $\mathfrak{N}(y)$ for all y in A. Further, x is a unit of L and $x^{-1}A$ (also Ax^{-1}) is a semi-order. We make these assumptions in the remainder of the paper. We showed in [**5**] that extending the base field does not disturb the Brandt condition for a module. This fact will be important later.

6. Invertibility. We begin by a series of lemmas, assuming throughout that L is a symmetric algebra.

LEMMA 1. *Let $A = {}_PA_Q$ be a module with $A = A^{\#\#}$. Then $A^\# = {}_Q(A^\#)_P$.*

Proof. $(A^\#, A) \subseteq R \Leftrightarrow (A^\#, PA) \subseteq R \Leftrightarrow (A^\# P, A) \subseteq R \Leftrightarrow A^\# P \subseteq A^\#$. Hence, P is contained in the right order of $A^\#$. By the same argument, the right order of $A^\#$ is contained in the left order of $A^{\#\#} = A$; thus, P is the right order of $A^\#$. The proof for Q is symmetric.

LEMMA 2. *Let $A = {}_PA_Q$ be a module. Suppose that A, P, Q, $AA^\#$, and $A^\# A$ are free modules. Then*

$$AA^\# = P^\# \quad \text{and} \quad A^\# A = Q^\#. \tag{1}$$

Proof. We prove the result for P only. Now

$$(x, AA^\#) \subseteq R \Leftrightarrow (xA, A^\#) \subseteq R \Leftrightarrow xA \subseteq A^{\#\#} = A \Leftrightarrow x \in P.$$

Hence $(AA^\#)^\# = P$. Since free modules are equal to their double dual, the result follows for P by taking duals in the last equality.

We define the ordered pair of modules $\langle A, B\rangle$ to be *concordant* if the right order of A equals the left order of B.

LEMMA 3. *Let the hypotheses be as in Lemma 2. Then if A and $A^\#$ are invertible as well, $P^\#$ and $Q^\#$ are invertible.*

Proof. Now $\langle A, A^\#\rangle$ and $\langle A^\#, A\rangle$ are concordant pairs of modules. In [**4**, Lemma 16], we showed that then $AA^\#$ and $A^\# A$ are invertible. The result follows from (1).

https://doi.org/10.4153/CJM-1971-001-1 Published online by Cambridge University Press

In the other direction, we have Lemma 5 below. But first, we need the following result.

LEMMA 4. *Let* $A = {}_PA_Q$. *Let* $A_1 \subseteq L$ *be a subset and* P_1 *an order. Suppose that* $AA_1 = P_1$ *and* $P_1A = A$. *Then* $P = P_1$ *and* A *is right invertible. Further, if* $QA_1 = A_1$, *then* $A_1 = A^{-1}$.

Proof. $P_1A = A$ implies that $P_1 \subseteq P$. But $PAA_1 = AA_1$, and so $PP_1 = P_1$ which implies that $P_1 \supseteq P$, i.e., equality.

Since now $AA_1 = P$, then all the more so, $AA^{-1} = P$ (since A_1 is obviously contained in A^{-1}). Thus, A is right invertible.

Further, if $QA_1 = A_1$, then, since $AA_1 = P$, we have:

$$A^{-1} = A^{-1}P = A^{-1}AA_1 \subseteq QA_1 = A_1,$$

and our proof is complete.

A similar statement holds for left invertibility.

COROLLARY 1. *Using the notation of Lemma* 4, *if* A *is invertible, then* $(A^{-1})^{-1} = A$ *and* $A^{-1} = {}_Q(A^{-1})_P$.

Proof. Stating the lemma for the right invertibility of A^{-1}, we see that $A^{-1}A = Q$ and $QA^{-1} = A^{-1}$ are exactly the conditions needed to show that A^{-1} is right invertible. Left invertibility follows similarly. Since $PA = A$, the lemma yields $A = (A^{-1})^{-1}$, and our proof is complete.

If L is commutative, Lemma 4 states that a module can be invertible as an ideal of an order, only in its associated order.

LEMMA 5. *Let* $A = {}_PA_Q$ *be a module with* A, P, Q, $AA^\#$, *and* $A^\#A$ *free over* R. *Then:*

(i) $P^\#$ $(Q^\#)$ *left invertible implies that* $A^\#$ (A) *is left invertible;*

(ii) $P^\#$ $(Q^\#)$ *right invertible implies that* A $(A^\#)$ *is right invertible.*

Proof. We prove (i) for $P^\#$ only. Let $P^\#$ have inverse B. Then, from Lemma 2, we have $BAA^\# = P$. We apply Lemma 4 with $A_1 = BA$ and $P_1 = P$ to show that $A^\#$ is left invertible, i.e., that A is right invertible.

COROLLARY 2. *Add to the hypotheses of Lemma* 5 *that* $P^\#$ *and* $Q^\#$ *are invertible. Then* A *and* $A^\#$ *are invertible.*

Proof. The proof is clear from Lemma 5.

We remark that Lemmas 3 and 5 combined imply that, for any module $B = {}_PB_Q$ to have the property that B and $B^\#$ are invertible, it is necessary and sufficient that there is one module $A = {}_PA_Q$ with this property.

7. Principal modules and the kernel. We call the module A *left principal* if $A = Px$ for some order P and some x in L. Since A spans L over K, x cannot be a zero divisor and since L is finite-dimensional over K, it follows that x

https://doi.org/10.4153/CJM-1971-001-1 Published online by Cambridge University Press

is a unit of L. Then it is clear that P is the left order of A. Further, since $A = x(x^{-1}Px)$, A is *right principal* as well, with right order $x^{-1}Px$. Thus, we may talk unambiguously of a module being *principal.*

(Z) We showed in [**5**, Theorem 1] that, *when R is a valuation ring, principal modules are Brandt.*

If $A = Px$ is principal, then clearly $A^{-1} = x^{-1}P$, and so, principal modules are invertible. The converse need not be true. *But if L is commutative modulo its nil radical, and R is quasilocal* (*i.e., R has a unique maximal ideal*), *then principality of a module is equivalent to its invertibility* (see [**4**, Lemma 13]). In this direction, also, we have the following result.

LEMMA 6. *Every invertible module in L is principal if and only if every invertible semi-order is an order.*

Proof. Necessity. A is an invertible module and $x \in A$ has minimal norm. Then $B = x^{-1}A$ is an invertible semi-order, and so, an order. Thus, $A = xB$ is principal.

Sufficiency. Suppose that $A = xQ$ is a principal semi-order with Q an order. Then $Q \subseteq A$. Since $x \in A$, x is integral over R. Suppose that x satisfies a monic polynomial with coefficients in R of degree n. Then,

$$Qx^n \subseteq \sum_{i=0}^{n-1} Qx^i.$$

Multiplying by x on the left, we obtain

$$Ax^n \subseteq \sum_{i=0}^{n-1} Ax^i. \tag{2}$$

Now, $Q = x^{-1}A$; so that $x^{-1} \in Q$. Then $x^{-i} \in Q$ for any positive integer i. Multiplying (2) on the right by $x^{-(n-1)}$ now yields $Ax \subseteq A$, i.e., $x \in Q$. But this means that

$$A = xQ \subseteq Q^2 = Q,$$

and our proof is complete.

Let R be a valuation ring. Let A be a module with left order P and with $x \in A$ of minimal norm. Then the semi-order $B = x^{-1}A$ contains P and has P as its left order. Further, $B = P$ if and only if

$$\Delta(B) = \Delta(P). \tag{3}$$

(Comparable modules with the same discriminant are equal.) By Lemma 6, $B = P$ is equivalent to A being principal. Substituting for B in terms of A in (3), we see that A is principal if and only if

$$\frac{\Delta(A)}{\mathfrak{N}(A)^2} = \Delta(P).$$

Thus motivated, we define the *kernel* of a free module A, written $\delta(A)$ to be

$$\delta(A) = \frac{\Delta(A)}{\mathfrak{N}(A)^2}. \tag{4}$$

THEOREM 1. *Let L be a finite-dimensional, symmetric, algebra with* 1 *over the quotient field K of a valuation ring R. Let P be an order in L. Then the following conditions are equivalent:*

(1) *$P^\#$ is principal;*

(2) *$\delta(P^\#) = \Delta(P)$;*

(3) *P satisfies the Brandt condition with equality.*

Proof. (1) $\Rightarrow$ (2). This follows by setting $A = P^\#$ in the definition of the kernel.

(2) $\Rightarrow$ (3). Using the fact that $\Delta(P^\#) = \Delta(P)^{-1}$, and clearing denominators, we see that $\Delta(P^\#)/\mathfrak{N}(P^\#)^2 = \Delta(P)$ is equivalent to $\mathfrak{N}(P^\#)^2\Delta(P)^2 = R$, the Brandt condition for P, squared. Since R is a valuation ring, we can take square roots to obtain the result.

(3) $\Rightarrow$ (1). This is trivial.

8. Orders of genus 1 and class number. If A and B are modules with left order P, we shall say that A is *right equivalent* to B, and write $A \sim B$, if there is an $x \in L$ (necessarily a unit) such that $B = Ax$. Then "$\sim$" is an equivalence relation among the modules with left order P. By the *right class number* of P we shall mean the number of equivalence classes of modules with respect to this equivalence relation. Similarly, we define *left equivalence* for modules with right order P and define the *left class number* of P.

In general, the left and right class numbers of an order require separate discussions. However, we have the following result.

LEMMA 7. *Let L be a symmetric algebra. Let P be an order in L such that all modules with either left or right order equal to P are free.* (*In particular, this will be true if R is a valuation ring.*) *Then the left and right class numbers of P are equal.*

Proof. If A and B are modules with left order P, then $A^\#$ and $B^\#$ are modules with right order P by Lemma 1. Since $A = Bx$ if and only if $A^\# = x^{-1}B^\#$, we obtain a one-to-one correspondence between inequivalent modules with left order P and inequivalent modules with right order P by taking duals, i.e., the left and right class numbers of P are equal.

If the left and right class numbers of an order are equal, we write $\mathfrak{n}(P)$, the *class number* of P, for their common value.

We have the following result.

COROLLARY 3. *Let P be an order. Then $\mathfrak{n}(P) = 1$ if and only if every module with left* (*symmetrically, right*) *order P is principal.*

Proof. $\mathfrak{n}(P) = 1$ means that any module A with left order P must satisfy $A = Px$ for some $x \in L$.

We call an order P a *genus* 1 *order* (over R) if any invertible module having either left or right order equal to P is principal. We call P a *strong genus* 1 *order* if every order containing P is a genus 1 order and if B is any semi-order with either order equal to P, then B^m is an order for some positive integer m. *We remark that if L is commutative modulo its nil radical or a *-algebra, and R is a valuation ring, then any order contained in L is a strong genus* 1 *order*. (* is an involution defined on L such that $x + x^*$ and xx^* are in K for all $x \in L$. See [**4**] for commutative algebras and [**6**] for *-algebras.)

We note that the order Q is *conjugate* to the order P if there is an $x \in L$ such that $Q = x^{-1}Px$. Conjugacy is an equivalence relation and we write $[P]$ for the conjugacy class of P.

The next theorem is valid for commutative and *-algebras (see [**4**; **6**] for hypothesis requirements) and provides a substantial improvement over Corollary 3.

THEOREM 2. *Let L be a finite-dimensional, symmetric algebra with* 1 *over the quotient field K of a valuation ring R. Let P be a genus* 1 *order in L with the property that a module has either both orders in $[P]$ or neither order in $[P]$. Then the following conditions are equivalent:*

(1) *$P^\#$ is principal;*

(2) $\delta(P^\#) = \Delta(P)$*;*

(3) *P satisfies the Brandt condition with equality;*

(4) $\mathfrak{n}(P) = 1$.

Proof. The equivalence of (1), (2), and (3) is simply Theorem 1.

(4) $\Rightarrow$ (1). Since $P^\#$ has left and right order equal to P by Lemma 1, then $P^\#$ is principal by Corollary 3.

(1) $\Rightarrow$ (4). Let A be a module with left order P and right order $x^{-1}Px$. If $P^\# = Py$, for some $y \in L$, then

$$(x^{-1}Px)^\# = x^{-1}P^\#x = x^{-1}Pyx = (x^{-1}Px)x^{-1}yx,$$

a principal module. Thus, A is invertible, and hence principal, by Corollary 2, i.e., $\mathfrak{n}(P) = 1$, and the proof is complete.

In [**5**, Theorem 3], we showed that if R is a valuation ring and if L is a Brandt algebra, then, for any module A, A or $A^\#$ is invertible. (Faddeev [**3**, Theorem 1] proved that a module or its dual is principal in any three-dimensional, commutative, separable algebra with 1 over the quotient field of a discrete valuation ring.) In Theorem 3, we obtain a strengthening of this result and a partial converse. But first we prove the following result.

LEMMA 8. *Let R be a valuation ring and L a symmetric algebra. Let P be a genus* 1 *order with* $\mathfrak{n}(P) \leqq 2$. *Let A be a module with left* (*or right*) *order P. Then A or $A^\#$ is principal and A is principal if and only if it is a Brandt module.*

Proof. If $\mathfrak{n}(P) = 1$, then all modules with left order P are principal and, by (Z), there is nothing to prove.

Suppose that $\mathfrak{n}(P) = 2$ and that A is a non-principal module with left order P. Since $\mathfrak{n}(P) = 2$, we must have both that $P^\#$ is not principal and that $A \sim P^\#$. (Otherwise, P itself would lie in a third equivalence class.) Then $A^\# \sim P$ (as right modules), i.e., $A^\#$ is principal.

To complete the proof, we need only show, by (Z), that A is not Brandt. Now, we always have $\Delta(P) \subseteq \delta(A)$ and, since A is not principal, the inclusion is strict. Since $A^\#$ is principal, we have $\delta(A^\#) = \Delta(P)$. Therefore

$$\frac{\Delta(A^\#)}{\mathfrak{N}(A^\#)^2} \subset \frac{\Delta(A)}{\mathfrak{N}(A)^2}$$

($\subset$ denotes strict inclusion). Clearing denominators, using the fact that $\Delta(A^\#) = \Delta(A)^{-1}$, and taking square roots, we see that

$$\mathfrak{N}(A^\#)\Delta(A) \supset \mathfrak{N}(A),$$

i.e., A is not a Brandt module.

THEOREM 3. *Let L be a finite-dimensional, symmetric algebra with* 1 *over the quotient field K of a valuation ring R. Suppose that all invertible modules contained in L are principal. Then L is a Brandt algebra if and only if, for every order P in L, $\mathfrak{n}(P) \leqq 2$.*

Proof. Sufficiency. Now P and $P^\#$ are modules with both orders equal to P. Then, it is enough to show that, if A is any module with left order P, then A is right equivalent to P or $P^\#$. Now A or $A^\#$ is principal by Lemma 8. If A is principal, it is right equivalent to P and our proof is complete. If not, since $A^\#$ has right order P, $A^\# = yP$ for some $y \in L$. Then, $A = P^\# y^{-1}$, as required.

Necessity. By Lemma 8, a module is principal if and only if it is a Brandt module. Since invertible modules are principal, L is a Brandt algebra, and our proof is complete.

In the direction of finiteness of class number, we prove the following result. The method of reducing this result to the case of modules contained in their orders was used by R. Tarsy [Thesis, University of Chicago] to prove a similar theorem for orders in central separable algebras over the quotient fields of discrete valuation rings.

THEOREM 4. *Let L be a finite-dimensional, symmetric algebra with* 1 *over the quotient field K of a discrete valuation ring R. Assume that R has finite residue class field. Let P be a strong genus* 1 *order in L. Then P has finite class number.*

Proof. Let $x \in P^\#$ have minimal norm. Then, the semi-order $P^\# x^{-1}$ contains its left order P, and $(P^\# x^{-1})^m = Q$ is an order for some integer m. Since $P \subseteq Q$, Q is a genus 1 order.

Let A be a module with left order P. Since $AA^\# = P^\#$, we see that $(AA^\# x^{-1})^m = Q$. Multiplying on the left by Q and rearranging, we see that

$$(QA)(A^\# x^{-1}(AA^\# x^{-1})^{m-1}) = Q,$$

so that, from Lemma 4, QA is a principal module with left order Q. Therefore, let $QAs = Q$ for some $s \in L$.

Choose $r \in R$ so that $rQ \subseteq P$. Then r depends only on P. Now $A \sim Asr$, and for Asr we have

$$Asr \subseteq QAsr = Qr \subseteq P$$

and

$$r^2 \in r^2Q = r^2QAs \subseteq rPAs = Asr.$$

Thus, every module with left order P is right equivalent to a module with left order P which is contained in P and contains r. It is, therefore, sufficient to find how many equivalence classes of modules of this latter kind there are.

If $M = tR$ is the maximal ideal of R, then $r^2R = t^jR = M^j$ for some non-negative integer j. Since R/M is finite, so is R/M^j and hence, so is P/PM^j. Since each of the modules being considered contains P/PM^j, the finiteness of P/PM^j implies that there can only be a finite number of them. Thus, $\mathfrak{n}(P)$ is finite and our proof is complete.

COROLLARY 4. *If L is finite-dimensional over K and is either a *-algebra or a symmetric, commutative algebra, and if R is a discrete valuation ring with finite residue class field, then any order in L has finite class number.*

9. Commutativity modulo the nil radical. We will prove the following theorem.

THEOREM 5. *Let L be a finite-dimensional, symmetric algebra with 1 over the quotient field K of the valuation ring R. Suppose that L is commutative modulo its radical. Let P be an order in L with the property that, if a module has one order in $[P]$, then it has both orders in $[P]$. Then $\mathfrak{n}(P) = 1$ if and only if $(P^\#)^2$ has order P.*

We shall proceed with a series of lemmas, but first, we need some definitions. Let A and B be modules. Then, we define

$$(A:B)_{\mathrm{l}} = \{x \in L \mid xB \subseteq A\} \qquad \text{and} \qquad (A:B)_{\mathrm{r}} = \{x \in L \mid Bx \subseteq A\}$$

to be the *left* and *right conductors*, respectively, of A in B. When R is a Prüfer ring, both these conductors are modules (see [**4**, Lemma 2]). Further, it is straightforward to verify that

$$(AB)^\# = (A^\#:B)_{\mathrm{r}} = (B^\#:A)_{\mathrm{l}}. \tag{5}$$

Let A have left order P. Then $A^{-1} = \{x \in L \mid Ax \subseteq P\} = (P:A)_{\mathrm{r}}$. Then, using (5) and assuming that R is a valuation ring (so that modules are equal to their double dual), we see that

$$(A^{-1})^\# = ((P:A)_{\mathrm{r}})^\# = (P^\#A)^{\#\#} = P^\#A. \tag{6}$$

Similarly, $(A^{-1})^\# = AQ^\#$, where Q is the right order of A.

We generalize a lemma of Krull [**1**, Lemma 1.3.2].

LEMMA 9 (Krull [**1**, Lemma 1.3.2]). *Let L have nil radical N and assume that L/N is commutative. Let A and B be modules in L such that $A^2 \subseteq A$ and $AB = B$. Then $1 \in A$, i.e., A is an order.*

Proof. Assume first, that $N = 0$, so that L is commutative. Let $b_1, \ldots, b_s$ be a basis of B over R. Then

$$b_i = \sum_{j=1}^{s} a_{ij} b_j$$

for each i, with $a_{ij} \in A$, for each i and j. Then,

$$\sum_{j=1}^{s} (a_{ij} - \delta_{ij}) b_j = 0 \quad \text{for each } i,$$

where δ_{ij} is the Kronecker delta. This implies that

$$(\det (a_{ij} - \delta_{ij})) b_k = 0$$

for every $k = 1, \ldots, s$. Since $B \cap K$ is not zero, we see that

$$\det (a_{ij} - \delta_{ij}) = 0.$$

The result in the commutative case now follows by expanding the determinant and from the fact that $A^2 \subseteq A$.

Now we consider the general case. Write $\bar{A} = A \pmod{N}$ and $\bar{x} = x \pmod{N}$ for any $x \in L$. Then the $\bar{b}_i$ generate $\bar{B}$ and $\bar{B} \cap K \neq 0$. The above commutative argument applied to L/N shows that $\bar{1} \in \bar{A}$; thus, $1 = a + n$ with $a \in A$ and $n \in N$. Let A have left order P. Then $A^2 \subseteq A$ implies that $A \subseteq P$. Thus, $n = 1 - a \in P$. Since $n^t = 0$ for some integer t, we have

$$a^{-1} = (1 - n)^{-1} = \sum_{i=0}^{t-1} n^i \in P.$$

Thus, $1 = a^{-1}a \in PA = A$, and our proof is complete.

LEMMA 10. *Let L be symmetric with nil radical N. Let R be a valuation ring. Let $A = {}_P A_Q$ be a module in L. Then for the following four statements:*

(1) *A is invertible,*

(2) $A^{-1} = {}_Q(A^{-1})_P$,

(3) $P^\# A A^{-1} = P^\#$ $(A^{-1} A Q^\# = Q^\#)$,

(4) $A^{-1} P^\# = A^\#$ $(Q^\# A^{-1} = A^\#)$,

(1) $\Rightarrow$ (2) $\Rightarrow$ (3); (1) $\Rightarrow$ (4). *Further, if L/N is commutative, then all four statements are equivalent.*

Proof. (1) $\Rightarrow$ (2). This is the corollary to Lemma 4.

(2) $\Rightarrow$ (3). Since $AA^{-1}x \subseteq P$ if and only if $A^{-1}x \subseteq A^{-1}$, then

$$(P\colon AA^{-1})_r = \text{the right order of } A^{-1} = P.$$

Taking duals, and using (6), we see that

$$P^\# = ((P: AA^{-1})_r)^\# = P^\# AA^{-1}.$$

(1) $\Rightarrow$ (4). Multiply $AA^\# = P^\#$ on the left by A^{-1}.

We complete the proof by showing that (3) $\Rightarrow$ (1) and (4) $\Rightarrow$ (1) when L/N is commutative. Now, $(AA^{-1})^2 \subseteq AA^{-1}P = AA^{-1}$. By (3), $P^\# AA^{-1} = P^\#$, and multiplying (4) by A on the left implies that $AA^{-1}P^\# = P^\#$. It now follows from Lemma 9 that $1 \in AA^{-1}$; similarly, $1 \in A^{-1}A$. Thus, our proof is complete.

COROLLARY 5. *With the assumptions as in Lemma* 10 (*L/N commutative*), *a module* $A = {}_P A_Q$ *is principal if and only if* $P^\# A = {}_P(P^\# A)_Q$.

Proof. By Lemma 10, A principal means that $A^{-1} = {}_Q(A^{-1})_P$, i.e., that $(A^{-1})^\# = {}_P(A^{-1})^\#{}_Q$ by Lemma 1. But, by (6), $(A^{-1})^\# = P^\# A$, and our proof is complete.

We can now complete the proof of Theorem 5 as follows. Substituting $A = P^\#$ in Corollary 5, we see that $P^\#$ is principal if and only if $(P^\#)^2$ has order P. This is equivalent to $\mathfrak{n}(P) = 1$ by Theorem 2, and the proof is complete.

Theorem 5 globalizes to the following result.

COROLLARY 6. *Let L be a finite-dimensional, symmetric algebra with* 1 *over the quotient field K of a Prüfer ring R. Suppose that L is commutative modulo its nil radical. Let P be an order in L with the property that if a module has one order in* $[P]$ *it has both orders in* $[P]$. *Then every module with orders in* $[P]$ *is invertible if and only if* $(P^\#)^2$ *has order P.*

We remark, finally, that Corollary 6 was proved by Faddeev [**2**] for L separable and commutative and R Dedekind. Lemma 10 involves some of his results.

REFERENCES

1. E. C. Dade, O. Taussky, and H. Zassenhaus, *On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field*, Math. Ann. *148* (1962), 31–64.

2. D. K. Faddeev, *An introduction to the multiplicative theory of modules of integral representations*, Trudy Mat. Inst. Steklov. *80* (1965), 145–182.

3. ——— *On the theory of cubic Z-rings*, Trudy Mat. Inst. Steklov. *80* (1965), 183–187.

4. H. E. Gorman, *Invertibility of modules over Prüfer rings*, Illinois J. Math. *14* (1970), 283–298.

5. ——— *The Brandt Condition and invertibility of modules*, Pacific J. Math. *32* (1970), 351–372.

6. I. Kaplansky, *Submodules of quaternion algebras*, Proc. London Math. Soc. (3) *19* (1969), 219–232.

Stanford University,
Stanford, California