ON LATTICES IN A MODULE OVER A MATRIX ALGEBRA

Nobuo Nobusawa

(received August 8, 1965)

1. Introduction. Let A be the matrix algebra of type $n \times n$ over a finite algebraic number field F, and V the module of matrices of type $n \times m$ over F. V is naturally an A-left module. Given a non-singular symmetric matrix S of type $m \times m$ over F, we have a bilinear mapping f of V on A such that $f(x, y) = xSy'$ for elements x and y in V where y' is the transpose of y. In this case, corresponding to the arithmetic of $A([1])$, the arithmetical theory of V will be discussed to some extent as we establish the arithmetic of quadratic forms over algebraic number fields ([2]). In this note, we shall define a lattice in V with respect to a maximal order in A and determine its structure (Theorem 1), and after giving a structure of a complement of a lattice (Theorem 2), we shall give a finiteness theorem of class numbers of lattices under some assumption (Theorem 3).

2. Definition and structure of a lattice. The matrix unit ε_{11} in A whose entries are all zero except the 1-1 entry 1 is used very effectively and will be denoted simply by ε. Consider εV and $\varepsilon A \varepsilon = F\varepsilon$. The latter is isomorphic to F and the former may be considered as a vector space over the latter; namely εV may be considered as a quadratic space over an algebraic number field $F\varepsilon$ in the sense of [2]. The structure of V as an A-module is easily derived from that of εV since $V = A \varepsilon V$. However, arithmetical properties of V are not so simply obtained from those of εV, since the arithmetic of V depends on maximal orders in A. Let us take and fix a maximal order $\mathcal{O}$ in A throughout this note.

Canad. Math. Bull. vol. 9, no. 1, 1966

https://doi.org/10.4153/CMB-1966-007-4 Published online by Cambridge University Press

Definition. A system of elements $x_1, \ldots, x_m$ in V is said to be a basis of V (over A) if $V = Ax_1 + \ldots + Ax_m$ is a direct sum of A-submodules Ax_i and if each Ax_i is a minimal A-left module.

When $\varepsilon x = x$ for an element x in V, we say x is ε-invariant. If all x_i of a basis of V are ε-invariant, we say the basis is an ε-invariant basis.

Definition. A subset L of V is said to be an $\mathcal{O}$-lattice if 1) L is an $\mathcal{O}$-left module, 2) L contains a basis of V, and 3) for a basis $x_1, \ldots, x_m$, there exists an element φ in F such that $\varphi L \subset \mathcal{O}x_1 + \ldots + \mathcal{O}x_m$.

Obviously the property 3) does not depend on a choice of a basis. Also, we see that for any basis $x_1, \ldots, x_m$, there exists an element ρ in F such that $\rho x_1, \ldots, \rho x_m$ is a basis of V contained in the lattice L. This shows that any $\mathcal{O}$-lattice contains an ε-invariant basis.

THEOREM 1. Given an $\mathcal{O}$-lattice L, there exists an ε-invariant basis $e_1, \ldots, e_m$ such that $L = \mathcal{Q}_1 e_1 + \ldots + \mathcal{Q}_m e_m$ with some $\mathcal{O}$-left ideals $\mathcal{Q}_i$ in A which satisfy $\mathcal{Q}_i \varepsilon \subset \mathcal{Q}_i$ for $i = 1, \ldots, m$.

Proof. Let $x_1, \ldots, x_m$ be an ε-invariant basis of V which is contained in L. Put $U = Ax_2 + \ldots + Ax_m$. Let $A_1 = \{\tau \in A \mid \tau x_1 \in L + U\}$. Then $L \equiv A_1 x_1 \mod U$. Put $\mathcal{Q}_1 = A_1 \varepsilon + \mathcal{O}\varepsilon_{22} + \ldots + \mathcal{O}\varepsilon_{nn}$ where ε_{ii} are matrices whose entries are all zero except the i-i entries 1. We shall show that $\mathcal{Q}_1$ is an $\mathcal{O}$-left ideal in A. $\mathcal{Q}_1$ is clearly an $\mathcal{O}$-left module, and it contains $\mathcal{O}$, since $A_1 \supset \mathcal{O}$ and $\mathcal{Q}_1 \supset \mathcal{O}\varepsilon + \mathcal{O}\varepsilon_{22} + \ldots + \mathcal{O}\varepsilon_{nn}$. Take φ in F such that $\varphi L \subset \mathcal{O}x_1 + \ldots + \mathcal{O}x_m$. Then $\varphi \mathcal{Q}_1 x_1 = \varphi \mathcal{Q}_1 \varepsilon x_1 = \varphi A_1 x_1 \subset \mathcal{O}x_1 = \mathcal{O}\varepsilon x_1$. Therefore $\varphi \mathcal{Q}_1 \varepsilon \subset \mathcal{O}\varepsilon$, since x_1 is ε-invariant and

https://doi.org/10.4153/CMB-1966-007-4 Published online by Cambridge University Press

Ax_1 is isomorphic to $A\varepsilon$ as a minimal left A-module. Take θ in F such that $\theta\varepsilon \in \mathfrak{O}$ and $\theta\varphi\varepsilon_{ii} \in \mathfrak{O}$ for $i = 2, \ldots, n$). Then $\theta\varphi\mathfrak{a}_1 \subset \mathfrak{O}\theta\varepsilon + \mathfrak{O}\theta\varphi\varepsilon_{22} + \ldots + \mathfrak{O}\theta\varphi\varepsilon_{nn} \subset \mathfrak{O}$ and $\mathfrak{a}_1$ is an $\mathfrak{O}$-left ideal as asserted. Obviously $\mathfrak{a}_1\varepsilon \subset \mathfrak{a}_1$, and $L \equiv \mathfrak{a}_1 x_1 \bmod U$. Now consider $\mathfrak{a}_1^{-1}$ in the sense of ideal theory in $A([1])$. We can take $\alpha_1, \ldots, \alpha_r$ in $\mathfrak{a}_1$ and $\beta_1, \ldots, \beta_r$ in $\mathfrak{a}_1^{-1}$ such that $\beta_1\alpha_1 + \ldots + \beta_r\alpha_r = 1$, because $\mathfrak{a}_1^{-1}\mathfrak{a}_1$ is a maximal order which naturally contains 1. If we put $\alpha_i x_1 = \ell_i + u_i$ with ℓ_i in L and u_i in U, then $x_1 = \Sigma\beta_i\ell_i + \Sigma\beta_i u_i$. Since $\varepsilon x_1 = x_1$, $x_1 = \Sigma\varepsilon\beta_i\ell_i + \Sigma\varepsilon\beta_i u_i$. Now put $e_1 = \Sigma\varepsilon\beta_i\ell_i$. It is ε-invariant, and $\mathfrak{a}_1 e_1 = \mathfrak{a}_1(\Sigma\varepsilon\beta_i\ell_i) = \mathfrak{a}_1\varepsilon(\Sigma\beta_i\ell_i) \subset \mathfrak{a}_1(\Sigma\beta_i\ell_i) \subset \mathfrak{a}_1\mathfrak{a}_1^{-1}L = \mathfrak{O}L = L$. Since $\mathfrak{a}_1 x_1 \equiv \mathfrak{a}_1 x_1 \equiv L \bmod U$, $L = \mathfrak{a}_1 e_1 + L \cap U$ (direct). Now $L \cap U$ is an $\mathfrak{O}$-lattice in U, and we can complete the proof of Theorem 1 by induction on the number of basis elements.

3. Complement of a lattice.

Definition. $L^* = \{t \in V \mid f(x,t) \in \mathfrak{O}\mathfrak{O}' \text{ for all } x \text{ in } L\}$ is called a complement of L, where $\mathfrak{O}'$ is the transpose of $\mathfrak{O}$.

If $e_1, \ldots, e_m$ is an ε-invariant basis, we can find an ε-invariant basis $e_1^*, \ldots, e_m^*$ such that $f(e_i, e_j^*) = \varepsilon$ or 0 according as $i = j$ or $i \neq j$ by the well known argument in εV. We call $e_1^*, \ldots, e_m^*$ a dual basis of $e_1, \ldots, e_m$.

THEOREM 2. If $L = \mathfrak{a}_1 e_1 + \ldots + \mathfrak{a}_m e_m$ as in Theorem 1, then $L^* = \mathfrak{a}_1^* e_1^* + \ldots + \mathfrak{a}_m^* e_m^*$ where $e_1^*, \ldots, e_m^*$ is a dual basis of $e_1, \ldots, e_m$ and $\mathfrak{a}_i^*$ are $\mathfrak{O}$-left ideals such that $\mathfrak{a}_i(\mathfrak{a}_i^*)' = \mathfrak{O}\mathfrak{O}'$ in the groupoid of normal ideals of A, where $(\mathfrak{a}_i^*)'$ are the transposes of $\mathfrak{a}_i^*$.

https://doi.org/10.4153/CMB-1966-007-4 Published online by Cambridge University Press

Proof. We have $f(L, \mathfrak{a}_i^* e_i^*) = f(\mathfrak{a}_i e_i, \mathfrak{a}_i^* e_i^*)$ $= \mathfrak{a}_i \varepsilon (\mathfrak{a}_i^*)' \subset \mathfrak{a}_i (\mathfrak{a}_i^*)' = \mathcal{O}\mathcal{O}'$. On the other hand, if $f(L, \alpha e_i^*) \subset \mathcal{O}\mathcal{O}'$, then $\mathfrak{a}_i \varepsilon \alpha' \subset \mathcal{O}\mathcal{O}'$ and $\varepsilon\alpha' \in \mathfrak{a}_i^{-1} \mathcal{O}\mathcal{O}'$ $= (\mathfrak{a}_i^*)'$. Therefore, $\alpha\varepsilon \in \mathfrak{a}_i^*$, and $\alpha e_i^* = \alpha\varepsilon e_i^* \in \mathfrak{a}_i^* e_i^*$, which proves Theorem 2.

COROLLARY. $(L^*)^* = L$.

4. Finiteness of class number of lattices. For an $\mathcal{O}$-lattice L, we consider εL. It is an $I\varepsilon$-module contained in εV, where I denotes the ring of all algebraic integers of F. Clearly, εL contains a basis of εV over $F\varepsilon$, namely an ε-invariant basis of V contained in L. If $L = \mathfrak{a}_1 e_1 + \ldots + \mathfrak{a}_m e_m$ as before, then $\varepsilon L = \varepsilon \mathfrak{a}_1 e_1 + \ldots + \varepsilon \mathfrak{a}_m e_m$. We can take an element φ in F such that $\varphi\varepsilon \mathfrak{a}_i \subset \mathcal{O}[I]$, where $\mathcal{O}[I]$ is the maximal order in A consisting of all matrices whose entries are algebraic integers in F. Then $\varphi\varepsilon\mathfrak{a}_i e_i$ $= \varphi\varepsilon \mathfrak{a}_i \varepsilon e_i \subset \varepsilon \mathcal{O}[I] \varepsilon e_i = I e_i$. Therefore $\varphi\varepsilon L \subset I e_1 + \ldots + I e_m$, which shows that εL is a lattice in a quadratic space εV in the usual sense [2].

Definition. We say L is integral if $f(L, L) \subset \mathcal{O}\mathcal{O}'$.

This definition is equivalent to $L \subset L^*$, where L^* is the complement of L. Now we consider an $\mathcal{O}$-lattice $\mathcal{O}\varepsilon L$. It is not necessarily contained in L, but we can take an element μ in F such that $\mathcal{O}\mu\varepsilon L \subset L$. When L is integral, $\mathcal{O}\mu\varepsilon L$ is naturally integral.

Definition. The volume of εL in sense of [2; p. 229] is called the ε-volume of L.

Lastly, a class of $\mathcal{O}$-lattices is introduced in a natural way. An A-automorphism T of an A-module V is called an automorphism of V if it satisfies $f(T(x), T(y)) = f(x, y)$. We say that two $\mathcal{O}$-lattices belong to the same class if and only if they are mapped into each other by some automorphisms of V.

https://doi.org/10.4153/CMB-1966-007-4 Published online by Cambridge University Press

If L and L' belong to the same class, then εL and $\varepsilon L'$ belong to the same class in εV in sense of [2], and conversely. For, an automorphism of V induces an automorphism of εV, and an automorphism of εV can be extended to that of V for $V = A \varepsilon V$. In this case, $\mathcal{O} \varepsilon L$ and $\mathcal{O} \varepsilon L'$ naturally belong to the same class. Now we have the last theorem.

THEOREM 3. The number of classes of all integral $\mathcal{O}$-lattices with the same ε-volume is finite.

Proof. Let L be an integral $\mathcal{O}$-lattice with the given ε-volume. Then we can take μ in F such that $\mathcal{O}\mu\varepsilon L \subset L$ as above. Here the choice of μ does not depend on L; namely we could choose μ such that $\mu\varepsilon \in \mathcal{O}$. Next, we take an element ν in I such that $\nu\mathcal{O} \subset \mathcal{O}[I]$. Then $\mathcal{O}\mu\nu\varepsilon L \subset L$, and $\mu\nu\varepsilon L$ is integral in εV, since $f(\mu\nu\varepsilon L, \mu\nu\varepsilon L) \subset I\varepsilon$. Since $\mu\nu\varepsilon L$ has a fixed volume and it is an integral lattice, it can belong to only a finite number of classes in εV by [2; p. 309]. Therefore, $\mathcal{O}\mu\nu\varepsilon L$ can belong to only a finite number of classes in V. Let us denote these finite number of classes by $K_1, \ldots, K_t$. Then for any automorphism T of V, $T(\mathcal{O}\mu\nu\varepsilon L) = T'(K_i)$ for some automorphism T' and some i $(1 \leq i \leq t)$. Then $S(\mathcal{O}\mu\nu\varepsilon L) = K_i$ with $S = T'^{-1}T$. Therefore $K_i \subset S(L)$. On the other hand, $S(L) \subset K_i^*$ since $S(L) \subset S(L)^* \subset K_i^*$. However, there are only a finite number of $\mathcal{O}$-lattices between K_i and K_i^*, because K_i and K_i^* are finite I-modules. This completes the proof of Theorem 3.

REFERENCES

1. M. Deuring, Algebren, Chelsea, 1948.

2. O. T. O'Meara, Introduction to quadratic forms, Springer, 1963.

University of Alberta, Calgary
and
Summer Research Institute, Canadian Mathematical Congress

https://doi.org/10.4153/CMB-1966-007-4 Published online by Cambridge University Press