On Arithmetic of Certain Matrix Algebras

By Hisaichi MIDORIKAWA

Department of Mathematics, Tsuda College

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1995)

1. Introduction. Let $GL(n, \boldsymbol{C})$ be the group of all invertible matrices of degree n with entries in the complex number field $\boldsymbol{C}$. An element A in $GL(n, \boldsymbol{C})$ is called *regular* if the centralizer T of A in $GL(n, \boldsymbol{C})$ forms a maximal split torus of the reductive group $GL(n, \boldsymbol{C})$. By $GL(n, \boldsymbol{Z})$ we denote the modular group of degree n over the ring of integers $\boldsymbol{Z}$. Let ζ be a regular element in $GL(n, \boldsymbol{Z})$ and $R = \boldsymbol{Z}[\zeta]$ the ring generated by ζ over $\boldsymbol{Z}$. We shall define as follows the ideal class semigroup $\boldsymbol{G}$ of R. An ideal $\mathfrak{a}$ of R is *nonsingular* if the index $(R : \mathfrak{a})$ of additive subgroup $\mathfrak{a}$ of R is finite. $N\mathfrak{a} = (R : \mathfrak{a})$ is called *the norm* of $\mathfrak{a}$. Let $\boldsymbol{Q}[\zeta]$ be the ring generated by ζ over the rational number field $\boldsymbol{Q}$. A R-submodule $\mathfrak{a}$ of $\boldsymbol{Q}[\zeta]$ is called a *fractional ideal* if there exists an invertible element α in $\boldsymbol{Q}[\zeta]$ such that $\alpha\mathfrak{a}$ is a nonsingular ideal of R. Let $\boldsymbol{A}$ be the set of all fractional ideals of R. $\boldsymbol{A}$ is a semigroup with the canonical multiplication. The group $\boldsymbol{Q}[\zeta]^{\times}$ of all invertible elements in $\boldsymbol{Q}[\zeta]$ acts on the set $\boldsymbol{A}$. We classify $\boldsymbol{A}$ into the orbit classes under $\boldsymbol{Q}[\zeta]^{\times}$. The set of these classes forms a semigroup $\boldsymbol{G}$ which will be called *the ideal class semigroup* of R (cf. [17]).

We recall that these algebras $R = \boldsymbol{Z}(\zeta)$ and the ideal class semigroups $\boldsymbol{G}$ of these algebras have already been studied in [14],[22], where a bijective mapping of $\boldsymbol{G}$ to the set of conjugacy classes $G_Z(f)/GL(n, \boldsymbol{Z})$ given in the following sense. Let $f(X)$ be the characteristic polynomial of ζ (which has only simple roots as ζ is regular). $G_Z(f)$ is the set of elements of $GL(n, \boldsymbol{Z})$ with the chracteristic polynomial $f(X)$, which is decomposed into $GL(n, \boldsymbol{Z})$ orbit classes, the action of an element of $GL(n, \boldsymbol{Z})$ being adjoint action. $G_Z(f)/GL(n, \boldsymbol{Z})$ means the orbit space. The finiteness of the space $G_Z(f)/GL(n, \boldsymbol{Z})$ has been proved by [19] ,[23](cf. also the related works [15], [21],[12] and [8]).

The purpose of this note is to develop the arithmetic of R and to introduce in particular Dirichlet series which can be utilized to calculate $|\boldsymbol{G}|$. The methods we have used in [17] are found here useful. The detailed discussion with proof will appear elsewhere.

We remind that zeta functions of various kinds have been introduced into the study of algebras in the papers [2]-[4], [6], [9]-[11], [13] and [20]. Particularly, Solomon's idea in dealing with group algebras in [20] and its generalization by Bushnell-Reiner [2], [3], concerning semisimple $\boldsymbol{Q}$-algebras, have given suggestions for this paper.

We shall define the norm in the ring $\boldsymbol{Q}[\zeta]$. Let T be the centralizer of ζ in $GL(n, \boldsymbol{C})$. We can choose a subset

$$\Omega = \{\zeta, \zeta', \dots, \zeta^{(n-1)}\}$$

of T satisfying

$$(1.1) \quad \Delta(\zeta) = \prod_{0 \le i < j < n} (\zeta^{(i)} - \zeta^{(j)}) \in GL(n, \boldsymbol{C}).$$

Ω is the set of algebraic conjugates of ζ. By (1.1) we can prove that the characteristic polynomial $f(X)$ of ζ is factorized as

$$(1.2) \quad f(X) = (X - \zeta)(X - \zeta') \cdots (X - \zeta^{(n-1)}).$$

Let α be an element in $\boldsymbol{Q}[\zeta]$ and $p[X]$ a polynomial with degree $< n$ satisfying $\alpha = p(\zeta)$. We define i-th conjugate $\alpha^{(i)}$ by $\alpha^{(i)} = p(\zeta^{(i)})$. The norm $N\alpha$ is defined by

$$N\alpha = \alpha\alpha' \cdots \alpha^{(n-1)}.$$

Finally we shall state the properties of the ring of integers O and of the unit group $\boldsymbol{E}_O$ of $\boldsymbol{Q}[\zeta]$. Bearing in mind that all eigenvalues of ζ are mutually distinct we see that $f(X)$ is decomposed into irreducible divisors

$$f_1(X), f_2(X), \dots, f_g(X)$$

over $\boldsymbol{Z}$ with multiplicity one. We put $h_i(X) = f(X)/f_i(X)$. Then there exist the polynomials $u_1(X), u_2(X), \dots, u_g(X)$ with rational coefficients such that

$$\sum_{i=1}^{g} u_i(X) h_i(X) = 1.$$

We put $e_i = u_i(\zeta) h_i(\zeta)$. Then we have

(1.3) $\quad 1 = \sum_{i=1}^{g} e_i$, *and* $e_i e_j = \delta_{i,j} e_i$

where $\delta_{i,j}$ is Kronecker delta. Let ζ_i be the restriction of $\boldsymbol{Q}$-linear endomorphism ζ of $\boldsymbol{Q}[\zeta]$ to $\boldsymbol{Q}[\zeta]e_i$. Then we have $\boldsymbol{Q}[\zeta]e_i = \boldsymbol{Q}[\zeta_i]e_i$. Furthermore ζ_i is a root of the irreducible polynomial $f_i(X)$. Therefore $k_i = \boldsymbol{Q}[\zeta_i]$ is an algebraic number field over $\boldsymbol{Q}$, and the ring $\boldsymbol{Q}[\zeta]$ is decomposed as

(1.4) $\quad \boldsymbol{Q}[\zeta] = k_1 e_1 \oplus k_2 e_2 \oplus \cdots \oplus k_g e_g.$

Since e_i is a root of the monic polynomial $X^2 - X$ in $\boldsymbol{Z}[X]$, e_i belongs to O. Let O_i be the ring of integers of k_i. Then we have

(1.5) $\quad O = O_1 e_1 \oplus O_2 e_2 \oplus \cdots \oplus O_g e_g.$

The following lemma is crucial to study the structure of the ring $\boldsymbol{Q}[\zeta]$ (cf. Cororally 4.7, [17]).

Lemma 1.1. *Let* $\alpha = \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_g e_g$ *be the decomposition of* α *in* $\mathbf{Q}[\zeta]$ *as in* (1.4). *Then we have*

$$N\alpha = N_{k_1}\alpha_1 N_{k_2}\alpha_2 \cdots N_{k_g}\alpha_g \times 1_n$$

where 1_n *is the identity matrix of degree* n.

We define the unit group $\boldsymbol{E}_O$ of $\boldsymbol{Q}[\zeta]$ by

(1.6) $\quad \boldsymbol{E}_O = \{\varepsilon \in O : N\varepsilon = \pm 1\}.$

Let $\boldsymbol{E}_i$ be the unit group of the algebraic number field k_i. By Lemma 1.1 $\boldsymbol{E}_O$ is decomposed as

(1.7) $\quad \boldsymbol{E}_O = \boldsymbol{E}_1 e_1 \oplus \boldsymbol{E}_2 e_2 \oplus \cdots \oplus \boldsymbol{E}_g e_g.$

It is well known that the unit group $\boldsymbol{E}_i$ is a direct product of a finite group and a free abelian group (cf. [1] or [5]). Hence by (1.7) $\boldsymbol{E}_O$ is a direct product of a finite group H_O and free abelian group E_O. We remark that the rank of E_O is equal to $r + c - g$ where r (resp. $2c$) is the number of all real (resp. complex) roots of $f(X)$.

2. Reduction theorem. Let $C(\mathfrak{a})$ be a fixed class in $\boldsymbol{G}$ represented by an integral ideal $\mathfrak{a}$ of $\boldsymbol{R}$. The *pseudo inverse ideal* $\breve{\mathfrak{a}}$ of $\mathfrak{a}$ is defined by

$$\breve{\mathfrak{a}} = \{\mu \in \boldsymbol{Q}[\zeta] : \mu\mathfrak{a} \subset R\}.$$

$\breve{\mathfrak{a}}$ is a fractional ideal of $\boldsymbol{R}$. Let R_i be the subring of $\boldsymbol{Q}(\zeta_i)$ defined by $Re_i = R_i e_i$. R_i is generated by ζ_i over $\boldsymbol{Z}$. We put

$$R^{\oplus} = R_1 e_1 \oplus R_2 e_2 \oplus \cdots \oplus R_g e_g.$$

$R^{\oplus}$ is a subring of O with finite index. In the same manner as we have defined $R^{\oplus}$, we can define $\mathfrak{a}^{\oplus}$ and $\breve{\mathfrak{a}}^{\oplus}$. $\mathfrak{a}^{\oplus}$ (resp. $\breve{\mathfrak{a}}^{\oplus}$) is an ideal (resp. a fractional ideal) of $R^{\oplus}$. Let $\boldsymbol{E}_{\mathfrak{a}}$ be the subgroup of $\boldsymbol{E}_O$ defined by

$$\boldsymbol{E}_{\mathfrak{a}} = \{\varepsilon \in \boldsymbol{E}_O : \varepsilon\mathfrak{a} \subset \mathfrak{a}\}.$$

Lemma 2.1. *The group index* $(\boldsymbol{E}_O : \boldsymbol{E}_{\mathfrak{a}})$ *is finite.*

Define $E_{\mathfrak{a}}$ and $H_{\mathfrak{a}}$ by

$$E_{\mathfrak{a}} = \boldsymbol{E}_{\mathfrak{a}} \cap E_O,\ H_{\mathfrak{a}} = \boldsymbol{E}_{\mathfrak{a}} \cap H_O.$$

$\boldsymbol{E}_{\mathfrak{a}}$ is a direct product of $E_{\mathfrak{a}}$ and $H_{\mathfrak{a}}$. Since $E_{\mathfrak{a}}$ stabilizes $\breve{\mathfrak{a}}^{\oplus}$, the set $\breve{\mathfrak{a}}^{\oplus}$ is classified in $E_{\mathfrak{a}}$-orbit classes. Let $(\breve{\mathfrak{a}}^{\oplus})^{\times}$ be the set of all invertible elements in $\breve{\mathfrak{a}}^{\oplus}$. $(\breve{\mathfrak{a}}^{\oplus})^{\times}/E_{\mathfrak{a}}$ is the set of all these orbit classes and $[\lambda]$ the class which is represented by λ in $(\breve{\mathfrak{a}}^{\oplus})^{\times}$.

Definition 2.1. *Let* B^* *be the character group of the finite group* $B = \breve{\mathfrak{a}}^{\oplus}/\breve{\mathfrak{a}}$. *For each* χ *in* B^* *we define a Dirichlet series* $L(s:\chi)$ *by*

$$L(s:\chi) = \sum_{[\lambda]\in(\breve{\mathfrak{a}}^{\oplus})^{\times}/E_{\mathfrak{a}}} \frac{\chi(\lambda \bmod \breve{\mathfrak{a}})}{(N\lambda\breve{\mathfrak{a}}^{\oplus})^{s}}.$$

We remark that $\chi(\lambda \bmod \breve{\mathfrak{a}})$ and hence $L(s:\chi)$ depend on the choice of the representatives λ. We shall consider for a moment a choice of these representatives as fixed.

Let $D^{\oplus}$ be the discriminant of the ring $R^{\oplus}$. $D^{\oplus}$ is given by

$$D^{\oplus} = \prod_{i=1}^{g} N_{k_i} f_i'(\zeta_i) \times 1_n.$$

Theorem. 2.2. *The series* $L(s:\chi)$ *is convergent on the complex half plane* $\Re(s) > 1$. *Furthermore we have*

$$\lim_{\sigma\to 1+0} (\sigma - 1)^g L(\sigma:\chi) = \begin{cases} \kappa(C), & \chi = 1 \\ 0, & \chi \neq 1 \end{cases}$$

where

$$\kappa(C) = \frac{2^{r+c}\pi^{c}(E_O : (E_{\mathfrak{a}})^{\oplus}) \mid R(E_O) \mid}{N\breve{\mathfrak{a}}^{\oplus}\, N\mathfrak{a}^{\oplus}\sqrt{\mid D^{\oplus} \mid}}.$$

The proof of this theorem is based on the standard method to calculate the density of ideals due to Dedekind and the Fourier analysis of one variable.

Definition 2.2. *Let* $C(\mathfrak{a})$ *be a fixed class in* $\boldsymbol{G}$. *We define the zeta function of the class* $C(\mathfrak{a})$ *by*

$$\zeta_C(s) = \sum_{\substack{\mathfrak{b}\in C(\mathfrak{a}) \\ \mathfrak{b}\subset R}} \frac{1}{(N\mathfrak{b})^{s}}.$$

The following reduction theorem is proved by the orthogonality relations of the characters of the finite group B (cf. Theorem 7.3, [7]).

Theorem 2.3. *We have*

$$\zeta_C(s) = \frac{((E_{\mathfrak{a}})^{\oplus} : E_{\mathfrak{a}})(N\mathfrak{a}^{\oplus})^{s}}{(\breve{\mathfrak{a}}^{\oplus} : \breve{\mathfrak{a}}) \mid H_{\mathfrak{a}} \mid (N\mathfrak{a})^{s}} \{ \sum_{\chi\in B^*} L(s:\chi)\}.$$

3. Main theorems. By Theorem 2.2 and Theorem 2.3 we can prove the following theorem.

Theorem 3.1. *Let* $\zeta_C(s)$ *be the zeta function of the class* $C(\mathfrak{a})$. *Then we have*

$$\lim_{\sigma\to 1+0}(\sigma-1)^g\zeta_C(s)=\frac{2^{r+c}\pi^c(\boldsymbol{E}_O:\boldsymbol{E}_{\mathfrak{a}})\,|\,R(\boldsymbol{E}_O)\,|}{N\check{\mathfrak{a}}N\mathfrak{a}\,|\,H_O\,|\,\sqrt{|\,D\,|}}$$

where $D=Nf'(\zeta)$ *is the discriminant of* R, $R(\boldsymbol{E}_O)$ *is the regulator of the unit group* $\boldsymbol{E}_O$, H_O *is the finite subgroup of* $\boldsymbol{E}_O$ *and* r (*resp.* $2c$) *is the number of all real* (*resp. complex*) *roots of* $f(X)$.

We define, for each ideal $\mathfrak{b}$ of R, $a(\mathfrak{b})$ by

$$a(\mathfrak{b})=\frac{N\mathfrak{a}N\check{\mathfrak{a}}}{(\boldsymbol{E}_O:\boldsymbol{E}_{\mathfrak{a}})}.$$

We see that $a(\mathfrak{b})$ is a class function (i.e. $a(\mathfrak{a})=a(\mathfrak{b})$ for all $\mathfrak{b}$ in $C(\mathfrak{a})$). Consequently by Theorem 4.1 we have the following.

Theorem 3.2. *Define a Dirichlet series* $\zeta_R(s)$ *by*

$$\zeta_R(s)=\sum_{\mathfrak{b}}\frac{a(\mathfrak{b})}{(N\mathfrak{b})^s}$$

where the summation runs over all nonsingular ideals of R. *Then* $\zeta_R(s)$ *is holomorphic on the complex half plane* $\mathfrak{R}(s)>1$, *and we have*

$$\lim_{\sigma\to 1+0}(\sigma-1)^g\zeta_C(\sigma)=|\,\boldsymbol{G}\,|\,2^{r+c}\pi^c\frac{|\,R(\boldsymbol{E}_O)\,|}{|\,H_O\,|\,\sqrt{|\,D\,|}}.$$

References

[1] Z. J. Borevich and I. R. Shafarevich: Number Theory. Academic Press (1964).

[2] C. J. Bushnell and I. Reiner: Zeta functions of arithemetic orders and Solomon's conjectures. Math., Z., **173**, 135–161 (1980).

[3] C. J. Bushnell and I. Reiner: L-functions of arithmetic orders and asymptotic distribution of ideals. J. reine angew. Math., **327**, 156–183 (1981).

[4] C. J. Bushnell and I. Reiner: Functional equations for L-functions for arithmetic order. J. reine angew. Math., **329**, 88–123 (1981).

[5] J. W. S. Cassels and A. Fröhlich: Algebraic Number Theory. Academic Press (1967).

[6] M. Eichler: Über die Idealklassenzahl total definiter Quaternionenalgebren. Math. Z., **43**, 102–109 (1938).

[7] W. Ellison and F. Ellison: Prime Numbers. Hermann, Paris (1975).

[8] A. Fröhlich: Locally free modules of arithmetic order. J. reine angew. Math., **274–275**, 112–138 (1975).

[9] T. Fujisaki: On L-functions of simple algebras over the field of rational numbers. J. Fac. Sci. Univ. Tokyo, Sect., **19**, 293–311 (1962).

[10] K. Hey: Analytische Zahlentheorie in System hyperkomplexer Zahlen. Diss., Hamburg (1929).

[11] Y. Hironaka: Zeta functions of integral group rings of metacyclic groups. Tsukuba J. Math., **5**, 267–283 (1981).

[12] H. Jacobinski: Genera and decomposition of lattice. Acta Mathematica, **121**, 1–29 (1968).

[13] M. Kinoshita: On ζ-functions of total matric algebra over the field of rational numbers. J. Math. Soc. Japan, **17** , 374–408 (1965).

[14] C. G. Latimer and C. C. MacDuffee: A correspondence between classes of ideals and classes of matrices. Ann. of Math., **34**, 313–316 (1933).

[15] J. M. Maranda: On the equivalence of representations of finite groups of automorphisms of modules over Dedekind rings. Canad. J. Math., **5**, 516–526 (1953).

[16] H. Midorikawa: On the number of regular elliptic conjugacy classes in the Siegel modular group of degree $2n$. Tokyo J. Math., **6**, 25–38 (1983).

[17] H. Midorikawa: Prime decompositions in a cyclotomic matrix ring over $\boldsymbol{Z}$ (preprint).

[18] M. Newman: Integral Matrices. Academic Press (1972).

[19] A. Speiser: Die Theorie der Gruppen von endlicher Ordnung. Berlin Aufl., **3** (1937).

[20] L. Solomon: Zeta-functions and integral representation theory. Adv. in Math., **26**, 306–326 (1977).

[21] S. Takahashi: Arithmetic of group representations. Tohoku Math. J., **11**, 216–246 (1959).

[22] O. Taussky: On a theorem of Latimer and MacDuffee. Canad. J. Math., **1**, 300–302 (1949).

[23] H. Zassenhaus: Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Áquivalenz endlicher ganzzahliger Substitutionsgruppen. Hamb. Abh., **12,** 276–288 (1937–1938).