NOTE ON THE IDEALS OF CYCLIC ALGEBRAS*

BY RALPH HULL

1. *Introduction.* The purpose of this note is the generalization of certain results in a recent paper by Latimer† on the number of ideals of given norm in a generalized quaternion algebra.

We consider rational cyclic division algebras D of prime degree $n(\geqq 2)$ over the field R of rational numbers. Let $\mathfrak{o}$ be any maximal order‡ of D. The reduced discriminant of $\mathfrak{o}$ is an invariant $\Delta = \Delta(D)$ of D called the discriminant of D, and is of the form $\Delta = \pm\sigma^{n(n-1)}$, where $\sigma = q_1 \cdots q_s$ is the product of the distinct rational primes $q_1 \cdots q_s$ which are ramified§ in D. For each such q, the two-sided ideal $q\mathfrak{o}$ is the nth power of an indecomposable two-sided prime ideal of $\mathfrak{o}$, and the q-adic extension D_q is a division algebra of degree n of R_q. For all other rational primes p, D_p is the algebra of all matrices of degree n over R_p and $\mathfrak{o}p$ is a two-sided prime ideal of $\mathfrak{o}$ having only one-sided ideal divisors.

By a (normal) ideal of D is meant an ideal (one or two-sided) with respect to some maximal order of D. Such an ideal is called integral if it is contained in its right or left order. We denote various maximal orders by $\mathfrak{o}, \mathfrak{o}_1, \mathfrak{o}_2, \cdots$, and an ideal $\mathfrak{a}$ by $\mathfrak{a}_{ij}$ if $\mathfrak{o}_i\mathfrak{a} = \mathfrak{a}\mathfrak{o}_j = \mathfrak{a}$ and it is necessary to indicate $\mathfrak{o}_i$ and $\mathfrak{o}_j$. The (reduced) norm of an ideal is an ideal of R such that, for a principal ideal $\alpha\mathfrak{o}$ (or $\mathfrak{o}\alpha$), α in D, $N(\alpha\mathfrak{o})$ (or $N(\mathfrak{o}\alpha)) = (N(\alpha))$, where $N(\alpha)$ is the reduced norm corresponding to the rank equation of degree n. Our object is to prove the following result.

THEOREM. *Let $\mathfrak{o}$ be any maximal order of D and let A be any rational integer. Write $A = A_1A_0$, where A_0 is prime to $\Delta(D)$ and every prime factor of A_1 divides $\Delta(D)$. Then the number of integral*

* Presented to the Society, April 9, 1937.

† C. G. Latimer, Transactions of this Society, vol. 40 (1936), pp. 439–450.

‡ Maximal orders for all D have been given explicitly. See Albert, this Bulletin, vol. 40 (1934), pp. 164–176, for $n=2$, and Hull, Transactions of this Society, vol. 38 (1935), pp. 515–530, for $n>2$.

§ We refer to Deuring, *Algebren*, Ergebnisse der Mathematik, Chapter VI, for all definitions and theorems used here except when explicit reference elsewhere is given.

$\mathfrak{o}$*-right ideals of norm* (A) *is equal to the number of classes of right associated integral matrices of degree* n *and determinant* A_0.

Two integral matrices M_1 and M_2 are said to be right associated* if there is an integral matrix U such that $|U| = \pm 1$ and $M_2 = M_1 U$. In case $n=2$, the number of such classes of matrices of given determinant A_0 is easily seen to be the sum of the divisors† of A_0.

2. *Preliminary Lemmas.* We need two lemmas easily obtained from the general ideal theory of linear algebras (Deuring, loc. cit.).

Let $\mathfrak{a} = \mathfrak{a}_{r+1,1}$ be an integral ideal and let

$$(1) \qquad N(a) = (A), \qquad A = p_r^{\gamma_r} \cdots p_1^{\gamma_1},$$

where the p's are distinct rational primes.

LEMMA 1. *The ideal* $\mathfrak{a} = \mathfrak{a}_{r+1,1}$ *has a special factorization*

$$(2) \qquad \mathfrak{a} = \overset{(r)}{\mathfrak{a}}_{r+1,r} \cdot \overset{(r-1)}{\mathfrak{a}}_{r,r-1} \cdots \overset{(1)}{\mathfrak{a}}_{2,1}, \quad \overset{(i)}{\mathfrak{a}} \text{ integral}, \quad N(\overset{(i)}{\mathfrak{a}}) = p_i^{\gamma_i}.$$

For a given order $p_r, \cdots, p_1$ *of the distinct prime divisors of* A *in* (1), *the special factorization* (2) *is unique.*

The existence of (2) is implied by the fact that there exists a factorization of $\mathfrak{a}$ into indecomposable ideals in which the order of the prime ideals to which the factors belong is arbitrarily assigned (Deuring, p. 106). To prove the uniqueness claimed we consider p-components and apply a theory due to Hasse (Deuring, pp. 94–107).

Let p be any rational prime. Then from (2)

$$(\mathfrak{a})_p = (\mathfrak{a}^{(r)})_p \cdots (\mathfrak{a}^{(1)})_p,$$

where $(\mathfrak{a})_p$ denotes the p-component, that is, p-adic limit set of $\mathfrak{a}$. If $(p, A) = 1$, $(\mathfrak{a})_p$ is a maximal order of D_p, and since $\mathfrak{o}_{r+1}\mathfrak{a} = \mathfrak{a}\mathfrak{o}_1 = \mathfrak{a}$, we have $(\mathfrak{a})_p = (\mathfrak{o}_{r+1})_p = (\mathfrak{o}_1)_p$. Similarly $(\mathfrak{a}^{(1)})_p = (\mathfrak{o}_2)_p = (\mathfrak{o}_1)_p$, $(\mathfrak{a}^{(2)})_p = (\mathfrak{o}_3)_p = (\mathfrak{o}_2)_p = (\mathfrak{o}_1)_p$, and so on, and it is clear that $(\mathfrak{a}^{(i)})_p = (\mathfrak{a})_p$, $(i=1, \cdots, r)$. If $p = p_i$, $(i=1, \cdots, r)$,

* MacDuffee, *The Theory of Matrices*, Ergebnisse der Mathematik, Chapter III.

† See Latimer, loc. cit.

we find in a similar way that $(\mathfrak{a}^{(r)})_p = \cdots = (\mathfrak{a}^{(i+1)})_p = (\mathfrak{o}_{r+1})_p$ and $(\mathfrak{a}^{(i-1)})_p = \cdots = (\mathfrak{a}^{(1)})_p = (\mathfrak{o}_1)_p$, whence $(\mathfrak{a}^{(i)})_p = (\mathfrak{a})_p$. Hence, for every rational prime p, the p-component of each $\mathfrak{a}^{(i)}$ is uniquely determined by $\mathfrak{a}$. It follows that each $\mathfrak{a}^{(i)}$ is uniquely determined by $\mathfrak{a}$ since each is determined by the totality of its p-components.

LEMMA 2. *If p is ramified in D, there is exactly one ideal of D_p of given norm p^ν. If p is not ramified in D, the number of right ideals of D_p with respect to a given maximal order of D_p, of given norm p^ν, is the number $\psi(p^\nu)$ of classes of right associated rational integral matrices of degree n and determinant p^ν.*

For the first part of Lemma 2 we have only to note that every ideal of D_p, p ramified in D, is a power of the single prime ideal of the unique maximal order of D_p. The second part is seen as follows. A maximal order $\mathfrak{o}_p$ of D_p, p not ramified in D, is of the form $\mathfrak{o}_p = \sum c_{ij}\mathfrak{g}_p$, where the c_{ij}, $(i, j = 1, \cdots, n)$, are matrix units and $\mathfrak{g}_p$ is the maximal order of R_p. Every $\mathfrak{o}_p$-right ideal is a principal ideal $\alpha\mathfrak{o}_p$, where α is of the form (Deuring, loc. cit. p. 101)

$$(3) \quad \alpha = p^{\mu_1}c_{11} + d_{21}c_{21} + p^{\mu_2}c_{22} + \cdots + d_{n1}c_{n1} + \cdots + p^{\mu_n}c_{nn},$$

where $\mu_1 + \mu_2 + \cdots + \mu_n = \nu$, and d_{ij} is uniquely determined modulo p^{μ_i}. The last part of the lemma is obvious from (3).

3. *Proof of the Theorem.* Since every integral ideal $\mathfrak{a}$ of norm (A), A as in (1), has the unique special factorization (2), we proceed to count the number of possible distinct sets $\mathfrak{a}^{(1)}, \cdots, \mathfrak{a}^{(r)}$ which yield an $\mathfrak{a}$.

Consider first $\mathfrak{a}^{(1)}$ whose right order is the fixed maximal order $\mathfrak{o}_1 = \mathfrak{o}$, of the theorem. For every rational prime $p \neq p_1$, we have $(\mathfrak{a}^{(1)})_p = (\mathfrak{o})_p$, and for $p = p_1$, $(\mathfrak{a}^{(1)})_p$ is a right ideal with respect to $(\mathfrak{o})_p$ of norm $p_1^{\nu_1}$. Thus $(\mathfrak{a}^{(1)})_p$ is unique for all $p \neq p_1$ and, by Lemma 2, there are precisely 1 or $\psi(p_1^{\nu_1})$ possibilities for $(\mathfrak{a}^{(1)})_{p_1}$ according as p_1 is ramified or unramified in D. Hence by an argument used in the proof of Lemma 1, there are precisely 1 or $\psi(p_1^{\nu_1})$ possibilities for the factor $\mathfrak{a}^{(1)}$ in the respective cases.

Suppose, next, that $\mathfrak{a}^{(1)}$ is fixed and consider $\mathfrak{a}^{(2)}$, whose right order $\mathfrak{o}_2$ is uniquely determined by $\mathfrak{a}^{(1)}$, since $\mathfrak{o}_2$ is the left order of $\mathfrak{a}^{(1)}$. The same argument made for $\mathfrak{a}^{(1)}$ and $\mathfrak{o}_1$ applies to $\mathfrak{a}^{(2)}$ and $\mathfrak{o}_2$, and we can proceed similarly with $\mathfrak{a}^{(3)}, \mathfrak{a}^{(4)}, \cdots$, successively. It is plain that the total number of sets $\mathfrak{a}^{(1)}, \cdots, \mathfrak{a}^{(r)}$ is $\prod\psi(p_j^{\nu_j})$, where j ranges over those of the integers $1, \cdots, r$ for which p_j is unramified in D, that is $\prod(p_j^{\nu_j}) = A_0$. To complete the proof of the theorem we have to show that $\prod\psi(p_j^{\nu_j}) = \psi(A_0)$. This follows from the following lemma.

LEMMA 3. *If $A = BC$, where A, B, C are rational integers such that $(B, C) = 1$, then $\psi(A) = \psi(B)\psi(C)$.*

To prove this lemma we apply the methods of §2 to the *simple* algebra S of all rational matrices of degree n. For a given system of matrix units c_{ij}, $(i, j = 1, \cdots, n)$, the set $\mathfrak{m} = \sum c_{ij}\mathfrak{g}$, where $\mathfrak{g}$ denotes the set of rational integers, is a maximal order of S. Every integral $\mathfrak{m}$-right ideal is a principal ideal (MacDuffee, loc. cit.) $\mathfrak{a} = M_1\mathfrak{m}$, where M_1 is an integral matrix and the reduced norm of $\mathfrak{a}$ is $(|M_1|) = (A)$, say. If also $\mathfrak{a} = M_2\mathfrak{m}$, then $M_2 = M_1 U$, U integral, $|U| = \pm 1$. Hence $\psi(A)$ is the number of integral $\mathfrak{m}$-right ideals of norm (A). In S, we have unique special factorizations* similar to those of Lemma 1. Hence if $A = BC$, we can count the number of $\mathfrak{m}$-right ideals of norm (A) by counting the number of right ideals, with respect to certain maximal orders of S, of norms (B) and (C). This yields the lemma.

4. *Applications of the Theorem.* In case the class number h of D is one,† our theorem yields interesting results concerning representations‡ by the norm form associated with a maximal order $\mathfrak{o}$ of D. Thus, if $h = 1$, every ideal of D is principal, $\mathfrak{a}_{ij} = \alpha\mathfrak{o}_j = \mathfrak{o}_i\beta$, α, β in D. If also, $a_{ij} = \alpha'\mathfrak{o}_j$, then $\alpha' = \alpha u$, where u is a unit of $\mathfrak{o}_j$, and the norm form associated with $\mathfrak{o}_j$ is universal. The number of sets of integral representations§ of A is $\psi(A_0)$. The representations of a set are connected by the automorphs of the form associated with the units of $\mathfrak{o}$.

UNIVERSITY OF MICHIGAN

* Every rational prime is unramified in S.

† M. Eichler, Journal für Mathematik, vol. 176 (1937), pp. 192–202, has proved general results on the class number of algebras which imply $h = 1$ for all D with $n > 2$ and for rational quaternion algebras with real splitting fields.

‡ Cf. L. E. Dickson, *Algebren und ihre Zahlentheorie*, §100.

§ We must have $A > 0$ for $n = 2$, D definite. In this case, the infinite prime spot of R is said to be ramified in D.