MAXIMAL ORDERS IN RATIONAL CYCLIC ALGEBRAS OF ODD PRIME DEGREE†

BY

RALPH HULL‡

1. **Introduction.** Throughout this paper R denotes the field of rational numbers and n is a fixed odd prime. We consider cyclic algebras of degree n, order n^2, over R, that is, algebras A of the following type:§

A has an R-basis of the form

$$u^i z_k \qquad (i = 0, \cdots, n-1;\ k = 1, \cdots, n), \tag{1}$$

where the z_k form an R-basis of a cyclic sub-corps Z of A of degree n over R and $1, u, \cdots, u^{n-1}$ form a Z-basis of A, with the relations

$$zu = uz^S \quad \text{for every } z \text{ of } Z, \tag{2}$$

where S is a generating element of the Galois group of Z over R and z^S is the element of Z corresponding to z under the automorphism S, and

$$u^n = \alpha \neq 0 \text{ in } R. \tag{3}$$

This is called a *cyclic generation* of A and is denoted by

$$A = (\alpha, Z, S). \tag{4}$$

Artin‖ has defined an order in a rational semi-simple algebra B as a subset I of elements of B with the following properties:

(a) The sum, difference, and product of any two elements of I are also in I.

(b) If b is any element of B there exists a rational integer μ such that μb is in I.

(c) The set I is of finite order, that is, there is a finite set of elements $a_1, a_2, \cdots, a_r$ of I such that every element a of I can be expressed in the form

$$a = \eta_1 a_1 + \cdots + \eta_r a_r$$

with rational integers $\eta_1, \cdots, \eta_r$.

† Presented to the Society, April 19, 1935; received by the editors March 13, 1935.

‡ National Research Fellow.

§ The description given here is that of Hasse: *Theory of cyclic algebras over an algebraic number field*, these Transactions, vol. 34 (1932), pp. 171–214. We shall refer to this paper hereafter as H. For complete bibliographies see H and the later paper by Hasse: *Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper*, Mathematische Annalen, vol. 107 (1933), p. 731.

‖ Artin, *Zur Arithmetik hyperkomplexer Zahlen*, Abhandlungen des Mathematischen Seminars, Hamburg Universität, vol. 5 (1927).

An order is called maximal if it cannot be imbedded properly in any other order. Suppose I is maximal in B. Then it can be shown that every element of I satisfies an equation with rational integral coefficients and highest coefficient 1, and also that I contains the modulus of B. Thus a maximal order is an integral set according to the definition of Dickson.†

The construction of an order in an algebra A is trivial. If, for example, in (3), α is a rational integer and the z_k in (1) are any basis of Z which is also a basis for the integers of Z, i.e., the unique maximal order in Z, then the totality of linear combinations of the basal units (1) with rational integral coefficients is an order in A which is independent of the particular basis $z_1, \cdots, z_n$ of the maximal order of Z and may be called the order in A associated with the cyclic generation (4) of A. An order thus associated with a particular cyclic generation of an algebra A is not in general a maximal order. The importance of constructing maximal orders in an algebra arises from the simplicity of the arithmetic in a maximal order as compared with that in a non-maximal order.

Albert‡ has determined explicitly maximal orders for every rational cyclic algebra of degree 2, that is, every rational generalized quaternion algebra Q. Following a similar plan but using more general methods we shall obtain maximal orders for every algebra A. First, by means of Hasse's theory of invariants of cyclic algebras we shall obtain for each A cyclic generations of an especially simple form. These will be called canonical generations. We shall then exhibit n distinct maximal orders in A containing the order in A associated with a given canonical generation in the manner described above. Finally, by a consideration of π-adic components at all rational prime spots π of R, we shall show that these are the only maximal orders in A which contain the order associated with a given canonical generation.

2. **Canonical generations of the algebras A.** An algebra A defined by a cyclic generation (4) clearly depends upon α, Z, and S but these are by no means uniquely determined by A, and a given A has infinitely many cyclic generations involving distinct sub-corps Z and, for a given Z, distinct α and S. All cyclic generations are determined by means of Hasse's theory of the invariants of a cyclic algebra (see H). A complete set of invariants of A consists of the degree n and the totality of the integers ν_π modulo n, where π ranges over all prime spots of R, defined in terms of the given generation (4) by

$$((\alpha, Z)/\pi) = S^{\nu_\pi},$$

where $((\alpha, Z)/\pi)$ is the norm residue symbol. A necessary and sufficient con-

† Dickson, *Algebren und ihre Zahlentheorie*, p. 198.

‡ Albert, *Integral domains in rational generalized quaternion algebras*, Bulletin of the American Mathematical Society, 1934, p. 164.

dition that A be a total matric algebra is that $\nu_\pi \equiv 0 \pmod{n}$ for every π. An algebra A is either a total matric algebra or a division algebra since n is a prime. We assume in this section that A is a division algebra. Then there are a finite number, s, of distinct primes $q_1, \cdots, q_s$ such that $\pi_{q_j} \not\equiv 0 \pmod{n}$ $(j = 1, \cdots, s)$ and

$$\sum_{j=1}^{s} q_j \equiv 0 \pmod{n}, \tag{5}$$

whereas $\nu_\pi \equiv 0 \pmod{n}$ for every π distinct from $q_1, \cdots, q_s$. In particular (5) shows that $s \geqq 2$. The primes $q_1, \cdots, q_s$ are characterized by the property that the q_j-adic fields R_{q_j} do not split A whereas R_π splits A for every other π. In the present case, n an odd prime, the single infinite prime spot π_∞ of R does not occur among the q_j since Z is real and hence R_{π_∞}, which is by definition the field of all real numbers, contains a subfield isomorphic to Z and so necessarily splits A. Thus $\sigma = q_1 \cdots q_s$ is a rational integer. For the purposes of this paper we now prove the existence of cyclic generations of A of the type, which we shall call canonical, described in

THEOREM 1. *Let A be a cyclic division algebra of odd prime degree n over R, and let $q_1, \cdots, q_s$ $(s \geqq 2)$ be the distinct rational primes at which A does not split. Let $\sigma = q_1 \cdots q_s$. Then there exist infinitely many rational primes p with the following properties: $p \equiv 1 \pmod{n}$ and is prime to σ; $q_1, \cdots, q_s$ are n-ic non-residues modulo p and σ is an n-ic residue modulo p; the unique cyclic field Z of degree n over R, of conductor (Führer) p, discriminant p^{n-1}, has an automorphism S such that (σ, Z, S) is a cyclic generation of A.*

We first prove the following

LEMMA.† *Let n be a fixed odd prime. If $q_1, \cdots, q_s$ $(s \geqq 2)$ are distinct rational primes and $\beta_2, \cdots, \beta_s$ are rational integers prime to n, then there exist infinitely many rational primes p with the following properties: $p \equiv 1 \pmod{n}$ and prime to σ; q_1 is an n-ic non-residue modulo p; there exist rational integers $y_2, \cdots, y_s$ such that*

$$q_1^{\beta_j} q_j \equiv y_j^n \pmod{p}. \tag{6}$$

To prove the lemma let ζ be a primitive nth root of unity and $K = R(\zeta)$. Let

$$\alpha_1 = q_1, \qquad \alpha_j = q_1^{\beta_j} q_j \qquad (j = 2, \cdots, s).$$

Suppose the quantity

† This lemma is similar to a lemma used by Artin in his proof of the general law of reciprocity. See Hasse's *Bericht*, II, Jahresbericht der Deutschen Mathematiker-Vereinigung, Ergänzungsband 6, p. 18.

$$P = \alpha_1^{x_1} \cdots \alpha_s^{x_s},$$

where $x_1, \cdots, x_s$ are rational integers, is the nth power of a quantity a of K. Then

$$P = a^n, \ a \text{ in } K,$$
$$P^{n-1} = N_{KR}(a^n) = (N_{KR}(a))^n.$$

Thus p^{n-1} is the nth power of the rational quantity $N_{KR}(a)$. It follows that P is itself the nth power of a rational quantity since $n-1$ is prime to n, and hence that $x_j \equiv 0 \pmod{n}$ $(j=1, \cdots, s)$. From this we can conclude that the fields

$$K(\alpha_1^{1/n}), \cdots, K(\alpha_s^{1/n})$$

are independent† and hence that, if

$$K_1 = K(\alpha_2^{1/n}, \cdots, \alpha_s^{1/n}), \ K_2 = K_1(\alpha_1^{1/n}),$$

K_2 is cyclic of degree n over K_1. It is known that K_2 is therefore a class field over K_1 for a certain cyclic ideal class group H of order n of the ideals of K_1. It is also known that in any generating class of H there are infinitely many prime ideals of the first degree relative to R and prime to $n\sigma$. Let $\mathfrak{p}$ be such a prime ideal of K_1 and $N_{KR}(\mathfrak{p}) = p$, a rational prime. Then p satisfies the conditions of the lemma as we shall now show.

Since $\mathfrak{p}$ is of the first degree relative to R we must have in K_1

$$\alpha_j^{1/n} \equiv y_j \pmod{\mathfrak{p}} \qquad (j = 2, \cdots, s), \tag{7}$$

where $y_2, \cdots, y_s$ are rational integers which are prime to p since $\mathfrak{p}$ was chosen prime to $n\sigma$ and hence does not divide the quantities on the left of (7). From (7) we get

$$q_1^{\beta_j} q_j \equiv y_j^n \pmod{\mathfrak{p}},$$

whence we get (6) since the quantities in the last congruence are rational. Suppose now we have $q_1 \equiv \gamma^n \pmod{p}$ with a rational integer γ. Then $q_1 \equiv \gamma^n \pmod{\mathfrak{p}}$. But by a known theorem‡ applied to the Kummer field $K_2 = K_1(\alpha_1^{1/n}) = K_1(q_1^{1/n})$, the power residue symbol $(q_1/\mathfrak{p})$ is 1 if and only if $\mathfrak{p}$ is in the identity class of the group H, whereas $\mathfrak{p}$ was chosen in a generating class of this group. This contradiction shows that q_1 is an n-ic non-residue modulo p, and hence also that $p \equiv 1 \pmod{n}$. This completes the proof of the lemma.

We turn now to the proof of Theorem 1. Let the invariants of A corre-

† *Bericht*, II, loc. cit., p. 43.

‡ *Bericht*, II, loc. cit., p. 51.

sponding to $q_1, \cdots, q_s$ be $\nu_1, \cdots, \nu_s$, respectively, so that we have $\nu_j \not\equiv 0 \pmod{n}$ $(j = 1, \cdots, s)$, and

$$\sum_{j=1}^{s} \nu_j \equiv 0 \pmod{n}. \tag{8}$$

We shall prove that a rational prime p satisfying the conditions of the lemma with rational integers $\beta_2, \cdots, \beta_s$, chosen such that

$$\nu_1\beta_j \equiv -\nu_j \pmod{n} \qquad (j = 2, \cdots, s), \tag{9}$$

satisfies the conditions of Theorem 1.

There is a unique cyclic field Z of degree n over R with the conductor p, discriminant p^{n-1}, namely, the class field over R for the ideal class group in R whose identity class consists of the ideals in R which are generated by n-ic residues modulo p. Since q_1 is an n-ic non-residue modulo p, q_1 is not in this identity class and hence the Frobenius-Artin symbol (Z/q_1) is not the identity automorphism E of Z over R. Since ν_1 is prime to n the automorphism S of Z defined by

$$S^{-\nu_1} = (Z/q_1)$$

is different from E. Thus $A' = (\sigma, Z, S)$ is a cyclic algebra of degree n over R. Denote its invariants by ν_π'. The ν_π' are easily calculated from the properties of the norm residue symbol (H, p. 175). Thus, for a prime π not contained in $p\sigma$, we have $((\sigma, Z)/\pi) = E$, and hence $\nu_\pi' \equiv 0 \pmod{n}$. To determine ν_{q_1}' we have

$$((\sigma, Z)/q_1) = (Z/q_1)^{-1} = S^{\nu_1}$$

by the definition of S, since q_1 is prime to the conductor p of Z and occurs exactly to the first power in σ. Hence $\nu_{q_1}' \equiv \nu_1 \pmod{n}$. Next let $j \geqq 2$. We have, as for q_1,

$$((\sigma, Z)/q_j) = (Z/q_j)^{-1}.$$

By the general law of reciprocity,† condition (3) of the lemma implies

$$(Z/q_j) = (Z/q_1)^{-\beta_j} \qquad (j = 2, \cdots, s).$$

Combining these results with the definition of S and (9) we get

$$((\sigma, Z)/q_j) = S^{\nu_i},$$

and hence $\nu_{q_j}' \equiv \nu_j \pmod{n}$ $(j = 2, \cdots, s)$. For the algebra A' the corresponding condition to (8) is

† *Bericht*, II, loc. cit., p. 11.

$$\sum_{j=1}^{s} \nu'_{q_j} + \nu'_p \equiv 0 \pmod{n},$$

which becomes, from what we have just shown,

$$\sum_{j=1}^{s} \nu_j + \nu'_p \equiv 0 \pmod{n}.$$

Then (8) implies $\nu'_p \equiv 0 \pmod{n}$.

We have now shown that the algebra A' has the same invariants as A. It is therefore isomorphic to A by Hasse's Theorem A (H, p. 176). In other words A has the cyclic generation (σ, Z, S). To complete the proof of the theorem we have only to point out that $q_1, \cdots, q_s$ are n-ic non-residues modulo p by the lemma, and that condition (8) is equivalent to the statement that σ is an n-ic residue modulo p.

3. **Maximal orders in the algebras A.** We consider in this section a fixed cyclic algebra A of degree n over R and propose to determine maximal orders in A. For convenience we use the term *basis*, as distinguished from *R-basis* and *Z-basis*, to refer to a basis with respect to rational integers of an order in A or in one of its sub-corps. As previously stated, A is either a total matric or a division algebra over R. Suppose that A is a total matric algebra. Then it is well known that any complete set of matrix units of A is also a basis of a maximal order in A. We assume henceforth that A is a division algebra.

By Theorem 1, A has infinitely many canonical generations. Let

$$A = (\sigma, Z, S) \tag{10}$$

be a fixed canonical generation of A so that Z is the unique cyclic field of degree n over R with a certain fixed prime conductor $p \equiv 1 \pmod{n}$, discriminant p^{n-1}, and $\sigma = q_1 \cdots q_s$, where the q_i and σ have the properties in Theorem 1. Let I denote the order in A associated with the generation (10). Then I has the basis

$$u^i z_k \qquad (i = 0, \cdots, n-1;\ k = 1, \cdots, n), \tag{11}$$

where the z_k form a basis for the integers of Z and the usual relations hold:

$$u^n = \sigma,\ zu = uz^S \text{ for every } z \text{ in } Z. \tag{12}$$

We shall exhibit n distinct maximal orders in A which contain I. We need certain properties of the field Z, and a well known representation of A as an algebra of matrices with elements in Z. These will now be described.

To describe the properties of Z let ξ be a primitive pth root of unity and let g be a primitive root modulo p. Then Z is the field $R(\eta)$, where η is the Gaussian period

$$\eta = \sum_{r=0}^{h-1} \xi^{g^{rh}}, \qquad p = hn + 1.$$

It is known that the n conjugates

$$\eta, \eta^S, \cdots, \eta^{S^{n-1}} \tag{13}$$

form a so-called *normal basis for the integers of* Z. We shall assume that $z_1, \cdots, z_n$ in (11) are the quantities (13) in that order. Then (12) implies

$$u^n = \sigma, \qquad z_k u = u z_{k+1} \qquad (k = 1, \cdots, n), \tag{14}$$

where we agree that $z_r = z_s$ if $r \equiv s \pmod{n}$. In Z a rational prime π factors as follows. If π is distinct from p, π is the product of n distinct prime ideal factors in Z or is itself a prime in Z according as it is an n-ic residue or an n-ic non-residue modulo p. The rational prime p is the power

$$p = \mathfrak{p}^n, \tag{15}$$

of a prime ideal $\mathfrak{p}$ which is a principal ideal, being generated, for example, by the quantity

$$\beta = \prod_{r=0}^{h-1} (1 - \xi^{g^{hn}}), \tag{16}$$

which is in Z and satisfies the relations

$$N_{ZR}(\beta) = p, \qquad \mathfrak{p} = (\beta). \tag{17}$$

We summarize these properties of Z in

THEOREM 2. *The integers of Z have a normal basis $z_1, \cdots, z_n$ such that in A the relations* (14) *hold. In Z, the rational prime p is the power $\mathfrak{p}^n$ of a prime ideal $\mathfrak{p}$ which is a principal ideal, and there exists a quantity β of Z such that* (17) *holds. A rational prime π distinct from p is the product of n distinct prime ideal factors or is itself a prime in Z according as it is an n-ic residue or an n-ic non-residue modulo p.*

The basis (11) of I is also an R-basis of A and by means of it one obtains in a well known manner an algebra $\bar{A}$ of matrices with elements in Z which is isomorphic to A. Thus, consider the vector $(1, u, \cdots, u^{n-1})$ and let a be any element of A. We get, using (14),

$$\begin{aligned} a(1, u, \cdots, u^{n-1}) &= (a, au, \cdots, au^{n-1}) \\ &= (1, u, \cdots, u^{n-1})\bar{a}, \end{aligned}$$

where $\bar{a}$ is an n-rowed square matrix with elements in Z. Let

$$a = \sum_{i,k} \alpha_{ik} u^i z_k, \qquad \alpha_{ik} \text{ rational.} \tag{18}$$

This may be written

$$a = \sum_i u^i x_i, \qquad x_i = \sum_k \alpha_{ik} z_k, \tag{19}$$

where the x_i are elements of Z. Denote the conjugates of x_i by

$$x_i^{(0)} = x_i, \; x_i^{(1)}, \cdots, x_i^{(n-1)},$$

where $x_i^{(1)} = x_i^S$ and so on. Then we have

$$a \longrightarrow \bar{a} = \begin{Vmatrix} x_0, & \sigma x_{n-1}^{(1)}, & \cdots, & \sigma x_1^{(n-1)} \\ x_1, & x_0^{(1)}, & \cdots, & \sigma x_2^{(n-1)} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ x_{n-1}, & x_{n-2}^{(1)}, & \cdots, & x_0^{(n-1)} \end{Vmatrix} \tag{20}$$

in which σ appears as a factor of every element above the main diagonal. The characteristic equation of $\bar{a}$ is the so-called principal equation of a, and the trace and determinant of $\bar{a}$ are the reduced trace and norm, respectively, of a. We shall denote them by $T(a)$ and $N(a)$. It is to be noted that $T(z)$ and $N(z)$, for a z in Z, are identical, respectively, with the trace and norm of z as an element of Z.

We now define the reduced discriminant of the order I. Let the basis (11) be denoted by the vector $v = (v_1, \cdots, v_{n^2})$ whose components are numbered as indicated by

$$v_1 = z_1, \cdots, v_n = z_n, v_{n+1} = uz_n, \cdots, v_{n^2} = u^{n-1} z_n. \tag{21}$$

Then the determinant

$$\Delta = \Delta(v) = \left| T(v_r v_t) \right| \qquad (r, t = 1, \cdots, n^2)$$

is called the reduced discriminant of the basis (11). Let P be any n^2-rowed non-singular rational matrix and define a vector w of elements of A by

$$w = Pv. \tag{22}$$

Then it can be shown that

$$\Delta(w) = |P|^2 \Delta(v). \tag{23}$$

Since a necessary and sufficient condition that w be a basis of I is that $|P| = 1$, the quantity Δ depends only upon I and is called the reduced discriminant of I. From (22) and (23) we are also led at once to the correspondence between

maximal orders and minimal discriminants here as in the case of algebraic number fields.†

The value of $\Delta(v) = \Delta(I)$ with the numbering (21) is easily calculated by means of the isomorphism $A \cong \bar{A}$, and the fact that the n-rowed determinant

$$| T(z_k z_j) | \qquad (k, j = 1, \cdots, n)$$

has the value p^{n-1} since it is the discriminant of Z. We find as the result of the calculations

$$\Delta = \Delta(I) = \sigma^{n(n-1)} p^{n(n-1)}. \tag{24}$$

This is the first part of

THEOREM 3. *The discriminant of I is given by* (24). *The discriminant of any maximal order in A which contains I is divisible by $\sigma^{n(n-1)}$.*

To prove the second part of Theorem 3 suppose the quantity a in (18) and (19) is in a maximal order I' which contains I. By closure the n^2 quantities av_t must also be in I'. We get, by combining (18) and (21) and multiplying by v_t $(t = 1, \cdots, n^2)$, n^2 equations of the form

$$av_t = \sum_{r=1}^{n^2} \alpha_r v_r v_t,$$

where the α_r are the α_{ik} renumbered. Taking traces and solving for the α_{ik} we see that the denominators of these rational coefficients are divisors of Δ, since the av_t must have integral traces. With a change of notation we can therefore write

$$\Delta \bar{a} = \begin{Vmatrix} x_0, & \sigma x_{n-1}^{(1)}, & \cdots, & \sigma x_1^{(n-1)} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ x_{n-1}, & x_{n-2}^{(1)}, & \cdots, & x_0^{(n-1)} \end{Vmatrix}, \tag{25}$$

where now the x_i are given by (19) with rational integers α_{ik} and are integers of Z.

Since a was assumed to be in a maximal order, its principal equation, i.e., the characteristic equation of $\bar{a}$, must have rational integral coefficients and highest coefficient 1. From this it follows in particular that $|\bar{a}|$ must be a rational integer. From (25) we get

$$\Delta^n | \bar{a} | = N(x_0) + \sigma Q,$$

† For details see Artin's paper cited in the Introduction.

where Q is a rational integer. Hence we must have

$$N(x_0) \equiv 0 \pmod{\sigma}. \tag{26}$$

By Theorem 1 each prime factor q of σ is an n-ic non-residue modulo p and is therefore a prime in Z by Theorem 2. Hence $N(x_0) \equiv 0 \pmod{q}$ implies $x_0 \equiv 0 \pmod{q}$, and (26) implies $x_0 \equiv 0 \pmod{\sigma}$ since the prime factors of σ are distinct. We use this in (25) which then implies that

$$\Delta^n \left| \bar{a} \right| = \sigma N(x_1) + \sigma^2 Q_1,$$

where Q_1 is a rational integer. This implies similarly that $x_1 \equiv 0 \pmod{\sigma}$. It is evident that the same argument then yields $x_2 \equiv 0 \pmod{\sigma}$ and so on, and we can cancel a factor σ in (25). Then we can repeat the whole argument for the resulting equation and so on. We are led ultimately to the condition

$$x_0 \equiv x_1 \equiv \cdots \equiv x_{n-1} \equiv 0 \pmod{\sigma^{n(n-1)}},$$

which implies that each α_{ik} in (19) is divisible by $\sigma^{n(n-1)}$.

We have now shown that *a necessary condition that a quantity of A be in a maximal order, say I', containing I, is that its coefficients, when it is expressed by means of the R-basis* (11) *of A, have denominators which are at most powers of p.* This condition is equivalent to the second part of Theorem 3. For it is easy to show by the usual argument that I' has a basis. Let its basis be w. Then w will be related to v as in (22) for some P, and (23) implies the equivalence just claimed.

We now construct a maximal order in A containing I. The congruence

$$\lambda^n \equiv \sigma \pmod{p} \tag{27}$$

has a rational integral solution by Theorem 1. Let λ be a fixed solution of (27), let $\alpha = \beta^{n-1}$, where β is the quantity in (16) and (17), and define a quantity y by

$$py = (\lambda - u)\alpha. \tag{28}$$

With these definitions we are ready to prove

THEOREM 4. *For a fixed rational integral solution λ of* (27), *the set $I(\lambda)$ of linear combinations with rational integral coefficients of the quantities*

$$y^i z_k \qquad (i = 0, \cdots, n-1; j = 1, \cdots, n), \tag{29}$$

where y is defined by (28) *with $\alpha = \beta^{n-1}$ and the z_k form the normal basis of the integers of Z described in Theorem* 2, *is a maximal order† in A.*

† Maximal orders similar to this in certain algebras A of degree 3 were found by F. S. Nowlan, *Arithmetics of rational division algebras of order nine*, Transactions of the Royal Society of Canada, (3), vol. 21 (1927).

To prove the theorem, we first verify that $I(\lambda)$ satisfies the order postulates (a), (b), and (c) stated in the Introduction, and then calculate the discriminant of its basis (29). From the value found for this discriminant the maximality of $I(\lambda)$ follows from Theorem 3.

The definition of $I(\lambda)$ is such that postulates (b) and (c) are automatically satisfied. It is also obvious that $I(\lambda)$ is closed under addition and subtraction. Of the order postulates there remains only to show that it is closed under multiplication. To do this it is clearly necessary and sufficient to show that y satisfies an equation of degree n with rational integral coefficients and highest coefficient 1, and that the n quantities $z_k y$ $(k=1, \cdots, n)$ are in $I(\lambda)$.

The quantity y satisfies the characteristic equation of the matrix $\bar{y}$ to which y corresponds in the isomorphism $A \cong \bar{A}$. Let the characteristic equation of $p\bar{y}$ be $f(t)=0$.

We have

$$(30) \qquad py \to p\bar{y} = \begin{Vmatrix} \lambda\alpha, & 0, & \cdots, & 0, & -\sigma\alpha^{(n-1)} \\ -\alpha, & \lambda\alpha^{(1)}, & \cdots & 0, & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0, & 0, & \cdots, & -\alpha^{(n-2)}, & \lambda\alpha^{(n-1)} \end{Vmatrix}$$

whence

$$f(t) = t^n - \lambda\gamma_1 t^{n-1} + \lambda^2\gamma_2 t^{n-2} - \cdots + \lambda^{n-1}\gamma_{n-1}t - \gamma_n,$$

where $\gamma_1, \cdots, \gamma_n$ are rational integers. Consider first a γ_k with $1 \leqq k \leqq n-1$. Then γ_k is the kth elementary symmetric function of α and its conjugates in Z and thus is of degree k in α and its conjugates. Since $\alpha = \beta^{n-1}$, by (17) we have $\alpha \equiv 0 \pmod{\mathfrak{p}^{n-1}}$, and since $\mathfrak{p}$ is unaltered by each of the automorphisms of Z, this implies $\alpha^{(j)} \equiv 0 \pmod{\mathfrak{p}^{n-1}}$ for $j=0, \cdots, n-1$. Hence

$$\gamma_k \equiv 0 \pmod{\mathfrak{p}^{k(n-1)}},$$
$$\gamma_k \equiv 0 \pmod{\mathfrak{p}^{(k-1)n+n-k}}.$$

This shows that γ_k/p^{k-1} is a rational integer such that

$$\gamma_k/p^{k-1} \equiv 0 \pmod{\mathfrak{p}^{n-k}},$$

whence

$$\gamma_k/p^{k-1} \equiv 0 \pmod{p},$$

since $n-k>0$. Hence $\gamma_k \equiv 0 \pmod{p^k}$. From (30) we see that $\gamma_n = N(\alpha)(\lambda^n - \sigma)$. Hence $\gamma_n \equiv 0 \pmod{p^n}$ since $N(\alpha) = p^{n-1}$ and (27) holds. These results show

that the characteristic equation of $\bar{y}$ which is satisfied by y is of the type required.

Now consider a product $z_k y$. We have

$$\begin{aligned} pz_k y &= z_k(\lambda - u)\alpha = z_k\lambda\alpha - z_k u\alpha \\ &= z_k\lambda\alpha - z_{k+1}\lambda\alpha + z_{k+1}\lambda\alpha - uz_{k+1}\alpha \\ &= \lambda\alpha(z_k - z_{k+1}) + pyz_{k+1} \\ &= b_k + pyz_{k+1}, \end{aligned}$$

where b_k is an integer of Z, which we shall show is divisible by p. We have $\alpha \equiv 0 \pmod{\mathfrak{p}^{n-1}}$. But $z_k - z_{k+1} \equiv 0 \pmod{\mathfrak{p}}$ for each $k = 1, \cdots, n$, since the so-called group of inertia (*Trägheitsgruppe*) of $\mathfrak{p}$ is the whole Galois group of Z and $z_{k+1} = z_k^S$. Thus $b_k \equiv 0 \pmod{\mathfrak{p}^n}$, $b_k \equiv 0 \pmod{p}$. Thus we can write $z_k y = b_k/p - yz_{k+1}$, where b_k/p is an integer of Z, which shows that $z_k y$ is in $I(\lambda)$. *This completes the proof that* $I(\lambda)$ *is an order.* That it contains I is trivial since it obviously contains $z_1, \cdots, z_k$ and also $u = \lambda + yp/\alpha$, where $p/\alpha = p/\beta^{n-1}$ is an integer of Z.

We now evaluate the discriminant of $I(\lambda)$. Let the elements of the basis (29) of $I(\lambda)$ be denoted by $w_1, \cdots, w_{n^2}$ with similar numbering to that in (21). We then have a relation (22) with a rational matrix P which is easily seen to be of the form

$$P = \begin{Vmatrix} P_1 & 0 & 0 & \cdots & 0 \\ \cdot & P_2 & \cdot & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & P_n \end{Vmatrix}$$

where the P_k are n-rowed square matrices, and P has zeros everywhere above these. The determinants $|P_k|$ are easily calculated. It is clear that P_1 is the n-rowed identity matrix and its determinant is 1. To find P_2 we have

$$pw_{n+1} = (\lambda - u)\alpha z_1, \cdots, pw_{2n} = (\lambda - u)\alpha z_n.$$

Since α is an integer of Z we have

$$\alpha z_k = \sum_{j=1}^{n} \alpha_{jk} z_k \qquad (k = 1, \cdots, n),$$

where the α_{jk} are rational integers. It is clear that $pP_2 = \|\alpha_{jk}\|$. But it is well known that $|\alpha_{jk}| = N(\alpha) = p^{n-1}$ and hence $|P_2| = 1/p$. The coefficients of u^2 in $p^2 w_{2n+1}, \cdots, p^2 w_{3n}$, respectively, are $\alpha\alpha^{(1)} z_1, \cdots, \alpha\alpha^{(1)} z_n$, and we see that $p^2 P_3$ is a rational matrix whose determinant is $N(\alpha\alpha^{(1)}) = p^{2(n-1)}$ so that $|P_3| = 1/p^2$. Similarly in general we find that $|P_k| = 1/p^k$. Thus we get

$$| P |^2 = | P_1^2 \cdots P_n^2 | = 1/p^{n(n-1)},$$

and $\Delta(w) = \sigma^{n(n-1)}$ by (23) and (24).

That $I(\lambda)$ is a maximal order in A now follows from the second part of Theorem 3 and the fact that an order with minimum discriminant is necessarily maximal. This completes the proof of Theorem 4.

In Theorem 4 a particular solution of (27) was chosen. The question now raises itself as to the effect of choosing a different solution of (27) or of replacing α in (28) by another integral quantity of Z whose norm is p^{n-1}. The latter would clearly have the effect only of yielding a different basis of the same order since any integral quantity of Z whose norm is p^{n-1} is the product of α and a unit of Z. The effect of the former is given in

THEOREM 5. *There are n distinct maximal orders in A which contain I, corresponding to the n distinct solutions modulo p of* (27). *These n maximal orders are such that each can be obtained from any of the others by transformation with a suitable power of* β.

Let λ_1 and λ_2 be distinct solutions of (27), and let y_1 and y_2 be the quantities defined by (28) for $\lambda = \lambda_1$ and λ_2, respectively. Then the matrix $\bar{y}_1 - \bar{y}_2$ to which $y_1 - y_2$ corresponds in the isomorphism $A \cong \bar{A}$ does not have an integral determinant as its form readily shows. Thus $I(\lambda_1)$ and $I(\lambda_2)$ must necessarily be distinct. This proves the first part of Theorem 5.

To prove the second part of the theorem we consider the effect of transforming $I(\lambda)$, for a given λ, by β. The set $I' = \beta^{-1} I(\lambda)\beta$ is clearly a maximal order in A with the basis $y'^i z_k$, where $y' = \beta^{-1} y \beta$. We shall show that I' is identical with a maximal order $I(\lambda_1)$ for a solution λ_1 of (27) such that $\lambda_1 \not\equiv \lambda \pmod{p}$. We have

$$\begin{aligned} py' &= p\beta^{-1} y \beta = \lambda\alpha - u\alpha(\beta/\beta^{(1)}), \\ \alpha\lambda\beta^{(1)}/\beta - u\alpha &= py'\beta^{(1)}/\beta. \end{aligned} \tag{31}$$

The quantity $\beta^{(1)}/\beta$ is a unit of Z, and since $\mathfrak{p}$ is of the first degree, we must have

$$\beta^{(1)}/\beta \equiv \gamma \pmod{\mathfrak{p}}, \qquad \beta^{(1)} \equiv \gamma\beta \pmod{\mathfrak{p}^2}, \tag{32}$$

where γ is a rational integer. To the first congruence in (32), we apply in succession the automorphisms $E = S^0, S, \cdots, S^{n-1}$, under which $\mathfrak{p}$ is invariant, and multiply the resulting congruences. We get $N(\gamma) \equiv N(\beta^{(1)}/\beta) \pmod{\mathfrak{p}}$ whence $\gamma^n \equiv 1 \pmod{p}$. Moreover, $\gamma \not\equiv 1 \pmod{p}$, since otherwise we would have from the second congruence (32)

$$\beta \equiv \beta^{(1)} \cdots \equiv \beta^{(n-1)} \pmod{\mathfrak{p}^2},$$

which with $T(\beta)\equiv 0 \pmod{p}$ would lead to $n\beta\equiv 0 \pmod{\mathfrak{p}^2}$, $\beta\equiv 0 \pmod{\mathfrak{p}^2}$, a contradiction.

We now set $\lambda_1=\gamma\lambda$. Then $\lambda_1^n\equiv\lambda^n\equiv\sigma$, $\lambda_1\not\equiv\lambda \pmod{p}$ and the results of the last paragraph show that we have

$$\alpha\lambda\beta^{(1)}/\beta \equiv \lambda_1\alpha \pmod{p}, \qquad \alpha\lambda\beta^{(1)}/\beta = \lambda_1\alpha + zp,$$

where z is an integer of Z, since $\alpha\equiv 0 \pmod{\mathfrak{p}^{n-1}}$ and $\beta^{(1)}/\beta\equiv\gamma \pmod{\mathfrak{p}}$. Substituting this in (31) we get

$$(\lambda_1 - u)\alpha = -pz + py'\beta^{(1)}/\beta,$$

which shows that $I(\lambda_1)\subseteq I'$ and hence that $I(\lambda_1)=I'$ since it is maximal.

By a continuation of this discussion it is easy to show that the transformation of a given $I(\lambda)$ by the powers $\beta, \beta^2, \cdots, \beta^{n-1}$ yields maximal orders in A corresponding, respectively, to the distinct solutions $\lambda\gamma, \cdots, \lambda\gamma^{n-1}$ of (27), where γ is the rational integer defined in the last paragraph. An obvious argument now yields the second part of Theorem 5.

We shall show in the next section by less direct methods that the n maximal orders in A corresponding to the distinct solutions modulo p of (27) are the only maximal orders in A which contain I.

4. **The number of maximal orders containing an order A.** In this section we consider the order I in A associated with a fixed canonical generation (10) of A and show that there are exactly n distinct maximal orders in A containing I. We have already seen by Theorems 4 and 5 that there are n distinct such maximal orders and we now show that there are not more than n. To do this we consider the π-components of any maximal order which contains I, where π ranges over all prime spots of R. By the π-component of an order, for a fixed π, we mean the π-adic limit set of the order,† which is easily shown to be an order in the algebra A_π obtained from A by extending the centrum to be R_π. Thus A_π is the π-adic limit set of A. Conversely, we have the following fundamental theorem due to Hasse:

THEOREM 6. *A maximal order in A is the intersection of the totality of its π-components and A.*

With a view to the application of this theorem to our problem we now determine the number of maximal orders in the algebra A_π, for a fixed π, which contain the π-component I_π of I.

First suppose π is distinct from p. Let a be any quantity of A which is in a maximal order containing I. It was proved in §3 that, if a is expressed in terms

† This definition, and the proof of Theorem 6 and other properties used here, are given by Hasse, *Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Mathematische Annalen, vol. 104 (1931), p. 495.

of the basis (11) of I, which is an R-basis of A, the rational coefficients have denominators which are at most powers of p. These denominators are units of R_π since $\pi \neq p$, and hence the π-adic limit set of any maximal order in A which contains I is I_π itself. In other words, if $\pi \neq p$, there is a single maximal order in A_π which contains I_π.

Now consider the case $\pi = p$. The algebra A_p is a total matric algebra by Theorem 2, since p is not one of the prime factors q of σ. Evidently A_p over R_p has the cyclic generation

$$A_p = (\sigma, Z_p, S_p),$$

where Z_p is the p-adic limit set of Z which is easily shown to be a cyclic field of degree n over R_p, and S_p is the automorphism of Z_p corresponding to the automorphism S of Z. We may regard A_p as the crossed product of Z_p and its Galois group with the operators $1, u, \cdots, u^{n-1}$ corresponding to the automorphisms $E, S_p, \cdots, S_p^{n-1}$, respectively, and the factor system consisting of 1's and σ's. The equation

$$x^n - \sigma = 0 \tag{33}$$

has a solution in R_p by a well known theorem on p-adic fields, since $x^n - \sigma$ factors modulo p into n distinct linear factors. Let ξ be a fixed solution in R_p of (33). We replace the operator u by v, where $u = \xi v$, which obviously has the effect of yielding a new factor system, equivalent to the former, consisting of 1's only.

With this operator v and factor system we can give explicitly all maximal orders in A_p. Let

$$V = 1 + v + \cdots + v^{n-1}.$$

Then every maximal order in A_p is of the form†

$$I(\mathfrak{m}) = \mathfrak{m}^* V \mathfrak{m},$$

where $\mathfrak{m}$ and $\mathfrak{m}^*$ are complementary moduls in Z_p. A necessary and sufficient condition that $I(\mathfrak{m})$ contain the maximal order of Z_p is that $\mathfrak{m}$ be an ideal of Z_p. The only ideals of Z_p are the prime ideal generated by the prime ideal $\mathfrak{p}$ of Z and its powers. We shall denote the prime ideal of Z_p also by $\mathfrak{p}$. Then the only maximal orders in A_p which contain the maximal order of Z_p are those of the form

† This explicit form for the maximal orders in a crossed product which is a total matric algebra over an algebraic number field was given by Emmy Noether: *Zerfallende verschränkte Produkte und ihre Maximalordnungen.* Actualités Scientifiques et Industrielles, No. 148 (Herbrand Memorial). A brief examination of Noether's proof of this and further consequences of it, in the case of an algebraic coefficient field, will show that the corresponding theorems hold almost trivially in the present case, namely, with the coefficient field R_p.

(34) $$I(\mathfrak{p}^r) = \mathfrak{p}^{r*}V\mathfrak{p}^r, \ r \text{ a rational integer},$$

where by $\mathfrak{p}^0$ will be meant the maximal order of Z_p. Since the different of Z_p is is $\mathfrak{p}^{n-1}$ we have

$$\mathfrak{p}^{r*} = \mathfrak{p}^{-r}\mathfrak{p}^{-(n-1)}.$$

The ideal $\mathfrak{p}^n$ of Z_p is the ideal generated by the rational prime p. Combining these we see that

$$I(\mathfrak{p}^{n+r}) = (\mathfrak{p}^{n+r})^*V\mathfrak{p}^{n+r} = (p\mathfrak{p}^r)^*Vp\mathfrak{p}^r = \mathfrak{p}^{r*}V\mathfrak{p}^r = I(\mathfrak{p}^r),$$

since $(p\mathfrak{p}^r)^* = \mathfrak{p}^{r*}/p$ and p is commutative with V. This shows that in the set (34) ($r = 0, \pm 1, \pm 2, \cdots$) there are at most n distinct maximal orders. Hence there are at most n distinct maximal orders in A_p which contain the maximal order of Z_p and a fortiori, at most n which contain I_p.

The results obtained for the two cases $\pi \neq p$ and $\pi = p$, combined with Theorem 6, show that there are at most n distinct maximal orders in A which contain I. For, by Theorem 6, two such maximal orders in A must have distinct π-components for at least one π. But we have shown that their π-components can differ only for $\pi = p$ and that here there are at most n distinct possibilities. We combine this with the earlier theorems of §§2 and 3 and summarize the results of this paper in

THEOREM 7. *A cyclic division algebra A of odd prime degree n over R has infinitely many distinct canonical generations of the type described in Theorem* 1. *The order in A associated with a fixed such generation in the manner described in the Introduction, can be imbedded in exactly n distinct maximal orders in A and these maximal orders are of the type given in Theorems* 4 *and* 5.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.