THE MAXIMAL ORDERS OF GENERALIZED QUATERNION DIVISION ALGEBRAS[*]

BY

RALPH HULL[†]

1. **Introduction.** A generalized quaternion division algebra Q is an algebra of degree 2, order 4, over the field R of all rational numbers. It can be written in the form $Q=(a, Z)=Z+uZ$, where Z is a quadratic field over R and $u^2=a$ is in R and is not the norm of an element of Z, and $Zu=uZ'$, elementwise, where the prime denotes the conjugate in Z. We say that Q has the generation $Q=(a, Z)$ and identify the unity elements[‡] of Q and Z with each other and with 1, the unity element of R. We call $1, u$, a Z-basis of Q. If ζ_1, ζ_2, and ζ_3, ζ_4, are any R-bases of Z then $\zeta_1, \zeta_2, u\zeta_3, u\zeta_4$, is an R-basis of Q.

An algebra Q has a representation as an algebra of matrices of degree 2 with elements in Z which can be obtained in the following manner. Regarding $(1, u)$ as a vector, for any $q=\zeta_0+u\zeta_1$ of Q, ζ_0 and ζ_1 in Z, we have $q\longleftrightarrow\bar{q}$, where

$$q(1, u) = (q, qu) = (1, u)\bar{q}, \quad \bar{q} = \left\| \begin{matrix} \zeta_0, & a\zeta_1' \\ \zeta_1, & \zeta_0' \end{matrix} \right\|.$$

We call $T(\bar{q})=T(q)=\zeta_0+\zeta_1$ the *reduced trace* of q. In a similar way, using an R-basis of Q we obtain a representation of Q as an algebra of matrices of degree 4 with elements in R.

The Q are cyclic algebras[§] and the theory of their invariants is included in the general theory of Hasse[||] which yields all generations of a given Q. There exist a finite number >0 of rational primes π such that the π-adic extension Q_π of Q is a division algebra whereas Q_p for all other rational primes p is a total matric algebra. We say that Q splits at the prime spots p of R. The number of π is even if Q has a real quadratic sub-field, and odd otherwise. In the former case, Q is said to split at the infinite prime spot of R.

A *maximal order*[¶] $\mathfrak{M}$ of Q, that is, an integral domain (Dickson, loc. cit.,

[*] Presented to the Society, December 31, 1935; received by the editors December 2, 1935.

[†] The paper had its inception while its author was a National Research Fellow.

[‡] The name *unity element* in preference to *modulus* or *unit element* was adopted at the suggestion of Professor A. A. Albert.

[§] Dickson, *Algebren und ihre Zahlentheorie*.

[||] Hasse, *Theory of cyclic algebras over an algebraic number field*, these Transactions, vol. 34 (1932), pp. 171–214.

[¶] Deuring, *Algebren*, Ergebnisse der Mathematik, vol. 4, part 1. Deuring gives a complete bibliography including references to the work of Darkow and Latimer.

p. 198), is a set of elements of Q with the properties:

U: $\mathfrak{M}$ contains the unity element.

B: $\mathfrak{M}$ contains an R-basis of Q.

I: The elements of $\mathfrak{M}$ are integral; that is, they satisfy equations with rational integral coefficients, highest coefficient 1.

C_a: $\mathfrak{M}$ is closed under addition.

C_m: $\mathfrak{M}$ is closed under multiplication.

M: $\mathfrak{M}$ is maximal; that is, it is not contained in a larger set having the first properties.

A set having properties $U, \cdots, C_m$, is called an *order* $\mathfrak{K}$ of Q.

Each Q has infinitely many $\mathfrak{M}$ of which special ones have been determined for certain Q by Dickson (loc. cit.), Darkow and Latimer, and for all Q by Albert.* It is the purpose of this paper to determine all $\mathfrak{M}$ for each Q.

First, every $\mathfrak{K}$ is shown to have a certain simple form relative to an arbitrary generation of Q. Second, the necessary and sufficient conditions for a set of elements of this form to be a $\mathfrak{K}$ are determined. Third, the maximality condition is introduced. Fourth, canonical generations of each Q found by Albert (loc. cit.) are described. Finally, conditions for the existence of maximal orders $\mathfrak{M}$ are determined by a study of the earlier results when expressed in terms of canonical generations.

Throughout the paper we denote by $\mathfrak{g}$ the maximal order of R. It is clear by Properties U and C_a that every $\mathfrak{K}$ contains $\mathfrak{g}$. Also, if v_1 and v_2 are fixed quantities and $\mathfrak{m}$ and $\mathfrak{n}$ are sets of quantities we write $v_1 \cdot \mathfrak{m} + v_2 \cdot \mathfrak{n}$ for the set of all quantities of the form $v_1\mu + v_2\nu$, μ in $\mathfrak{m}$ and ν in $\mathfrak{n}$.

2. **The form of an order.** Any order $\mathfrak{K}$ of an algebra Q has the simple form relative to an arbitrary generation $Q=(a, Z)$, described in

THEOREM 1. *If* $\mathfrak{K}$ *is any order of* $Q=(a, Z)$ *the intersection* $\mathfrak{m}_c$ *of* $\mathfrak{K}$ *and* Z *is an order of* Z *whose conductor is a positive integer* c. *There exists a unique* $\mathfrak{m}_c$*-modul* $\mathfrak{n}$, *which is a finite* $\mathfrak{g}$*-modul, of elements of* Z, *and a quantity* λ *of* Z *such that*

$$\mathfrak{K} = 1 \cdot \mathfrak{m}_c + (\lambda + u) \cdot \mathfrak{n}. \tag{1}$$

By the definition of $\mathfrak{m}_c$ and the order properties of $\mathfrak{K}$ it is evident that $\mathfrak{m}_c$ is an order of Z. It is known that the conductor of every order of a quadratic field is a positive integer c, uniquely determining the order, such that c^2d is the discriminant of the order, where d is the discriminant of the field.

By Property B, $\mathfrak{K}$ contains elements of the form $\nu_0 + u\nu$, $\nu \neq 0$ and ν_0 in Z. Let $\mathfrak{n}$ be the set of all ν, including $\nu=0$, which occur when all elements of $\mathfrak{K}$ are

* Albert, *Integral domains of rational generalized quaternion algebras*, Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 164–176.

written in this form. By Property C_m, $\mathfrak{R}\mathfrak{m}_c \subset \mathfrak{R}$ whence $\mathfrak{n}\mathfrak{m}_c \subset \mathfrak{n}$. Hence $\mathfrak{n}$ is an $\mathfrak{m}_c$-modul since Property C_a of $\mathfrak{R}$ implies that $\mathfrak{n}$ is a modul.

To prove that $\mathfrak{n}$ is a finite $\mathfrak{g}$-modul we prove more, namely, that $\mathfrak{R}$ is a finite $\mathfrak{g}$-modul. For, $\mathfrak{R}$ contains an R-basis, say v_0, v_1, v_2, v_3, of Q by Property B. Let q be any element of $\mathfrak{R}$. Then we have

$$q = \sum_{i=0}^{3} \alpha_i v_i, \qquad \alpha_i \text{ in } R, \qquad q v_j = \sum_{i=0}^{3} \alpha_i v_i v_j \qquad (j = 0, \cdots, 3).$$

From these equations we get

$$T(qv_j) = \sum_{i=0}^{3} \alpha_i T(v_i v_j) \qquad (j = 0, \cdots, 3),$$

where all traces are in $\mathfrak{g}$ by Properties C_m and I. Solution shows that $|T(v_i v_j)|\alpha_k$ is in $\mathfrak{g}$ for $k=0, \cdots, 3$, where $|T(v_i v_j)| = \Delta(v_0, \cdots, v_3)$ is in $\mathfrak{g}$, is independent of q in $\mathfrak{R}$ and is not zero since Q is semi-simple. This proves that $\mathfrak{R}$ is a finite $\mathfrak{g}$-modul and it is evident, therefore, that $\mathfrak{n}$ is a finite $\mathfrak{g}$-modul. We call $\Delta(v_0, \cdots, v_3)$ the *reduced discriminant* of the R-basis $v_0, \cdots, v_3$.

From the properties of $\mathfrak{n}$ just proved it follows in the usual way that there exist $\nu_1 \neq 0$ and $\nu_2 \neq 0$ in $\mathfrak{n}$ such that $\mathfrak{n} = \nu_1 \cdot \mathfrak{g} + \nu_2 \cdot \mathfrak{g}$. Then $\mathfrak{R}$ contains quantities $\nu_{01} + u\nu_1$, $\nu_{02} + u\nu_2$, ν_{01} and ν_{02} in Z. By Property C_m, $\mathfrak{R}$ also contains

$$(\nu_{01} + u\nu_1)(\nu_{02} + u\nu_2) = \nu_{01}\nu_{02} + a\nu_1'\nu_2 + u(\nu_1\nu_{02} + \nu_2\nu_{01}'),$$

whence $\nu_1\nu_{02} + \nu_2\nu_{01}'$ is in $\mathfrak{n}$. By Property I,

$$T(\nu_{01} + u\nu_1) = \nu_{01} + \nu_{01}' = g$$

is in $\mathfrak{g}$. Hence

$$\nu_1\nu_{02} - \nu_2\nu_{01} = \nu_1\nu_{02} + \nu_2\nu_{01}' - g\nu_2$$

is in $\mathfrak{n}$ and there exist g_1 and g_2 in $\mathfrak{g}$ such that

$$\nu_1\nu_{02} - \nu_2\nu_{01} = g_2\nu_1 - g_1\nu_2, \qquad (\nu_{01} - g_1)\nu_2 = (\nu_{02} - g_2)\nu_1.$$

We define $\lambda = (\nu_{01} - g_1)/\nu_1 = (\nu_{02} - g_2)/\nu_2$ and prove (1).

We have $(\lambda + u)\nu_1 = \nu_{01} + u\nu_1 - g_1$ in $\mathfrak{R}$ by Property C_a since $\mathfrak{g} \subset \mathfrak{R}$. Similarly, $(\lambda + u)\nu_2$ is in $\mathfrak{R}$ and hence by C_a, $(\lambda + u)\mathfrak{n} \subset \mathfrak{R}$. For an arbitrary $\nu_0 + u\nu$ in $\mathfrak{R}$, whence ν is in $\mathfrak{n}$, we have $\nu_0 + u\nu = \mu + (\lambda + u)\nu$, $\mu = \nu_0 - \lambda\nu$, where μ is in Z and also in $\mathfrak{R}$ by Property C_a and hence in $\mathfrak{m}_c$. Since $\mathfrak{m}_c \subset \mathfrak{R}$ and $(\lambda + u)\mathfrak{n} \subset \mathfrak{R}$, we have (1).

An order $\mathfrak{m}_c$ of Z and a finite $\mathfrak{g}$-modul $\mathfrak{n}$ of elements of Z such that $\mathfrak{n}\mathfrak{m}_c \subset \mathfrak{n}$, have $\mathfrak{g}$-bases of a special form needed later. We state*

* For the first part of the theorem, see Fricke, *Lehrbuch der Algebra*, vol. 3, p. 249. The second part is easily proved as a consequence of the properties of $\mathfrak{n}$.

Theorem 2. *The order* $\mathfrak{m}_c$ *of* Z, *with the conductor* c, *can be written*

$$\mathfrak{m}_c = 1\cdot\mathfrak{g} + c\omega\cdot\mathfrak{g}, \qquad \omega = (d + d^{1/2})/2, \tag{2}$$

where d *is the discriminant of* Z. *A finite* $\mathfrak{g}$-*modul* $\mathfrak{n}$ *of elements of* Z *such that* $\mathfrak{n}\mathfrak{m}_c \subset \mathfrak{n}$, *can be written*

$$\mathfrak{n} = r\cdot\mathfrak{g} + r\nu\cdot\mathfrak{g}, \qquad \nu = (g_1 + c\omega)/g_2, \tag{3}$$

where r *is in* R *and* g_1 *and* g_2 *are in* $\mathfrak{g}$ *and such that*

$$g_1^2 - cdg_1 + c^2(d^2 - d)/4 \equiv 0 \pmod{g_2}. \tag{4}$$

3. **The closure and integral conditions.** Let $\mathfrak{m}_c$ and $\mathfrak{n}$ be given by (2), (3), and (4). Let

$$\lambda = e_0 + e_1\omega, \qquad e_0 \text{ and } e_1 \text{ in } R, \tag{5}$$

whence λ is in Z. We consider the set

$$\mathfrak{S} = 1\cdot\mathfrak{m}_c + (\lambda + u)\cdot\mathfrak{n}, \tag{6}$$

of elements of Q. Evidently $\mathfrak{S}$ has Properties U, C_a, and B, since 1 is in $\mathfrak{m}_c$, $\mathfrak{m}_c$ and $\mathfrak{n}$ have Property C_a, and v_0, v_1, v_2, v_3, where

$$v_0 = 1, \qquad v_1 = c\omega, \qquad v_2 = (\lambda + u)r, \qquad v_3 = (\lambda + u)r\nu, \tag{7}$$

is an R-basis of Q in $\mathfrak{S}$. We shall determine necessary and sufficient conditions that $\mathfrak{S}$ have Properties I and C_m, and hence be an order of Q. We first prove

Lemma 1. *The trace* $T(s)$ *is in* $\mathfrak{g}$ *for every* s *of* S *if and only if* $T(\lambda r) = k_1$ *and* $T(\lambda r\nu) = k_2$ *are in* $\mathfrak{g}$. *These conditions are equivalent to*

$$\begin{aligned} rce_0 &= \{g_1 + c(d+1)/2\}k_1 - g_2k_2, \\ rcde_1 &= -(2g_1 + cd)k_1 + 2g_2k_2, \end{aligned} \tag{8}$$

with k_1 *and* k_2 *in* $\mathfrak{g}$.

If $s = \mu + (\lambda + u)\eta$ is in $\mathfrak{S}$, we have μ in $\mathfrak{m}_c$ and η in $\mathfrak{n}$. Then $T(\mu)$ is in $\mathfrak{g}$ and $T(s) = T(\mu) + T(\lambda\eta)$ is in $\mathfrak{g}$ if and only if $T(\lambda\eta)$ is in $\mathfrak{g}$. From (3) and the linearity of the trace function we obtain at once the lemma, where (8) is the solution of $T(\lambda r) = k_1$ and $T(\lambda r\nu) = k_2$ for e_0 and e_1.

We leave Property I and consider C_m assuming (2), $\cdots$, (8). Since $\mathfrak{m}_c\cdot\mathfrak{m}_c = \mathfrak{m}_c$ and $\mathfrak{n}\cdot\mathfrak{m}_c = \mathfrak{n}$, it follows from (6) that $\mathfrak{S}$ has Property C_m if and only if we have simultaneously:

$$\mu(\lambda + u)\eta \textit{ in } \mathfrak{S} \textit{ for every } \mu \textit{ in } \mathfrak{m}_c,\ \eta \textit{ in } \mathfrak{n}, \tag{9}$$

and

$$(\lambda + u)\eta_1(\lambda + u)\eta_2 \textit{ in } \mathfrak{S} \textit{ for every } \eta_1,\ \eta_2 \textit{ in } \mathfrak{n}. \tag{10}$$

By (2) and (3) it is necessary and sufficient for (9) that $c\omega(\lambda+u)r$ and $c\omega(\lambda+u)rv$ be in $\mathfrak{S}$. Using (2), $\cdots$, (8) we find

$$
\begin{aligned}
c\omega(\lambda + u)r &= -(g_1 + cd)k_1 + g_2k_2 + k_1c\omega + (\lambda + u)c\omega'r,\\
c\omega(\lambda + u)rv &= -g_3k_1 + g_1k_2 + k_1c\omega + (\lambda + u)c\omega'r,
\end{aligned}
\tag{11}
$$

where $g_3g_2 = g_1^2 + cdg_1 + c^2(d^2-d)/4$, whence g_3 is in $\mathfrak{g}$ by (4). Since $c\omega'$ is in $\mathfrak{m}_c$, $c\omega'r$ and $c\omega'rv$ are in $\mathfrak{n}$. Hence (11) shows that (2), $\cdots$, (8) imply (9).

Next, we have

$$
(\lambda + u)\eta_1(\lambda + u)\eta_2 = \{a - N(\lambda)\}\eta_1'\eta_2 + (\lambda + u)\eta_2T(\lambda\eta_1),
\tag{12}
$$

where $N(\lambda) = \lambda\lambda'$. For every η_1, η_2 in $\mathfrak{n}$, $T(\lambda\eta_1)$ is in $\mathfrak{g}$ by Lemma 1 and hence $\eta_2T(\lambda\eta_1)$ is in $\mathfrak{n}$. Hence, by (3), (4), and (12) it is necessary and sufficient for (10) that $\{a-N(\lambda)\}\eta_1'\eta_2$ be in $\mathfrak{m}_c$ in the four cases: $\eta_1=\eta_2=r$; $\eta_2=rv$; $\eta_1=rv$, $\eta_2=r$; $\eta_1=\eta_2=rv$. In the second of these cases (10) requires that $r^2\{a-N(\lambda)\}v$ be in $\mathfrak{m}_c$ which holds, by (3), if and only if

$$
r^2\{a - N(\lambda)\} = k_3g_2, \qquad k_3 \text{ in } \mathfrak{g}.
\tag{13}
$$

It is readily seen that the first and third cases require no additional conditions. In view of (4), (13) is also necessary and sufficient in the fourth case. This completes the proof of

LEMMA 2. *If the elements of* $\mathfrak{S}$ *have integral traces,* $\mathfrak{S}$ *has Property* C_m *if and only if* (13) *holds.*

We now return to Property I and prove

LEMMA 3. *If* $\mathfrak{S}$ *has Property* C_m *then* $\mathfrak{S}$ *has Property* I.

It is plain that (7) is a $\mathfrak{g}$-basis of $\mathfrak{S}$. For any s in $\mathfrak{S}$ we have

$$
s = \sum_{i=0}^{3} \sigma_i v_i, \qquad \sigma_i \text{ in } \mathfrak{g} \qquad (i = 0, \cdots, 3).
$$

By means of this basis, in the manner indicated in the Introduction, we form the representation of Q as an algebra of matrices of degree 4 with elements in R. In this representation s in $\mathfrak{S}$ corresponds to a matrix with elements in $\mathfrak{g}$ by Property C_m. Hence s is integral since it satisfies the characteristic equation of this matrix.

Combining Lemmas 1, 2, and 3 we have

THEOREM 3. *The set* $\mathfrak{S}$ *in* (6) *is an order of* Q *if and only if* (8) *and* (13) *hold with* k_1, k_2, *and* k_3 *in* $\mathfrak{g}$.

4. The maximality condition. We now study Property M in connection with the reduced discriminant, for brevity, discriminant, of an order.

This is defined* for algebras Q over R, as the discriminant of any $\mathfrak{g}$-basis (see §2) of the order. By the following lemma, the discriminant of an order is independent of the $\mathfrak{g}$-basis.

LEMMA. *If $v_0, \cdots, v_3$, and $u_0, \cdots, u_3$, are two R-bases of Q, such that $(u_0, \cdots, u_3) = A(v_0, \cdots, v_3)$, where A is a rational matrix of degree* 4, *then*

$$\Delta(u_0, \cdots, u_3) = |A|^2 \Delta(v_0, \cdots, v_3).$$

The lemma is a well known consequence of the linearity and symmetry of the trace function. If the u's and v's are $\mathfrak{g}$-bases of the same order, $|A|^2 = 1$.

The discriminant of $\mathfrak{K}$ in Theorems 1 and 2 is

$$\Delta(\mathfrak{K}) = -r^4c^4a^2d^2/g_2^2. \tag{14}$$

This can be verified by computing the discriminant of the $\mathfrak{g}$-basis (7) of $\mathfrak{K}$ by means of the lemma from $\Delta(1, c\omega, u, uc\omega)$ which is easily found directly.

The discriminant of a maximal order $\mathfrak{M}$ of Q, which is invariant for all $\mathfrak{M}$, is called the discriminant $\Delta(Q)$ of Q. It is known (cf. Reichardt, loc. cit.) that π^2 divides $\Delta(Q)$, π^3 does not divide $\Delta(Q)$, for each of the primes π described in the Introduction, and that $\Delta(Q)$ is not divisible by any other rational prime. For the purposes of the next section it is convenient to define a_0 as the product of the π or as the negative of their product according as the number of π is even or odd. With (14) and the lemma these remarks imply $\Delta(Q) = -a_0^2$ and yield

THEOREM 4. *An order of Q given by Theorems* 1, 2, *and* 3 *is maximal if and only if*

$$r^4c^4a^2d^2 = a_0^2g_2^2. \tag{15}$$

5. **Canonical generations.** We now describe canonical generations of the Q in

THEOREM 5. *Each Q has a canonical generation $Q = (a_0, P)$, where a_0 is the quantity defined in* §4 *and P is any quadratic field with the following properties. The discriminant of P is $-p$, where p is a prime such that $p \equiv 3$* (mod 4) *and each prime factor of a_0 is a quadratic non-residue, while a_0 is a quadratic residue modulo p. The discriminant of Q is $-a_0^2$.*

This theorem follows at once from theorems of Albert (loc. cit., Theorems 1, 2, and 3) by verifying, either by the use of Hasse's theory, or by computing the discriminant of the special maximal orders found by Albert, that the

* See Reichardt, *Die Diskriminante einer normalen einfachen Algebra*, Journal für Mathematik, vol. 172 (1935), pp. 31–35, for the extension of the definition to the case of an algebra over an algebraic number field and for the form of the discriminant in terms of ideals of the coefficient field.

quantity σ of Albert's Theorem 3 is the quantity a_0 we defined in §4. Similar canonical generations exist* for cyclic division algebras of odd prime degree over R.

To express the conditions of Theorems $1, \cdots, 4$ in terms of a canonical generation we replace a by a_0 and d by $-p$. We assume, without loss of generality, that $g>0$ and $r>0$. Then from (15) we get $g_2^2=r^4c^4p^2$, $g_2=r^2c^2p$, whence $g_2=pg^2$, g in $\mathfrak{g}$, $r=g/c$. Next, (4) requires $g_1=ph$, h in $\mathfrak{g}$, and

$$ph^2 - cph + c^2(p+1)/4 = g_3g^2 \equiv 0 \pmod{g^2}. \tag{16}$$

From (5) and (8), we now obtain

$$\begin{aligned} \lambda &= e_0 + e_1\omega, \\ ge_0 &= \{ph - c(p-1)/2\}k_1 - pg^2k_2, \\ ge_1 &= (2h - c)k_1 - 2g^2k_2. \end{aligned} \tag{17}$$

Finally, we compute $N(\lambda)=\lambda\lambda'$ from (17) and substitute in (13) which becomes

$$a_0 - g_3k_1^2 + p(2h-c)k_1k_2 - pg^2k_2^2 = k_3c^2p \equiv 0 \pmod{c^2p}. \tag{18}$$

This completes the proof of

Theorem 6. *Let $Q=(a_0, P)$ be a canonical generation. Every maximal order $\mathfrak{M}$ of Q is of the form*

$$\mathfrak{M} = 1\ \mathfrak{m}_c + (\lambda + u)\mathfrak{n}, \tag{19}$$

where

$$\mathfrak{m}_c = 1\cdot\mathfrak{g} + c\omega\cdot\mathfrak{g}, \qquad \omega = \{-p + (-p)^{1/2}\}/2, \qquad c \geqq 1 \textit{ in } \mathfrak{g}, \tag{20}$$

is the intersection of $\mathfrak{M}$ and P;

$$\mathfrak{n} = r\cdot\mathfrak{g} + rv\cdot\mathfrak{g}, \qquad r = g/c, \qquad v = (ph + c\omega)/pg^2, \tag{21}$$

where g and h are in $\mathfrak{g}$ and satisfy (16), *and λ in Z is given by* (17) *for k_1, and k_2 in $\mathfrak{g}$ such that* (18) *holds. Conversely, if c, g, and h are such that* (16) *holds and there exists a solution k_1, k_2 in $\mathfrak{g}$ of* (18), *define $\mathfrak{m}_c$ and $\mathfrak{n}$ by* (20) *and* (21). *Then if λ is given by* (17) *with any solution of* (18), *$\mathfrak{M}$ in* (19) *is a maximal order of Q whose intersection with P is $\mathfrak{m}_c$.*

The question as to the existence of maximal orders $\mathfrak{M}$, that is, the existence of integers c, g, h, etc., satisfying the conditions of Theorem 6, is deferred to the next section. For the sake of completeness we here adjoin the multiplication table of a $\mathfrak{g}$-basis of $\mathfrak{M}$ in (19). No use is made of this in what follows. We have

* Cf. Hull, these Transactions, vol. 38 (1935), p. 517.

$$\mathfrak{M} = v_0\cdot\mathfrak{g} + v_1\cdot\mathfrak{g} + v_2\cdot\mathfrak{g} + v_3\cdot\mathfrak{g},$$
$$v_0 = 1, \qquad v_1 = c\omega, \qquad v_2 = (\lambda + u)r, \qquad v_3 = (\lambda + u)rv,$$

where all quantities are as defined in Theorem 6. The following relations hold:

$$v_0v_i = v_iv_0 = v_i \qquad (i = 0, \cdots, 3)$$
$$v_1^2 = -c^2(p^2+p)/4 - cpv_1,$$
$$v_1v_2 = pg^2k_2 - p(h-c)k_1 + k_1v_1 + p(h-c)v_2 - pg^2v_3,$$
$$v_1v_3 = hpk_2 - g_3k_1 + k_2v_1 + g_3v_2 - hpv_3,$$
$$v_2v_1 = -hpv_2 + pg^2v_3, \qquad v_2^2 = pg^2k_3 + k_1v_2,$$
$$v_2v_3 = hpk_3 + k_3v_1 + k_1v_3, \qquad v_3v_1 = -g_3v_2 + p(h-c)v_3,$$
$$v_3v_2 = p(h-c)k_3 - k_3v_1 + k_2v_2, \qquad v_3^2 = g_3k_3 + k_2v_3.$$

6. **On the existence of maximal orders.** As a special case of a general theorem of Schilling* on division algebras of prime degree over an algebraic field, we have the following existence theorem.

THEOREM 7. *There exists a maximal order of $Q=(a_0, P)$ whose intersection with P is a given order $\mathfrak{m}_c$ of P if and only if c is prime to the discriminant of Q, that is, if and only if*

$$(c, a_0) = 1. \tag{22}$$

This theorem can also be proved directly by means of Theorems 5 and 6. We shall indicate a proof of the sufficiency of (22) later. The necessity can be shown as follows. If π is an odd prime dividing a_0 the Legendre symbol $(\pi/p)=-1$ by Theorem 5. This is equivalent to $(-p/\pi)=-1$ by the quadratic reciprocity law and $p\equiv 3 \pmod 4$. From this it follows that the highest power of π which divides any value of the quadratic form px^2+y^2, x and y in $\mathfrak{g}$, is even. Multiply (18) by $4g^2$, apply (16) and complete the square. There results

$$p\{(2h-c)k_1 - 2g^2k_2\}^2 + c^2k_1^2 = 4g^2(a_0 - k_3c^2p). \tag{23}$$

If π divides c, evidently the highest power of π which divides (23) is odd since π^2 does not divide a_0. This contradiction, with a similar one in case 2 divides a_0, implies (22).

Henceforth let $c\geqq 1$ be fixed and assume (22). To determine all $\mathfrak{M}$ whose intersection with P is $\mathfrak{m}_c$ we have first, by Theorem 6, to determine all $\mathfrak{n}=\mathfrak{n}(g, h)$ of the form (16) and (21) such that (18) has solutions and then, for a fixed $\mathfrak{n}$, to determine the effect of taking distinct solutions of (18). We now seek a criterion for the $\mathfrak{n}(g, h)$ such that (18) has solutions.

* Schilling, Mathematische Annalen, vol. 111 (1935), p. 376.

The quadratic form

$$f = f(k_1, k_2) = g_3k_1^2 - p(2h - c)k_1k_2 + pg^2k_2^2 \tag{24}$$

belongs to a class* of quadratic forms of discriminant $-c^2p$, $p\equiv 3 \pmod 4$, uniquely determined by $\mathfrak{n}$. For, $f=c^2pN(k_2r-k_1rv)$ and a unimodular substitution on the $\mathfrak{g}$-basis (21) of $\mathfrak{n}$ corresponds to a similar substitution on k_1 and k_2. A prime which divides each of g_3, $p(2h-c)$ and pg^2 divides c by (16). Hence, by (22), *a necessary condition that* (18) *have solutions is that f be primitive.* Then f has the following characters.† If $c>1$, let

$$c = 2^\alpha p^\beta q_1^{\alpha_1} \cdots q_s^{\alpha_s}, \qquad (q_1 \cdots q_s, 2p) = 1, \tag{25}$$

be the canonical factorization of c into prime powers. If $\alpha=0$ or 1, f has the (only) characters (f/p) and (f/q_i) $(i=1, \cdots, s)$. If $\alpha=2$, f has the (only) additional character $\delta(n)=(-1)^{(n-1)/2}$, n odd and represented by f. If $\alpha\geqq 3$, f has the (only) additional characters δ and $\epsilon(n)=(-1)^{(n^2-1)/8}$, n odd and represented by f. Since $(a_0, c^2p)=1$ by (22) and Theorem 5, the Legendre symbols (a_0/p) and (a_0/q_i) and the quantities $\delta(a_0)$, $\epsilon(a_0)$ if δ and ϵ occur for f, define a total character $C(a_0)$ for the discriminant $-c^2p$. The congruence $f\equiv a_0 \pmod{c^2p}$ is easily shown to have solutions if and only if the characters of f have the values prescribed by $C(a_0)$. This is the criterion sought. We have proved

THEOREM 8. *Let c be fixed and satisfy* (22). *Then* (18) *has solutions for all and only those $\mathfrak{m}_c$-moduls $\mathfrak{n}(g, h)$ for which the associated forms f are primitive and such that their characters have the values prescribed by $C(a_0)$.*

The conditions of Theorem 8 lead to necessary conditions on the integers g. We first prove the

LEMMA. *The form f associated with $\mathfrak{n}(g, h)$ is primitive if and only if h can be chosen so that*

$$(g_3, c^2p) = 1. \tag{26}$$

If (26) *holds* (18) *has solutions if and only if $C(g_3)=C(a_0)$.*

The sufficiency of (26) for the primitivity of f is obvious by an earlier remark. To prove the necessity, first let $\beta\geqq 0$. Then (18) requires $(g_3, p)=1$ and (16) implies $g=p^\beta g_0$, $(g_0, p)=1$, $h=p^\beta h_0$. We cancel $p^{2\beta}$ in (16) and have $(g_3, p)=1$. Moreover, $(g_3/p)=1$. Second, suppose q_i, for a fixed i, does not

* If $\mathfrak{n}$ is a regular $\mathfrak{m}_c$-modul, that is, an $\mathfrak{m}_c$-ideal, the class to which f belongs is primitive and corresponds in the usual way (see Fricke, loc. cit.) to the ideal-class of the order $\mathfrak{m}_c$ to which $\mathfrak{n}$ belongs.

† See Dickson, *Introduction to the Theory of Numbers*, pp. 82–87, or, *Studies in the Theory of Numbers*, p. 37.

divide g. Then, without altering $\mathfrak{n}(g, h)$, we can take $(h, q_i)=1$ and have $(g_3, q_i)=1$ trivially. Moreover, then $(g_3/q_i)=(p/q_i)$. If q_i divides g, (16) implies q_i divides h. Then the primitivity of f requires $(g_3, q_i)=1$. Since h is uniquely determined modulo g^2 by $\mathfrak{n}$, in this case g_3 is uniquely determined modulo q_i by $\mathfrak{n}$. Third, if $\alpha>0$, we proceed for factors 2 as for q_i. In this case, if g is odd, we obtain the additional results that $g_3\equiv p$ (mod 4) or (mod 8) in case $\alpha=2$ or $\alpha\geqq 3$, respectively, and if g is even, g_3 is uniquely determined modulo 4 or 8 in case $\alpha=2$ or $\alpha\geqq 3$, respectively.

The last part of the lemma is obvious since g_3 is represented by f and, if (26) holds, $C(g_3)$ is the total character of f.

The additional conditions on g_3 stated in the proof of the lemma, together with the lemma, lead easily to the following theorem, the details of whose proof we omit.

THEOREM 9. *An integer g, such that* (16) *has solutions, leads to $\mathfrak{m}_c$-moduls $\mathfrak{n}(g, h)$ satisfying the conditions of Theorem* 8 *only if*

$$g = 2^{\alpha_0}p^{\beta}Q_1g_0, \qquad (g_0, p) = 1, \tag{27}$$

where β is given in (25), *Q_1 is the product of the prime powers $q_i^{\alpha_i}$ in* (25) *for which $(p/q_i)\neq(a_0/q_i)$, and $\alpha_0=0$ if $\alpha=0$ or* 1, *$\alpha_0=0$ or* 1 *if $\alpha=2$ according as $p-a_0\equiv 0$ or* 2 (mod 4) *and $\alpha_0=0$, $\alpha-1$, $\alpha-2$, or $\alpha-1$ if $\alpha\geqq 3$ according as $p-a_0\equiv 0$, 2, 4, or* 6 (mod 8), *respectively.*

It should be noted that g_0 is required by Theorem 9 to be prime to p, but not necessarily prime to $2Q_1$. Naturally, g_0 must be such that (16) have a solution h. The sufficiency of (22) in Theorem 7 can be proved by showing that there exist $\mathfrak{n}(g, h)$ satisfying Theorem 8 for g given by (27) with $g_0=1$. We omit the details of this proof.

We now assume that $\mathfrak{n}(g, h)$ is fixed and such that (18) has solutions. Let $\lambda^{(1)}$ and $\lambda^{(2)}$ be given by (17) with solutions $k_1^{(1)}$, $k_2^{(1)}$ and $k_1^{(2)}$, $k_2^{(2)}$, respectively, of (18). It is plain that $\mathfrak{M}(\lambda^{(1)})=\mathfrak{M}(\lambda^{(2)})$ if and only if

$$(\lambda^{(2)} - u)\mathfrak{n} \subset \mathfrak{M}(\lambda^{(1)}) \tag{28}$$

since $\mathfrak{M}(\lambda^{(2)})$ is maximal. It is readily shown that (28) holds if and only if $r(\lambda^{(2)}-\lambda^{(1)})$ and $rv(\lambda^{(2)}-\lambda^{(1)})$ are in $\mathfrak{m}_c$ and that the conditions, written in (29) below, on the coefficients of ω in these expressions are necessary and sufficient. In this way we obtain

THEOREM 10. *Let c and $\mathfrak{n}(g, h)$ be fixed and such that* (18) *has solutions. Then for two solutions $k_1^{(1)}$, $k_2^{(1)}$ and $k_1^{(2)}$, $k_2^{(2)}$ of* (18), *and $\lambda^{(1)}$ and $\lambda^{(2)}$ defined by* (17) *with these solutions, $\mathfrak{M}(\lambda^{(1)})=\mathfrak{M}(\lambda^{(2)})$ if and only if, simultaneously,*

$$(29)\qquad \begin{aligned} (2h - c)(k_1^{(2)} - k_1^{(1)}) - 2g^2(k_2^{(2)} - k_2^{(1)}) &\equiv 0 \pmod{c^2}, \\ 2g_3(k_1^{(2)} - k_1^{(1)}) - p(2h - c)(k_2^{(2)} - k_2^{(1)}) &\equiv 0 \pmod{c^2 p}. \end{aligned}$$

The conditions found in this section become very simple when $c=1$. Then, by Theorem 9, we must have $(g, p)=1$. For every $\mathfrak{n}(g, h)$ with $(g, p)=1$ and $c=1$, the form f has the (only) character $(f/p)=1=(a_0/p)$, and (18) always has exactly two distinct solutions modulo p which do not satisfy (29). Moreover, without altering (18) modulo p, we may take $k_1 \equiv 0 \pmod{2g^2}$ and then take k_2 such that $e_1=0$. Then λ is in $\mathfrak{g}$. The special maximal orders found by Albert (loc. cit.) are the $\mathfrak{M}$ of Theorem 6 with $c=g=1$. Except for certain particular algebras Q (cf. Schilling, loc. cit.) it is not known that an arbitrary maximal order $\mathfrak{M}$ of Q contains the maximal order of some canonical splitting field P, nor, indeed, that $\mathfrak{M}$ contains the maximal order of any splitting field of Q.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.