$B-B\cdot T=H_2+H_1\cdot B$, and $H_2\cdot C=0$, contrary to the lemma.

6. *Conclusion.* In conclusion attention is called to the desirability of clearing up, in the general case, the possibilities for the power of the class of all sets $[H(N)]$ in a compact space for any system T, such as has already been done by Mazurkiewicz and Alexandroff (see papers in Fundamenta Mathematicae, vols. 19 and 20) in the special case of the dimensional components. Also a more detailed study of the structure of continua M of varying degrees of connectivity and local connectivity with respect to the sets $H(N)$, in particular in the case* considered in §5, would be highly desirable.

THE JOHNS HOPKINS UNIVERSITY

INTEGRAL DOMAINS OF RATIONAL GENERALIZED QUATERNION ALGEBRAS†

BY A. A. ALBERT

1. *Introduction.* We shall consider generalized quaternion algebras

$$Q = (1, i, j, ij), \qquad ji = -ij, \qquad i^2 = \alpha, \qquad j^2 = \beta,$$

over the field R of all rational numbers. It is easily shown that, by a trivial transformation on the basis of Q, we may take α and β to be integers without square factors.

Of great interest in the theory of algebras Q are the integral sets of Q. L. E. Dickson‡ has called a set S of quantities of Q an integral set if S satisfies the following postulates:

R: The quantities of S have minimum equations with ordinary whole number coefficients and leading coefficient unity.

C: S is closed under addition, subtraction, and multiplication.

U: S contains $1, i, j$.

M: S is maximal.

---

* A further study of this case is made in the author's paper *Cyclic elements of higher order*, to appear in the American Journal of Mathematics, vol. 56 (1934).

† Presented to the Society, June 19, 1933.

‡ See Dickson's *Algebren und ihre Zahlentheorie*, pp. 154–197, for his theory as well as references to the work of Latimer and Darkow. See also Latimer's later paper, Transactions of this Society, vol. 32 (1930), pp. 832–846.

Using the above definition for S, Dickson considered the integral sets for algebras Q with $\alpha = -1$. By a further transformation on the basis of algebras Q, Dickson showed, for his case $\alpha = -1$, that β could be taken to have no prime factors $p = 4n+1$. He then obtained the sets S. Latimer considered algebras Q with $\alpha \equiv \beta \equiv 1 \pmod 2$, and with $\alpha \equiv 2$, $\beta \equiv 1 \pmod 8$ and, after transformations on the basis of Q, obtained many sets S for each algebra Q. Similar considerations were made by Marguerite Darkow for the case $\alpha \equiv \beta \equiv 2 \pmod 4$. These latter results of Latimer and Darkow are very complicated and do not *complete* the problem of finding an integral set for every generalized quaternion algebra.

The above division into special cases is certainly not desirable. Nor is it necessary. For it is obvious that at least an attempt should be made to show that transformations carrying all the cases into a canonical form are possible and it is this canonical form which should be studied.

In the present paper such a canonical form is obtained. It is shown that every rational generalized quaternion algebra is equivalent to an algebra with $\alpha = \tau \equiv 1 \pmod 4$, where $-\tau$ is a positive prime. The integer $\beta = \sigma$ is also restricted. In particular it is evident that integral sets S should contain the integers of the field $R(i)$ and hence 1, $P = (1+i)/2$, is a basis of such integers. Hence the postulate U is replaced here by

U': $\qquad\qquad S$ contains $1, P, j$.

But then it is shown that there exist two* sets $S, \overline{S}$ satisfying R, C, U', M, and the bases of these sets are explicitly determined.

2. *Transformations on Algebras* Q. Let R be the field of all rational numbers and let Q be any normal simple algebra of degree two over R. Then

$$(1) \quad Q = Q(\alpha, \beta) = (1, i, j, ij), \quad ji = -ij, \quad i^2 = \alpha, \quad j^2 = \beta,$$

where $\alpha \neq 0$ and $\beta \neq 0$ are in R. Conversely, every algebra (1) is normal simple.

---

* Essentially only one set, as we show here that $\sigma = \epsilon\tau + 4\mu^2$ and obtain a corresponding set S. But then $\sigma = \epsilon\tau + 4(-\mu)^2$ and $\overline{S}$ is obtained from S by replacing μ by $-\mu$.

If we have $i_0=\lambda i$, $j_0=(\lambda+\nu i)j$, then $j_0 i_0=-i_0 j_0$, $i_0^2=\lambda^2\alpha$, $j_0^2=(\mu^2-a\nu^2)\beta$, and $Q=(1, i_0, j_0, i_0 j_0)$. Hence we have the following lemma.

LEMMA 1. *If λ, μ, ν are rational numbers, then $Q(\alpha, \beta)=Q(\gamma, \delta)$, where $\gamma=\lambda^2\alpha$, $\delta=(\mu^2-\alpha\nu^2)\beta$.*

Next let $i_0=x_1 i+x_2 j+x_3 ij$, so that

$$i_0^2 = \gamma = f(x_1, x_2, x_3) = x_1^2\alpha + x_2^2\beta - x_3^2\alpha\beta. \tag{2}$$

Then I have proved* the following fact.

LEMMA 2. *If $\gamma=f(x_1, x_2, x_3)\not\equiv x_1^2\alpha$ of (2) for rational x_1, x_2, x_3, then $Q(\alpha, \beta)=Q(\gamma, \delta)$, where in fact $\delta=-\alpha\beta(x_2^2-x_3^2\alpha)$.*

If α is rational, then $\alpha=\rho\epsilon^{-1}$, where ρ and ϵ are relatively prime integers. Then $\rho\epsilon=\xi^2\alpha_0$, where ξ and α_0 are integers and α_0 has no square factors. If $\alpha_1=\xi\epsilon^{-1}$, then $\alpha=\alpha_1^2\alpha_0$ and we call α_0 the *kernel* of α.

By Lemma 2 any integer having the form $x_1^2\alpha+x_2^2\beta-x_3^2\alpha\beta$ for rational x_1, x_2, x_3 may be chosen as a new α. Let $\alpha_0, \beta_0, \gamma_0$ be the kernels of $\alpha, \beta, -\alpha\beta$, respectively, so that every value of the form $F(x, y, z)=\alpha_0 x^2+\beta_0 y^2+\gamma_0 z^2$ for integral x, y, z is represented *rationally* by (2) and may be taken to replace α.

Evidently γ_0 is the kernel of $-\alpha_0\beta_0$, so that not all three of $\alpha_0, \beta_0, \gamma_0$ are even. Moreover, one of $\alpha_0, \beta_0, \gamma_0$ is negative. Either $\alpha_0\equiv\beta_0\equiv\gamma_0\equiv 3 \pmod 4$, so that $F(1, 1, 1)\equiv 9\equiv 1 \pmod 4$, or one letter, say a, is even, and one, say b, satisfies the congruence $b\equiv 3 \pmod 4$, whence $a\cdot 1^2+b\cdot 1^2\equiv 2+3\equiv 1 \pmod 4$.

If $\alpha>0$, then one of β_0 and γ_0, say b, is negative, so that $\rho=\alpha+4b\alpha^2=\alpha(1+4\alpha\beta)<0$, $\rho\equiv 1 \pmod 4$, and is a value of $f(x_1, x_2, x_3)$. Hence we may take $\alpha<0$, $\alpha\equiv 1 \pmod 4$.

Let us now apply Lemma 1 to replace $\alpha=\alpha_1^2\alpha_0$, $\beta=\beta_1^2\beta_0$ by their kernels α_0, β_0. This is evidently accomplished when we have $\lambda=\alpha_1^{-1}$, $\mu=\beta_1^{-1}$, $\nu=0$. Hence take $\alpha_0\equiv 1 \pmod 4$, $\alpha_0<0$.

Let π be the greatest common divisor of α_0, β_0, so that $\alpha_0=\alpha_2\pi$, $\beta_0=\beta_2\pi$. Then α_2, β_2, π are relatively prime in pairs since α_0 and β_0 have no square factors. It follows that α_0 is prime to $\beta_2(\pi-\alpha_2)$. But if $\lambda=1, \mu=1, \nu=\pi^{-1}$ in Lemma 1, then

* See my paper in this Bulletin, vol. 37 (1933), pp. 257–258, for the results implying Lemmas 1 and 2.

$\gamma=\alpha_0$, $\delta=(1-\pi^{-2}\alpha_2\pi)\pi\beta_2=\beta_2/(\pi-\alpha_2)$. We use Lemma 1 to replace $\beta_2(\pi-\alpha_2)$ by its kernel and thus prove the following theorem.

THEOREM 1. *Every normal simple algebra of degree two over R is equivalent to an algebra $Q(\alpha, \beta)$, where α and β are relatively prime integers without square factors, $\alpha<0$, $\alpha\equiv 1 \pmod 4$.*

The quadratic form $\phi=-\alpha x^2-4\beta y^2$ has relatively prime coefficients, positive leading coefficient, and discriminant $\Delta=-16\alpha\beta$. Evidently Δ is an integral square if and only if $-\alpha\beta=1$, $-\alpha=\beta=1$, which is impossible since $-\alpha\equiv 3 \pmod 4$. By the Dirichlet Theorem,* ϕ represents infinitely many positive primes p. Since $-\alpha\beta$ has only a finite number of prime divisors, infinitely many positive primes p represented by ϕ are prime to $-\alpha\beta$. If $\tau=-p$, then

$$\tau = \alpha x^2 + 4\beta y^2, \qquad -\alpha\beta x^2 \equiv (2\beta y)^2 \pmod \tau.$$

If $x\equiv 0 \pmod \tau$, then necessarily $y\equiv 0 \pmod \tau$, so that $\alpha x^2+4\beta y^2=\tau\equiv 0 \pmod{\tau^2}$, which is impossible. Hence x is prime to τ, $tx\equiv 1 \pmod \tau$ for integral t, $-\alpha\beta\equiv(2\beta yt)^2 \pmod \tau$, and $-\alpha\beta=4\mu^2+\epsilon\tau$ for integral μ, ϵ. By Lemma 2, with $x_1=x$, $x_2=y$, $x_3=0$, we have $\delta=-4\alpha\beta x_2^2$ whose kernel is $-\alpha\beta$. Hence the following theorem is established.

THEOREM 2. *Every normal simple algebra of degree 2 over R is equivalent to an algebra $Q(\tau, \sigma)$, where σ has no square factors and is prime to τ, $-\tau$ is a prime, and $\sigma = 4\mu^2 + \epsilon\tau$ when $\tau < 0$ and $\tau \equiv 1 \pmod 4$, for integral μ, ϵ.*

3. *The Removal of Certain Factors of σ.* It is well known that the quadratic form

$$x^2 - \tau y^2 - \rho z^2, \qquad (\tau, \rho) = 1, \tag{3}$$

is a zero form, for τ prime to ρ, if and only if τ is a quadratic residue of ρ and ρ is a quadratic residue of τ.

Evidently τ is a quadratic residue of 2. But 2 is a quadratic residue of τ if and only if $\tau\equiv 1 \pmod 8$. For if $\tau=-t$, t a prime, then

* See A. Meyer, Journal für Mathematik, vol. 103 (1888), pp. 98–116.

$$(4)\quad \begin{cases} (2\,|\,\tau) = (2\,|\,t) = (-1)^{(t^2-1)/8} = 1, \quad t^2 \equiv r^2 \equiv 1 \pmod{16}, \\ (4n+1)^2 \equiv 8n+1 \equiv 1 \pmod{16}, \ n \equiv 0 \pmod 2, \\ \qquad\qquad\qquad\qquad\qquad\qquad \tau = 8n_1 + 1. \end{cases}$$

Let ρ be the product of all the odd prime factors q of σ such that τ is a quadratic residue of each such q. Let $\rho_0 = 2\rho$ if $\tau \equiv 1 \pmod 8$ and σ is even, while $\rho_0 = \rho$ if either σ is odd or $\tau \not\equiv 1 \pmod 8$. Then $x^2 - \tau y^2 - \rho_0 z^2 = 0$ for integral x, y, z not all zero. For τ is a quadratic residue of ρ_0, and ρ_0 is a quadratic residue of τ if and only if $(\rho\,|\,\tau) = 1$, since $-\tau = t$ is a prime.* But

$$(5)\quad (\rho\,|\,\tau) = (\rho\,|\,t) = (-1)^e(t\,|\,\rho) = (-1)^f(\tau\,|\,\rho) = (-1)^f = 1,$$

$$e = \frac{\rho-1}{2}\cdot\frac{t-1}{2}, \qquad f = e + \frac{\rho-1}{2} = \frac{\rho-1}{2}\cdot\frac{t+1}{2},$$

since $(\tau\,|\,\rho) = 1$, $t+1 = -\tau+1 \equiv -1+1 \equiv 0 \pmod 4$.

The integer $z \neq 0$, since $x^2 - y^2\tau$ is not a zero form when $-\tau > 1$, is a prime. Hence $\rho_0 = \lambda^2 - \nu^2\tau$ for rational λ, ν. Moreover $\rho_0 = \eta^2 \pmod \tau$, where η is prime to τ. Hence $\eta\zeta \equiv 1 \pmod \tau$ for integral ζ, so that, if $\sigma = \sigma_0\rho_0$, then $\rho_0\sigma_0 \equiv 4\mu^2 \pmod \tau$, $\sigma_0 \equiv 4(\mu\zeta)^2 \pmod \tau$. But $Q(\tau,\sigma) = Q(\tau, \sigma_0)$ by Lemma 1 and the following fact is proved.

THEOREM 3. *In Theorem 2 we may take τ a quadratic non-residue of every odd prime factor of σ and σ odd if $\tau \equiv 1 \pmod 8$.*

It is well known that $Q(\tau, \sigma)$ is a division algebra if and only if the form

$$(6)\qquad x_1^2 - \tau x_2^2 - \sigma x_3^2$$

is not a zero form. Evidently if (6) is a zero form, then $\sigma > 0$. But necessarily if (6) is a zero form, then τ is a quadratic residue of σ. Since τ is a quadratic non-residue of every odd prime factor of σ, then $\sigma = 1, 2$. If $\sigma = 2$, then (6) implies that 2 is a quadratic residue of τ, so that $\tau \equiv 1 \pmod 8$, a contradiction of Theorem 3. Hence $\sigma = 1$. Conversely, if $\sigma = 1$, then $(j-1)(j+1) = 0$ and Q is not a division algebra.

THEOREM 4. *The algebras of Theorem 3 are all division algebras except for $\sigma = 1$.*

* For of course τ is already a quadratic residue of ρ_0 and $(2\,|\,\tau) = 1$ in the case where ρ_0 is even; whence $\tau \equiv 1 \pmod 8$.

Consider now the congruence $x^2\sigma+y^2\tau-z^2\equiv 0 \pmod{4\sigma}$. Then $y^2\tau-z^2\equiv 0 \pmod{\sigma}$. If q is any odd prime factor of σ not dividing y, then τ is a quadratic residue of q, a contradiction. But σ has no square factors so that $\sigma=\sigma_0$ or $2\sigma_0$, where σ_0 is odd, $y\equiv 0 \pmod{\sigma_0}$ so that $z\equiv 0 \pmod{\sigma_0}$. If σ_1 is even, then $\tau\not\equiv 1 \pmod 8$, $x^2\sigma+y^2\tau-z^2\equiv 0 \pmod 8$. But $y^2\tau-z^2\equiv 0 \pmod 2$, since σ is even. Hence $y\equiv z \pmod 2$ so that, since $\tau\equiv 1 \pmod 4$, we shall have $y^2\tau-z^2\equiv 0 \pmod 4$, $x^2\sigma\equiv 0 \pmod 4$, $x\equiv 0 \pmod 2$, $x^2\sigma\equiv 0 \pmod 8$, and $y^2\tau\equiv z^2 \pmod 8$. If y is odd, then z is odd and $y^2\tau-z^2\equiv\tau-1\equiv 0 \pmod 8$, which is a contradiction. Hence y is even, $y\equiv z\equiv 0 \pmod 2$, and we have proved the following result.

THEOREM 5. *The integral congruence* $x^2\sigma+y^2\tau-z^2\equiv 0 \pmod{4\sigma}$ *implies that* $y\equiv z\equiv 0 \pmod{\sigma}$.

4. *On Domains of Integrity.* Let D be a rational semi-simple algebra of order n. A set S of quantities of D is called a domain of integrity if it is closed under addition, subtraction, multiplication. Assume also that the quantities of S satisfy integral equations and that S contains the modulus 1 of D. Then if S has order n, it is well known* that S has a basis

$$\omega_{10}, \omega_{20}, \cdots, \omega_{n0} = 1. \tag{7}$$

We may evidently write

$$\omega_{i0} = \sum_{j=1}^{n} \alpha_{ij} u_{j0}, \qquad (i = 1, \cdots, n),$$

where the u_{j0} are a basis of D, the α_{ij} are rational, and

$$u_{n0} = 1. \tag{8}$$

Then the matrix $A=\|\alpha_{ij}\|$ is non-singular and

$$A = \alpha^{-1}\|\beta_{ij}\| = \alpha^{-1}B, \tag{9}$$

where B is an integer matrix, α is an integer. If $C=\|c_{ij}\|$ is an integer matrix of determinant unity, the transformation

$$\omega_{i0}' = \sum c_{ij}\omega_{i0} \tag{10}$$

evidently replaces the ω_{j0} by a new basis of S. But it is well

* See Dickson, *Algebren und ihre Zahlentheorie*, p. 212.

known† that there exists such a matrix C such that

$$CB = B_0 = \|\gamma_{ij}\| \tag{11}$$

has elements below the diagonal all zero. Then

$$\omega_i' = \alpha^{-1} \sum \gamma_{ij} u_{j0} = \sum \delta_{ij} u_{j0}. \tag{12}$$

But now re-arrange the u_{i0} so that $u_i = u_{n-i,0}$ and similarly $\omega_i = \omega_n'_{-i}$. Then

$$\omega_i = \sum_{j=1}^{i} a_{ij} u_j, \tag{13}$$

with rational a_{ij}. In particular

$$\omega_1 = a_{11} \cdot 1, \qquad (a_{11} \text{ in } R), \tag{14}$$

satisfies an integral equation so that a_{11} is integral. But unity is in S so that, since each ω_i contains one more basal unit than ω_{i-1}, we evidently must have unity an integral multiple of ω_1. Hence $a_{11} = 1$.

THEOREM 6. *If D is a rational semi-simple algebra of order n and S is a domain of integrity of the nth order in D such that the quantities of S satisfy integral equations and the modulus $u_1 = 1$ of A is in S, then S has a basis*

$$\omega_i = \sum_{j=1}^{i} a_{ij} u_j, \qquad (\omega_1 = 1, \ a_{ij} \text{ in } R), \tag{15}$$

for $i = 1, \cdots, n$.

In particular let S contain the basal quantities of D. Then

$$u_i = \sum_{j=1}^{n} \eta_{ij} \omega_j, \qquad (i = 1, \cdots, n), \tag{16}$$

with integer η_{ij}. Since the u_i are linearly independent in R, and ω_n contains u_n, but no other ω_i, $(i < n)$, contains u_n, we evidently have $\eta_{in} = 0$, $(i < n)$. Similarly $\eta_{ij} = 0$, $(j = i+1, \cdots, n)$, so that

$$u_i = \sum_{j=1}^{i-1} \eta_{ij} \omega_j + \eta_{ii} \omega_i.$$

† Ibid., p. 221.

Again applying the linear independence of the u_i to coefficients of the u_i, we have

$$1 = a_{ii}\eta_{ii}, \tag{17}$$

so that we have proved the following theorem.

THEOREM 7. *If S contains the basal quantities of A and if* (15) *holds we have*

$$a_{ii} = \frac{1}{\alpha_{ii}}, \tag{18}$$

*where the α_{ii} are integral.**

Let us consider now a generalized quaternion algebra

$$Q = (1, i, j, ij), \qquad ji = -ij, \qquad i^2 = \tau, \qquad j^2 = \sigma, \tag{19}$$

with integer τ and σ. Then if S is a domain of integrity of Q which contains the quantities 1, i, j, and hence ij, and which is such that the quantities of S satisfy integral equations, then S has a basis

$$\begin{aligned} \omega_1 &= 1, & \omega_3 &= \beta_1 + \beta_2 i + \beta_3 j, \\ \omega_2 &= \alpha_1 + \alpha_2 i, & \omega_4 &= \gamma_1 + \gamma_2 i + \gamma_3 j + \gamma_4 ij, \end{aligned} \tag{20}$$

with rational α_i, β_i, γ_i. Every quantity

$$x = \delta_1 + \delta_2 i + \delta_3 j + \delta_4 ij \tag{21}$$

satisfies

$$\omega^2 - 2\delta_1\omega + N(x) = 0, \tag{22}$$

where x satisfies an integral equation only for integer

$$2\delta_1, \qquad N(x) = \delta_1^2 - \delta_2^2\tau - \delta_3^2\sigma + \delta_4^2\tau\sigma. \tag{23}$$

Hence $2\alpha_1$, $2\beta_1$, $2\gamma_1$, are rational integers. Also $i\omega_2 = \alpha_2\tau + \alpha_1 i$

---

* Notice that in fact

$$\omega_i = \alpha_{ii}^{-1}\left(u_i - \sum_{j=1}^{i-1} \alpha_j\omega_j\right)$$

which may simplify the determination of ω_i after the ω_j are determined. This fact is not used here.

satisfies an integral equation (22), so that $2\alpha_2\tau$ is integral. Similarly $2\beta_2\tau$, $2\beta_3\sigma$, $2\gamma_2\tau$, $2\gamma_3\sigma$, $2\gamma_4\sigma\tau$ are integers. But α_2, β_3, γ_4 are the reciprocals of integers by Theorem 6. Hence we have proved the following theorem.

THEOREM 8. *Let Q be a generalized quaternion algebra* (19) *over R and let S be a domain of integrity of Q containing* $1, i, j, ij$, *and with all its quantities satisfying integral equations. Then S has a basis*

$$(24)\quad \begin{cases} \omega_1 = 1, \quad \omega_2 = \dfrac{\xi_1}{2} + \dfrac{1}{\xi_2} i, \quad \omega_3 = \dfrac{\eta_1}{2} + \dfrac{\eta_2}{2\tau} i + \dfrac{1}{\eta_3} j, \\ \omega_4 = \dfrac{\zeta_1}{2} + \dfrac{\zeta_2}{2\tau} i + \dfrac{\zeta_3}{2\sigma} j + \dfrac{1}{\zeta_4} ij, \end{cases}$$

where the ξ_i, η_i, ζ_i are integers, and

$$(25)\quad 2\tau \equiv 0 \pmod{\xi_2}, \quad 2\sigma \equiv 0 \pmod{\eta_3}, \quad 2\sigma\tau \equiv 0 \pmod{\zeta_4}.$$

5. *Two Integral Sets of Q.* We shall consider generalized quaternion division algebras Q over R. Our algebras are therefore algebras of Theorem 4 with $\sigma \neq 1$. Consider the quantities

$$(26)\quad v_1 = 1, \quad v_2 = \frac{1+i}{2}, \quad v_3 = j, \quad v_4 = \frac{i(2\mu + j) + \tau j}{2\tau}.$$

Since $\tau = 4n+1$, $\sigma = 4\mu^2 + \epsilon\tau$, we have

$$(27)\quad v_3^2 = \sigma, \quad v_2^2 = v_2 + n, \quad v_4^2 = \epsilon n + \mu^2,$$

so that the quantities (26) satisfy integral equations.

We study the set S of linear combinations

$$(28)\quad \sum_{i=1}^{n} \lambda_i v_i$$

with integer λ_i. Evidently S satisfies U', since S contains 1, $P = v_2$, j. Also S is closed under addition and subtraction. It is evident that, since the basal quantities (26) of S satisfy integral equations, S will satisfy postulates R and C if and only if S is closed under multiplication. In order to prove this closure we need only prove that S contains

$$v_2v_3, \quad v_3v_2, \quad v_2v_4, \quad v_4v_2, \quad v_3v_4, \quad v_4v_3. \tag{29}$$

In particular S contains

$$j = v_3, \quad i = 2v_2 - 1, \quad ij = 2\tau v_4 - 2\mu i - \tau j. \tag{30}$$

We compute

$$v_3v_2 = \frac{j(i+1)}{2} = \frac{(1-i)j}{2} = (1 - v_2)v_3 = v_3 - v_2v_3, \tag{31}$$

which is in S if and only if v_2v_3 is in S. But

$$v_2v_3 = \frac{(1+i)}{2} j = \tau v_4 - \mu i - 2\eta j \tag{32}$$

is in S. Also

$$\begin{cases} v_4v_3 = \dfrac{i(2\mu j + \sigma) + \sigma\tau}{2\tau} = 2\mu v_4 + \dfrac{\sigma - 4\mu^2}{2\tau} i - \mu j + \dfrac{\sigma}{2} \\ \quad = 2\mu v_4 - \mu v_3 + \dfrac{\lambda i + \sigma}{2} \\ \quad = 2\mu v_4 - \mu v_3 + 2n\epsilon + \epsilon\left(\dfrac{1+i}{2}\right) \\ \quad = 2(\mu^2 + n\epsilon) + \epsilon v_2 - \mu v_3 + 2\mu v_4 \end{cases} \tag{33}$$

is in S, while

$$v_3v_4 + v_4v_3 = \sigma, \tag{34}$$

so that v_3v_4 is in S.

It remains to prove v_2v_4 and v_4v_2 in S. Now

$$v_2v_4 = \frac{1+i}{2} \cdot \frac{2\mu i + ij + \tau j}{2\tau} = \frac{2\mu\tau + 2\mu i + 2\tau j + (\tau + 1)ij}{4\tau}. \tag{35}$$

Since

$$\frac{ij}{2\tau} = v_4 - \frac{2\mu i + \tau j}{2\tau}, \tag{36}$$

we have

$$(37)\quad \begin{cases} v_2v_4 = \dfrac{\tau+1}{2}v_4 + \dfrac{2\tau j + 2\mu i + 2\mu\tau - (\tau+1)(2\mu i + \tau j)}{4\tau} \\ \quad = (2n+1)v_4 + \dfrac{\tau(1-\tau)j + 2\mu\tau(1-i)}{4\tau} \\ \quad = (2n+1)v_4 - nv_3 + \mu v_2 - \mu \end{cases}$$

in S. Finally

$$(38)\quad \begin{cases} v_2v_4 + v_4v_2 = v_2v_4 + \dfrac{2\mu\tau + 2\mu i + (1-\tau)ij}{4\tau} \\ \qquad = \mu + \dfrac{4\mu i + 2\tau j + 2ij}{4\tau} = \mu + v_4 \end{cases}$$

is in S, so that v_4v_2 is in S. We have therefore proved that S satisfies properties R, C, U'.

Since $\sigma = 4\mu^2 + \epsilon\tau$, we have also $\sigma = 4(-\mu)^2 + \epsilon\tau$, so that our above argument by which we proved that S has properties R, C, U' also proves that the set $\overline{S}$ with basis

$$(39)\quad y_i = v_i, \qquad (i = 1, 2, 3), \qquad y_4 = \frac{i(-2\mu + j) + j\tau}{2\tau},$$

also has properties R, C, U'. Moreover S and $\overline{S}$ are actually distinct. For otherwise y_4 is in S, $v_4 + y_4 - j = \tau^{-1}ij$ is in S, whence $-\tau^{-2}\sigma\tau = -\sigma\tau^{-1}$ is an integer, contrary to our hypothesis that $\sigma \not\equiv 0 \pmod{\tau}$.

We shall now prove that every set T which satisfies R, C, U' is either in S or in $\overline{S}$ and hence each of S and $\overline{S}$ is maximal. We will then have proved S and $\overline{S}$ the only sets satisfying R, C, U', M.

Let then T satisfy R, C, U'. Since T is a domain of integrity, it has a basis (24). Hence $\omega_1 = 1$ is in S, $\overline{S}$. Also ω_2 is an integer of the algebraic field $R(i)$ and hence, as is well known,* is an integral linear combination of 1, v_2. Hence ω_2 is in S, $\overline{S}$.

We next write

$$(40)\quad \omega_3 = \frac{\eta_1}{2} + \frac{\eta_2 i}{2}\tau + \frac{1}{\eta_3}j, \qquad 2\sigma \equiv 0 \pmod{\eta_3}.$$

* Dickson, loc. cit., p. 149.

But then

$$\omega_3' = \omega_3 - \eta_1 v_2 = \frac{\eta_2 - \eta_1\tau}{2} i + \frac{1}{\eta_3} j$$

is in T, since T has property C. Hence without loss of generality we may take $\eta_1 = 0$ in (40).

The quantity ω_3 must have an integral minimum equation. This equation evidently is

$$\omega_3^2 = \frac{\eta_2^2\eta_3^2 + 4\sigma\tau}{4\tau\eta_3^2},$$

so that

$$\eta_2^2\eta_3^2 + 4\sigma\tau \equiv 0 \pmod{4\tau\eta_3^2}.$$

Then $4\sigma\tau \equiv 0 \pmod{\eta_3^2}$. Since $\sigma\tau$ has no square factor, we have $4 \equiv 0 \pmod{\eta_3^2}$, $\eta_3 = \pm 1, \pm 2$. But then $\eta_2^2 \equiv 0 \pmod{\tau}$, so that

$$\eta_2 = \eta\tau, \qquad \omega_3 = \frac{\eta i}{2} + \frac{1}{\eta_3} j.$$

Compute

$$v_2\omega_3 = \left(\frac{1+i}{2}\right)\left(\frac{\eta i}{2} + \frac{1}{\eta_3} j\right) = \frac{\eta\tau}{4} + \frac{\eta i}{4} + \frac{j}{2\eta_3} + \frac{ij}{2\eta_3},$$

which must have integral minimum equation (22). Hence $\eta\tau/2$ is an integer, so that $\eta = 2\eta_0$ is even, $\omega_3 - \eta_0 i = \eta_3^{-1} j$ is in T and has integral minimum equation $\omega^2 = \sigma\eta_3^{-2}$. Since σ has no square factor, we have $\eta_3 = \pm 1$, and $\omega_3 = \eta_0 i \pm j$ is in S, $\overline{S}$ as desired.

We finally consider the quantity ω_4. By the above transformation on ω_3 we may take $\zeta_1 = 0$ in (21) and write

$$\omega_4 = \frac{\zeta_2 i}{2\tau} + \frac{\zeta_3 j}{2\sigma} + \frac{ij}{\zeta_4}, \tag{41}$$

where $2\sigma\tau \equiv 0 \pmod{\zeta_4}$. Then $2\sigma\tau = \zeta_4\zeta_5$ and

$$\omega_4 = \frac{\zeta_2 i}{2\tau} + \frac{\zeta_3 j}{2\sigma} + \frac{\zeta_5 ij}{2\sigma\tau}, \tag{42}$$

so that

$$\omega_4^2 = \frac{\zeta_2^2\tau}{4\tau^2} + \frac{\zeta_3^2\sigma}{4\sigma^2} - \frac{\zeta_5^2\sigma\tau}{4\sigma^2\tau^2} = \frac{\zeta_2^2\sigma + \zeta_3^2\tau - \zeta_5^2}{4\sigma\tau} \tag{43}$$

must be integral.

By Theorem 5 we have $\zeta_3 = x_3\sigma, \zeta_5 = x_5\sigma$, and $\zeta_2^2 + (x_3^2\tau - x_5^2) \equiv 0 \pmod{4\tau}$, which is equivalent to

$$(44) \qquad \zeta_2^2 - x_5^2\sigma \equiv 0 \pmod{\tau}, \quad \zeta_2^2 + x_3^2\tau - x_5^2 \equiv 0 \pmod{4}.$$

Also

$$\omega_4 = \frac{\zeta_2 i}{2\tau} + \frac{x_3 j}{2} + \frac{x_5 ij}{2\tau},$$

so that, since $v_2 = 1 + i/2$ is in T, so is

$$v_2\omega_4 = \frac{\zeta_2}{4} + \frac{\zeta_2}{4\tau} i + \frac{x_3 + x_5}{4} j + \frac{x_3\tau + x_5}{4\tau} ij.$$

Since then $v_2\omega_2$ must have integral minimum equation, we see that $\zeta_2/2$ is integral, $\zeta_2^2 \equiv 0 \pmod 4$, $x_3^2\tau - x_5^2 \equiv 0 \pmod 2$ and $x_3 \equiv x_5 \pmod 2$. But then $x_3^2\tau - x_5^2 \equiv 0 \pmod 4$ and $(44)_2$ is satisfied. We write $x_3 = x_5 + 2\lambda$.

Since $\sigma \equiv 4\mu^2 \pmod{\tau}$, we have $\zeta_2^2 \equiv (2\mu x_5)^2 \pmod{\tau}$. But $-\tau$ is a prime so that $\zeta_2 \equiv \pm 2\mu x_5 \pmod{\tau}$, $\zeta_2 = \pm 2\mu x_5 + y\tau$. Since ζ_2 is even, so is $y = 2z$ and

$$\omega_4 = x_5\left(\frac{\pm 2\mu i + \tau j + ij}{2\tau}\right) + \lambda j + zi,$$

which is evidently in S or $\overline{S}$ according as the above sign is plus or minus. Hence T is contained in S or $\overline{S}$ as desired.

THEOREM 9. *Every generalized quaternion division algebra in its canonical form of Theorem* 4 *has precisely two sets* S, $\overline{S}$ *of integral quantities satisfying* R, C, U', M, *and with*

$$\omega_1 = 1, \quad \omega_2 = \frac{1 + i}{2}, \quad \omega_3 = j, \quad \omega_4 = \frac{i(2\mu + j) + \tau j}{2},$$

as a basis of S, *while* $\overline{S}$ *has the corresponding basis*

$$\omega_1 = 1 \quad \omega_2 = \frac{1 + i}{2}, \quad \omega_3 = j, \quad \overline{\omega}_4 = \frac{i(-2\mu + j) + \tau j}{2\tau}.$$

It is evident that the two sets S, $\overline{S}$ have almost identical properties and hence that there is essentially one set (either S or $\overline{S}$) of integral quantities of Q.

THE INSTITUTE FOR ADVANCED STUDY