ARITHMETICS OF RATIONAL GENERALIZED QUATERNION ALGEBRAS

D. M. BROWN

1. **Introduction.** A rational generalized quaternion algebra is a linear associative algebra of order four and rank two, having a principal modulus I_0, ranging over the field of rational numbers. A basis (I_0, I_1, I_2, I_1I_2) may be found[1] such that

$$(1) \quad I_1^2 = \alpha, \quad I_2^2 = \beta, \quad I_1I_2 = -I_2I_1, \qquad \alpha \text{ and } \beta \text{ rational integers.}$$

An algebra in such form will be denoted by $Q(\alpha, \beta)$, a number in it by

$$(2) \qquad Q = a_0I_0 + a_1I_1 + a_2I_2 + a_{12}I_1I_2, \qquad a\text{'s rational,}$$

and its norm by

$$(3) \qquad N(Q) = a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_{12}^2.$$

Q satisfies its rank equation

$$(4) \qquad X^2 - 2a_0X + N(Q) = 0.$$

a_0 is called the real part of Q.

An arithmetic S of $Q(\alpha, \beta)$ is a set of numbers having the following properties:

C_a: S is closed with respect to algebraic addition.

C_m: S is closed with respect to multiplication.

R: For every number of S, (4) has integral coefficients.

U: S contains I_0, I_1 and I_2 (and hence I_1I_2 by C_m).

M: S is maximal; that is, S is contained in no larger set having Properties C_a, C_m, R and U.

It is the purpose of this paper to determine a set of bases for the arithmetics of those algebras for which α and β contain no squared prime factors.[2] In any case, it has been proved[3] that for a given arith-

[1] Dickson, L. E., *Algebren und ihre Zahlentheorie*, Zurich, 1927, pp. 43–44. The definition of an arithmetic is made there also.

[2] If α and β contain squared prime factors, the number of arithmetics varies with the form of those factors. See M. Eichler, *Untersuchungen in der Zahlentheorie der rationalen Quaternionalgebren*, Journal für die reine und angewandte Mathematik, vol. 174 (1936), p. 149, Theorem 12.

[3] Latimer, C. G., *The classes of integral sets in a quaternion algebra*, Duke Mathematical Journal, vol. 3 (1937), pp. 246–247, §7. On pages 237–238, §2, of this reference is stated a theorem giving necessary and sufficient conditions that a basis of $Q(\alpha, \beta)$ be a basis of an *arithmetic* of $Q(\alpha', \beta')$.

metic S in the algebra, a basis $(I_0', I_1', I_2', I_1'I_2')$ can be found such that $I_1'^2=\alpha', I_2'^2=\beta', I_1'I_2'=-I_2'I_1', \alpha'$ and β' containing no squared prime factors, and such that the given arithmetic is an arithmetic of $Q(\alpha', \beta')$. The problem of determining bases for the arithmetics of such algebras has been solved by Latimer[4] when $\alpha\equiv\beta\equiv 1 \pmod 2$, and by Darkow[5] when $\alpha\equiv\beta\equiv 0 \pmod 2$. Darkow's results can be extended to apply to the remaining cases (when $\alpha+\beta\equiv 1 \pmod 2$).[6] All possible cases are treated in this paper, with greatly simplified results.[7]

Albert[8] has shown that every rational generalized quaternion *division* algebra $Q(\alpha, \beta)$ may be transformed into $Q(\tau, \sigma)$, in which τ and σ have special properties. Concerning the treatments by Latimer and Darkow (similar to that used in this paper) Albert writes:[9]

> The · · · 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 cases into a canonical form are possible, and it is this canonical form which should be studied. · · · In particular, it is evident that the integral sets of S should contain the integers of the realm $R(i)$.

Concerning the above quotation, a few comments seem pertinent. Albert's results are readily obtainable from the results of this paper or those of Latimer and Darkow. His canonical form is not unique, and the number (two) of arithmetics obtained by it is, in general, much less than the number of arithmetics as defined by this paper. There being no essential difference between the basal elements I_1 and I_2, or, for that matter, I_1I_2, there seems to be little reason for requiring that the integers of the realm $R(I_1)$ be contained in an integral set (arithmetic) in preference to those of realms $R(I_2)$ or $R(I_1I_2)$. Albert's results apply only to division algebras, while those of Latimer and Darkow and the writer apply to all algebras. The norm of a number of $Q(\alpha, \beta)$, given in (3), being of a form of great interest in number theory, it would seem particularly useful to have

---

[4] Latimer, C. G., *Arithmetics of generalized quaternion algebras*, American Journal of Mathematics, vol. 48 (1926), pp. 57–66.

[5] Darkow, M. D., *Determination of a basis for the integral elements of certain generalized quaternion algebras*, Annals of Mathematics, (2), vol. 28 (1926), pp. 263–270.

[6] Latimer, C. G., *On the class number of a quaternion algebra with a negative fundamental number*, Transactions of this Society, vol. 40 (1936), p. 320.

[7] The writer is greatly indebted to Dr. Claiborne G. Latimer for valuable suggestions enabling much greater simplification than he had previously obtained.

[8] Albert, A. A., *Integral domains of rational generalized quaternion algebras*, this Bulletin, vol. 40 (1934), pp. 164–176.

[9] Albert, A. A., loc. cit., p. 165. The i used there is the same as the I used in this paper.

available a method of obtaining the arithmetics of an algebra expressed in terms of parameters α and β which yield that exact norm. Clearly Albert's canonical form would not suffice, so that methods of treatment as given here are conceivably not only useful but necessary.

As mentioned above, the method of treatment in this paper is similar to that used by Latimer and Darkow, the work being more direct in some places.[10]

2. **Notations, transformations and definitions used.** The letters r, s and t will be used exclusively to denote permutations of 1, 2, and 3. Let $(g-1)(g+1)=0$ such that

$$g = \begin{cases} 1 \text{ if the number of inversions of } (rst) \text{ is even,} \\ -1 \text{ otherwise.} \end{cases} \tag{5}$$

Let the g.c.d. of α and β be

$$(\alpha, \beta) = \gamma_3 \text{ (positive or negative)} \tag{6}$$

and $\alpha = -\gamma_2\gamma_3$, $\beta = \gamma_3\gamma_1$. Let

$$I_1 I_2 = \gamma_3 I_3, \tag{7}$$

so that from (1), $I_r^2 = -\gamma_s\gamma_t$, and $I_r I_s = g\gamma_t I_t$. From the results of Latimer and Darkow, it can easily be shown that I_3 is in each arithmetic, as are I_1 and I_2. Hence from (6) and (7), I_1, I_2, and I_3 are formally identical, as are the γ's, the latter being formally identical to their negatives. $Q(\alpha, \beta)$ will hereafter be written in the symmetric notation

$$Q(\gamma_1, \gamma_2, \gamma_3) \equiv Q(\alpha, \beta). \tag{8}$$

Making the unitary transformation

$$\begin{gathered} i_0 = gI_0, \qquad i_1 = gI_r, \qquad i_2 = gI_s, \qquad i_3 = gI_t, \\ \gamma_r = \alpha_1, \qquad \gamma_s = \alpha_2, \qquad \gamma_t = \alpha_3, \end{gathered} \tag{9}$$

one has $i_r^2 = -\alpha_s\alpha_t$ and $i_r i_s = g\alpha_t i_t$, which is abstractly identical with (9). $Q(\gamma_1, \gamma_2, \gamma_3)$ now becomes $Q(\alpha_1, \alpha_2, \alpha_3)$. After proper change of sign of the γ's, one finds that γ_t is odd or even, $\gamma_s \equiv 1 \pmod 4$, γ_r is odd, and $\gamma_r \equiv 1 \pmod 4$ if γ_t is odd. Choosing

$$(\theta - 1)(\theta - 2) = 0, \tag{10}$$

$Q(\alpha_1, \alpha_2, \alpha_3)$ is such that

[10] Latimer and Darkow obtain their results for $Q(\alpha, -\beta)$. Each mentions a "tentative" process for obtaining bases. See Latimer, loc. cit., footnote 3, pp. 61 and 65; Darkow, loc. cit., p. 263 and p. 267 ff.

(11) $\alpha_3 \equiv \theta \pmod{2\theta}$, $\alpha_2 \equiv 1 \pmod 4$, $\alpha_1 \equiv \alpha_2 \pmod{2(3-\theta)}$.

In what follows, it will be assumed that (9) has been made so that (11) holds. All other symbols introduced hereafter will represent integers, unless they are obviously not integers. The parameters θ, m, k, n, A_r, B_r, ξ and H_j, used frequently hereafter, and most easily determined in the order given, are defined by the following, each being unique save n and H_j:

θ: $\alpha_3 \equiv \theta \pmod{2\theta}$; $(\theta-1)(\theta-2)=0$.

m: $(\alpha_1+\alpha_2+m\alpha_3) \equiv 2-\theta \pmod{4\theta}$; $(m-1)(m+1)[(\theta-1)m(m+2)+2-\theta]=0$.

k: $2(m^2+m+1)k=(m+1)(m+2)$.[11]

n: $kn^2-n=0$.

A_r, B_r: $\alpha_r = A_r B_r$, and

$$\left(\frac{-\alpha_s\alpha_t}{A_r}\right) = 1, \qquad \left(\frac{-\alpha_s\alpha_t}{B_r}\right) = -1,$$

B_r positive and a minimum.[12]

ξ: ξ is the number of prime factors (all distinct) of $A_1A_2A_3$.

H_j: $(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)H_j^2 \equiv -1 \pmod{A_1A_2A_3}$, $(j=1, 2, \cdots, \xi)$.[13] If H_j is even, then $H_j' = H_j \pm A_1A_2A_3$ is odd. Let $f_7=(1-2m)$ and $f_8=2\theta k-2k+2$. Then if $A_2B_1H_j' \not\equiv f_7 \pmod{f_8}$, it can be shown that $H_j'' = H_j' \pm A_1A_2A_3$ is such that $A_2B_1H_j'' \equiv f_7 \pmod{f_8}$. Since H_j, H_j', and H_j'' are all in the same residue class, modulo $A_1A_2A_3$, it follows (and will be so assumed hereafter) that H_j may always be chosen such that (f_7 is odd and f_8 is even, so H_j will be odd)

$$A_2B_1H_j \equiv f_7 \pmod{f_8}. \tag{12}$$

The following symbols will also be used:

$$\begin{aligned} f_1 &= (2-\theta)kn, \quad f_2 = (\theta n - 2n + 2), \quad f_3 = k(m + \theta n - 2n), \\ f_4 &= (2-\theta)(m - 2n - k + 1) + n, \quad f_5 = (2n - \theta n - k + 2), \\ f_6 &= (\theta - 1)(m - 2k + 2), \quad f_7 = (1 - 2m), \quad f_8 = 2\theta k - 2k + 2, \end{aligned} \tag{13}$$

[11] If $e=1-k$, then k may also be defined by $(\alpha_1+\alpha_2+\alpha_3)(\alpha_1+\alpha_2)(\alpha_2+\alpha_3)(\alpha_3+\alpha_1) \equiv 8e \pmod{16}$. See Latimer, C. G., *On the fundamental number of a rational generalized quaternion algebra*, Duke Mathematical Journal, vol. 1 (1935), p. 435, theorem and second footnote.

[12] In these conditions

$$\left(\frac{A}{P}\right)$$

is the Legendre symbol for quadratic residues.

[13] This congruence has exactly ξ distinct solutions. See Dickson, L. E., *Introduction to the Theory of Numbers*, University of Chicago Press, 1929, p. 12, Theorem 16.

$$(14)\quad M_j = \frac{\alpha_1 H_j i_1 + i_2}{2A_3}, \qquad N_j = \tfrac{1}{2} i_0 + \frac{-\alpha_1 H_j i_1 + \alpha_2 H_j i_2 + i_3}{2A_1 A_2}.$$

3. **The fundamental form of a number Q in an arithmetic.** From the relations given by (2), (3), (7) and (9), a number in $Q(\alpha_1, \alpha_2, \alpha_3)$ is such that

$$(15)\quad \begin{aligned} Q &= b_0 i_0 + b_1 i_1 + b_2 i_2 + b_3 i_3, \\ N(Q) &= b_0^2 + \alpha_2\alpha_3 b_1^2 + \alpha_3\alpha_1 b_2^2 + \alpha_1\alpha_2 b_3^2 \end{aligned}$$

(the b's rational). By Property C_m, if Q is in S, then so are Qi_0, Qi_1, Qi_2 and Qi_3, whose real parts are b_0, $-\alpha_2\alpha_3 b_1$, $-\alpha_3\alpha_1 b_2$ and $-\alpha_1\alpha_2 b_3$, respectively, and by Property R and (4), one may write $2b_0 = X_0$, $2b_r\alpha_s\alpha_t = X_r$, so that (15) becomes

$$(16)\quad \begin{aligned} Q &= \frac{1}{2}\left[X_0 i_0 + \frac{X_1 i_1}{\alpha_2\alpha_3} + \frac{X_2 i_2}{\alpha_3\alpha_1} + \frac{X_3 i_3}{\alpha_1\alpha_2}\right], \\ N(Q) &= \frac{1}{4}\left[X_0^2 + \frac{X_1^2}{\alpha_2\alpha_3} + \frac{X_2^2}{\alpha_3\alpha_1} + \frac{X_3^2}{\alpha_1\alpha_2}\right] \end{aligned}$$

and, by Property R,

$$(17)\quad \alpha_1\alpha_2\alpha_3 X_0^2 + \alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3 X_3^2 \equiv 0 \pmod{4\alpha_1\alpha_2\alpha_3}.$$

Using (11), (17) becomes equivalent to

$$(18)\quad \begin{aligned} &\alpha_1\alpha_2\alpha_3 X_0^2 + \alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3 X_3^2 \equiv 0 \pmod{4\theta} \\ &\qquad \text{if also } \alpha_r X_r^2 + \alpha_s X_s^2 \equiv 0 \pmod{\alpha_t}. \end{aligned}$$

Let δ_t be any prime factor of α_t. If δ_t divides X_r, it also divides X_s. But if $(X_r, \delta_t) = 1$, then there exists an integer p_r such that $p_r X_r \equiv 1 \pmod{\delta_t}$. Hence from (18), $p_r^2\alpha_r X_r^2 + p_r^2\alpha_s X_s^2 \equiv 0 \pmod{\delta_t}$, $\alpha_r + p_r^2\alpha_s X_s^2 \equiv 0 \pmod{\delta_t}$, or $(p_r\alpha_s X_s)^2 \equiv -\alpha_r\alpha_s \pmod{\delta_t}$. Hence

$$\left(\frac{-\alpha_r\alpha_s}{\delta_t}\right) = 1,$$

and from (13), X_r may be prime to each factor of A_t, but must be divisible by each factor of B_t, and hence by B_t itself. Therefore B_t divides X_r and X_s, and one may write

$$(19)\quad X_0 = x_0, \qquad X_r = B_s B_t x_r,$$

and (16) and (18) become, respectively,

$$(20)\qquad \begin{aligned} Q_x &= \frac{1}{2}\left[x_0 i_0 + \frac{x_1 i_1}{A_2A_3} + \frac{x_2 i_2}{A_3A_1} + \frac{x_3 i_3}{A_1A_2}\right], \\ N(Q) &= \frac{1}{4}\left[x_0^2 + \frac{B_2B_3x_1^2}{A_2A_3} + \frac{B_3B_1x_2^2}{A_3A_1} + \frac{B_1B_2x_3^2}{A_1A_2}\right], \end{aligned}$$

and

$$(21)\qquad \begin{aligned} \alpha_1\alpha_2\alpha_3x_0^2 + \alpha_1x_1^2 + \alpha_2x_2^2 + \alpha_3x_3^2 &\equiv 0 \pmod{4\theta}, \\ (A_sB_rx_s)^2 &\equiv -\alpha_r\alpha_sx_r^2 \pmod{A_t}. \end{aligned}$$

Hereafter, the numbers x_0, x_1, x_2, x_3 will be referred to as the *coordinates of a number Q_x in S*, and (20) will be called the *fundamental form of Q in S*. Using the definition of H_j to obtain $\alpha_r\alpha_sH_j^2 \equiv -1 \pmod{A_t}$, and multiplying both members of (21b) by H_j^2, one obtains $(A_sB_rH_jx_s)^2 \equiv -\alpha_r\alpha_sH_j^2x_r^2 \equiv x_r^2 \pmod{A_t}$, or, reducing to linear congruences, $x_r \equiv A_sB_r(\pm H_j)x_s \pmod{A_t}$. Now if H_j is a solution of its congruence, then $-H_j$ is another, distinct from H_j, and one may finally write

$$(22)\qquad x_r \equiv gA_sB_rH_jx_s \pmod{A_t},$$

where g is defined as in (5). Hence from (20), (21) and (22) one concludes:

THEOREM I. *If a number Q is in an arithmetic, it is necessary that it have the form* (20), *whose coordinates satisfy* (21a) *and* (22).

4. **Analysis of the conditions imposed on the coordinates of a number Q of fundamental form lying in an arithmetic.** It can be shown that two numbers of fundamental form have Property C_a if and only if their coordinates satisfy (22) *for the same value of j*. Hereafter H_j will be replaced by H whenever the value of j is fixed in an argument. Let Q_x and Q_y be in an arithmetic, and hence satisfy (22) for the same value of j. Then by Property C_m, Q_xQ_y must also lie in S. A study of the coordinates of this new number reveals that in addition to (21a) and (22), the following conditions must hold:[14]

$$(23)\qquad \begin{aligned} \alpha_1\alpha_2\alpha_3x_0y_0 + \alpha_1x_1y_1 + \alpha_2x_2y_2 + \alpha_3x_3y_3 &\equiv 0 \pmod{2\theta}, \\ x_0y_1 + y_0x_1 + y_2x_3 + x_2y_3 &\equiv 0 \pmod 2, \\ x_0y_2 + y_0x_2 + y_3x_1 + x_3y_1 &\equiv 0 \pmod 2, \\ \theta(x_0y_3 + y_0x_3) + y_1x_2 - x_1y_2 &\equiv 0 \pmod{2\theta}. \end{aligned}$$

[14] Here begins the direct method, as opposed to the "tentative" process of Latimer and Darkow. See footnote 10.

Exhaustive analysis of (21a), (22) and (23) further reveals that the conditions that must hold in order for Q_x and Q_y *to have property M* are as follows:

$$
\begin{aligned}
x_0 &= [(2-\theta)n + (\theta-1)km]x_1 \\
&\quad + (2-\theta)(1-n)x_2 + (\theta-1)x_3 \pmod 2, \\
x_1 &\equiv 0 \pmod{\theta + k - \theta k}, \\
x_1 &\equiv (1-2n)x_2 + 2mx_0 \pmod{\theta k + 2\theta - 2k}, \text{ for fixed } n, \\
x_3 &\equiv (2-\theta)[(1-n)x_1 + nx_2] \pmod{3-\theta}
\end{aligned} \tag{24}
$$

$$
x_1 \equiv B_1H(A_2x_2 - A_3x_3) \pmod{A_2A_3}, \qquad x_2 \equiv A_3B_2Hx_3 \pmod{A_1}, \tag{25}
$$

which is equivalent to (22). Letting P_0, P_1, P_2, and P_3 be arbitrary integers, the f's integers as defined in (13), and M_j and N_j as in (14), then (24) and (25) can be reduced to

$$
\begin{aligned}
x_0 &= 2P_0 + f_1P_1 + f_3P_2 + P_3, \\
x_1 &= f_2A_2A_3P_1 + (f_4A_2A_3 + f_5A_2\alpha_1H)P_2 + (f_6A_2A_3 - A_3B_1H)P_3, \\
x_2 &= f_5A_1P_2 + A_3B_2HP_3, \\
x_3 &= P_3, \qquad \text{for fixed } n.
\end{aligned} \tag{26}
$$

Substituting these in (20a) one has

$$
\begin{aligned}
Q_{xjn} &= P_0i_0 + \tfrac{1}{2}(f_1i_0 + f_2i_1)P_1 + [\tfrac{1}{2}(f_3i_0 + f_4i_1) + f_5M_j]P_2 \\
&\quad + [\tfrac{1}{2}f_6i_1 + N_j]P_3, \qquad j = 1, 2, \cdots, \xi.
\end{aligned} \tag{27}
$$

Now let

$$
\begin{aligned}
U_{0jn} &= i_0, & U_{1jn} &= \tfrac{1}{2}(f_1i_0 + f_2i_1), \\
U_{2jn} &= \tfrac{1}{2}(f_3i_0 + f_4i_1) + f_5M_j, & U_{3jn} &= \tfrac{1}{2}f_6i_1 + N_j.
\end{aligned} \tag{28}
$$

(27) then becomes

$$
Q_{xjn} = P_0U_0 + P_1U_1 + P_2U_2 + P_3U_3. \tag{29}
$$

All such numbers, for a fixed j and n, form an integral set of numbers with (28) as a basis. Since (28) is equivalent to (26) and (20) combined, and since (26) and (20) establish necessary and sufficient conditions that Properties C_a, C_m, R and M hold, and it is easily shown that i_1, i_2 and i_3 are of the form (29), so that Property U holds, it follows that (28) gives the bases of the algebra—one for each value of j and n. But n has $k+1$ values, and j has ξ values. By use of the inverse of the unitary transformation (9), and of (7), it is clear that the arith-

metics of $Q(\alpha_1, \alpha_2, \alpha_3)$ are also the arithmetics of $Q(\gamma_1, \gamma_2, \gamma_3)$ and of $Q(\alpha, \beta)$. Hence

THEOREM II. *The numbers of* (28) *constitute the bases for the arithmetics of* $Q(\alpha_1, \alpha_2, \alpha_3)$, *of* $Q(\gamma_1, \gamma_2, \gamma_3)$, *and of* $Q(\alpha, \beta)$. *There are* $2^k\xi$ *such arithmetics.*

The number of arithmetics agrees with that determined by Latimer and Darkow, and the bases were checked by applying the theorem mentioned in footnote 3. In this theorem the fundamental number d of the algebra is used. By a known result[11]

$$d = \pm 2^{1-k} B_1 B_2 B_3,$$

the sign being positive if $\alpha_1, \alpha_2, \alpha_3$ are all of the same sign, and negative otherwise; that is, according as $N(Q)$ (see (3)) is a definite or indefinite form. It is also known that $Q(\alpha, \beta)$ is a division algebra if and only if $d \neq -1$.[15]

5. **The method of writing down the arithmetics of $Q(\alpha, \beta)$, or of $Q(\gamma_1, \gamma_2, \gamma_3)$, α and β containing no squared prime factors.** By use of (7) and (9), and a few new symbols, the arithmetics may readily be written down in terms of the original basis, (I_0, I_1, I_2, I_1I_2). Let the following definitions and order of procedure be made:

(a) $(\alpha, \beta) = \gamma_3$ (positive or negative), so that $\alpha = -\gamma_2\gamma_3$, $\beta = -\gamma_3\gamma_1$.

(b) $\gamma_r = \Gamma_r\Delta_r$, and

$$\left(\frac{-\gamma_s\gamma_t}{\Gamma_r}\right) = 1, \qquad \left(\frac{-\gamma_s\gamma_t}{\Delta_r}\right) = -1,$$

Δ_r a positive minimum and (rst) a permutation of (123).

(c) Arrange $\gamma_1, \gamma_2, \gamma_3$ (changing signs of all simultaneously if necessary) and determine θ so that $\gamma_t \equiv \theta \pmod{2\theta}$, $\gamma_s \equiv 1 \pmod 4$, $\gamma_r \equiv \gamma_s \pmod{2(3-\theta)}$.

(d) Then determine m so that $\gamma_r + \gamma_s + m\gamma_t \equiv 2-\theta \pmod{4\theta}$, $(m-1)(m+1)[(\theta-1)m(m+2)+2-\theta] = 0$.

(e) Determine k and n such that $2(m^2+m+1)k = (m+1)(m+2)$, and $kn^2 - n = 0$.

(f) Determine $f_1, f_2, \cdots, f_8$ according to Table I.

(g) Determine the ξ solutions H_j $(j = 1, 2, \cdots, \xi)$ of $(\gamma_1\gamma_2 + \gamma_2\gamma_3 + \gamma_3\gamma_1)H_j^2 \equiv -1 \pmod{\Gamma_1\Gamma_2\Gamma_3}$, ξ being the number of prime factors of $\Gamma_1\Gamma_2\Gamma_3$. If any H_j is even, replace it by $H_j \pm \Gamma_1\Gamma_2\Gamma_3$ to make it odd.

---

[15] Latimer, C. G., loc. cit., footnote 11. See §1, next to last paragraph, and the corollary to the theorem on page 435.

If then any H_j be such that $\Gamma_s\Delta_r H_j \not\equiv f_7 \pmod{f_8}$, replace it by $H_j \pm \Gamma_1\Gamma_2\Gamma_3$ and find that $\Gamma_s\Delta_r H_j \equiv f_7 \pmod{f_8}$.

(h) Then determine V_{0jn}, V_{1jn}, V_{2jn}, V_{3jn}, as the desired bases, for each value of j and n, where

$$
\begin{aligned}
V_{0jn} &= I_0, \qquad V_{1jn} = \frac{f_1 I_0 + f_2 I_r}{2}, \\
V_{2jn} &= \frac{f_3 I_0 + f_4 I_r}{2} + f_5 \frac{\gamma_r H_j I_r + I_s}{2\Gamma_t}, \\
V_{3jn} &= \frac{I_0 + f_6 I_r}{2} + \frac{-\gamma_r H_j I_r + \gamma_s H_j I_s + I_t}{2\Gamma_r\Gamma_s}.
\end{aligned} \tag{30}
$$

(i) Finally, replace $\alpha_3 I_3$ by $I_1 I_2$, giving the final forms.

Hull[16] has solved the problem of determining a set of bases for all

TABLE I

θ	1	1	1	2	2	2	2	2	2
m	−1	1	1	1	1	0	0	−1	−2
k	0	1	1	1	1	1	1	0	0
n	0	0	1	0	1	0	1	0	0
f_1	0	0	1	0	0	0	0	0	0
f_2	2	2	1	2	2	2	2	2	2
f_3	0	1	0	1	1	0	0	0	0
f_4	0	1	0	0	1	0	1	0	0
f_5	2	1	2	1	1	1	1	2	2
f_6	0	0	0	1	1	0	0	1	0
f_7	3	−1	−1	−1	−1	1	1	3	5
f_8	2	2	2	4	4	4	4	2	2

the arithmetics of *division* algebras, by showing that every arithmetic may be obtained from some one of an infinite number of canonical generations of the algebra (merely a non-unitary transformation of units carrying α and β into α' and β' having special properties). Latimer has obtained similar results without the restriction that the algebras be division algebras.[3] However, the method of determining which canonical generations will give the arithmetics for a given un-

[16] Hull, Ralph, *The maximal orders of generalized quaternion division algebras*, Transactions of this Society, vol. 40 (1936), pp. 1–11.

altered α and β is not stated in either paper. Hull showed that the canonical forms determined by Albert[8] are special cases of his canonical generations.

One problem remains to be solved, namely a method of writing down the arithmetics of $Q(\alpha, \beta)$ when α and β contain squared prime factors.

UNIVERSITY OF ILLINOIS