Mahler

Dr. Simon
With kind regards from K. Mahler

74

74

December, 1942

48 A 5

PROCEEDINGS

OF THE

ROYAL IRISH ACADEMY

VOLUME XLVIII, SECTION A, No. 5

K. [redacted]. L MAHLER

ON IDEALS IN THE CAYLEY-DIXON ALGEBRA

DUBLIN:

HODGES, FIGGIS & CO.

LONDON: WILLIAMS & NORGATE

1942

Price One Shilling

V.

ON IDEALS IN THE CAYLEY-DICKSON ALGEBRA.

By K. MAHLER (Manchester).

[Read 22 June. Published 7 December, 1942.]

RESULTS on the approximation of quaternions which I found in a recent paper (see footnote 3) can be applied to a similar question in the non-associative algebra discovered by Cayley and studied in more detail by Dickson (for references, see his book on Algebras). I show in this way that *this algebra allows a Euclidean algorithm,* if integral Cayley numbers are defined according to Dickson. I deduce that *all* (left or right) *ideals are principal,* and that *the basis of an odd ideal is a rational integer.*

I am indebted to Dr. Olga Taussky for advice during the preparation of this paper.

§ 1.—*The Cayley-Dickson algebra.*

Let K be the field of all quaternions

$$x = x^0 + x^1 i_1 + x^2 i_2 + x^3 i_3,$$

where x^0, x^1, x^2, x^3 are real numbers. We denote by

$$\bar{x} = x^0 - x^1 i_1 - x^2 i_2 - x^3 i_3,$$
$$S(x) = x + \bar{x} = 2x^0,$$
$$N(x) = x\bar{x} = (x^0)^2 + (x^1)^2 + (x^2)^2 + (x^3)^2,$$

the conjugate to x, its trace, and its norm.

A *Cayley number* or *C-number* is a pair $X = (x \mid y)$ of quaternions x and y. Two C-numbers $X_1 = (x_1 \mid y_1)$ and $X_2 = (x_2 \mid y_2)$ are equal, if and only if $x_1 = x_2$ and $y_1 = y_2$. Sum and product of two C-numbers X_1 and X_2 are defined as

$$X_1 + X_2 = (x_1 + x_2 \mid y_1 + y_2),$$
$$X_1 X_2 = (x_1 x_2 - \bar{y}_2 y_1 \mid y_2 x_1 + y_1 \bar{x}_2).$$

The *conjugate to* $X = (x \mid y)$ is given by $\bar{X} = (\bar{x} \mid -y)$, its *trace* and its *norm* by

$$S(X) = S(x) = x + \bar{x},$$
$$N(X) = N(x) + N(y) = x\bar{x} + y\bar{y}.$$

$X = (x \mid y)$ is *real*, if $X = \bar{X}$, i.e. if x is a real quaternion, and $y = 0$.

The set C of all C-numbers forms an Abelian group with respect to addition, with $0 = (0 \mid 0)$ as the unit element. Addition and multiplication satisfy the two distributive laws. On the other hand, multiplication is not in general commutative. Nor is it associative, for if $X_1 = (x_1 \mid y_1)$, $X_2 = (x_2 \mid y_2)$, and $X_3 = (x_3 \mid y_3)$, then

$$X_1 (X_2 X_3) = (x_1 x_2 x_3 - x_1 \bar{y}_3 y_2 - \bar{x}_2 \bar{y}_3 y_1 - x_3 \bar{y}_2 y_1 \mid y_3 x_2 x_1 + y_2 \bar{x}_3 x_1 + y_1 \bar{x}_3 \bar{x}_2 - y_1 \bar{y}_2 y_3)$$

and

$$(X_1 X_2) X_3 = (x_1 x_2 x_3 - \bar{y}_2 y_1 x_3 - \bar{y}_3 y_2 x_1 - \bar{y}_3 y_1 \bar{x}_2 \mid y_3 x_1 x_2 - y_3 \bar{y}_2 y_1 + y_2 x_1 \bar{x}_3 + y_1 \bar{x}_2 \bar{x}_3),$$

and these two C-numbers are in general different.

There are, however, some special cases in which the ordinary rules hold:

If X_1 or X_2 *is real, then* $X_1 X_2 = X_2 X_1$. (1)

If X_1, X_2, or X_3 *is real, then* $(X_1 X_2) X_3 = X_1 (X_2 X_3.)$ (2)

Both assertions are obvious, since multiplication of $X = (x \mid y)$ with the real C-number $(a \mid 0)$ means that both x and y are multiplied with the real quaternion a. We therefore may identify the real C-number $(a \mid 0)$ with the real number a, so that

$$a = (a \mid 0), \qquad aX = Xa = (ax \mid ay).$$

For the multiplication of conjugate numbers, the following rules hold:

$$X\bar{X} = X\bar{X} = N(X). \tag{3}$$

$$X_1 (\bar{X}_1 X_2) = (X_1 \bar{X}_1) X_2 = N(X_1) X_2; \; (X_1 X_2) \bar{X}_2 = X_1 (X_2 \bar{X}_2) = X_1 N(X_2). \tag{4}$$

$$\overline{(X_1 X_2)} = \bar{X}_2 \bar{X}_1. \tag{5}$$

We further have *Cayley's identity*

$$N(X_1 X_2) = N(X_1) N(X_2), \tag{6}$$

which may be directly verified.

Similarly for the trace function:

$$X + \bar{X} = \bar{X} + X = S(X), \tag{7}$$

$$S(X_1 X_2) = S(X_2 X_1), \tag{8}$$

$$S\big((X_1 X_2) X_3\big) = S\big(X_1 (X_2 X_3)\big), \tag{9}$$

as may be verified directly.

To every C-number $A \neq 0$, there is an inverse

$$A^{-1} = N(A)^{-1}\bar{A}$$

such that

$$AA^{-1} = A^{-1}A = 1 = (1 \mid 0).$$

Hence, by (4), both equations

$$AX = B \quad \text{and} \quad YA = B$$

have solutions, namely,

$$X = A^{-1}B \quad \text{and} \quad Y = BA^{-1}.$$

By the distributive laws and by Cayley's formula, these are the only solutions.

These results show that C is a non-commutative and non-associative division algebra.

§ 2.—*The ring of all integral C-numbers.*

Let $A_1, A_2, \ldots, A_8$ be the eight C-numbers

$$A_1 = (i_1 \mid 0),\quad A_2 = (i_2 \mid 0),\quad A_3 = (i_3 \mid 0),\quad A_4 = \left(\frac{1+i_1+i_2+i_3}{2} \,\middle|\, 0\right),$$
$$A_5 = (0 \mid 1),\quad A_6 = \left(\frac{1+i_1}{2} \,\middle|\, \frac{1+i_2}{2}\right),\quad A_7 = \left(\frac{1+i_2}{2} \,\middle|\, \frac{1+i_1}{2}\right),\quad A_8 = \left(\frac{1+i_3}{2} \,\middle|\, \frac{1+i_2}{2}\right). \qquad (10)$$

We say that the C-number G is *integral* if it can be written as

$$G = \sum_{\nu=1}^{8} g_\nu A_\nu, \qquad (11)$$

where the coefficients $g_1, g_2, \ldots, g_8$ are arbitrary rational integers. The sum and the difference of integral C-numbers are again integral; Dickson has shown that the same is true for the product.[1] The integral C-numbers therefore form a ring J.

Since the numbers (10) are linearly independent over the real field, any C-number may be written as

$$X = \sum_{\nu=1}^{8} r_\nu A_\nu = (x \mid y), \qquad (12)$$

[1] Journal de Mathématique, ser. 9, vol. 2 (1923), in particular 319 f.

where $r_1, r_2, \ldots, r_8$ are real numbers, and

$$x = \frac{r_4 + r_6 + r_7 + r_8}{2} + \frac{2r_1 + r_4 + r_6}{2} i_1 + \frac{2r_2 + r_4 + r_7}{2} i_2 + \frac{2r_3 + r_4 + r_8}{2} i_3,$$

$$y = \frac{2r_5 + r_6 + r_7 + r_8}{2} + \frac{r_7}{2} i_1 + \frac{r_6}{2} i_2 + \frac{r_8}{2} i_3. \qquad (13)$$

It is easy to establish the following result.

If $\quad x = x^0 + x^1 i_1 + x^2 i_2 + x^3 i_3, \qquad y = y^0 + y^1 i_1 + y^2 i_2 + y^3 i_3,$

then $X = (x \mid y)$ *belongs to* J *if and only if all eight numbers*

$$2x^0,\ 2x^1,\ 2x^2,\ 2x^3, \qquad 2y^0,\ 2y^1,\ 2y^2,\ 2y^3,$$

are rational integers such that

$$\begin{aligned} 2x^0 + 2x^1 &\equiv 2y^0 + 2y^2 \pmod 2,\\ 2x^0 + 2x^2 &\equiv 2y^0 + 2y^1 \pmod 2,\\ 2x^0 + 2x^3 &\equiv 2y^0 + 2y^3 \pmod 2,\\ 2x^0 + 2x^1 + 2x^2 + 2x^3 &\equiv 2y^0 + 2y^1 + 2y^2 + 2y^3 \equiv 0 \pmod 2. \end{aligned} \qquad (14)$$

Hence, in Hurwitz's notation,[2] the two quaternions x and y are both integral, or neither of them is integral.

It is easily verified that there are 240 integral C-numbers of norm 1, and 2160 integral C-numbers of norm 2.

Theorem 1: *To every C-number* X *there is an integral C-number* G *such that*

$$N(X - G) \leqslant \tfrac{15}{16}. \qquad (15)$$

Proof: Write X and G in the form (11) and (12) and put

$$Y = X - G = \sum_{\nu=1}^{8} s_\nu A_\nu = (x^* \mid y^*),$$

so that

$$s_\nu = r_\nu - g_\nu \qquad (\nu = 1, 2, \ldots, 8)$$

and

$$x^* = \frac{s_4 + s_6 + s_7 + s_8}{2} + \frac{2s_1 + s_4 + s_6}{2} i_1 + \frac{2s_2 + s_4 + s_7}{2} i_2 + \frac{2s_3 + s_4 + s_8}{2} i_3,$$

$$y^* = \frac{2s_5 + s_6 + s_7 + s_8}{2} + \frac{s_7}{2} i_1 + \frac{s_6}{2} i_2 + \frac{s_8}{2} i_3.$$

It is obviously possible to determine the integers g_5, g_6, g_7, g_8 such that

$$\left|\frac{2s_5 + s_6 + s_7 + s_8}{2}\right| \leqslant \tfrac{1}{2}, \quad \left|\frac{s_7}{2}\right| \leqslant \tfrac{1}{4}, \quad \left|\frac{s_6}{2}\right| \leqslant \tfrac{1}{4}, \quad \left|\frac{s_8}{2}\right| \leqslant \tfrac{1}{4}.$$

[2] Zahlentheorie der Quaternionen (Berlin, 1919), Vorlesung 4.

It is further possible[3] to determine g_1, g_2, g_3, g_4 such that

$$\left(\frac{s_4+s_6+s_7+s_8}{2}\right)^2+\left(\frac{2s_1+s_4+s_6}{2}\right)^2+\left(\frac{2s_2+s_4+s_7}{2}\right)^2+\left(\frac{2s_3+s_4+s_8}{2}\right)^2\leqslant\tfrac{1}{2}.$$

Then, since

$$N(y)=\left(\frac{s_4+s_6+s_7+s_8}{2}\right)^2+\left(\frac{2s_1+s_4+s_6}{2}\right)^2+\left(\frac{2s_2+s_4+s_7}{2}\right)^2+\left(\frac{2s_3+s_4+s_8}{2}\right)^2+$$
$$+\left(\frac{2s_5+s_6+s_7+s_8}{2}\right)^2+\left(\frac{s_7}{2}\right)^2+\left(\frac{s_6}{2}\right)^2+\left(\frac{s_8}{2}\right)^2,$$

we find that

$$N(X-G)\leqslant\tfrac{1}{2}+(\tfrac{1}{2})^2+(\tfrac{1}{4})^2+(\tfrac{1}{4})^2+(\tfrac{1}{4})^2=\tfrac{15}{16},$$

as was to be proved.

The constant (15/16) in (15) is not the best possible one; the exact constant is 1/2. But this is not easy to prove; I therefore omit the proof, since the less exact inequality suffices for our purpose.

§ 3.—*The ideals in J.*

As usual, a set $\mathfrak{a}$ of integral C-numbers is called a left (right) ideal, if with any two elements G_1 and G_2 it also contains $G_1 \pm G_2$, and with G also HG (respectively GH), where H is an arbitrary integral C-number.

Suppose that the left ideal $\mathfrak{a}$ does not consist only of the zero C-number. Then among its non-vanishing elements there is at least one, say the element G_0, which has smallest possible norm. Let A be an arbitrary C-number in $\mathfrak{a}$. By Theorem 1, there is an integral C-number G such that

$$N(AG_0^{-1}-G)\leqslant\tfrac{15}{16}<1.$$

---

[3] In a paper which is to appear in the Proceedings of the London Mathematical Society, I proved the following lemma: "If

$$A(x_1,x_2,x_3,x_4)=\left(x_1+\frac{x_4}{2}\right)^2+\left(x_2+\frac{x_4}{2}\right)^2+\left(x_3+\frac{x_4}{2}\right)^2+\left(\frac{x_4}{2}\right)^2=$$
$$=x_1^2+x_2^2+x_3^2+x_4^2+(x_1+x_2+x_3)x_4,$$

then to any four real numbers x_1, x_2, x_3, x_4 there are four integers g_1, g_2, g_3, g_4 such that

$$A(x_1-g_1,\ x_2-g_2,\ x_3-g_3,\ x_4-g_4)\leqslant\tfrac{1}{2}."$$

From this lemma, the inequality in the text follows on defining x_1, x_2, x_3, x_4 by the formulae

$$x_4=r_4+s_6+s_7+s_8,\qquad 2x_1+x_4=2r_1+r_4+s_6,$$
$$2x_2+x_4=2r_2+r_4+s_7,\qquad 2x_3+x_4=2r_3+r_4+s_8,$$

so that

$$s_4+s_6+s_7+s_8=x_4-g_4,\qquad 2s_1+s_4+s_6=2(x_1-g_1)+(x_4-g_4),$$
$$2s_2+s_4+s_7=2(x_2-g_2)+(x_4-g_4),\qquad 2s_3+s_4+s_8=2(x_3-g_3)+(x_4-g_4).$$

Therefore by (4), (6), and the definition of the inverse,

$$N(A - GG_0) = N\Big((AG_0^{-1})\,G_0 - GG_0\Big) = N(AG_0^{-1} - G)\,N(G_0) < N(G_0).$$

Since the C-number $A - GG_0$ is integral and lies in $\mathfrak{a}$, it must therefore vanish. Hence every element A of $\mathfrak{a}$ is of the form

$$A = GG_0, \tag{16}$$

where G is an element of J. Conversely, any product of this form belongs to $\mathfrak{a}$; we have therefore proved that *every left ideal is a principal ideal.*

The fact that multiplication in C is not associative, allows us to derive further consequences from this result. Let G_1 and G_2 be two arbitrary integral C-numbers. Then by definition of $\mathfrak{a}$ the number G_2G_0 and therefore also the number $G_1(G_2G_0)$ belong to $\mathfrak{a}$. Hence there exists a third integral C-number G_3, such that

$$G_1(G_2G_0) = G_3G_0. \tag{17}$$

By specializing G_1 and G_2 in this equation, we derive properties of G_0.

§ 4.—*The basis of an ideal.*

In order to apply this method, put $G_0 = (g \mid h)$, and let

$$G_1 = (i_\alpha \mid 0), \quad G_2 = (i_\beta \mid 0),$$

where (α, β, γ) is a cyclic permutation of (1, 2, 3), hence

$$i_\alpha i_\beta = -i_\beta i_\alpha = i_\gamma.$$

Then we find that

$$G_1(G_2G_0) = (i_\gamma g \mid -hi_\gamma) = G_3G_0,$$

and therefore

$$G_3 = \{G_1(G_2G_0)\}G_0^{-1} = \{G_1(G_2G_0)\}\frac{\bar{G}_0}{N(G_0)} = \left(i_\gamma\,\frac{g\bar{g} - h\bar{h}}{g\bar{g} + h\bar{h}} \,\middle|\, -\frac{2hi_\gamma g}{g\bar{g} + h\bar{h}}\right).$$

As we have proved, G_3 is an integral C-number; hence

$$\frac{g\bar{g} - h\bar{h}}{g\bar{g} + h\bar{h}},$$

or twice this number is a rational integer. The second case is excluded by the congruences (14), since the first quaternion component of G_3 is a multiple of the quaternion unit i_γ. Therefore either

$$g\bar{g} - h\bar{h} = 0; \tag{18}$$

or

$$g\bar{g} - h\bar{h} = \mp(g\bar{g} + h\bar{h}). \tag{19}$$

If (18) holds, then the first quaternion component of the integral C-number

$$G_3 = \left(0 \,\middle|\, \frac{-hi_\gamma g}{g\bar{g}}\right)$$

vanishes. Therefore the second component

$$-\frac{hi_\gamma g}{g\bar{g}} = -(hi_\gamma g)(g^{-1}\bar{g}^{-1}) = -hi_\gamma\bar{g}^{-1} = \varepsilon_\gamma$$

is an integral quaternion, so that by $i_\gamma^2 = -1$,

$$h = \varepsilon_\gamma \bar{g} i_\gamma.$$

This equation holds for $\gamma = 1, 2, 3$; by (18), the three quaternions ϵ_γ are units. Obviously

$$\varepsilon_\alpha \bar{g}\, i_\alpha = \varepsilon_\beta \bar{g}\, i_\beta,$$

hence

$$\bar{g}\, i_\alpha i_\beta = \bar{g}\, i_\gamma = -\varepsilon_\alpha^{-1}\varepsilon_\beta \bar{g},$$

and therefore

$$h = \varepsilon_\gamma \bar{g} i_\gamma = -\varepsilon_\gamma \varepsilon_\alpha^{-1}\varepsilon_\beta \bar{g},$$

so that

$$h = \tau \bar{g}, \tag{20}$$

where $\tau = -\varepsilon_1\varepsilon_2^{-1}\varepsilon_3 = -\varepsilon_2\varepsilon_3^{-1}\varepsilon_1 = -\varepsilon_3\varepsilon_1^{-1}\varepsilon_2.$

The number τ is a unit, since it is a product of units.

We further have

$$\bar{g}\, i_\gamma \bar{g}^{-1} = j_\gamma, \quad \text{where} \quad j_\gamma = -\varepsilon_\alpha^{-1}\varepsilon_\beta. \tag{21}$$

These three numbers j_γ are units; from their definition

$$j_1^2 = j_2^2 = j_3^2 = -1, \qquad j_\alpha j_\beta = -j_\beta j_\alpha = j_\gamma.$$

Hence, by a result of Hurwitz[4],

$$j_\alpha = \sigma_\alpha i_{\nu_\alpha} \qquad (\alpha = 1, 2, 3),$$

where ν_1, ν_2, ν_3 is a permutation of 1, 2, 3, and where the σ_α are signs ∓ 1 such that

$$\sigma_1\sigma_2\sigma_3 = 1.$$

Since $\bar{g}^{-1} = g/N(g)$, (21) takes the form

$$\bar{g}\, i_\alpha g = \sigma_\alpha i_{\nu_\alpha} N(g).$$

Now, if

$$g = g_0 + g_1 i_1 + g_2 i_2 + g_3 i_3,$$

---

[4] *l.c.* [2], Vorlesung 5.

then

$$\bar{g}\, i_1 g = (g_0^2 + g_1^2 - g_2^2 - g_3^2)\, i_1 + 2\,(g_1 g_2 - g_0 g_3)\, i_2 + 2\,(g_1 g_3 + g_0 g_2)\, i_3,$$

$$\bar{g}\, i_2 g = 2\,(g_1 g_2 + g_0 g_3)\, i_1 + (g_0^2 - g_1^2 + g_2^2 - g_3^2)\, i_2 + 2\,(g_2 g_3 - g_0 g_1)\, i_3,$$

$$\bar{g}\, i_3 g = 2\,(g_1 g_3 - g_0 g_2)\, i_1 + 2\,(g_2 g_3 + g_0 g_1)\, i_2 + (g_0^2 - g_1^2 - g_2^2 + g_3^2)\, i_3.$$

Here, on the right-hand side, only one coefficient in each line, namely, that of i_{ν_a} is different from zero. A simple discussion of the 6 possible cases shows that therefore either

$$g = \delta\varepsilon \qquad \text{or} \qquad g = \delta\varepsilon\,(1 + i_1), \tag{22}$$

where δ is a rational number and ϵ one of the 24 quaternion units. Therefore G_0 is of one of the two forms

$$G_0 = \delta\,(\varepsilon \mid \tau\bar{\varepsilon}) \qquad \text{or} \qquad G_0 = \delta\,(\varepsilon\,(1 + i_1) \mid \tau\,(1 - i_1)\,\bar{\varepsilon}).$$

This equation for G_0 can also be written as

$$G_0 = \delta\,(\varepsilon \mid \varepsilon^*) \qquad \text{or} \qquad G_0 = \delta\,(\varepsilon\,(1 + i_1) \mid \varepsilon^*\,(1 + i_1)), \tag{23}$$

where ϵ and ϵ^* are two quaternion units.

The first number $(\epsilon \mid \epsilon^*)$ has the norm 2; hence $G_0 = \delta(\epsilon \mid \epsilon^*)$ is an integral C-number only if δ is a rational integer.

The second number $(\epsilon(1 + i_1) \mid \epsilon^*(1 + i_1))$ has the norm 4 and can be written as

$$(\mp\, i_\alpha \mp i_\beta \mid \mp\, i_{\alpha'} \mp i_{\beta'}), \tag{24}$$

where $\alpha \neq \beta$, $\alpha' \neq \beta'$; here α, β, α', β' are four indices 0, 1, 2, 3, and we have put $i_0 = 1$. The congruences (14) determine in which cases the C-number (24) is divisible by 2, and when this is not possible.

We have thus the final result:

"*If the integral C-number G_0 is of the form* (18), *then*

$$G_0 = \delta G^*,$$

where δ is a rational integer, and where G^* is either a unit C-number

$$G^* = \left(\frac{\mp\, i_\alpha \mp i_\beta}{2} \,\middle|\, \frac{\mp\, i_{\alpha'} \mp i_{\beta'}}{2}\right), \tag{25}$$

or a C-number of norm 2 *of the form*

$$G^1 = (\varepsilon|\varepsilon^*) \quad (\varepsilon,\ \varepsilon^*\ \textit{quaternion units}), \tag{26}$$

or a C-number of norm 4 *of the form*

$$G^* = (\mp\, i_\alpha \mp i_\beta \mid \mp\, i_{\alpha'} \mp i_{\beta'})." \tag{27}$$

§ 5.—*The basis of an ideal (concluded).*

We now assume that G_0 satisfies (19) and so is of one of the two forms

$$G_0 = (g \mid 0) \quad \text{or} \quad G_0 = (0 \mid h),$$

where g, respectively h, is evidently an integral quaternion.

Let again (α, β, γ) be a cyclic permutation of (1, 2, 3). Then

$$(0 \mid i_\alpha)\{(0 \mid i_\beta)(g \mid 0)\} = (-gi_\gamma \mid 0),$$
$$(0 \mid i_\alpha)\{(0 \mid i_\beta)(0 \mid h)\} = (0 \mid i_\gamma h),$$

and therefore G_3 has the values

$$\Big((0 \mid i_\alpha)\{(0 \mid i_\beta)(g \mid 0)\}\Big)(g \mid 0)^{-1} = (-gi_\gamma \mid 0)\Big(\frac{\bar{g}}{N(g)} \mid 0\Big) = \Big(-\frac{gi_\gamma\bar{g}}{N(g)} \mid 0\Big),$$

$$\Big((0 \mid i_\alpha)\{(0 \mid i_\beta)(0 \mid h)\}\Big)(0 \mid h)^{-1} = (0 \mid i_\gamma h)\Big(0 \mid -\frac{h}{N(h)}\Big) = \Big(\frac{\bar{h}i_\gamma h}{N(h)} \mid 0\Big).$$

Since G_3 is integral, we have so obtained the conditions that the quaternions

$$\frac{gi_\gamma\bar{g}}{N(g)} \qquad (\gamma = 1, 2, 3),$$

respectively the quaternions

$$\frac{\bar{h}i_\gamma h}{N(h)} \qquad (\gamma = 1, 2, 3)$$

are integral. That allows to find the form of these quaternions; it will be sufficient to carry this out in the case of g. Let

$$g = g_0 + g_1 i_1 + g_2 i_2 + g_3 i_3.$$

Then

$$gi_1\bar{g} = (g_0^2 + g_1^2 - g_2^2 - g_3^2)i_1 + 2(g_1g_2 + g_0g_3)i_2 + 2(g_1g_3 - g_0g_2)i_3,$$
$$gi_2\bar{g} = 2(g_1g_2 - g_0g_3)i_1 + 2(g_0^2 - g_1^2 + g_2^2 - g_3^2)i_2 + 2(g_2g_3 + g_0g_1)i_3,$$
$$gi_3\bar{g} = 2(g_1g_3 + g_0g_2)i_1 + 2(g_2g_3 - g_0g_1)i_2 + (g_0^2 - g_1^2 - g_2^2 + g_3^2)i_3.$$

The real parts of these quaternions vanish; they are therefore divisible by $N(g) = g_0^2 + g_1^2 + g_2^2 + g_3^2$ if and only if the coefficients of i_1, i_2, i_3 are divisible by $N(g)$. That gives the conditions that the rational numbers

$$2(g_\mu^2 + g_\nu^2), \quad 4g_\mu g_\nu \qquad (\mu, \nu = 0, 1, 2, 3;\ \mu \neq \nu)$$

are all integral multiples of $N(g)$ and therefore themselves integers.

There are now two cases. If $2g_0, 2g_1, 2g_2, 2g_3$ are all odd integers, then $N(g)$ is a divisor of the odd integer $4g_0g_1$ and therefore also odd. Let p be a prime factor of $N(g)$. Then at least one of the integers $2g_\mu$ is divisible by p, say the number $2g_{\mu_0}$. Since the three numbers

$$(2g_{\mu_0})^2 + (2g_\nu)^2 \qquad (\nu = 0, 1, 2, 3;\ \nu \neq \mu_0)$$

are integral multiples of $N(g)$, all integers $2g_\nu$ are divisible by p. Hence the highest power of p dividing $N(g)$ is even; $N(g)$ is therefore the square

$$N(g) = \delta^2$$

of an odd integer, and g has the form

$$g = \delta\epsilon,$$

where ϵ is a quaternion unit of the form

$$\epsilon = \frac{\mp 1 \mp i_1 \mp i_2 \mp i_3}{2}.$$

Next let all coefficients g_μ be integers. The same proof as in the last case shows that every odd prime factor of $N(g)$ divides g_0, g_1, g_2, g_3 and therefore is a square factor of $N(g)$. Further let 2^ζ be the highest power of 2 which divides all coefficients g_μ, say

$$g_\mu = 2^\zeta g_\mu^* \qquad (\mu = 0, 1, 2, 3).$$

Then at least one coefficient g_0^*, g_1^*, g_2^*, g_3^* is relatively prime to 2; on the other hand, the expressions

$$2\,(g_\mu^{*2} + g_\nu^{*2}),\ 4g_\mu^* g_\nu^* \qquad (\mu, \nu = 0, 1, 2, 3\,;\ \mu \neq \nu) \tag{28}$$

are all divisible by at least the same power of 2 as $2^{-2\zeta} N(g)$. If all integers g_μ^* are odd, then the expressions (28) are divisible by 4 but not by 8, and $2^{-2\zeta}N(g)$ is exactly divisible by 4. In this case $2^{-\zeta-1}g$ is still an integral quaternion, so that we come back to the preceding case: Again

$$g = \delta\epsilon,$$

where δ is a rational integer (which is now even), and ϵ is a unit

$$\epsilon = \frac{\mp 1 \mp i_1 \mp i_2 \mp i_3}{2},$$

Finally assume that at least one number g_μ^* is even and at least one is odd. Then the expressions (28) are divisible by no higher power of 2 than the first power, and the same holds for $2^{-2\zeta} N(g)$. Hence now

$$g = \delta\epsilon,$$

where δ is an odd or even rational integer, and where ϵ either is one of the units

$$\epsilon = \mp 1, \mp i_1, \mp i_2, \mp i_3$$

or one of the integral quaternions of norm 2,

$$\mp 1 \mp i_1,\ \ \mp 1 \mp i_2,\ \ \mp 1 \mp i_3,\ \ \mp i_2 \mp i_3,\ \ \mp i_1 \mp i_3,\ \ \mp i_1 \mp i_2.$$

This exhausts the possibilities for g. Since $\bar{h}$ satisfies the same conditions as g, there are identical results for h. We have therefore proved:

"*If the integral C-number* G_0 *is of the form* (19), *then*

$$G_0 = \delta G^*,$$

where δ *is a rational integer, and where* G^* *is either a unit C-number*

$$G^* = (\varepsilon \mid 0) \quad \text{or} \quad G^* = (0 \mid \varepsilon), \tag{29}$$

with a quaternion unit ϵ, *or where* G^* *is a C-number of norm* 2,

$$G^* = (\mp i_\mu \mp i_\nu \mid 0) \quad \text{or} \quad G^* = (0 \mid \mp i_\mu \mp i\,)." \tag{30}$$

Combining the results of §§ 3–5, we have thus found:

Theorem 2: *Every left ideal in the ring of all integral C-numbers is a principal ideal, and is generated by an integral C-number*

$$G_0 = \delta G^*,$$

where δ *is a rational integer, and* G^* *an integral C-number with norm* 1 *or* 2 *or* 4.

This theorem does not assert that every integral C-number of the forms (25), (26), (27), (29), (30) which has norm 1 or 2 or 4 generates an ideal. In fact this is not so, for it can be shown that the C-number $(g \mid g)$, where

$$g = \tfrac{1}{2}(1 + i_1 + i_2 + i_3),$$

does not generate an ideal, since

$$\{(i_1 \mid 0)\,[(0 \mid i_2)\,(g \mid g)]\}\,\tfrac{1}{2}\,(\bar{g} \mid -g) = (\tfrac{1}{2}(-i_2 - i_3) \mid \tfrac{1}{2}(-1 + i_1)\,),$$

which is not an integral C-number because the congruences (14) are not satisfied.