P. J. C. Lamont.

On Arithmetics in Cayley's Algebra and Multiplicative Functions.

A thesis for the degree of Doctor of Philosophy in the University of Glasgow.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

I wish to thank Professor R. A. Rankin who has supervised my course in Mathematical Research.

PREFACE.

The aim of this thesis is to discuss fully the characterization and basic properties of the arithmetics of Cayley's algebra C and to define certain multiplicative functions by summing homogeneous polynomials in four (or eight) indeterminates over the coordinates of all elements of fixed norm m of an arithmetic of C.

Firstly (§1), we introduce the algebra C by reviewing work by Cayley, Dickson, Artin, Zorn and others. In the following section (§2) we are able to discuss the full meaning of Dickson's condensed law of multiplication in C and also to obtain automorphisms of C.

Next we define a characteristic unit for any element of an arithmetic of C. In so doing, we show conclusively that there are seven maximal arithmetics in C which are isomorphic and that in C there are sixteen arithmetics each of which contains the units $1, i_1, \ldots i_7$. Further results are deduced from this characterization for use in later sections.

In §4, we define congruence modulo a rational integer in any maximal arithmetic of C and establish the following theorem.

Any element ξ of odd norm of a maximal arithmetic J_w of C is congruent modulo 2 in J_w to an element, unique apart from sign, of norm 1 of J_w. (Theorem 4.4).

Results on factorization in the arithmetics of C, needed for the construction of multiplicative functions, can then be established.

The section on ideals in C (§5) contains some improvements on Mahler's results on the same subject. For example, we prove that the basis of any ideal in C is a rational integer.

In the last five sections (§§6 - 10), we give a systematic account of identities and multiplicative functions defined as above by using the arithmetics of C not previously used by Rankin for this purpose. While the identities and multiplicative functions defined by using Hurwitz maximal quaternion arithmetic are easily related to those constructed by Rankin, the remaining arithmetics not considered by Rankin appear to give new identities and functions.

CONTENTS.

1. Introduction. Cayley's Algebra.

Cayley [5] defined a real linear algebra with the eight basic units $i_0 = 1, i_1, i_2, i_3, i_4, i_5, i_6, i_7$. A general number $\xi = \sum_{t=0}^{7} x_t i_t$ of the algebra was defined to have norm $N\xi = \sum_{t=0}^{7} x_t^2$. The real numbers $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7$ were called the components of ξ. In order to ensure that the algebra would have multiplicative norm (i.e. the norm of a product equal to the product of the norms of the factors) Cayley made the following choice of sign in the multiplication table of the units

(1.1) $i_0^2 = i_0$, $i_1^2 = i_2^2 = i_3^2 = i_4^2 = i_5^2 = i_6^2 = i_7^2 = -1$
$i_1 i_2 = i_3 = -i_2 i_4$, $i_2 i_3 = i_1 = -i_3 i_2$,
$i_3 i_1 = i_2 = -i_1 i_3$

and the six similar sets of relations obtained by replacing 123 by 145, 624, 653, 725, 734 and 176.

The multiplication table (1.1) specifies one of the algebras with multiplicative norm considered by Cayley [7]. The algebra defined by (1.1) is denoted by C and referred to as Cayley's Algebra.

Cayley displayed the product of two elements of C in the following way. Let

$$\overline{st} = x_s y_t - x_t y_s \quad \text{and}$$

$$(ot) = x_o y_t + x_t y_o .$$

If $\zeta = \xi\eta$ where

$$\zeta = \sum_{s=0}^{7} z_s i_s, \quad \xi = \sum_{s=0}^{7} x_s i_s, \quad \eta = \sum_{s=0}^{7} y_s i_s$$

$$z_0 = x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7$$

$$z_1 = \overline{23} + \overline{45} + \overline{76} + (01)$$
$$z_2 = \overline{31} + \overline{46} + \overline{57} + (02)$$
$$z_3 = \overline{12} + \overline{65} + \overline{47} + (03)$$
$$z_4 = \overline{51} + \overline{62} + \overline{73} + (04)$$
$$z_5 = \overline{14} + \overline{36} + \overline{72} + (05)$$
$$z_6 = \overline{24} + \overline{53} + \overline{17} + (06)$$
$$z_7 = \overline{25} + \overline{34} + \overline{61} + (07)$$

Corresponding to each element

$$\xi = x_0 + x_1i_1 + x_2i_2 + x_3i_3 + x_4i_4 + x_5i_5 + x_6i_6 + x_7i_7$$

of C we define

$$\overline{\xi} = x_0 - x_1i_1 - x_2i_2 - x_3i_3 - x_4i_4 - x_5i_5 - x_6i_6 - x_7i_7$$

to be the <u>conjugate</u> of ξ. Then

$$\overline{\xi}\,\xi = \xi\,\overline{\xi} = N\xi.$$

It is clear that the only elements of C with rational integral components which satisfy $N\xi = 1$ are the multiplicatively closed set of 16 units $\pm 1, \pm i_1, \pm i_2, \pm i_3, \pm i_4, \pm i_5, \pm i_6, \pm i_7$.

Cayley's algebra is associative and commutative under addition. Under multiplication Cayley's algebra is distributive but not commutative. In fact for any two distinct units u, v different from ± 1, $uv = -vu$. It is thus seen that for any elements ξ_1, ξ_2 of C $\overline{\xi_1\xi_2} = \overline{\xi}_2\,\overline{\xi}_1$.

Cayley's algebra is not associative under multiplication. A set of three units for which the associative law holds is called an <u>associative triad</u>. If two units of a triad are the same or if a unit is ± 1 the triad is associative. A set of three units for which the corresponding basic units are distinct and none of which is 1, is called a <u>proper triad</u>. There are seven proper associative triads of basic units. If (u, v, w) is one of the remaining 28 proper triads of basic units

$$(uv)w = -u(vw) = \pm u_t ,$$

where u_t is a basic unit other than 1. A triad of this type is called <u>anti-associative</u>. A proper triad is thus seen to be associative if and only if the product of any two of its elements equals the third with some sign affixed.

Multiplication by real numbers is, of course, associative and commutative and, further, multiplication of elements which are linear combinations of the units in an associative triad is associative.

Dickson [9] represented the algebra as a quasi-binary algebra with real quaternionic coordinates. He was thus able to give a condensed law of multiplication for the algebra. Let $i_1 = i$, $i_2 = j$, $i_3 = k$, $i_4 = e$, $i_5 = ie$, $i_6 = je$, $i_7 = ke$. Any element of the algebra can then be written in the form $\xi_0 + \xi_1 e$ where ξ_0, ξ_1 are quaternions in 1, i, j, k.

Dickson noted that

$$(1.2)\qquad \xi\eta = (\xi_0 + \xi_1 e)(\eta_0 + \eta_1 e)$$
$$= \xi_0\eta_0 - \overline{\eta}_1\xi_1 + (\eta_1\xi_0 + \xi_1\overline{\eta}_0)e,$$

where $\overline{\eta}_0$ is the quaternion conjugate to η_0. Cayley's algebra is formed from the quaternions by the adjunction of the new imaginary e and multiplication is defined by (1.2).

The relations (1.3) to (1.7) below follow from (1.1) or (1.2). For any Cayley numbers $\alpha_1, \alpha_2, \alpha_3$

$$(1.3)\qquad N(\alpha_1+\alpha_2) = N\alpha_1 + N\alpha_2 + 2R(\alpha_1\overline{\alpha}_2)$$
$$(1.4)\qquad R(\alpha_1\alpha_2) = R(\alpha_2\alpha_1)$$

where $2R(\alpha_3) = \alpha_3 + \overline{\alpha}_3$ and $R(\alpha_3)$ is called the real part of α_3.
Any Cayley number α satisfies the rank equation

$$(1.5)\qquad \alpha^2 - 2R(\alpha)\alpha + N\alpha = 0.$$

$$(1.6)\qquad \alpha_1\alpha_2 + \alpha_2\alpha_1 = 2\{R(\alpha_1)\alpha_2 + R(\alpha_2)\alpha_1 - R(\alpha_1\overline{\alpha}_2)\}$$

$$(1.7)\qquad R\{(\alpha_1\alpha_2)\alpha_3\} = R\{\alpha_1(\alpha_2\alpha_3)\}.$$

Using (1.2) as a definition of multiplication in C, Dickson proved that the algebra is in fact a division algebra i.e. that right hand and left hand division except by zero are always possible and unique. Thus to every Cayley number $\alpha \neq 0$ there corresponds a unique inverse $\alpha^{-1} = \frac{1}{N\alpha}\overline{\alpha}$.

From (1.2) it also follows that for any two elements α, β of the algebra

(1.8) $(\alpha\alpha)\beta = \alpha(\alpha\beta)$, $(\alpha\beta)\alpha = \alpha(\beta\alpha)$ and $(\beta\alpha)\alpha = \beta(\alpha\alpha)$.

In a similar way it can be shown that

(1.9) $(\overline{\alpha}\alpha)\beta = (\overline{\alpha}\alpha)\beta = \overline{\alpha}(\alpha\beta)$, $(\overline{\alpha}\beta)\alpha = \overline{\alpha}(\beta\alpha)$ and $(\beta\alpha)\overline{\alpha} = \beta(\alpha\overline{\alpha}) = (N\alpha)\beta$.

Thus for all α, β, $\alpha \neq 0$

(1.10) $\beta = (\alpha^{-1}\alpha)\beta = \alpha^{-1}(\alpha\beta)$, $(\alpha^{-1}\beta)\alpha = \alpha^{-1}(\beta\alpha)$ and $(\beta\alpha)\alpha^{-1} = \beta(\alpha\alpha^{-1}) = \beta$.

It follows at once from (1.7) and (1.9) that

(1.11) $R\{(\xi\xi)(\overline{\xi}\eta)\} = N\xi \cdot R(\xi\eta)$.

(1.8) shows that C is what Zorn [50] called an alternative ring. Artin's Theorem [50] states that the ring generated by 2 elements α, β of an alternative ring is associative. Thus any subring of C generated by two elements of C is associative.

Albert [1] noticed that for u any unit of C other than ± 1 and arbitrary v, w units of C

(1.12) $u\{(vw)u\} = (uv)(wu)$, $(uvu)(uw) = -u(vw)$ and $(vu)(uwu) = -(vw)u$.

It follows at once that if α, β are any elements of C

(1.13) $\quad u\{(\alpha\beta)u\} = (u\alpha)(\beta u),$

and

(1.14) $\quad (u\alpha u)(u\beta) = -u(\alpha\beta)$ and

$\qquad (\alpha u)(u\beta u) = -(\alpha\beta)u.$

Define for any elements $\alpha_1, \alpha_2, \alpha_3$ of C

$$[\alpha_1, \alpha_2, \alpha_3] = (\alpha_1\alpha_2)\alpha_3 - \alpha_1(\alpha_2\alpha_3).$$

Then if r, s, t, take any of the values 1, 2, 3

$$[\alpha_r, \alpha_s, \alpha_t] = \epsilon_{rst}[\alpha_1, \alpha_2, \alpha_3]$$

where ϵ_{rst} equals 1 or -1 according as r, s, t is an even or odd permutation of 1, 2, 3 and is zero when r, s, t is not a permutation of 1, 2, 3. Now from (1.13)

$$\begin{aligned}[\alpha, \beta, \gamma\alpha] - \alpha[\beta, \gamma, \alpha] &= (\alpha\beta)(\gamma\alpha) - \alpha\{\beta(\gamma\alpha)\} + \alpha\{\beta(\gamma\alpha)\} \\ &\qquad - \alpha\{(\beta\gamma)\alpha\}. \\ &= 0.\end{aligned}$$

Thus $\quad [\alpha, \beta, \gamma\alpha] = \alpha[\alpha, \beta, \gamma].$

It follows that

(1.15) $\quad \{\alpha(\gamma\alpha)\}\beta = \alpha\{\gamma(\alpha\beta)\}$

and

(1.16) $\quad \{(\alpha\beta)\gamma\}\beta = \alpha\{\beta(\gamma\beta)\}.$

In a system such as C satisfying (1.10), (1.14), (1.15) and (1.16) it has been established [39] that any three elements α, β, γ for which

$$[\alpha, \beta, \gamma] = 0$$

generate a group under multiplication.

The properties (1.14), (1.15) and (1.16) are in fact equivalent [5]. Linnik has proved (1949) that Cayley's algebra and its subalgebras are the only algebras of rank 2 over the real numbers having the properties (1.10).

2. Dickson's Condensed Law. Automorphisms.

In the first part of this section the following results are proved.

Theorem 2.1. For any proper associative triad (v_1, v_2, v_3) of units of C, for any other unit $v_4 \neq \pm 1$, $v_4 \neq \pm v_s$ $(s = 1, 2, 3)$ and for any ξ, η elements of C, we may write

$$\xi = \xi_0 + \xi_1 v_4$$
$$\eta = \eta_0 + \eta_1 v_4$$

where ξ_0, η_0, ξ_1 and η_1 are linear combinations of the units 1, v_1, v_2 and v_3 of C.

We establish that with this notation

Theorem 2.2.

$$\xi\eta = \xi_0\eta_0 - \bar{\eta}_1\xi_1 + \{\eta_1\xi_0 + \xi_1\bar{\eta}_0\}v_4.$$

From Dickson's condensed law (1.2) of multiplication in Cayley's algebra C, we have already seen that the quaternions occur as a subalgebra of C. In fact seven subalgebras of C with basic units chosen from the basic units of C are equivalent to the quaternion algebra. viz. the algebra with units $1, i_1, i_2, i_3$ and the six further algebras with basic units obtained from $1, i_1, i_2, i_3$ by replacing the suffixes 123 by 145, 624, 653, 725, 734 and 176. In each case the basic units of the subalgebra are 1 along with a proper associative triad of basic units of C.

As before, we reserve the name basic unit for elements of the set consisting of 1, i_1, i_2, i_3, i_4, i_5, i_6, i_7. Define for any basic unit u of C, $|\pm u| = u$. We see from (1.1) that for any units u, v of C

$$|\,|u|\,|v|\,| = |uv| = |\,|v|\,|u|\,| .$$

This extends easily to products involving any number of units. Suppose w is any product of any fixed set of units of C. Then $|w|$ is the same basic unit of C for all such products w i.e. $|w|$ is independent of the order and grouping of its factors.

Suppose v_1, v_2, v_3 are any three distinct units of C such that

$$|v_1 v_2 v_3| = 1, \qquad |v_s| \neq 1, \quad (s = 1, 2, 3).$$

Here v_1, v_2, v_3 are not necessarily basic units. Then by reordering if necessary

$$v_1(v_2 v_3) = (v_1 v_2)v_3 = -1.$$

The subalgebra of C with units 1, v_1, v_2, v_3 satisfies the definition of a quaternion algebra.

Let v_4 be any unit of C for which $|v_4|$ is different from 1, $|v_s|$ for s = 1, 2, 3. Then 1, $|v_s|$, $|v_4|$, $|v_s v_4|$ (s = 1, 2, 3) are the eight distinct basic units of C. For if

$$|v_s| = |v_t v_4| \text{ for some } s, t \quad (1 \leq s, t \leq 3)$$

it follows that

$$|\,|v_s v_t|\,|v_4|\,| = |v_s v_t v_4| = |\,|v_s|\,|v_t v_4|\,| = 1.$$

Thus it follows that $|v_s v_t| = v_4$. This implies that $|v_4|$ is one of 1, $|v_1|$, $|v_2|$, $|v_3|$ which is a contradiction. Therefore 1, v_1, v_2, v_3, v_4, $v_1 v_4$, $v_2 v_4$, $v_3 v_4$ are the eight distinct units of C with some signs affixed.

If we wish to ensure that 1, v_1, v_2, v_3, v_4, $v_1 v_4$, $v_2 v_4$, $v_3 v_4$ are all basic units of C, we must demand that $|v_s| = v_s$, $|v_4| = v_4$ and $|v_s v_4| = v_s v_4$ for $s = 1, 2, 3$. Thus v_1, v_2, v_3, v_4 must, of course, be themselves basic units of C. Also for each s v_s, v_4 must appear in their natural order in the unique associative triad in which they occur. There is precisely one choice of v_4 for which this is true for each triad (v_1, v_2, v_3). e.g. if $v_1 = i_1$, $v_2 = i_2$ and $v_3 = i_3$ we must of course take $v_4 = i_4$, while for $v_1 = i_3$, $v_2 = i_4$ and $v_3 = i_7$ we must choose $v_4 = i_6$ and for $v_1 = i_6$, $v_2 = i_5$, $v_3 = i_3$ we must take $v_4 = i_1$. We call v_4 the basic unit <u>assigned</u> to the triad (v_1, v_2, v_3).

A Cayley number α is called a <u>quasiquaternion</u> in u_1, u_2, u_3 if

$$\alpha = a_0 + a_1 u_1 + a_2 u_2 + a_3 u_3$$

for real a_0, a_1, a_2, a_3 where u_1, u_2, u_3 are distinct units of C other than ± 1 such that $|u_1 u_2 u_3| = 1$ or, without loss of generality by reordering if necessary, such that $u_1(u_2 u_3) = -1$.

Clearly, within any set of quasiquaternions in the same units u_1, u_2, u_3 of C the properties of quaternion addition and multiplication are satisfied. In particular, the associative law of multiplication is satisfied by any three quasiquaternions which are linear combinations of the same units u_1, u_2, u_3 of C.

Again let v_1, v_2, v_3 be any three distinct units of C such that $|v_1 v_2 v_3| = 1$ and $|v_s| \neq 1$ $(s = 1, 2, 3)$. Further let v_4 be any unit other than ± 1 such that $|v_4| \neq |v_s|$ for $s = 1, 2, 3$. Let ξ, η be any Cayley numbers. Then by Theorem 2.1 we can write

$$\xi = \xi_0 + \xi_1 v_4$$

$$\eta = \eta_0 + \eta_1 v_4$$

where ξ_0, ξ_1, η_0, η_1 are quasiquaternions in v_1, v_2, v_3.
Then

$$\xi\eta = (\xi_0 + \xi_1 v_4)(\eta_0 + \eta_1 v_4)$$

$$= \xi_0\eta_0 + (\xi_1 v_4)(\eta_1 v_4) + \xi_0(\eta_1 v_4) + (\xi_1 v_4)\eta_0 .$$

Now

$$(\xi_1 v_4)(\eta_1 v_4) = (v_4\overline{\xi_1})(\eta_1 v_4)$$

$$= v_4\{(\overline{\xi_1}\,\eta_1)v_4\} \qquad \text{by (1.13)}$$

$$= -\overline{(\overline{\xi_1}\,\eta_1)}$$

$$= -\overline{\eta_1}\,\xi_1 .$$

Also

$$\xi_0(\eta_1 v_4) = (\eta_1 \xi_0)v_4$$

since in either product an antiassociative triad occurs when and only when the units from ξ_0, η_1 are distinct and different from ± 1. The same sign changes are thus made by commuting η_1 and ξ_0.

Similarly

$$\begin{aligned}(\xi_1 v_4)\eta_0 &= (v_4 \overline{\xi}_1)\eta_0 \\ &= v_4(\eta_0 \overline{\xi}_1) \\ &= (\overline{\eta_0 \overline{\xi}_1})v_4 \\ &= (\xi_1 \overline{\eta}_0)v_4.\end{aligned}$$

Thus

$$(2.1)\quad \xi\eta = \xi_0\eta_0 - \overline{\eta}_1\xi_1 + \{\eta_1\xi_0 + \xi_1\overline{\eta}_0\}v_4.$$

Dickson's condensed law (1.2) for multiplication is thus preserved when the units i_1, i_2, i_3, i_4 are replaced by any set v_1, v_2, v_3, v_4 of units of C different from ± 1 in which v_1, v_2, v_3 form a proper associative triad of units of C and $|v_4| \neq |v_s|$ for $s = 1, 2, 3$. Any such mapping of C onto itself is an automorphism of C.

An <u>automorphism</u> Θ of Cayley's algebra C is a (1-1) reversible mapping of C onto itself under which

$$\text{(i)}\quad \Theta(\xi \pm \eta) = \Theta(\xi) \pm \Theta(\eta)$$
$$\text{(ii)}\quad \Theta(\xi\eta) = \Theta(\xi).\Theta(\eta).$$

and

(iii) $\theta(u) = v$

for ξ, η any elements of C, u any unit of C and v a corresponding unit of C.

Thus since $\theta 1.\theta 1 = \theta 1 \neq 0$ it follows that $\theta 1 = 1$. Also

$-1 = \theta(-1) = \theta(i_1 i_2 i_3) = \theta(i_1 i_2).\theta i_3 = (\theta i_1.\theta i_2)\theta i_3$.

Thus $(\theta i_1, \theta i_2, \theta i_3)$ is a proper associative triad of units of C. Any one of the seven proper associative triads of basic units can be chosen. Also there are six possible permutations of the elements of each triad. Further, θi_4 can be chosen as any one of four units. Thus counting only the members of the set of automorphisms of C which give permutations of the basic units of C we have 168 automorphisms of C. Thus there are 8.168 automorphisms of C of which 168 give distinct permutations of the basic units of C. This set of 168 automorphisms, written as a set of permutations on the suffixes of the basic units of C, forms the simple 168 group generated by the permutations (12)(47) and (2143576). Suitable sign changes must of course be applied to the units when necessary.[8].

The above discussion of Dickson's condensed law and automorphisms enables us to choose an appropriate triad of units of C and corresponding condensed law (2.1) to deal with a problem in any prescribed arithmetic of C. (§ 3 below).

We now widen the class of automorphisms to be considered. We omit condition (iii) from definition of automorphisms of C given above.

Suppose the set V of Cayley numbers v_0, v_1, v_2, v_3, v_4, v_5, v_6, v_7 satisfy the multiplication table (1.1) of Cayley's algebra C. Then $v_0^2 = v_0 \neq 0$ and therefore $v_0 = 1$. Also $v_t^2 = -v_0 = -1$ for $1 \leq t \leq 7$. Hence $v_t = -\overline{v_t}$. Thus $R(v_t) = 0$ for $1 \leq t \leq 7$.

Suppose v_1, v_2 are units of C with some signs affixed. Since $v_1 v_2 v_3 = -1$, $v_1 v_2 = v_3$ and v_3 is a unit.

Now if V contains a fourth unit it is simply a set of Cayley units with some signs affixed.

Suppose τ is contained in V where τ is not a Cayley unit. Then $\tau^2 = -1$ and $R(\tau) = 0$. But the rank equation $\xi^2 = 2R(\xi)\xi - N\xi$ holds for any Cayley number ξ. Hence $N\tau = 1$. Then since $\pm v_s \tau$ is an element of V for $s = 1, 2, 3$ $(v_s \tau)^2 = -1$ and hence $R(v_s \tau) = 0$ for $s = 1, 2, 3$. Thus we may write $\tau = \tau_1 e$ where e is a unit of C such that $|e| \neq 1, |v_s|$ $(s = 1, 2, 3)$ and τ_1 is a quasiquaternion in v_1, v_2, v_3 and the set V consists of 1, v_1, v_2, v_3, $\tau_1 e$, $(\tau_1 v_1)e$, $(\tau_1 v_2)e$ and $(\tau_1 v_3)e$.

We now show how such automorphisms can be produced by multiplication by explicit Cayley numbers. By using the method to be described, automorphisms of C under which the set of images of the units contains only one unit can be produced.

For α an arbitrary unit of C, we may denote a mapping θ of C onto itself by (α, Θ_α). A set of Cayley numbers $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6, \ldots \rho_n$ is said to induce an automorphism of C if the mapping $(\alpha, \rho_n(\rho_{n-1}(\rho_{n-2}\ldots(\rho_1\alpha\rho_1^{-1})\ldots\rho_{n-2}^{-1})\rho_{n-1}^{-1})\rho_n^{-1})$ is an automorphism of C. In particular, ρ is said to induce an automorphism of C if $(\alpha, \rho\alpha\rho^{-1})$ is an automorphism of C.

It is to be noted that certain automorphisms satisfying condition (iii) can be induced by a set of six Cayley numbers. Certain automorphisms so far discussed which do not satisfy this condition can be induced by a single quasiquaternion. We find necessary and sufficient conditions for $(\alpha, \rho\alpha\rho^{-1})$ to be an automorphism of C where ρ is a quasiquaternion.

The following result is proved.

Theorem 2.2. *A quasiquaternion ρ which is not purely real induces an automorphism $(\alpha, \rho\alpha\rho^{-1})$ of C if and only if*

$$\frac{\rho \cdot R^2(\rho)}{N\rho} = 1.$$

We first note that if ρ, β are quasiquaternions in v_1, v_2, v_3 and v_4 is a fourth unit different from ± 1 and $\pm v_s$ for $s = 1, 2, 3$

$$\rho(\beta v_4)\rho^{-1} = (\beta \rho^*)v_4$$

where

$$\rho^* = \frac{2.R(\rho)\rho}{N\rho} - 1$$

$$= \frac{1}{N\rho}\rho^2 .$$

This follows since

$$\rho(\beta v_4)\rho^{-1} = \left\{(\beta v_4)\bar{\rho}\right\}\frac{1}{N\rho}\rho$$

$$= (\beta v_4)\frac{1}{N\rho}\bar{\rho}^2$$

$$= (\beta v_4)\frac{1}{N\rho}(2R(\rho).\bar{\rho} - N\rho)$$

$$= \left\{\frac{2R(\rho)}{N\rho}\rho - 1\right\}(\beta v_4)$$

$$= \rho^{\omega}(\beta v_4)$$

$$= (\beta \rho^*)v_4 .$$

Also since $\rho^* = \frac{1}{N\rho}\rho^2$, we have $N\rho^* = 1$.

Let ξ, η be any Cayley numbers and suppose that that $\zeta = \xi\eta$. Also write $\xi = \xi_0 + \xi_1 v_4$ and

$\eta = \eta_0 + \eta_1 v_4$ where ξ_0, ξ_1, η_0, η_1 are quasiquaternions in v_1, v_2, v_3 and $|v_4|$ is different from 1 and $|v_s|$ for $s = 1, 2, 3$. Then from above we have

$$\zeta = \xi_0\eta_0 - \bar{\eta}_1\xi_1 + (\eta_1\xi_0 + \xi_1\bar{\eta}_0)v_4 .$$

Thus

$$(\rho\Sigma\rho^{-1})(\rho\eta\rho^{-1})$$

$$= (\rho\Sigma_0\rho^{-1} + \rho(\Sigma_1 v_+)\rho^{-1})(\rho\eta_0\rho^{-1} + \rho(\eta_1 v_+)\rho^{-1})$$

$$= (\rho\Sigma_0\rho^{-1} + (\Sigma_1\rho^*)v_+)(\rho\eta_0\rho^{-1} + (\eta_1\rho^*)v_+)$$

$$= \rho\Sigma_0\rho^{-1}\rho\eta_0\rho^{-1} + \overline{\eta_1\rho^*}\Sigma_1\rho^* + (\eta_1\rho^*\rho\Sigma_0\rho^{-1} + \Sigma_1\rho^*\rho\eta_0\rho^{-1})v_+ .$$

$$= \rho\Sigma_0\eta_0\rho^{-1} + \overline{\rho^*}\,\overline{\eta_1}\Sigma_1\rho^* + (\eta_1\rho^*\rho\Sigma_0\rho^{-1} + \Sigma_1\rho^*\rho\overline{\eta_0}\rho^{-1})v_+ .$$

In order that this should equal $\rho\Sigma\rho^{-1}$ it is necessary that

$$\overline{\rho^*}\,\overline{\eta_0}\Sigma_1\rho^* = \rho\overline{\eta_0}\Sigma_1\rho^{-1}$$

i.e. that $\overline{\eta_0}\Sigma_1\rho^*\rho = \rho^*\rho\,\overline{\eta_0}\Sigma_1$.

But $\overline{\eta_0}\Sigma_1$ can take any value as a quasiquaternion in v_1, v_2, v_3. Thus $\rho^*\rho$ must be a scalar c, say, since it commutes with every quasiquaternion in v_1, v_2, v_3. Hence ρ^3 must be real. But

$$\rho^3 = (4R^2(\rho) - N\rho)\rho - 2R(\rho).N\rho.$$

Thus we must have

$$4R^2(\rho) = N\rho.$$

The condition is therefore necessary.

If we have

$$\frac{4R^2(\rho)}{N\rho} = 1,$$

$$\rho^* = \frac{2R(\rho)}{N\rho}\rho - 1 = \frac{2R(\rho)}{N\rho}\overline{\rho} = -\frac{\overline{\rho}}{2R(\rho)}$$

and, therefore, $\rho^*\rho = -2R(\rho)$.

Thus

$$\bar{\rho}^* \bar{\eta}_1 \xi_1 \rho^* = \frac{2R(\rho)}{N\rho} \rho \bar{\eta}_1 \xi_1 \cdot \frac{2R(\rho)}{N\rho} \bar{\rho}$$
$$= \rho \bar{\eta}_1 \xi_1 \rho^{-1}.$$

Also

$$\eta_1 \rho^* \rho \xi_0 \rho^{-1} = \eta_1 (-2R(\rho)) \xi_0 \frac{1}{N\rho} \bar{\rho}$$
$$= \eta_1 \xi_0 \rho^*$$

and

$$\xi_1 \rho^* \rho \bar{\eta}_0 \rho^{-1} = \xi_1 \bar{\eta}_0 \rho^*$$

Hence

$$(\rho \xi \rho^{-1})(\rho \eta \rho^{-1}) = \rho(\xi_0 \eta_0 - \bar{\eta}_1 \xi_1)\rho^{-1} + \rho\{(\eta_1 \xi_0 + \xi_1 \bar{\eta}_0) v_4\}\rho^{-1}$$
$$= \rho \zeta \rho^{-1}.$$

The theorem has thus been established. Also we have

<u>Corollary 2.3.</u> <u>A Cayley number</u> ρ <u>different from zero induces an automorphism of</u> C <u>if and only if</u>

$$\rho^3 = -2.R(\rho).N\rho.$$

If we demand that ρ should have rational coordinates it follows that ρ must have norm a perfect square. Further if ρ has norm 1 and 2ρ has integral coordinates we must have

$$(2.2) \quad \rho = \frac{1}{2}(\epsilon_0 + \epsilon_1 v_1 + \epsilon_2 v_2 + \epsilon_3 v_3)$$

where the ϵ's equal ± 1 and (v_1, v_2, v_3) is a proper associative triad of units of C.

A set ρ_1, ρ_2, ρ_3, $\rho_4 \cdots \rho_n$ of quasiquaternions of the form (2.2) induces an automorphism of C. For $n \leq 7$, a different choice of associative triad can be made for each of ρ_1, ρ_2, $\rho_3 \cdots \rho_n$. For $n = 1$, automorphisms are produced which satisfy the condition: for three basic units u of C other than 1, $\theta u = \pm v$ where v is a basic unit of C. For $n = 2$, the set of images of the units contains only one basic unit other than 1 provided ρ_1 and ρ_2 are quasiquaternions in different associative triads.

No other Cayley numbers which alone induce an automorphism of C have been found. In fact it has been shown that if ρ is of the form (2.2) where $(v_1 v_2)v_3 \neq \pm 1$, ρ cannot induce an automorphism of C.

3. Maximal and Non Maximal Arithmetics in Cayley's Algebra C.

A set of elements of an algebra is defined to be a set of integral elements or arithmetic of the algebra if the set has the following three properties

(i) For any element α of the set the coefficients of the rank equation,

$$\alpha^2 - 2.R(\alpha)\alpha + N\alpha = 0,$$

are rational integers.

(ii) The set is closed under addition, subtraction and multiplication.

(iii) The set contains 1.

An arithmetic is called maximal if

(iv) it is not contained in any larger set having properties (i), (ii), (iii).

This definition of a maximal arithmetic of an algebra was stated by Dickson [12].

Let Q be the quaternion subalgebra of C all of whose elements are linear combinations of 1, i_1, i_2, i_3. The set of all elements of Q with rational integral coordinates is denoted by $H_\circ$. Clearly $H_\circ$ is an arithmetic of Q. Hurwitz [26] defined an integral quaternion to be a quaternion with coordinates either all integers or all half odd integers. Denote the set of all Hurwitz integral quaternions in Q by H. Then H is the unique maximal arithmetic of Q.

We define J_0 to be the set of all elements of C with rational integral coordinates. Clearly J_0 satisfies (i), (ii) and (iii) in C. In this section we find the seven maximal sets of integral elements of C containing J_0. The systems are characterized as J_w where w is any one of the seven basic units of C other than 1. A simple method is described by which it is immediately clear whether a given Cayley number α belongs to one of the seven maximal systems J_w. Also, it is immediately clear to which of the seven systems J_w such a Cayley integer belongs. Further, nine non maximal sets of integral elements containing J_0 of Cayley's algebra C are described.

We prove the following results.

Theorem 3.1. There are nine non maximal arithmetics which contain J_0 in Cayley's algebra C. They are characterized below as J^*, J_1, J_2, J_3, J_4, J_5, J_6, J_7 and, of course, J_0.

Theorem 3.2. The seven arithmetics J_1, J_2, J_3, J_4, J_5, J_6, J_7 are isomorphic. Each contains a different isomorph of Hurwitz integral quaternions and each contains J_0.

Theorem 3.3. There are precisely seven maximal sets of integral elements in Cayley's algebra C. They are characterized below as J_{i_1}, J_{i_2}, J_{i_3}, J_{i_4}, J_{i_5}, J_{i_6}, J_{i_7}.

Let w be a basic unit of C other than 1. We then have

Theorem 3.4. Any element α of a maximal arithmetic J_w with four coordinates half odd rational integers has characteristic unit, defined below, 1 or w. Conversely, any such element α of C belongs to J_w provided that if the characteristic unit of α is 1, w occurs in the corresponding associative triad. All other elements of J_w have their coordinates all rational integers or all half odd rational integers

Theorem 3.5. The seven maximal arithmetics J_{i_1}, J_{i_2}, J_{i_3}, J_{i_4}, J_{i_5}, J_{i_6}, J_{i_7} are isomorphic. Each contains three of the non maximal arithmetics J_1, J_2, J_3, J_4, J_5, J_6, J_7. Thus each of J_{i_1}, J_{i_2}, J_{i_3}, J_{i_4}, J_{i_5}, J_{i_6}, J_{i_7} contains three isomorphs of Hurwitz integral quaternions.

We first recall the following elementary lemmas.

Lemma 3.1. Any two distinct proper associative triads of basic units of C have precisely one element in common.

Let (u_1, u_2, u_3) and (v_1, v_2, v_3) be two such triads. The triads cannot have two elements in common for if so they have three elements in common the third being the product of the other two.

The triads cannot have an element in common for if so we can choose basic unit w such that $1, u_1, u_2, u_3, v_1, v_2, v_3, w$ are the eight basic units of C. This implies that

$$\begin{aligned} 1 &= (i_1 i_2 i_3)(i_4 i_5 i_6 i_7) \\ &= (u_1 u_2 u_3)(v_1 v_2 v_3 w) \\ &= (w)(u_1 u_2 u_3)(v_1 v_2 v_3) \\ &= w \end{aligned}$$

which cannot be so. The lemma has been established by contradiction.

Lemma 3.2. Any basic unit of C other than 1 appears in three and only three proper associative triads of basic units of C.

The unit i_1 appears in (i_1, i_2, i_3), (i_1, i_4, i_5) and (i_1, i_7, i_6) and in no other such triad. The result follows by Lemma 3.1 and the automorphisms established in § 2.

We now prove Theorem 3.1. Let J be a set of integral elements of C. Suppose that J contains J_0. Let α be an element of J. Then by property (i) for an arithmetic $2R(\alpha)$ and $N\alpha$ are rational integers. Further, since for any unit u of C, αu is contained in J, it follows that

$$\alpha = \sum_{s=0}^{7} a_s i_s$$

where $2a_s$ is a rational integer for each s $(0 \leq s \leq 7)$.

If any one coordinate of α is half an odd rational integer then four or eight coordinates of α are half odd rational integers, since $N\alpha$ is a rational integer. Otherwise, all the coordinates of α are rational integers. Now the units of C are elements of J and J is closed under addition and subtraction. Thus we need only consider which elements ξ, of the form

(3.1) $$\xi = \frac{1}{2}\sum_{t=1}^{4} w_t,$$

where w_1, w_2, w_3, w_4 are distinct basic units of C and which elements η, of the form

(3.2) $$\eta = \frac{1}{2}\sum_{s=0}^{7} i_s,$$

belong to J. It is noted that there are seventy elements ξ of C of the form (3.1).

Define for any ξ of the form (3.1) the <u>characteristic unit</u> $\chi(\xi)$ of ξ to be

$$\chi(\xi) = |w_1 w_2 w_3 w_4|.$$

Then $\chi(\xi)$ is a basic unit of C. We note that for any unit u of C

$$\chi(u\xi) = \chi(\xi).$$

Further, if α is of the form $\alpha_0 + \xi$, where α_0 is an element of J_0 and ξ is of the form (3.1), we define

$$\chi(\alpha_0) = 0$$

and

$$\chi(\alpha_0 + \xi) = \chi(\xi).$$

It follows that element α with coordinates not all half odd rational integers satisfies the condition (i) for an element of an arithmetic of C if and only if $\chi(\alpha)$ is defined.

Let ξ be any one of the seventy elements of the form (3.1). Then $\chi(\xi)$ is defined and equals a basic unit of C. Thus $\chi(\xi) = 1$ or $\chi(\xi) = u$ where u is a basic unit of C for which $u^2 = -1$. In either case, we have $w_t = 1$, for some t, or w_t different from 1 for all t $(1 \leq t \leq 4)$. Four cases are, therefore, to be considered.

If $\chi(\xi) = 1$ and $w_1 = 1$, say, we write $w_2 = u_1$, $w_3 = u_2$ and $w_4 = u_3$. Then

$$\xi = \frac{1}{2}(1 + u_1 + u_2 + u_3).$$

But, since $\chi(\xi) = 1$, it follows that $|u_1 u_2 u_3| = 1$. Thus (u_1, u_2, u_3) is a proper associative triad of basic units of C. Hence there exists a unique basic unit u, say, of C assigned to (u_1, u_2, u_3). We define ξ_u to be

$$\frac{1}{2}(1 + u_1 + u_2 + u_3).$$

Clearly there are seven elements ξ_u of this form (viz. ξ_{i_r} for $r = 1, 2, \ldots 7$).

We now consider the seven elements $\xi_u u$ where $u = i_r$ $(1 \leq r \leq 7)$. We have

$$\chi(\xi_u u) = \chi(\xi_u) = 1.$$

Also u, u_1u, u_2u, u_3u are basic units of C other than 1, since u is the basic unit assigned to the triad (u_1, u_2, u_3). Thus $\xi_u u$ is of the form (3.1) and such that $w_t \neq 1$ $(1 \leq t \leq 4)$. Further, no two elements $\xi_u u$, $\xi_v v$ $(u \neq v)$ are equal. We write $\xi_u^* = \xi_u u$. Thus

$$\xi_u^* = \frac{1}{2}(1 + u_1 + u_2 + u_3)u.$$

Now suppose that $\chi(\xi)$ is a basic unit of C other than 1. If $w_1 = 1$ say we have

$$\xi = \frac{1}{2}(1 + w_2 + w_3 + w_4)$$

Suppose that $\chi(\xi) = w$. Then $|w_2 w_3 w_4| = w$. We may write $w_2 = v_1' w$, $w_3 = v_2' w$ and $w_4 = v_3' w$. Let $|v_1'| = v_1$, $|v_2'| = v_2$ and $|v_3'| = v_3$. Then, since $|v_1 v_2 v_3| = 1$, (v_1, v_2, v_3) is a proper associative triad of basic units of C. Thus for each of the seven possible triads of basic units, w must be such that $w \neq 1$, $w \neq v_s$ $(s = 1, 2, 3)$. Alternatively, by lemma 3.2, we see that, if w is chosen as any one of the seven basic units, (v_1, v_2, v_3) must be one of the four proper associative triads of basic units not containing w. We write

$$\xi_{w,v} = \frac{1}{2}(1 + |v_1 w| + |v_2 w| + |v_3 w|)$$
$$= \frac{1}{2}\{1 + (\epsilon_1 v_1 + \epsilon_2 v_2 + \epsilon_3 v_3)w\}$$

where the sign coefficients ϵ are chosen so that $\xi_{w,v}$ is of the form (3.1) and where (v_1, v_2, v_3) is the proper associative triad of basic units of C with assigned unit v.

Thus there are 28 elements $\xi_{w,v}$ of the form (3.1). Also, for each $\xi_{w,v}$, $\chi(\xi_{w,v}) = w$ and $w_t = 1$ for some t $(1 \leq t \leq 4)$.

Finally we consider elements of the form

$$\xi^*_{w,v} = \frac{1}{2}(w + v_1 + v_2 + v_3)$$

where, as before, w is any basic unit of C and where (v_1, v_2, v_3) is a proper associative triad of basic units of C with assigned unit v and not containing w. From lemma 3.2, it is easy to see that there are 28 elements $\xi^*_{w,v}$ defined all of which are of the form (3.1). Also, for each $\xi^*_{w,v}$ defined, $\chi(\xi^*_{w,v}) = w$ and $w_t \neq 1$, $(1 \leq t \leq 4)$.

We have thus dealt with all elements ξ of the form (3.1). It is to be noted that all sums of the form $\xi_u + \xi^*_u$ and of the form $\xi_{w,v} + \xi^*_{w,v}$ are of the form (3.2). Since the units of C are elements of arithmetic J and since J is closed under addition, subtraction and multiplication, it follows that ξ_u is an element of J if and only if ξ^*_u is an element of J and that $\xi_{w,v}$ is an element of J if and only if $\xi^*_{w,v}$ is an element of J.

Let J_1 be the set of all elements α of C which can be written in the form

$$\alpha = \alpha_0 + \delta_1 \xi_{i_1} + \delta_2 \xi^*_{i_1}$$
$$= \alpha_0 + \frac{1}{2}\delta_1(1 + i_6 + i_5 + i_3) + \frac{1}{2}\delta_2(1 + i_6 + i_5 + i_3)\, 1_1$$

where α_0 belongs to J_0 and $\delta_1, \delta_2 = 0$ or 1.

Then $2R(\alpha)$ and $N\alpha$ are rational integers. Clearly, J_1 is closed under addition and subtraction. Also (i_6, i_5, i_3) is the proper associative triad of basic units of C with assigned unit i_1. It follows from Theorem 2.2 that J_1 is closed under multiplication. Since J_0 contains 1, J_1 also contains 1. Thus J_1 is a set of integral elements of C.

The above argument can be used for each of the seven proper associative triads of basic units of C. Hence we have

Definition of the Non Maximal Arithmetics J_r of C. For each basic unit i_r of C other than 1 we define J_r to be the set of all elements α_r of C of the form

$$\alpha_r = \alpha_0 + \delta_1 \xi_{i_r} + \delta_2 \xi^*_{i_r}$$

where α_0 is contained in J_0, $\delta_1, \delta_2 = 0$ or 1 and ξ_{i_r} and $\xi^*_{i_r}$ are as defined above.

Clearly the intersection of the seven arithmetics $J_1, J_2, J_3, J_4, J_5, J_6, J_7$ contains J_0. Further this intersection strictly contains J_0 since η of the form (3.2) belongs to each of the seven non maximal arithmetics J_r $(r = 1, 2, \ldots 7)$ but η is not contained in J_0. We define the intersection of $J_1, J_2, J_3, J_4, J_5, J_6, J_7$ to be J^*. Then

$$J^* = \bigcap_{r=0}^{7} J_r .$$

It is easy to see that the intersection of any set of arithmetics of an algebra is itself an arithmetic of that algebra. Thus J^* is a non maximal arithmetic of C. Finally we note that for rational integers r, s such that $r \neq s$ and $1 \leq r, s \leq 7$

$$J_r \cap J_s = J^*.$$

To complete the proof of theorem 3.1 we must show that $J_1, J_2, J_3, J_4, J_5, J_6, J_7$ are non maximal arithmetics of C.

Let K_1, K_2 be any subsystems of C which are closed under addition, subtraction and multiplication. A (1-1) reversible mapping θ of K_1 onto K_2 is called an <u>isomorphism</u> of K_1 onto K_2 if under θ addition, subtraction and multiplication are preserved. If such a mapping θ exists, K_1 and K_2 are said to be <u>isomorphic</u> and K_2 is called an isomorph of K_1.

From § 2 it follows that the automorphism ϕ of C associated with the permutation (2143576), on the suffixes of the units of C, is an isomorphism of any arithmetic J onto a second aritnmetic J', say. Thus $\phi J_1 = J_4$, $\phi J_4 = J_3$ and so on, while $\phi J^* = J^*$. Therefore $J_1, J_2, J_3, J_4, J_5, J_6, J_7$ are isomorphic. Theorem 3.2 has thus been proved.

We now proceed to find the maximal arithmetics of C. First we prove

Lemma 3.3. Any sum $\xi_u + \xi_v$ satisfies condition (i) for an element of an arithmetic J of C and

$$\chi(\xi_u + \xi_v) = 1.$$

By lemma 3.1 we assume without loss of generality that $u_1 = v_1$. Then

$$\xi_u + \xi_v = 1 + u_1 + \tfrac{1}{2}(u_2 + u_3 + v_2 + v_3).$$

Thus $\chi(\xi_u + \xi_v) = |u_2 u_3 v_2 v_3| = |u_1 v_1| = 1$. This completes the proof of the lemma.

Now we prove

Lemma 3.4. Any product $\xi_u \xi_v$ satisfies condition (i) for an element of an arithmetic J of C. $\chi(\xi_u \xi_v)$ equals the basic unit which triads (u_1, u_2, u_3) and (v_1, v_2, v_3) have in common.

Again suppose that $u_1 = v_1$. Then by straight forward multiplication

$$\xi_u \xi_v = \tfrac{1}{2}(u_1 + u_2 + v_3 + u_2 v_3)$$

which satisfies condition (i) for an element of an arithmetic of C. Hence $\chi(\xi_u \xi_v)$ is defined and

$$\begin{aligned} \chi(\xi_u \xi_v) &= |u_1 u_2 v_3 u_2 v_3| \\ &= |u_1 u_2 u_2 v_3 v_3| \\ &= u_1 . \end{aligned}$$

This completes the proof of Lemma 3.4. We note that $\xi_u \xi_v = \xi^*_{u_1, x}$ where x is the basic unit assigned to the triad $(u_2, v_3, u_2 v_3)$ provided that $|u_2 v_3| = u_2 v_3$.

Lemma 3.5. Two elements $\xi_{w,v}$, $\xi_{w',v'}$ of C cannot both be contained in the same arithmetic J of C unless $w = w'$.

We have

$$\xi_{w,v} = \tfrac{1}{2}(1 + |v_1 w| + |v_2 w| + |v_3 w|)$$

and

$$\xi_{w',v'} = \tfrac{1}{2}(1 + |v_1' w'| + |v_2' w'| + |v_3' w'|)$$

Again, without loss of generality, we let $v_3 = v_3'$. Then

$$|v_3 w| \xi_{w,v} = \tfrac{1}{2}(|v_3 w| + v_2 + v_1 + 1) + \xi_0 .$$

and

$$|v_3 w'| \xi_{w',v'} = \tfrac{1}{2}(|v_3 w'| + v_2' + v_1' + 1) + \xi_0'$$

where ξ_0 and ξ_0' are elements of J_0. Suppose that $\xi_{w,v}$ and $\xi_{w',v'}$ belong to J. Then $|v_3 w| \xi_{w,v}$ and $|v_3 w'| \xi_{w',v'}$ also belong to J. Hence

$$\alpha = |v_3 w| \xi_{w,v} - |v_3 w'| \xi_{w',v'}$$
$$= \tfrac{1}{2}(|v_3 w| - |v_3 w'|) + \tfrac{1}{2}(v_1 + v_2 - v_1' - v_2') + \alpha_0$$

must be an element of J. Now α must satisfy condition (i) for an element of an arithmetic of C. But (v_1 , v_2) and (v_1' , v_2') have either two elements in common or no elements in common. Hence we must have $|v_3 w| = |v_3 w'|$. This holds if $w = w'$. Thus Lemma 3.5 has been established.

Now any element of C for which a characteristic unit is defined has characteristic unit equal to 0, 1 or w where w is a basic unit of C other than 1.

Hence we see at once from Lemma 3.5 that Lemma 3.6 holds.

Lemma 3.6. All elements of any given arithmetic J of C with characteristic units different from 0 or 1 have equal characteristic units.

We now prove

Lemma 3.7. $\xi_u + \xi_{w,v}$ satisfies the condition (i) for an element of an arithmetic J of C if and only if w is an element of the triad (u_1, u_2, u_3) with assigned unit u. If this condition holds $\chi(\xi_u + \xi_{w,v}) = w$.

We have

$$\xi_u + \xi_{w,v} = 1 + \tfrac{1}{2}(u_1 + u_2 + u_3 + |v_1 w| + |v_2 w| + |v_3 w|).$$

Clearly (u_1, u_2, u_3) and $(|v_1 w|, |v_2 w|, |v_3 w|)$ cannot have three elements in common since $|u_1 u_2 u_3| = 1$ while $|v_1 w \cdot v_2 w \cdot v_3 w| = w$. If the triads have an even number of elements in common, $N(\xi_u + \xi_{w,v})$ is not a rational integer and $\xi_u + \xi_{w,v}$ is, therefore, not contained in J. Assume that $\xi_u + \xi_{w,v}$ is an element of J. Then (u_1, u_2, u_3) and $(|v_1 w|, |v_2 w|, |v_3 w|)$ must have precisely one element in common. Also, by Lemma 3.1, we may take $u_3 = v_3$. Then if $|v_1 w|$ belongs to the triad (u_1, u_2, u_3) we have $|v_1 w| = u_s$ $(s = 1, 2 \text{ or } 3)$. Now $|v_1 w| = u_3$ implies that $|v_2 w| = |v_3 v_1 w| = |u_3 u_3| = 1$, which is not so. $|v_1 w| = u_s$ $(s = 1 \text{ or } 2)$ implies that $|v_2 w| = |v_3 v_1 w| = |u_3 u_s| = u_t$ $(t = 1 \text{ or } 2)$ and then (u_1, u_2, u_3) and $(|v_1 w|, |v_2 w|, |v_3 w|)$ have two elements in common. This cannot hold.

Similarly, we cannot have

$$|v_2 w| = u_s \quad \text{for } s = 1, 2 \text{ or } 3.$$

Hence we must have

$$|v_3 w| = u_s \quad \text{for some } s \quad (1 \leq s \leq 3).$$

But, since $|v_3 w| = |u_3 w|$, we have $w = |u_3 u_s|$. Now $w \neq 1$ and, therefore, $u_3 \neq u_s$. Hence, since $u_1(u_2 u_3) = -1$, we have $w = u_t$ for some t $(1 \leq t \leq 3)$ i.e. w belongs to the triad (u_1, u_2, u_3) with assigned unit u.

To complete the proof we suppose without loss of generality that $w = u_2$. Then, since $v_3 = u_3$, we can write

$$\xi_u + \xi_{w,v} = 1 + \tfrac{1}{2}(u_1 + u_2 + u_3 + |v_1 u_2| + |v_2 u_2| + u_1)$$

$$= 1 + u_1 + \tfrac{1}{2}(u_2 + u_3 + |v_1 u_2| + |v_2 u_2|).$$

Thus

$$\chi(\xi_u + \xi_{w,v}) = |u_2 u_3 v_1 u_2 v_2 u_2|$$

$$= |u_2 u_3 v_1 v_2|$$

$$= |u_1 v_3|$$

$$= |u_1 u_3|$$

$$= u_2$$

$$= w.$$

This completes the proof of Lemma 3.7.

For products of the form $\xi_{w,v}\xi_{w,v'}$ it follows from Lemma 3.6 that we need only consider the case when $w = w'$. It is easy to prove by direct multiplication that the following lemma holds.

Lemma 3.8. The product of two elements $\xi_{w,v}$ and $\xi_{w,v'}$ of C satisfies the condition (i) for an element of an arithmetic of C and $\chi(\xi_{w,v}\xi_{w,v'})$ equals 1 or w.

In the same way the following lemma can be simplified for the present argument.

Lemma 3.9. The product of two elements ξ_u and $\xi_{w,v}$ belongs to an arithmetic of C if and only if w is an element of the triad (u_1, u_2, u_3).

In fact to complete our argument we see from Lemma 3.7 that we need only consider products $\xi_u\xi_{w,v}$ for which $w = u_s$ for some s $(1 \leq s \leq 3)$. The details of the proof involving straight forward multiplication of a quasiquaternion and $\xi_{w,v}$ are omitted. For each such product $\chi(\xi_u\xi_{w,v})$ is equal to 1 or w.

We are now in a position to establish Theorem 3.3. Suppose J is an arithmetic of C containing the quasiquaternions ξ_u, ξ_v. Let the associative triads with assigned units u, v, $u \neq v$, have unit w in common. Then by Lemma 3.4 J contains an element with characteristic unit w.

Also, from the result and proof of Lemma 3.3, it follows that J contains the third quasiquaternion of the form (3.1) with corresponding associative triad containing w.

Now suppose that J contains quasiquaternion

$$\xi_{u'} = \tfrac{1}{2}(1 + u'_1 + u'_2 + u'_3)$$

of the form (3.1) for which $u'_s \neq w \quad (1 \leq s \leq 3)$. i.e. (u'_1, u'_2, u'_3) is one of the four proper associative trieds of basic units not containing w. Then from Lemma 3.4 it follows that $\chi(\xi_u \xi_{u'})$ is equal to a basic unit of C other than 1 or w. Therefore, by Lemma 3.6, $\xi_u \xi_{u'}$ cannot be an element of J. Hence J cannot contain $\xi_{u'}$.

<u>Definition of the Maximal Arithmetics</u> J_w <u>of</u> C.

For each basic unit w of C other than 1 we define J_w to be the set of all elements $\alpha_{(w)}$ of C of the form

$$(3.3) \quad \alpha_{(w)} = \alpha_0 + \delta_1 \xi_{(w)} + \delta_2 \eta$$

where α_0 is contained in J_0, $\delta_1, \delta_2 = 0$ or 1, $\xi_{(w)} = \xi_u$ where $w = u_s$ for some s $(1 \leq s \leq 3)$ or $\xi_{(w)} = \xi_{w,v}$ and $\eta = \frac{1}{2} \sum_{s=0}^{7} i_s$.

We have proved in the above lemmas that for $w = i_1, i_2, i_3, i_4, i_5, i_6, i_7$ J_w is a maximal arithmetic of C. This completes the proof of Theorems 3.3 and 3.4.

It follows from Lemma 3.2 that each maximal arithmetic J_w of C contains three distinct non maximal arithmetics J_r, J_s, J_t, $(1 \leq r,s,t \leq 7)$. i_r, i_s, i_t are the basic units assigned to the proper associative triads of basic units containing w.

The permutation (2143576), as explained in § 2, when applied to the suffixes of the basic units of C, gives an automorphism of C for suitable sign changes on the units. Thus J_{i_1}, J_{i_2}, J_{i_3}, J_{i_4}, J_{i_5}, J_{i_6}, J_{i_7} are isomorphic. For any such isomorphism Θ, $\Theta J_u = J_v$, if and only if, $\Theta u = v$.

Given any element α of C which satisfies condition (i) for an element of an arithmetic of C, we can immediately see to which of the maximal arithmetics J_w it belongs. Any such element α can be written in the form (3.3) for some basic unit w. Clearly, if ξ_1, ξ_2 are both zero, then α belongs to J_0, while, if $\xi_1 = 0$ and $\xi_2 \neq 0$, α is contained in J^*. If $\xi_1 \neq 0$, then α is an element of one or three of the maximal arithmetics J_w $(w = 1,..7)$ For example, if

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

we have $\xi_{(w)} = \xi_{i_4}$, since $\chi(\xi_{(w)}) = 1$. We see at once that α is an element of J_{i_1}, J_{i_2} and J_{i_3}.

However, if

$$\xi_{(w)} = \tfrac{1}{2}(1 + i_5 + i_6 + i_7)$$

we have

$$\xi_{(w)} = \tfrac{1}{2}\{ 1 + (i_1 + i_2 + i_3) i_4 \}$$
$$= \eta_{i_4, i_4}$$

since $\mathcal{R}(\xi_{(w)}) = i_4$. Thus we see that e is only contained in J_{i_4}.

It is now easy to write down the set of elements of norm 1 of any maximal arithmetic J_w of C. There are 16 units of C_0, the 48 quasi-quaternions involving linear combinations of the proper associative triads containing $\pm w$ and the 48 elements obtained from the quasi-quaternions by multiplying by the corresponding assigned units. Also there are 64 elements of the form

$$\tfrac{1}{2}(\pm 1 \pm u_1 w \pm u_2 w \pm u_3 w)$$

and 64 elements of the form

$$\tfrac{1}{2}(\pm w \pm u_1 \pm u_2 \pm u_3)$$

where (u_1, u_2, u_3) is a proper associative triad of basic units of C not involving w. Thus J_w contains 240 elements ρ, say, of norm 1.

We note that all elements ξ_{λ}^{μ}, $\eta_{w,v}^{\mu}$ of the form (3.1) have real part zero. Also the units of C are elements of norm 1 of any maximal arithmetic J_w of C.

Thus $R(\rho) = 0$ for 126 of the elements ρ of J_w of norm 1. For these 126 elements we see at once from the rank equation that $\rho^2 = -1$.

The remaining elements of norm 1 other than ± 1 have real part equal to $\pm\frac{1}{2}$. Thus $R(\rho) = \pm\frac{1}{2}$ for 112 elements of norm 1 of J_w and, in this case, $\rho^3 = \mp 1$. Hence it follows from Corollary 2.3 that an element of norm 1 of any maximal arithmetic J_w of C induces an automorphism of C if and only if $\rho^3 = \pm 1$.

As we saw in § 2, it follows at once from Dickson's condensed law (1.2) of multiplication in C that the permutation (123)(567) applied to the suffixes of the units of Cayley's algebra gives an automorphism of the algebra. In effect this fact was used by Dickson [13] in finding three of the maximal sets of integral elements of C viz. J_{t_1}, J_{t_2}, and J_{t_3}.

In order to treat the same subject Kirmse [28] defined a <u>module</u> in Cayley's algebra to be a set of Cayley numbers with rational coefficients closed under subtraction and containing eight linearly independent members. A module is called an <u>integral domain</u> if it is closed under multiplication.

For example, the module J_0 consisting of all Cayley numbers with rational integral coefficients is an integral domain. Kirmse then defined a maximal integral domain to be an extension of J_0 which cannot be further extended without ceasing to be an integral domain. Kirmse's maximal integral domains, if correctly derived, are the same as the seven maximal sets of Cayley integers obtained above.

We now prove the following result on the intersections of the maximal arithmetics of C.

Theorem 3.6. For (u, v, w) a proper associative triad of basic units of C, the intersection of J_u, J_v and J_w is J_r where i_r is the basic unit assigned to (u, v, w).

For any anti-associative triad (u', v', w') of basic units of C, the intersection of $J_{u'}$, $J_{v'}$, $J_{w'}$ equals J^* where

$$J^* = \bigcap_{s=1}^{7} J_s = \bigcap_{s=1}^{7} J_{i_s}$$

The result is immediate. Suppose that

$$\xi = \tfrac{1}{2}(1 + u + v + w).$$

Since $\chi(\xi) = 1$, we see that ξ is an element of the intersection of J_u, J_v and J_w. Also J_0 is contained in this intersection. Let i_r be the basic unit assigned to (u, v, w). Then, since J_r is formed by adjoining the element ξ to J_0, it follows that the intersection of J_u, J_v and J_w is J_r.

To prove the second part of the theorem we note that no such common element ξ' can be found. This follows since

$$J_{u} \cap J_{v} = J_{u'} \cap J_{v'} \cap J_{u'v'} = J_{s}$$

where i_s is the basic unit assigned to the proper associative triad $(u', v', |u'v'|)$. But

$$\tfrac{1}{2}(1 + u' + v' + |u'v'|)$$

is not contained in J_w. Thus the result follows. This completes the proof of Theorem 3.6.

We make the following definitions for use in §§ 4 and 9 below.

Let D be a <u>defining set of Cayley units for</u> J_w if D is of one of the following three types.

(i) D is the empty set of units of C.

(ii) D is a set (u_1, u_2, u_3, u_4) of units of C for which

$$\tfrac{1}{2}\sum_{s=1}^{4} u_s$$

is contained in J_w.

(iii) D is a set consisting of the eight basic units of C with some signs affixed.

Further, define D' to be a <u>basic</u> defining set of Cayley units for J_w if D' is a set (u'_1, u'_2, u'_3, u'_4) of basic units of C for which

$$\tfrac{1}{2}\sum_{s=1}^{4} u'_s$$

is contained in J_w.

To form a table of the basic defining sets of Cayley units for maximal arithmetic J_w of C we proceed as follows. Let v be any basic unit of C other than 1 and w. Then (w, v, |wv|) is a proper associative triad of basic units of C. Let the unit assigned to triad (w, v, |wv|) be u. Then the basic defining sets of units for J_w are

(3.4)

(1, w, v, |wv|)	(u, wu, vu, |wv| u)
(1, w, u, wu)	(v, |wv| , vu, |wv| u)
(1, w, vu, |wv| u)	(v, |wv| , u, wu)
(1, v, u, |wv| u)	(w, |wv| , wu, vu)
(1, |wv|, u, vu)	(w, v, wu, |wv| u)
(1, v, wu, vu)	(w, |wv| , u, |wv| u)
(1, |wv| , wu, |wv| u)	(w, v, u, vu).

Thus if we wish to find the basic defining sets of units for J_{i_1}, for example, we put $w = i_1$ and choose $v = i_2$, say. Then, since i_4 is the unit assigned to the triad (i_1, i_2, i_3) we have, $u = i_4$. In table II we give the basic defining sets for $J_{i_1} = J_1$ in both Cayley and Dickson notation.

Finally, for use in § 9, we give the following definition and lemma on sets of basic units of C. Here no two units of the same set are equal. Also, as before, the order of the units within a set is unimportant.

A set A_1 of basic units is said to be replaceable for arithmetic J_w of C by a set A of basic units of C if

(i) A_1 and A_2 contain the same number of elements and if

(ii) corresponding to each basic defining set D_1' of units for J_w there exists a basic defining set D_2' for J_w such that $A_1 \cap D_1'$ and $A_2 \cap D_2'$ contain the same number of elements and such that as D_1' equals the 14 basic defining sets in turn D_2' equals the same 14 sets in a possibly different order.

We now prove

Lemma 3.10. Any set A_1 consisting of t basic units of C is replaceable for J_w by any set A_2 of t basic units of C provided that $t = 1, 2$ or 3.

The lemma can be proved by inspection of the basic defining sets for J_w given in (3.4) and from the fact that in (3.4) v is any basic unit of C other than 1 or w. Hence each unit occurs in precisely seven of the defining sets. Therefore, the lemma holds for $t = 1$. Any two units occur in three basic defining sets and do not occur in three such sets. The defining sets occur in pairs, the union of which equals the set of eight basic units of C. Thus precisely one unit of any pair of units occurs in each of the eight remaining sets.

By considering elements ξ_{u_1}, ξ_{u_1,v_1} for suitably chosen u_1, v_1, we see that any set of three units occurs in one and only one basic set. Hence precisely two of the three units must occur in 6 sets and precisely one of the three in the remaining six sets. The lemma has thus been established. For $t = 4$, the result does not hold.

4. Factorization and Congruence.

We now treat factorization and congruence in the arithmetics of Cayley's algebra C. Firstly, we discuss isotopisms of C. Results, proved by Rankin [45] , on the number of factorizations of a given element in the arithmetics H_0 and J_0 are reviewed. Further, results on congruence, established below, are used to find the number of factorizations of a prescribed element in the remaining arithmetics of C. As before, we define our terms as they occur in the general discussion.

Let J be any arithmetic of Cayley's algebra C. If, for any two elements ζ, ξ of an arithmetic J of C, there exists an element η of J such that

$$\zeta = \xi\eta \tag{4.1}$$

ζ is said to be *divisible by ξ on the left in* J and ξ is said to *divide* ζ *on the left in* J. Similarly we define ζ to be divisible by η on the right in J if there exists an ξ of J such that (4.1) holds. In both cases ζ is said to have the *factorization* $\xi\eta$ *in* J and ξ, η are called the *factors* of ζ *in* J. We write

$$\zeta = \xi\eta \quad \text{in J.}$$

For example, an element ρ of norm 1 in J divides any element ζ of J on the left and on the right in J. Also, clearly, a rational integer m divides an element ζ of J on the right in J if and only if m divides ζ on the left in J.

An element ζ of J is said to be a <u>Cayley prime</u> for J if, for all factorizations $\xi\eta$ of ζ in J, either $N\xi = 1$ or $N\eta = 1$. For example, suppose that ζ has norm a rational prime p, say. Then it follows, since $N\zeta = N\xi . N\eta = p$, that either ξ or η has norm 1. In this case, ζ is a Cayley prime.

If, for given quaternions α, β, γ,

$$\alpha = \beta\gamma$$

it follows, by the associative law of multiplication for quaternions, that for any quaternion δ

$$\alpha = (\beta\delta)(\delta^{-1}\gamma)$$

Thus if β divides α on the left in a quaternion arithmetic H' of C, it follows that, for any element δ of norm 1 belonging to H', $\beta\delta$ divides α on the left in H'.

If ζ, ξ, η are Cayley numbers and $\zeta = \xi\eta$ the relation

$$\zeta = (\xi\delta)(\delta^{-1}\eta)$$

in general only holds when δ ~~= $\pm m$ where m~~ is a non zero ~~rational integer~~ real number.

The question naturally arises of whether it is possible to choose (1-1) mappings θ, ϕ of C onto itself such that, for any given Cayley numbers ζ, ξ, η for which $\zeta = \xi\eta$,

$$\zeta = \theta\xi \cdot \phi\eta .$$

To discuss this question, we make the following definition.

An ordered triple of (1-1) mappings (θ, ϕ, ψ) of C onto itself is defined to be an isotopism of C if

$$\theta\xi \cdot \phi\eta = \psi\xi\eta \quad \text{for all } \xi, \eta \text{ in C.}$$

An isotopism in which the mappings θ, ϕ, ψ denote multiplication by reals is called trivial. For example, the isotopism $(\iota, -\iota, -\iota)$ where ι is the identity mapping and $-\iota$ maps every element onto its negative is a trivial isotopism of C.

Albert's identities (1.13) and (1.14) provide convenient examples of isotopisms of C which are non trivial.

The triple of mappings (θ, ϕ, ι) of C upon itself, if an isotopism, is called a principal isotopism of C. We prove

Theorem 4.1. There does not exist a non trivial principal isotopism of C.

Suppose that (θ, ϕ, ι) is a principal isotopism of C. Let i_s ($s = 0, 1, \ldots 7$) be as usual the basic units of C. Write

$$\theta i_s = u_s, \quad \phi i_s = w_s \text{ for } 0 \leq s \leq 7.$$

Then the sets u_s, w_s for $s = 0, 1, \ldots 7$ are not necessarily units of C. Let $Nw_s = c_s$.

Then $$u_s w_t = \theta i_s . \phi i_t = i_s i_t .$$

and $$u_0 w_0 = i_0 i_0 = 1.$$

Hence

$$c_0 u_0 = \overline{w}_0 . \tag{4.2}$$

Also $$u_0 w_t = i_0 i_t = i_t$$

and $$u_t w_0 = i_t i_0 = i_t$$

Therefore

$$c_0 u_t = i_t \overline{w}_0 . \tag{4.3}$$

For $1 \leq t \leq 7$, we have

$$u_t w_t = i_t i_t = -1.$$

Thus

$$c_t u_t = -\overline{w}_t . \tag{4.4}$$

For $1 \leq s \leq 7$

$$u_t w_s = i_t i_s$$

and therefore by (4.4) we have

$$c_s u_t = (i_t i_s)\, \overline{w}_s = -(i_t i_s)\, c_s u_s .$$

Hence

$$u_t = -(i_t i_s)\, u_s . \tag{4.5}$$

It follows by (4.2) and (4.3) that for $1 \leq t \leq 7$

$$c_o u_t = i_t \bar{u}_o = c_o i_t u_o$$

Thus

(4.6) $$u_t = i_t u_o .$$

By (4.5) and (4.6) for $1 \leq t, s \leq 7$

(4.7) $$i_t u_o = -(i_t i_s)\, u_s = -(i_t i_s)\,(i_s u_o).$$

Now let $u_o = \xi_o + \xi_1 v$ where ξ_o, ξ_1 are quasiquaternions in $(i_t, i_s, i_t i_s)$ and v is another unit different from ± 1. We assume that $t \neq s$. Then the right hand side of (4.7) equals

$$\begin{aligned} -(i_t i_s)\,(i_s \xi_o + i_s(\xi_1 v)) &= -(i_t i_s)\,(i_s \xi_o + (\xi_1 i_s) v) \\ &= i_t \xi_o - (i_t i_s)\,((\xi_1 i_s) v) \\ &= i_t \xi_o - (\xi_1 i_t) v \\ &= i_t \xi_o - i_t(\xi_1 v) \\ &= i_t(\xi_o - \xi_1 v). \end{aligned}$$

But the left hand side of (4.7) equals $i_t(\xi_o + \xi_1 v)$. Thus

$$\xi_o + \xi_1 v = \xi_o - \xi_1 v.$$

Therefore

$$\xi_1 = 0.$$

Now i_t, i_s can be chosen as any pair of units of C for which $|i_t| \neq 1$ and $|i_s| \neq 1$. Thus u_o is real. The result follows by (4.2), (4.3) and (4.4), i.e. all principal isotopisms of Cayley's algebra C are trivial.

Suppose that, for $N\xi = N\xi'$ and $N\eta = N\eta'$,

$$\zeta = \xi\eta = \xi'\eta'$$

are two different factorizations in arithmetic J of element ζ of J of C. Then by the above theorem it follows that no explicit relation corresponding to a principal isotopism of C can exist between (ξ, η) and (ξ', η') other than

$$\xi = -\xi', \quad \eta = -\eta'$$

unless ζ or ζu is a quasiquaternion for some unit u of C or ζ is of some other special form.

We shall see that factors of a given element of J_w can be characterized up to a factor of ± 1 by considering congruence modulo 2 in J_w.

For any rational integer $m>0$ and Cayley integers ξ, η of J_w, we define ξ to be congruent to η modulo m in J_w if $\xi - \eta$ is divisible by m in J_w. We write

$$\xi \equiv \eta \quad (\text{modulo } m \text{ in } J_w)$$

or, when no confusion can arise,

$$\xi \equiv \eta \quad (\text{mod } m).$$

It is clear that for this definition congruence is well defined in the sense that it is an equivalence relation.

If

$$\xi \equiv \xi_1 \pmod{m}, \qquad \eta \equiv \eta_1 \pmod{m}$$

then

$$\xi\eta \equiv \xi_1\eta_1 \pmod{m}.$$

We only consider modulum m for m a rational integer.

We first prove

Theorem 4.2. For any elements η and η' of J_w such that

$$\eta \equiv \eta' \quad (\text{modulo } 2 \text{ in } J_w)$$

$N\eta$ and $N\eta'$ are either both even or both odd rational integers.

We have $\eta = \eta' + 2\zeta$ where ζ is an element of J_w. Therefore, by (1.3),

$$N\eta = N\eta' + 4N\zeta + 2R(2\eta'\overline{\zeta}).$$

But $\eta'\overline{\zeta}$ is an element of J_w. Hence $R(2\eta'\overline{\zeta})$ must be an integer. The result follows.

Also we have

Theorem 4.3. Any element ζ of maximal arithmetic J_w is congruent modulo 2 in J_w to an element τ of an arithmetic J, containing J_0, of C if and only if ζ is itself an element of J.

We have

$$\zeta \equiv \tau \quad (\text{mod } 2 \text{ in } J_w).$$

Thus

$$\zeta = \tau + 2\alpha$$

where α is an element of J_w. Thus 2α is contained in J_o. Hence ζ belongs to J if and only if τ belongs to J.

We now prove the more difficult

Theorem 4.4. Any element ξ of odd norm of a maximal arithmetic J_w of Cayley's algebra C is congruent modulo 2 in J_w to an element, unique apart from sign, of norm 1 of J_w.

Let ξ be any given element of odd norm of J_w. Then, from the definition of J_w, it follows, since ξ has odd norm that

$$\xi = \alpha_o + \delta_1 \xi_{(w)}$$

where α_o is an element of J_o, $\xi_{(w)}$ equals ξ_u, ξ_{u^*}, $\xi_{w,v}$ or $\xi_{w,v}^*$ and u is a basic unit assigned to an associative triad containing w and v is a basic unit assigned to a triad not containing w.

Suppose that $\delta_1 = 0$. Then $\xi = \alpha_o$ and

$$\alpha_o \equiv \sum_{s=0}^{7} a_s i_s \quad (\text{mod } 2)$$

where each a_s is 0 or 1. Since $N\alpha_o$ is odd, the number of coefficients r, say, for which $a_s = 1$ $(0 < s < 7)$ must be odd.

If $r = 1$ the result follows.

If $r = 3$ we have

$$\alpha_0 = i_{s_1} + i_{s_2} + i_{s_3} \pmod 2.$$

It is easy to prove that there exists a basic unit i_t of C for which $(i_t, i_{s_1}, i_{s_2}, i_{s_3})$ is a basic defining set of Cayley units for J_w. (§3). But for any such set (u_1, u_2, u_3, u_4)

$$\sum_{l=1}^{4} u_l \equiv 0 \pmod 2$$

Thus in this case

$$\alpha_0 \equiv i_t \pmod 2$$

If $r = 5$ we have, since

$$\sum_{l=0}^{7} i_l \equiv 0 \pmod 2,$$

α_0 congruent modulo 2 in J_w to the sum of three different basic units of C. The case $r = 5$ has thus been reduced to the case $r = 3$.

Similarly the result follows if $r = 7$.

If $\delta_1 = 1$, we have

$$\xi = \alpha_0 + \xi_{(w)}.$$

From above we see that if $N\alpha_0$ is odd α_0 is congruent modulo 2 in J_w to a basic unit i_t, say, of J_0. Now write

$$\xi_{(w)} = \frac{1}{2} \sum_{l=1}^{8} w_l$$

where w_s $(1 \leq s \leq 8)$ are the eight basic units of J_0.

Then we have $i_t = w_{\ell_1}$ for some ℓ_1 $(1 \leq \ell_1 \leq 4)$ for if not ξ is congruent modulo 2 in J_w to an element of even norm of J_w which cannot be true. Thus

$$\xi \equiv \tfrac{1}{2}(-w_{\ell_1} + w_{\ell_2} + w_{\ell_3} + w_{\ell_4}) \pmod 2$$

and the result follows.

Now suppose that $N\alpha_0$ is even. Then

$$\alpha_0 \equiv \sum_{s=0}^{7} a_s i_s \pmod 2$$

where each $a_s = 0$ or 1. Since $N\alpha_0$ is even the number r of coefficients $a_s = 1$ must be even.

If $r = 0$ or 8 the result follows at once.

If $r = 2$ or 6 we have

$$\xi \equiv i_{s_1} + i_{s_2} + \xi_{(w)} \pmod 2$$

where as before

$$\xi_{(w)} = \tfrac{1}{2}\sum_{\ell=1}^{4} w_\ell$$

and w_1, w_2, w_3, w_4 form a set D, say, of four basic units of C. Precisely one of i_{s_1} and i_{s_2} cannot occur in D, for ξ must be congruent modulo 2 in J_w to an element of odd norm. If neither i_{s_1} nor i_{s_2} occurs in D the result follows as before. We now suppose that both i_{s_1} and i_{s_2} occur in the set D. In this case it is easy to prove that there exist two elements w_{s_1}, w_{s_2} of D for which $(i_{s_1}, i_{s_2}, w_{s_1}, w_{s_2})$ is a basic defining set of units for J_w. We assume this result.

We deduce that

$$i_{s_1} + i_{s_2} \equiv w_{s_1} + w_{s_2} \pmod 2$$

Hence

$$\xi \equiv \tfrac{1}{2}(-w_{s_1} - w_{s_2} + w_{s_3} + w_{s_4}) \pmod 2$$

Finally we suppose that $r = 4$. Then

$$\xi \equiv i_{s_1} + i_{s_2} + i_{s_3} + i_{s_4} + \tfrac{1}{2}(w_1 + w_2 + w_3 + w_4) \pmod 2$$

Clearly the sets $(i_{s_1}, i_{s_2}, i_{s_3}, i_{s_4})$ and (w_1, w_2, w_3, w_4) must have an even number of elements in common for otherwise ξ is congruent modulo 2 in J_w to an element of even norm. If the sets have no elements in common or four elements in common the result is immediate. If they have precisely two elements in common the argument reduces to the previous case.

Thus for any element contained in J_w

$$\xi \equiv \rho \quad (\text{modulo } 2 \text{ in } J_w)$$

where ρ is an element of norm 1 of J_w. If also

$$\xi \equiv \rho' \quad (\text{modulo } 2 \text{ in } J_w)$$

where $N\rho' = 1$ it follows that $\rho = \pm\rho'$.
Theorem 4.4 has thus been proved.

As an example we consider the element

$$\xi = 1 + i_1 + \tfrac{1}{2}(i_4 + i_5 + i_6 + i_7)$$

Since $\chi(\xi) = 1$ and

$$\xi = 1 + i_1 + \tfrac{1}{2}\{(1 + i_1 + i_2 + i_3)i_4\}$$
$$= \alpha_0 + \xi_{(w)}$$

where $\alpha_0 = 1 + i_1$ and $\xi_{(w)} = \xi i_4^*$, we can take $w = i_1$, i_2 or i_3.

In J_{i_3} we have

$$\beta = 1 + i_1 + i_4 + i_6 \equiv 0 \pmod 2$$

since $\chi(\tfrac{1}{2}\beta) = i_3$. Thus in J_{i_3}

$$\xi \equiv -i_4 - i_6 + \tfrac{1}{2}(i_4 + i_5 + i_6 + i_7) \pmod 2$$
$$\equiv \tfrac{1}{2}(-i_4 + i_5 - i_6 + i_7) \pmod 2$$

while in J_{i_1} we have

$$\xi \equiv \tfrac{1}{2}(+i_4 + i_5 - i_6 - i_7) \pmod 2$$

Next we deduce from Theorem 4.4

Theorem 4.5. Any element η of even norm of a maximal arithmetic J_w of Cayley's algebra C is congruent modulo 2 in J_w to the sum of two elements of J_w of norm 1 or to 0.

This follows since any such element η can be written as $\eta_1 + \eta_2$ where η_1 and η_2 are linear combinations of disjoint defining sets of units for J_w and are such that $N\eta_1$ and $N\eta_2$ are odd.

Theorems 4.4 and 4.5 are used to characterize and count the numbers of distinct factors in maximal arithmetic J_w of a given element ζ of J_w. However, we must first relate the number of representations of odd rational integer mn as $\sum_{s=0}^{7} z_s^2$ where $\sum_{s=0}^{7} z_s i_s$ is an element of J_w to the number of representations of rational integers m and n of this form.

We define $r_h(m)$ to be the number of different representations of m as $\sum_{s=0}^{7} x_s^2$ where $\sum_{s=0}^{7} x_s i_s$ is contained in fixed arithmetic J_h of C for $h = 0, 1, \ldots 7, i_1, i_2, \ldots i_7$. Further we write $r_0(m) = r(m)$. Clearly, $r_s(m) = r_t(m)$ and $r_{i_s}(m) = r_{i_t}(m)$ for s, t such that $1 \leq s,t \leq 7$. For example, $r(1) = 16$, $r_s(1) = 48$ and $r_{i_s}(1) = 240$ for $1 \leq s \leq 7$.

We state without proof some results on the number of distinct representations of a rational integer as the norm of an element of any fixed arithmetic of C containing the eight basic units of C.

Theorem 4.6.

(i) For m an odd rational integer

$$r_h(m)\, r(1) = r(m)\, r_h(1).$$

(ii) For m, n odd rational integers such that $(m,n) = 1$

$$r_h(m)\, r_h(n) = r_h(mn)\, r_h(1).$$

Theorem 4.6.

(iii) For p a rational prime and integer $t > 0$

$$r_h(p) = r_h(1).(1 + p^3)$$

and

$$r_h(1)\, r_h(p^{t+1}) = r_h(p)\, r_h(p^t) - r_h(1).p^3.r_h(p^{t-1}).$$

(iv) For integer $t > 0$

$$r(2^t) = 16\left\{\sum_{r=1}^{t} 2^{3r} - 1\right\}$$

where in each case h may take any one of the values $0, 1, 2, \ldots 7, i_1, i_2, \ldots i_7$.

The results for r(m) are given in Rankin's paper [45]. Then it follows that, for m odd,

$$r(4m) = \tfrac{1}{16} r(4)\, r(m) = 7 \cdot 1 r(m).$$

Hence the number of representations of 4m as a sum of eight squares of integers, four of which are odd, is $7 \cdot 0 r(m)$. Thus, from Theorem 4.6 (i), it follows that

$$r_{i_s}(m) = 15\, r(m)$$

and

$$r_s(m) = 3\, r(m) \quad \text{for } 1 \leq s \leq 7.$$

An independent proof of Theorem 4.6 can be given by means of the methods indicated by Rankin (l.c.).

We now prove

Theorem 4.7. Any element ζ of maximal arithmetic J_w of C for which $N\zeta = mn$ where m, n are positive rational integers such that $(m,n) = 1$ has precisely 240 different factorizations $\xi\eta$ in J_w for which $N\xi = m$ and $N\eta = n$.

If $N\xi_1 = m = N\xi_2$ and $\xi_1 \neq \pm\xi_2$ then the absolute value of $R(\overline{\xi}_1, \xi_2)$ is less than m. For if

$$\xi_t = \sum_{s=0}^{7} x_{ts} i_s \qquad (t = 1, 2)$$

we have

$$\begin{aligned} N(\xi_1 \pm \xi_2) &= \sum_{s=0}^{7} (x_{1s} \pm x_{2s})^2 \\ &< 2 \sum_{s=0}^{7} (x_{1s}^2 + x_{2s}^2) \\ &= 4m. \end{aligned}$$

Further, suppose that ζ is divisible on the left by ξ_1 and ξ_2 in J_w where $N\xi_1 = N\xi_2 = m$. Write

$$\zeta = \xi_1\eta_1 \quad \text{and} \quad \zeta = \xi_2\eta_2.$$

Then

$$\zeta\overline{\eta}_2 = (\xi_2\eta_2)\overline{\eta}_2 = \xi_2 n.$$

Similarly,

$$\eta_1\overline{\zeta} = n\overline{\xi}_1.$$

Thus

$$n^2 \overline{\xi}_1 \xi_2 = (\eta_1\overline{\zeta})(\zeta\overline{\eta}_2).$$

Hence, by (1.11),

$$n^2 R(\overline{\xi}_1, \xi_2) = N\zeta \cdot R(\eta_1, \overline{\eta}_2).$$

But $(m,n) = 1$. Therefore,

$$R(\overline{\xi}_1, \xi_2) = 0 \text{ or } \pm\tfrac{1}{2}m.$$

Suppose further that

$$\xi_1 \equiv \xi_2 \pmod{2 \text{ in } J_w}.$$

Then

(4.8) $$\overline{\xi}_1 \xi_2 \equiv 1 \pmod{2 \text{ in } J_w}$$

Thus, by Theorem 4.3, $\overline{\xi}_1\xi_2$ is contained in J_0. Hence

(4.9) $$R(\overline{\xi}_1 \xi_2) = 0.$$

Now $N(\overline{\xi}_1 \xi_2) = m^2$ and m is odd. Therefore, $\overline{\xi}_1\xi_2$ has one or five odd rational integral coordinates. It is easy to show that any set of five basic units of C contains a basic defining set of units for J_w. Thus the sum of any five such basic units is congruent modulo 2 in J_w to one of the five units. Hence

(4.10) $$\overline{\xi}_1 \xi_2 \equiv i_t \pmod{2}$$
for some t $(1 \leq t \leq 7)$.

But (4.8) and (4.10) cannot both hold. Hence

(4.11) $$\xi_1 \not\equiv \xi_2 \pmod{2}$$

From (4.11), Theorem 4.4 and the fact that

$$r_w(1) = 240$$

it follows that any ζ of odd norm mn where $(m,n) = 1$ has at most 240 factorizations $\xi\eta$ in J_w such that $N\xi = m$, $N\eta = n$.

Now suppose there exists a ζ in J_w of norm mn with less than 240 such factorizations. For all such ζ for which $N\zeta = mn$ the number of factorizations of this form is given by $r_w(m)\, r_w(n)$.

We deduce that

$$r_w(m)\, r_w(n) < 240 \sum_{N\zeta = mn} 1$$
$$= 240\, r_w(mn)$$

But this contradicts Theorem 4.6 (ii) with h = w. This completes the proof of Theorem 4.7.

Next we prove

Theorem 4.8. Any element ζ of maximal arithmetic J_w of C for which $N\zeta = p^{l+1}$ where p is an odd rational prime and $l > 0$ has precisely

(i) $240(1 + p^3)$ distinct factorizations $\xi\eta$ in J_w for which $N\xi = p$ and $N\eta = p^l$ if p divides ζ in J_w

or (ii) 240 such factorizations if p does not divide ζ in J_w.

(i) Suppose that p divides ζ in J_w. Then $\zeta = p\zeta'$ where ζ' is contained in J_w. Let ξ be any element of J_w of norm p and suppose that $\eta = \bar{\xi}\zeta'$. Then η is contained in J_w. Also $\xi\eta = \xi(\bar{\xi}\zeta') = p\zeta' = \zeta$. Thus ζ has as many distinct factorizations $\xi\eta$ such that $N\xi = p$ and $N\eta = p^l$ as there are distinct elements of norm p in J_w. The result follows from (iii) of Theorem 4.6.

(ii) Suppose now that p does not divide ζ in J_w. Let ζ have distinct factorizations $\xi_1\eta_1$ and $\xi_2\eta_2$ in J_w for which $N\xi_1 = N\xi_2 = p$ and $N\eta_1 = N\eta_2 = p^l$.

Suppose that

$$\xi_1 \equiv \xi_2 \pmod{2 \text{ in } J_w}$$

Then

$$\xi_1 \bar{\xi}_2 \equiv 1 \pmod{2 \text{ in } J_w}$$

Thus by Theorem 4.3 $\xi_1 \bar{\xi}_2$ is an element of J_o.

Now by (1.4) and (1.7) we have

(1.10) $R\{\xi_1(\bar{\xi}_2\zeta) + (\bar{\zeta}\xi_1)\bar{\xi}_2\} = R(\zeta)\, 2R(\xi_1\bar{\xi}_2)$.

But by (1.9) $\xi_1(\bar{\xi}_2\zeta) = p\,\xi_1\eta_2$ and $(\bar{\zeta}\xi_1)\bar{\xi}_2 = p\,\bar{\eta}_1\bar{\xi}_2$. Therefore p divides $2R(\zeta)\, R(\xi_1\bar{\xi}_2)$. Since odd prime p does not divide ζ in J_w it does not divide $2R(\zeta)$. Therefore, p divides $R(\xi_1\bar{\xi}_2)$. But $R(\xi_1\bar{\xi}_2)$ is an integer and $N(\xi_1\bar{\xi}_2) = p^2$. Now $\xi_1 \neq \pm\xi_2$. Therefore $\xi_1\bar{\xi}_2 \neq p$. Hence $R(\xi_1\bar{\xi}_2) = 0$ and $\xi_1\bar{\xi}_2$ has one or five odd rational integral coefficients. Thus, as in the proof of Theorem 4.7, $\xi_1\bar{\xi}_2$ is congruent modulo 2 in J_w to a basic unit of J_o other than ± 1. Therefore each element ξ of norm p which divides ζ on the left in J_w is congruent modulo 2 to a distinct element of norm 1 of J_w. Hence there exist at most 240 distinct factorizations $\xi\eta$ in this case. For all ζ of norm p^{l+1} in J_w the number of factorizations of this form is given by $r_w(p)\, r_w(p^l)$. Suppose that there exists a ζ in J of norm p^{l+1} which is not divisible by p in J_w with less than 240 factorizations of the type described.

Then

$$r_{11}(p)\, r_w(p^l) < 240 \sum_{\substack{N\zeta = p^{l+1} \\ p \nmid \zeta}} 1 + 240(1 + p^3) \sum_{\substack{N\zeta = p^{l+1} \\ p \mid \zeta}} 1$$

$$= 240 \{ r_{11}(p^{l+1}) - r_w(p^{l-1}) \} + 240(1 + p^3)\, r_w(p^{l-1})$$

$$= 240\, r_w(p^{l+1}) + 240\, p^3 r_w(p^{l-1})$$

$$= r_w(p)\, r_w(p^l).$$

Hence no such ζ exists. The result has thus been proved by contradiction. This completes the proof of Theorem 4.8.

Let ζ be any element of an arithmetic J_h for some h $(h = 0, 1, \ldots 7, i_1, i_2, \ldots i_7)$ of C. Suppose that $N\zeta = m \neq 0$. For use in later sections, we adopt a notation similar to that of Rankin [45] and define

$$G_h(\zeta ; m, n) = G_h(\zeta)$$

to be the set of all factorizations $\xi\eta$ of ζ in J_h for which $N\xi = m$ and $N\eta = n$. Also we define

$$S_h(\zeta ; m, n) = S_h(\zeta)$$

to be the number of such factorizations.

Thus we have proved for w a basic unit of C other than 1

<u>Theorem 4.7.</u> <u>For m, n odd positive rational integers such that</u> $(m, n) = 1$,

$$S_w(\zeta ; m, n) = 240$$

Also we have proved

Theorem 4.8. For p an odd rational prime and $\ell > 0$

(i) if p divides ζ in J_w

$$S_w(\zeta ; p, p^\ell) = 240(1 + p^3)$$

or (ii) if p does not divide ζ in J_w

$$S_w(\zeta ; p, p^\ell) = 240$$

From Theorems 4.7 and 4.8 we deduce the following results.

Theorem 4.9. For m, n odd positive rational integers such that $(m,n) = 1$

$$S_o(\zeta ; m, n) = 16.$$

Theorem 4.10. For p an odd rational prime and $\ell > 0$

(i) if p divides ζ in J_o

$$S_o(\zeta ; p, p^\ell) = 16(1 + p^3)$$

or (ii) if p does not divide ζ in J_o

$$S_o(\zeta ; p, p^\ell) = 16.$$

Theorem 4.11. For m, n odd positive rational integers such that $(m,n) = 1$ and any t $(1 \leq t \leq 7)$

$$S_t(\zeta ; m, n) = 48.$$

Theorem 4.12. For p an odd rational prime, $\ell > 0$ and any t $(1 \leq t \leq 7)$

(i) if p divides ζ in J_t

$$S_t(\zeta ; p, p^\ell) = 48(1 + p^3)$$

or (ii) if p does not divide ζ in J_t

$$S_t(\zeta ; p, p^\ell) = 48.$$

The methods used to establish Theorems 4.7 and 4.8 above were first used by Rankin [45] to establish Theorems 4.9 and 4.10 above. We have used the idea of congruence modulo 2 in J_w while Rankin used the fact that the eight basic units of C are linearly independent and generate J_o over the rational integers.

We have already seen that J_o occurs as a subset of J_w for any basic unit w of C other than 1 and that J_t $(1 \leq t \leq 7)$ occurs as a subset of J_w for three basic units w of C for which $w \neq 1$. Further the elements of J_w which belong to J_s $(0 \leq s \leq 7)$ are characterized as the elements of J_w congruent modulo 2 in J_w to an element of J_s of norm 1. Thus Theorems 4.9 and 4.11 follow from Theorems 4.6 and 4.7, while from Theorems 4.6 and 4.8 we deduce Theorems 4.10 and 4.12.

5. Ideals.

This section is on ideals in Cayley's algebra C. Mahler in his paper [33] on the same subject used his results on the approximation of quaternions [34] to show that the algebra C admits a Euclidean algorithm. Results are restricted to the maximal arithmetics of C. Mahler deduced that all (left or right) ideals are principal and that the basis of an odd ideal is a rational integer. Firstly, we review Mahler's work in terms of any maximal arithmetic of C. Then we extend the results to show that the basis of any ideal is a rational integer.

Mahler [33] defines any element δ of C to be integral if it can be written as

$$\delta = \sum_{s=1}^{8} d_s \delta_s'$$

for rational integers $d_1, d_2, \ldots d_8$ and $\delta_1', \delta_2', \ldots \delta_8'$ the eight elements of C

$$\delta_1' = i_1, \quad \delta_2' = i_2, \quad \delta_3' = i_3, \quad \delta_4' = \tfrac{1}{2}(1 + i_1 + i_2 + i_3),$$
$$\delta_5' = i_4, \quad \delta_6' = \tfrac{1}{2}(1 + i_1 + i_4 + i_6)$$
$$\delta_7' = \tfrac{1}{2}(1 + i_2 + i_4 + i_5), \quad \delta_8' = \tfrac{1}{2}(1 + i_3 + i_4 + i_7).$$

Mahler noted that the linearly independent set $\delta_1', \delta_2' \ldots \delta_8'$ generates one of the three maximal arithmetics found by Dickson [13] . Clearly, δ_4' and δ_8' are quasiquaternions in distinct proper associative triads having unit i_3 in common.

Also, we see that

$$\chi\delta'_6 = \chi\delta'_7 = i_3.$$

Thus, from the definition of a maximal arithmetic of C, it follows that $\delta'_1, \delta'_2, \ldots \delta'_8$ generate J_{i_3} over the rational integers.

Now let J_w be any maximal arithmetic of C where w is a basic unit of C other than 1. Let $\delta_1, \delta_2, \ldots \delta_8$ be the images of $\delta'_1, \delta'_2 \ldots \delta'_8$ respectively under the automorphism θ of C for which $\theta J_{i_3} = J_w$. Then since $\delta_1, \delta_2, \ldots \delta_8$ are linearly independent over the real field any element ξ of C is expressible in the form

$$\xi = \sum_{s=1}^{8} x_s \delta_s$$

where $x_1, x_2, \ldots x_8$ are real numbers.

From Kohler's result for J_{i_3}, we have at once

Theorem 5.1 For any element ξ of C and any maximal arithmetic of C, there exists an element δ of J_w for which

$$N(\xi - \delta) \leq \frac{15}{16}.$$

We now define left and right ideals for any maximal arithmetic J_w of C. A set $\mathfrak{m}$ of elements of J_w is called a left (or right) ideal for J_w if

(i) whenever α_1, α_2 are contained in $\mathfrak{m}$, $\alpha_1 \pm \alpha_2$ is contained in $\mathfrak{m}$ and

(ii) whenever α is contained in $\mathfrak{m}$ and δ is any element of J_w, $\delta\alpha$ (or $\alpha\delta$) is contained in $\mathfrak{m}$.

A ~~right~~ left (or ~~left~~ right) ideal $\mathfrak{w}$ for $J_\mathfrak{w}$ is called a principal left (or right) ideal for $J_\mathfrak{w}$ if there exists an element α^* of $\mathfrak{w}$ for which every element of $\mathfrak{w}$ is expressible in the form $\delta\alpha^*$ (or $\alpha^*\delta$) for some δ contained in $J_\mathfrak{w}$. We say that left (or right) ideal $\mathfrak{w}$ for $J_\mathfrak{w}$ is generated by element α^* of $J_\mathfrak{w}$.

Next we have

Theorem 5.2. Every left (or right) ideal for any maximal arithmetic $J_\mathfrak{w}$ of C is a principal left (or right) ideal.

Let $\mathfrak{w}$ be any left ideal for maximal arithmetic $J_\mathfrak{w}$ of C. Suppose that $\mathfrak{w}$ contains at least one element other than 0. Then there must exist an element α^*, say, of smallest positive norm in $\mathfrak{w}$. Let α be any element of $\mathfrak{w}$. Then, by Theorem 5.1, there exists an element δ of $J_\mathfrak{w}$ for which

$$N(\alpha\alpha^{*-1} - \delta) < \tfrac{15}{16}.$$

But $\alpha - \delta\alpha^*$ is an element of $\mathfrak{w}$ and

$$\begin{aligned} N(\alpha - \delta\alpha^*) &= N\{(\alpha\alpha^{*-1} - \delta)\alpha^*\} \\ &= N(\alpha\alpha^{*-1} - \delta)\cdot N\alpha^* \\ &< \tfrac{15}{16} N\alpha^*. \end{aligned}$$

Now α^* has smallest positive norm in $\mathfrak{w}$. Thus $\alpha - \delta\alpha^*$ must equal 0. The result has thus been established for left ideals for any maximal arithmetic $J_\mathfrak{w}$ of C. A similar proof holds for right ideals for $J_\mathfrak{w}$.

We see at once from the definition of an ideal for J_w that

Lemma 5.1. Any rational integral multiple of an element of norm 1 of J_w generates an ideal in J_w.

As in Theorem 5.2, results proved below for left ideals can be proved similarly for right ideals.

Suppose that $\mathfrak{a}$ is any left ideal for J_w. Then by Theorem 5.2 we may suppose that $\mathfrak{a}$ is generated by element α^* of J. Then for any elements δ_1, δ_2 of J_w, $\delta_1(\delta_2\alpha^*)$ is contained in $\mathfrak{a}$. Thus there exists an element δ_3 of J_w such that

$$\delta_1(\delta_2\alpha^*) = \delta_3\alpha^*. \tag{5.1}$$

By Theorem 2.1 we may write

$$\alpha^* = \alpha_0 + \alpha_1 u$$

where α_0, α_1 are quasiquaternions in proper associative triad (u_1, u_2, u_3) of units of C for which $|u_s| \neq |u|$ $(s = 1, 2, 3)$ and u is a unit of C other than ± 1.

Suppose now that

$$u_1u_2 = u_3 = -u_2u_1.$$

Then take $\delta_1 = u_1$, $\delta_2 = u_2$. We have

$$\begin{aligned} u_1(u_2\alpha^*) &= u_1\{u_2(\alpha_0 + \alpha_1 u)\} \\ &= u_1u_2\alpha_0 + (\alpha_1 u_2u_1)u \\ &= u_3\alpha_0 - (\alpha_1 u_3)u. \end{aligned} \tag{5.2}$$

Hence there exists an element ρ of J_w such that

(5.3) $$u_1(u_2\alpha^*) = \rho\alpha^*.$$

Clearly, ρ must be one of the 240 elements of J_w of norm 1. We have from (5.2) and (5.3)

(5.4) $$\begin{aligned}\rho &= \{u_3\alpha_0 - (\alpha_1 u_3)u\}\frac{\overline{\alpha^*}}{N\alpha^*} \\ &= \frac{1}{N\alpha^*}\{u_3\alpha_0 - (\alpha_1 u_3)u\}\{\overline{\alpha_0} - \alpha_1 u\} \\ &= \frac{1}{N\alpha^*}\{u_3(N\alpha_0 - N\alpha_1) - 2(\alpha_1 u_3\alpha_0)u\}\end{aligned}$$

Now we suppose that u is one of u_1, u_2, u_3. Then $\frac{1}{2}(\pm 1 \pm u_1 \pm u_2 \pm u_3)u$ is an element of J_w. Hence

$$\frac{N\alpha_0 - N\alpha_1}{N\alpha^*} \quad \text{or} \quad \frac{N\alpha_0 - N\alpha_1}{N\alpha_0 + N\alpha_1} = 0 \quad \text{or} \quad \pm 1.$$

Thus we have proved that one of the following relations holds.

(5.5) $$N\alpha_0 = N\alpha_1$$

(5.6) $$N\alpha_0 = 0$$

(5.7) $$N\alpha_1 = 0$$

for each expression $\alpha^* = \alpha_0 + \alpha_1 u$ for α^* in terms of quasiquaternions in an associative triad involving $\pm u$.

We are now in a position to prove the following lemma.

Lemma 5.2. If α^* generates a left ideal for J_w then there exists a proper associative triad (u_1, u_2, u_3) of basic units of C containing w and with assigned unit u, say, for which

$$\alpha^* = \alpha_0 + \alpha_1 u$$

where α_0, α_1 are quasiquaternions of equal norm in (u_1, u_2, u_3) provided that α^* is not of one of the following three forms

(i) 0

(ii) $a_r i_r$

(iii) $a_r i_r + a_s i_s$ where $|i_r i_s| = w$, $i_r \neq i_s$ and a_r, a_s are non zero rational integers $(0 \leq r, s \leq 7)$.

This lemma follows at once from the above discussion when we note that there are three possible choices of proper associative triad (u_1, u_2, u_3) of basic units of C containing w. If (5.6) or (5.7) holds for all three choices of triad containing w then we must have α^* of the form (i), (ii) or (iii).

We now consider α^* such that, for at least one fixed triad (u_1, u_2, u_3) containing w, $N\alpha_0 = N\alpha_1$. Then we have from (5.4)

$$\rho = -\frac{2}{N\alpha^*}(\alpha_1 u_3 \bar{\alpha}_0)u.$$

But $N\alpha^* = 2N\alpha_0 = 2\alpha_0\bar{\alpha}_0$. Thus

$$\rho = -(\alpha_1 u_3 \bar{\alpha}_0^{-1})u$$
$$= \tau_3 u, \text{ say,}$$

where τ_3 is a quasiquaternion of norm 1 in (u_1, u_2, u_3).

We have

(5.8) $$\alpha_1 = \tau_3 \bar{\alpha}_0 u_3.$$

We repeat this argument for cyclic permutations of the triad (u_1, u_2, u_3) and define

$$\alpha_l = \tau_j \bar{\alpha}_0 u_l \qquad \text{for} \qquad l = 1, 2, 3.$$

Also since β belongs to J_w, τ_l is for each l $(l=1,2,3)$ an element of norm 1 of J_w. Thus

(5.9) $$\tau_1 \bar{\alpha}_0 u_1 = \tau_2 \bar{\alpha}_0 u_2 = \tau_3 \bar{\alpha}_0 u_3.$$

Hence

(5.10) $$\bar{\alpha}_0 u_3 = \bar{\alpha}_0 u_1 u_2 = - \bar{\tau}_1 \tau_2 \bar{\alpha}_0$$

Therefore, by (5.8),

(5.11) $$\alpha_1 = - \tau_3 \bar{\tau}_1 \tau_2 \bar{\alpha}_0 = \tau \alpha_0, \text{ say,}$$
where $\tau = - \tau_3 \bar{\tau}_1 \tau_2$

Clearly τ is a quasiquaternion of norm 1 in (u_1, u_2, u_3). Also

(5.12) $$\tau = - \tau_3 \bar{\tau}_1 \tau_2 = - \tau_1 \bar{\tau}_2 \tau_3 = - \tau_2 \bar{\tau}_3 \tau_1.$$

Further from (5.9) and (5.10) we have

(5.13) $$\bar{\alpha}_0 u_l \bar{\alpha}_0^{-1} = w_l \quad \text{where} \quad w_l = - \bar{\tau}_{l_1} \tau_{l_2} \text{ and}$$
(l_1, l_2, l_3) is any cyclic permutation of $(1, 2, 3)$.

But w_1, w_2, w_3 are quasiquaternions of norm 1 in (u_1, u_2, u_3). Also

$$w_1^2 = w_2^2 = w_3^2 = (\bar{\alpha}_0 u_3 \bar{\alpha}_0^{-1})^2 = -1.$$

Further,

$$w_1 w_2 w_3 = -\bar{\tau}_2\tau_3 \cdot \bar{\tau}_3\tau_1 \cdot \bar{\tau}_1\tau_2 = -1.$$

But for $\ell = 1, 2, 3$ τ_ℓ belongs to J_w. Thus, by (5.13), w_1, w_2, w_3 are elements of J_w. It follows from (1.5) that w_1, w_2, w_3 are themselves units of C other than ± 1. Since $w_1 w_2 w_3 = -1$, $|w_1|, |w_2|, |w_3|$ must be distinct basic units of C. (w_1, w_2, w_3) is itself a permutation of (u_1, u_2, u_3) with suitable sign changes. Thus from (5.13) we have

$$\bar{\alpha}_0 u_\ell \alpha_0 = \pm N\alpha_0 \cdot u_s \tag{5.14}$$

where, as ℓ takes the values 1, 2, 3 in turn, s runs through a permutation of the same values. Also the signs are such that

$$\bar{\alpha}_0 u_1 \alpha_0 \cdot \bar{\alpha}_0 u_2 \alpha_0 \cdot \bar{\alpha}_0 u_3 \alpha_0 = -(N\alpha_0)^3 .$$

Now let

$$\alpha_0 = a_0 + a_1 u_1 + a_2 u_2 + a_3 u_3$$

where a_0, a_1, a_2, a_3 are rational numbers. Expanding the left side of (5.14) for $\ell = 1, 2, 3$ we have

$$\begin{aligned}
\bar{\alpha}_0 u_1 \alpha_0 &= (a_0^2 + a_1^2 - a_2^2 - a_3^2)u_1 + 2(a_1 a_2 - a_0 a_3)u_2 + 2(a_1 a_3 + a_0 a_2)u_3 \\
\bar{\alpha}_0 u_2 \alpha_0 &= 2(a_1 a_2 + a_0 a_3)u_1 + (a_0^2 - a_1^2 + a_2^2 - a_3^2)u_2 + 2(a_2 a_3 - a_0 a_1)u_3 \\
\bar{\alpha}_0 u_3 \alpha_0 &= 2(a_1 a_3 - a_0 a_2)u_1 + 2(a_2 a_3 + a_0 a_1)u_2 + (a_0^2 - a_1^2 - a_2^2 + a_3^2)u_3 .
\end{aligned}$$

In each case we see from the right side of (5.14) that two coefficients in each expansion are zero and that $\pm N\alpha_0$ equals the remaining non zero coefficient. There are six possible cases to discuss and it is easy to show that α_0 is of the form $\sqrt{N\alpha_0}\,\rho$ or of the form $\sqrt{N\alpha_0}\,\rho(1 + u_3)$ where ρ is a quasiquaternion in (u_1, u_2, u_3) of norm 1 and $1 \leq \alpha \leq 3$. Hence, by (5.11) and since α'^{α} must itself be an element of J_w, it follows that α'^{α} is of the form $n\rho^{\alpha}$ where n is a rational integer and ρ^{α} is an element of J_w of norm 1, an element of J_w of norm 2 or the sum of four units of C for which $\frac{1}{2}\rho^{\alpha}$ is not contained in J_w.

Thus we have proved

Lemma 5.3. *Any element α'^{α} of J_w for which*

$$\alpha'^{\alpha} = \alpha_0 + \alpha_1 u$$

where α_0, α_1 are quasiquaternions of equal norm in a proper associative triad (u_1, u_2, u_3) of basic units with assigned unit u_3 cannot generate a left or right ideal for J_w unless it is of the form $n\beta^{\alpha}$ for n a rational integer and β^{α}

(i) *an element of J_w of norm 1,*

(ii) *an element of J_w of norm 2 of the form $\beta_1 + \beta_2 u$ where β_1, β_2 are quasiquaternions of norm 1 in (u_1, u_2, u_3)*

or (iii) *an element 2ρ where ρ is an element of norm 1 which belongs to some maximal arithmetic J_w of C but not to J_w.*

Mahler proved this lemma in J_k. He then proceeded to discuss cases (5.6) and (5.7) separately. He was then able to deduce his result on odd ideals. By lemma 5.2, we need not discuss all possibilities for α^* satisfying (5.6) or (5.7). It is easy to show that

Lemma 5.4. *An element α^* of J_w generates an ideal in J_w if and only if for every rational integer m $m\alpha^*$ generates an ideal for J_w.*

We therefore proceed by showing that the particular cases stated in Lemma 2(iii) and Lemma 3(ii), (iii) above give rise to elements α^* no rational integral multiple of which can generate an ideal for J_w.

First, however, we note that

$$1 + u + w + uw,$$

for (u, w, uw) a proper associative triad of basic units of C, has 24 factorizations into factors of norm 2 in the maximal quasiquaternion arithmetic in (u, w, uw). They are

(5.15)

$(1+u)(1+w)$,	$(u-w)(w-uw)$,
$(1+w)(1+uw)$,	$(uw-u)(u-w)$,
$(1+uw)(1+u)$,	$(w-uw)(uw-u)$,
$(u+w)(1-u)$,	$(1-w)(u+w)$,
$(uw+u)(1-uw)$,	$(1-u)(u+uw)$,
$(w+uw)(1-w)$,	$(1-uw)(w+uw)$,

and the 12 further factorizations obtained by changing the signs of the factors.

We now prove

Lemma 5.5. No rational integral multiple of

$$i_s \pm i_t, \qquad 0 \le s,t \le 7, \qquad s \ne t,$$

can generate an ideal for J_w.

We give particular examples which contradict (5.1) above by choosing δ_1, δ_2 suitably. Let (u_1, u_2, u_3) be a proper associative triad with $u_3 = w$ and assigned unit u.

In (5.1) put

$$\delta_2 = \tfrac{1}{2}(1 + u_1 + u_2 + u_3) \qquad \text{and}$$

$$\delta_1 = \tfrac{1}{2}(1 + u_1 + u_1 u + u_3 u).$$

Then if $\alpha^* = 1 + w = 1 + u_3$ we have

$$\delta_3 = [\delta_1(\delta_2 \alpha^*)]\,\alpha^{*-1}$$

$$= \tfrac{1}{2}(1 + u_1 + u + u_3 u).$$

But here $\mathcal{U}(\delta_3) = |u_2|$. Thus δ_3 is not contained in J_w. Therefore $1+w$ cannot generate a left ideal for J_w. Similarly for $\alpha^* = 1 - w = 1 - u_3$ we have for the same choice of δ_1, δ_2

$$\delta_3 = \tfrac{1}{2}(u_1 + u_3 + u_1 u + u_3 u).$$

Here $\mathcal{U}(\delta_3) = |u_1|$ and again δ_3 does not belong to J_w. Hence $1 - w$ cannot generate a left ideal for J_w.

For the same elements δ_1, δ_2 of J_w and for α' equal to $1 + u_1$, $u_3 + u_1$, $u_1 + u_2$ and $(1 + u)u$ in turn, we have δ_3 equal to

$$\tfrac{1}{2}(u_1 + u_3 + u_1 u - u_2 u),$$

$$\tfrac{1}{2}(u + u_3 u + u_3 + u_1),$$

$$\tfrac{1}{2}(u_1 + u_3 - u_2 u + u_1 u) \quad \text{and}$$

$$\tfrac{1}{2}(u_1 + u_2 + u + u_1 u)$$

respectively. Here $\gamma(\delta_3) = |u_1|$, $|u_1|$, $|u_1|$ and $|u_2|$ in that order. Thus in each case δ_3 is not contained in J_w. Hence no such α' can generate a left ideal for J_w.

By using the automorphisms of O which preserve w we obtain the result for left ideals of J_w. A similar argument proves the result for right ideals.

The above lemma is used to prove

Lemma 5.6. *No element of J_w of the form*

$$a_r i_r + a_s i_s ,$$

where $|i_r i_s| = w$, $0 < r, s < 7$, $r \neq s$ and a_r, $a_s \neq 0$ are rational integers, can generate an ideal for J_w.

If a_r, a_s are both even we consider

$$\tfrac{1}{2}(a_r i_r + a_s i_s).$$

If a_r, a_s are both odd, we first consider $a_0 + a_3 w$. Let (u, v, uv) be a proper associative triad of units containing $w = uv$, say.

In (5.1) let

$$\delta = \tfrac{1}{2}(uv + u)(a_0 - a_3 uv)$$
$$= \tfrac{1}{2}(a_3 + a_0 u + a_3 v + a_0 uv).$$

Then δ is an element of J_w and

$$\delta (a_0 + a_3 w) = \tfrac{1}{2}(a_0^2 + a_3^2)(uv + u).$$

Now taking δ_1, δ_2 as in the proof of Lemma 5.5 and

$$\alpha^* = a_0 + a_3 w$$

we have

$$\delta_3 = \{ \delta_1 [\delta_2 (\delta \alpha^*)] \} \alpha^{*-1}$$
$$= \tfrac{1}{2}(a_0^2 + a_3^2) \{ \delta_1 [\delta_2 (uv + u)] \} \alpha^{*-1}$$

Now $\tfrac{1}{2}(a_0^2 + a_3^2)$ is an odd rational integer and from the proof of Lemma 5.5 $\{ \delta_1 [\delta_2 (uv + u)] \} \alpha^{*-1}$ is not contained in J_w. Hence δ_3 is not contained in J_w. The result follows for $a_0 + a_3 w$. Similarly, the result can be proved for i_r, i_s both different from 1.

If one of a_r, a_s is even and the other odd the result follows as above by writing

$$a_r i_r + a_s i_s = i_r + [(a_r - 1) i_r + a_s i_s]$$

for a_r even and applying the method described to $[(a_r - 1) i_r + a_s i_s]$. Lemma 5.6 has thus been established.

Again let β be a quasiquaternion of the form $\tfrac{1}{2}(1 \pm u_1 \pm u_2 \pm u_3)$ in triad (u_1, u_2, u_3) with assigned unit u and such that $u_3 = w$.

Now we prove

Lemma 5.7. No integral multiple of an element of J_w of the form

$$u_s \pm \gamma u \quad \text{or} \quad \gamma \pm u_s u \qquad (s = 0,1,2,3)$$

can generate an ideal of J_w.

Here any such element has five non zero coordinates. Suppose that the element generates an ideal for J_w. The element cannot be such that it satisfies (5.6) or (5.7) above for any of the three possible choices of proper associative triad. But the element cannot satisfy (5.5) in all three cases since four of its coordinates equal $\pm\frac{1}{2}$ and only one is ± 1. The result follows.

Next we prove

Lemma 5.8. No integral multiple of an element of J_w of the form

$$\pm\tfrac{1}{2}(1 \pm i_1 \pm i_2 \pm i_3 \pm i_4 \pm i_5 \pm i_6 \pm i_7)$$

generates an ideal for J_w.

Let α^* be any one of the elements given. Suppose that α^* generates a left ideal for J_w. Let

$$\alpha^* = \mathcal{E} + \mathcal{E}_1 u$$

where $\mathcal{E}$ and $\mathcal{E}_1$ are quasiquaternions of norm 1 in proper associative triad (u_1, u_2, u_3) with assigned unit u. Suppose that $u_3 = w$. Since $\mathcal{E} + \mathcal{E}_1 u$ generates a left ideal in J_w we have for any elements δ_1, δ_2 of J_w an element δ_3 of J_w such that

$$\delta_1[\delta_2(\mathcal{E} + \mathcal{E}_1 u)] = \delta_3(\mathcal{E} + \mathcal{E}_1 u).$$

Thus

$$\delta_3 = \{\delta_1[\delta_2(\varepsilon + \varepsilon_1 u)]\} \cdot \tfrac{1}{2}(\bar{\varepsilon} - \varepsilon_1 u).$$

Let (u_r, u_s, u_t) be a cyclic permutation of (u_1, u_2, u_3) and let $\delta_1 = u_r$, $\delta_2 = \varepsilon u$. Then

$$\delta_3 = \tfrac{1}{2}\{\bar{\varepsilon}_1 u_r - u_r \bar{\varepsilon}_1 + [u_r \varepsilon + \varepsilon_1 u_r \bar{\varepsilon}_1 \varepsilon] u\}$$
$$= \tfrac{1}{2}\{\bar{\varepsilon}_1 u_r - u_r \bar{\varepsilon}_1 + [(u_r + \varepsilon_1 u_r \bar{\varepsilon}_1)\varepsilon] u\}$$

Now $\bar{\varepsilon}_1 u_r$, $u_r \bar{\varepsilon}_1$, $u_r \varepsilon$ and $(\varepsilon_1 u_r \bar{\varepsilon}_1)\varepsilon$ are members of the set of 24 Hurwitz integral quaternions of norm 1 in u_1, u_2, u_3. The coefficients of 1 and u_r in δ_3 are zero while the coefficients of u_s and u_t are equal to $\pm\frac{1}{2}$.

Now let

$$\varepsilon = c_0 + c_1 u_r + c_2 u_s + c_3 u_t \qquad \text{and}$$

$$\varepsilon_1 = c_0' + c_1' u_r + c_2' u_s + c_3' u_t.$$

Then

$$\varepsilon_1 u_r \bar{\varepsilon}_1 = 2[(c_0' c_3' + c_1' c_2') u_s + (-c_0' c_2' + c_1' c_3') u_t].$$

Hence $\varepsilon_1 u_r \bar{\varepsilon}_1 = \pm u_s$ or $\pm u_t$. Now

$$(u_r + u_s)\varepsilon = \tfrac{1}{2}(u_r + u_s)(c_0 + c_1 u_r + c_2 u_s + c_3 u_t)$$
$$= \tfrac{1}{2}\{-c_1 - c_2 + (c_0 + c_3) u_r + (c_0 - c_3) u_s + (-c_1 + c_2) u_t\}$$

and

$$(u_r + u_t)\varepsilon = \tfrac{1}{2}(u_r + u_t)(c_0 + c_1 u_r + c_2 u_s + c_3 u_t)$$
$$= \tfrac{1}{2}\{-c_1 - c_3 + (c_0 - c_2) u_r + (-c_3 + c_1) u_s + (c_2 - c_0) u_t\}.$$

Similar expansions can be written down for $u_r - u_s$ and $u_r - u_t$ as left multipliers of ε.

It follows that the following sets are the only sets of units which can have non zero coordinates equal to $\pm\frac{1}{2}$ in the elements $\mathfrak{S}_3$.

$$
\begin{array}{l}
(u_s , u_t , \quad u, u_r u) \\
(u_3 , u_t , \quad u, u_s u) \\
(u_s , u_t , u_r u, u_t u) \\
(u_3 , u_t , u_s u, u_t u) \\
(u_s , u_t , \quad u, u_t u) \\
(u_s , u_t , u_s u, u_r u).
\end{array}
$$

The corresponding elements have characteristic units equal to $1, u_t, u_t, 1, u_s$ and u_s respectively. We therefore choose $u_t = u_3, u_1, u_1, u_3, u_3$ and u_3 in that order. Then in each case $\mathfrak{S}_3$ is not an element of $J_{W'}$ $(u_3 = w)$. Thus no member of the set

$$\tfrac{1}{2}(\pm 1 \pm i_1 \pm i_2 \pm i_3 \pm i_4 \pm i_5 \pm i_6 \pm i_7)$$

of elements of $J_{W'}$ generates an ideal in J_W.

We have now proved

<u>Theorem 5.3.</u> <u>No rational integral multiple of an element of J_W of norm 2 can generate an ideal for J_W.</u>

We must now discuss the cases given in (iii) of Lemma 5.3 above. We prove

<u>Lemma 5.9.</u> <u>No rational non zero integral multiple of an element α^* of J_W of the form</u>

$$\alpha^* = \pm w_1 \pm w_2 \pm w_3 \pm w_4$$

<u>where each w_s $(1 \leq s \leq 4)$ is a different basic unit of C and for which $\frac{1}{2}\alpha^*$ is not contained in J_W can generate an ideal for J_W.</u>

Suppose that $\chi(\frac{1}{2}\alpha^*) = 1$. $\frac{1}{2}\alpha^*$ is not contained in J_w. Therefore, either 1 or w occurs in the set (w_1, w_2, w_3, w_4). Thus we may write α^* as ε, $\bar{\varepsilon}$, εw or $\bar{\varepsilon} w$ where ε is a quasiquaternion of the form $\pm(1 + v_1 + v_2 + v_3)$ in proper associative triad (v_1, v_2, v_3) with fourth unit w.

First let us suppose that ε generates an ideal for J_w. Then for any elements δ_1, δ_2 of J_w there exists, as we have seen above, an element δ_3 of J_w such that

$$\delta_1(\delta_2\varepsilon) = \delta_3\varepsilon .$$

Thus

$$\begin{aligned}\delta_3 &= [\delta_1(\delta_2\varepsilon)]\varepsilon^{-1} \\ &= \tfrac{1}{4}[\delta_1(\delta_2\varepsilon)]\bar{\varepsilon}\end{aligned}$$

Let

$$\begin{aligned}\delta_1 &= \alpha_0 + \alpha_1 w \\ \delta_2 &= \beta_0 + \beta_1 w\end{aligned}$$

where α_0, α_1, β_0, β_1 are quasiquaternions in (v_1, v_2, v_3). Then

$$\delta_3 = \tfrac{1}{4}[4\alpha_0\beta_0 - \varepsilon\bar{\beta}_1\alpha_1\bar{\varepsilon} + (\beta_1\bar{\varepsilon}\,\alpha_0\varepsilon + \alpha_1\bar{\varepsilon}\,\bar{\beta}_0\varepsilon)w]$$

Let

$$\alpha_0 = \tfrac{1}{2}(v_1 + v_2) \qquad \alpha_1 = \tfrac{1}{2}(v_1 + v_2)$$

$$\beta_0 = \tfrac{1}{2}(1 - v_1) \qquad \beta_1 = \tfrac{1}{2}(-1 + v_1)$$

Then δ_1 and δ_2 are contained in J_w since $\chi(\delta_r) = 1$ and neither 1 nor w occurs with non zero coefficient in δ_r for $r = 1, 2$.

Here we are considering $\varepsilon = (1 + v_1 + v_2 + v_3)$.

Now

$$\alpha_0\beta_0 = \tfrac{1}{4}\varepsilon \qquad \text{and} \qquad \bar{\beta}_1\alpha_1 = \tfrac{1}{4}\bar{\varepsilon}\ .$$

Therefore

$$\bar{\varepsilon}\,\alpha_0\beta_0 = 1 = \bar{\beta}_1\alpha_1\varepsilon\ .$$

Thus

$$\beta_1\bar{\varepsilon}\,\alpha_0 = \alpha_1\varepsilon\,\bar{\beta}_0.$$

We have

$$\begin{aligned}\delta_3 &= \tfrac{1}{4}[\varepsilon - \bar{\varepsilon} + (\alpha_1\varepsilon\,\bar{\beta}_0\varepsilon + \alpha_1\bar{\varepsilon}\,\bar{\beta}_0\varepsilon)w] \\ &= \tfrac{1}{4}[\varepsilon - \bar{\varepsilon} + \{\alpha_1(\varepsilon + \bar{\varepsilon})\,\bar{\beta}_0\varepsilon\}\,w]\end{aligned}$$

But

$$\begin{aligned}\tfrac{1}{4}\alpha_1\bar{\beta}_0\varepsilon &= \tfrac{1}{8}(v_1 + v_2)(1 + v_1)(1 - v_1)(v_1 + v_3) \\ &= \tfrac{1}{4}(-1 + v_1 - v_2 - v_3).\end{aligned}$$

Thus

$$\delta_3 = \tfrac{1}{2}(v_1 + v_2 + v_3) + \tfrac{1}{4}(-1 + v_1 - v_2 - v_3)w.$$

Clearly, δ_3 is not contained in any arithmetic of C. Therefore ε cannot generate an ideal for J_w. Similar methods can be applied for the other value of ε and for $\bar{\varepsilon}$.

We now consider εw. Let $\varepsilon = (1 + v_1 + v_2 + v_3)$. As in the first part of the proof, for any elements δ_1, δ_2 of J_w there exists an element δ_3 of J_w such that

$$\delta_1\{\delta_2(\varepsilon w)\} = \delta_3(\varepsilon w)$$

provided that εw generates an ideal for J_w.

Then

$$\delta_3 = \tfrac{1}{4}[\delta_1(\delta_2(\varepsilon w))](-w\bar{\varepsilon}).$$

We write $\delta_1 = \alpha_0 + \alpha_1 w$ and $\delta_2 = \beta_0 + \beta_1 w$ as before. Then

$$\delta_3 = \tfrac{1}{4}[4\beta_0\alpha_0 - \bar{\varepsilon}\alpha_1\bar{\beta}_1\varepsilon + \{\varepsilon(\alpha_0\bar{\varepsilon}\beta_1 + \bar{\beta}_0\bar{\varepsilon}\alpha_1)\}w].$$

Now choose δ_1, δ_2 such that

$$\beta_0\alpha_0 = \tfrac{1}{4}\varepsilon \quad , \qquad \alpha_1\bar{\beta}_1 = \tfrac{1}{4}\bar{\varepsilon} \ .$$

Then

$$\beta_0\alpha_0\bar{\varepsilon} = 1 = \varepsilon\alpha_1\bar{\beta}_1 .$$

Therefore,

$$\alpha_0\bar{\varepsilon}\beta_1 = -\bar{\beta}_0\varepsilon\alpha_1 .$$

We let

$$\alpha_0 = \tfrac{1}{2}(1 - v_1) \qquad \alpha_1 = \tfrac{1}{2}(-1 - v_1)$$

$$\beta_0 = \tfrac{1}{2}(v_1 + v_2) \qquad \beta_1 = \tfrac{1}{2}(-v_1 - v_2).$$

Then δ_1, δ_2 are elements of J_w. For δ_3 we have

$$\begin{aligned}\delta_3 &= \tfrac{1}{4}(\varepsilon - \bar{\varepsilon}) + \tfrac{1}{4}[\varepsilon\bar{\beta}_0(\varepsilon + \bar{\varepsilon})\alpha_1]\, w \\ &= \tfrac{1}{2}(v_1 + v_2 + v_3) + \tfrac{1}{4}[(-1+v_2)(-v_1 - v_2)(v_1 + v_2)(1+v_1)]w \\ &= \tfrac{1}{2}(v_1 + v_2 + v_3) + \tfrac{1}{4}(-1 - v_1 + v_2 - v_3)w.\end{aligned}$$

Thus δ_3 is not contained in J_w. Thus no rational integral multiple of any element of J_w of the form $\varepsilon w \neq 0$ can generate an ideal in J_w. Similar methods can be applied to the remaining cases for which $\chi(\tfrac{1}{2}\alpha^*)$ equals 1.

Now suppose that $\chi(\pm\alpha^*) \neq 1, w$. Write

$$\alpha^* = \alpha_0 + \alpha_1 u$$

where α_0, α_1 are quasiquaternions in any proper associative triad, containing w, of basic units of C with assigned unit u. We have proved that for each of the three choices of triad one of the following relations holds: $N\alpha_0 = 0$, $N\alpha_1 = 0$ or $N\alpha_0 = N\alpha_1$. Since $N\alpha_0 = 0$ and $N\alpha_1 = 0$ both imply that $\chi(\pm\alpha^*) = 1$ we must have $N\alpha_0 = N\alpha_1$ for each of the three possible choices of triad. Thus α_0 must equal $\pm 1 \pm w$. We may therefore write $w_1 = 1$, $w_2 = w$. Then since $(w, w_3, |ww_3|)$ and $(w, w_4, |ww_4|)$ are both proper associative triads containing w of basic units of C we clearly have a contradiction. This completes the proof of the lemma.

We have thus proved that the only ideals for J_w are those generated by elements of J_w of the form $m\mathfrak{S}$ where m is a rational integer and $\mathfrak{S}$ is an element of norm 1 of J_w.

Further we have

Lemma 5.10. For any element $\mathfrak{S}$, of J_w of norm 1 the right and left ideals generated by $m\mathfrak{S}$ are the same as the ideal generated by rational integer m for J_w.

Suppose that m generates ideal $\mathfrak{b}$ for J_w while $m\mathfrak{S}$ generates ideal $\mathfrak{b}_1$ for J_w on the left.

Let α be any element of $\mathfrak{b}$. Then $\alpha = \alpha_1 m$ where α_1 is contained in J_w. Hence $\alpha = \alpha_1 \delta^{-1}(m\delta)$ is an element of $\mathfrak{b}_1$. Thus $\mathfrak{b}$ is a subset of $\mathfrak{b}_1$. Suppose that β is any element of $\mathfrak{b}_1$. Then $\beta = \beta_1(m\delta)$ for some β_1 contained in J_w. Thus $\beta = (\beta_1\delta)m$ and since $\beta_1\delta$ is contained in J_w it follows that β is contained in $\mathfrak{b}$. Hence $\mathfrak{b}_1$ is a subset of $\mathfrak{b}$. Therefore $\mathfrak{b} = \mathfrak{b}_1$. The result is established when we note that a similar proof holds for $\mathfrak{b}_1$ a right ideal of J_w.

We have thus proved

Theorem 5.4. A set of elements $\mathfrak{m}$ of J_w is an ideal if and only if there exists a rational integer n which generates $\mathfrak{m}$.

If element α of J_w generates an ideal $\mathfrak{m}$ for J_w we write $\mathfrak{m} = (\alpha)_w$. For example, in Dickson's notation, we have

$$(\pm 1 \pm i \pm j \pm k)_k = (2)_k = (\pm 1 \pm ie \pm je \pm k)_k$$

and

$$(\pm 1 \pm e \pm ke \pm k)_e = (2)_e = (\pm j \pm k \pm je \pm ke)_e.$$

We denote by $(m)_w(n)_w$ the set of all elements of J_w expressible in the form $\alpha\beta$ where α belongs to $(m)_w$ and β to $(n)_w$. Then

$$(m)_w(n)_w = (mn)_w.$$

There is a (1-1) correspondence between the rational integers and the ideals for any maximal arithmetic J_w of C. The correspondence is preserved under multiplication.

6. Certain Multiplicative Functions. Introduction.

The function $\psi(n)$ defined for every positive rational integer n is called multiplicative if

(6.1) $\psi(mn) = \psi(m) \cdot \psi(n)$ when $(m,n) = 1$.

Most of the multiplicative functions which are discussed in the following sections possess one or both of the following properties.

(6.2) $\psi(p^{\ell+1}) = \psi(p) \cdot \psi(p^{\ell}) - p^{r}\psi(p^{\ell-1})$

for fixed r and $\ell > 0$

(6.3) $\psi(2^{\ell+1}) = \psi(2) \cdot \psi(2^{\ell})$

for $\ell > 0$

where p is an odd rational prime and r, ℓ, m, n are rational integers.

Multiplicative functions, possibly satisfying (6.2) and (6.3), appear chiefly in the theory of elliptic modular functions. The functions appear as coefficients in the Fourier expansions of modular forms of negative dimensions. Their multiplicative properties can then be shown by means of known results in elliptic function theory. The multiplicative properties of Ramanujan's function $\tau(n)$ were first demonstrated by Mordell [5] in this way.

Rankin in his paper [45] devises a method by which certain arithmetic functions which occur in elliptic function theory can also be defined by using results on the arithmetics of algebras with multiplicative norms.

"The arithmetic functions", considered by Rankin (l.c.) , "are all of the form

$$(6.4) \quad \delta(m) = \sum P_r(x_0, x_1 \ldots x_{s-1})$$

where r, s are fixed positive integers, P_r is a homogeneous polynomial of <u>weight</u> r in $x_0, x_1, \ldots x_{s-1}$ (i.e. the sum of the exponents of the x's is equal to r for every term) and the summation is conducted over all integral values of the x's which satisfy the relation

$$x_0^2 + x_1^2 \ldots + x_{s-1}^2 = m.$$

"The only values of s which are considered are s = 1, 2, 4 and 8. The reason for this restriction is given by a famous theorem of Hurwitz (see [51] , or preferably Dickson [10]) which states that, with the exception of these values of s, there can exist no identity of the form

$$\sum_{i=0}^{s-1} x_i^2 \sum_{j=0}^{s-1} y_j^2 = \sum_{k=0}^{s-1} z_k^2$$

where the z_k are bilinear forms in the x_i and y_j . When s takes one of the four permitted values, identities of this type do exist and correspond to the theorem

$$N\xi \cdot N\eta = N\zeta \qquad \text{when} \quad \xi\eta = \zeta ,$$

where ξ , η and ζ are vectors of an appropriate hypercomplex system and N denotes the norm.

This hypercomplex system is identical with the algebras of the real numbers, the complex number, quaternion, and Cayley numbers in the cases $s = 1, 2, 4$ and 8 respectively." Thus for $s = 4, 8$ we note that (6.4) can be written as

$$(6.5) \qquad \mathfrak{f}(m) = \sum_{\xi, m} P_k(\xi)$$

where ξ takes all values of norm m in H_o and J_o respectively.

In his paper [45], Rankin continues: "It is possible to construct multiplicative functions of the form (6.4) by using theorems of the type

$$(6.6) \qquad A \sum_{\xi, mn} F(\xi) = \sum_{\xi, m} \sum_{\eta, n} F(\xi\eta)$$

for $(m,n) = 1$ and $A = 2s$

where the vectors ξ, η, ζ have integral components and $F(\zeta)$ is any function of the s components of ζ. Similar but more complicated results hold when $m = p$, $n = p^{\ell}$ where p is an odd prime and $\ell > o$." Rankin establishes theorems of the form (6.6) for H_o and J_o. In the discussion, he also uses identities of the form

$$(6.7) \qquad \sum_{\xi, m} F(\xi) = 0$$

which were derived in the paper Rankin [44].

It is natural to enquire whether the remaining quaternion and Cayley arithmetics can be usefully employed to give similar elementary definitions of certain such multiplicative functions. We show below that it is in fact possible to use the properties of the arithmetics, not used by Rankin, to find such functions and to prove them multiplicative. A discussion using Hurwitz maximal arithmetic H is given first (§§ 7,8).

7. Identities related to representations in H.

In this section we consider the summation of polynomials $P(\xi)$ of fixed weight in the coordinates x_0, x_1, x_2, x_3 of quaternion ξ over all the elements ξ of maximal arithmetic H of norm some fixed rational integer n, say. Such a summation is written

$$\sum_{\xi,H,m} P(\xi) \tag{7.1}$$

or when no confusion can arise

$$\sum_{\xi,m} P(\xi) \tag{7.2}$$

Here our main object is to find classes of polynomials $P(\xi)$ for which

$$\sum_{\xi,m} P(\xi) = 0 \tag{7.3}$$

The expression $[x_0^{\ell_0} x_1^{\ell_1} x_2^{\ell_2} x_3^{\ell_3}]$ is used to denote the symmetric function of the four variables x_0, x_1, x_2, x_3 which consists of all terms of the type $x_{\sigma_0}^{\ell_0} x_{\sigma_1}^{\ell_1} x_{\sigma_2}^{\ell_2} x_{\sigma_3}^{\ell_3}$

each term occurring once only.

We denote the symmetric functions

$$\sum_{s=0}^{\infty} x_s^r, \qquad \sum_{s=0}^{\infty} y_s^r, \qquad \sum_{s=0}^{\infty} z_s^r$$

by X_r, Y_r and Z_r respectively.

We prove

Theorem 7.1. *If for any polynomial* $P(\xi)$ *in the coordinates* x_0, x_1, x_2, x_3 *of* ξ

$$f(n) = \sum_{\xi,m} P(\xi)$$

then there exists a polynomial $Q(\xi)$ *in the symmetric functions* X_2, X_3, X_4, X_5 *such that*

$$f(n) = \sum_{\xi,m} Q(\xi).$$

To prove this theorem we first note that if η_1 is obtained from an element ξ of norm m in H by any sign changes on the coordinates of ξ then η_1 also belongs to H and has norm m. Thus any terms of polynomial $P(\xi)$ which is an odd function of any coordinate x_s, $0 \leq s \leq 3$, contributes nothing to f(n) and may be omitted. Next we note that if η_2 is obtained from ξ by permuting the coordinates of ξ in any way then η_2 belongs to H and has norm m.

Hence each term of $P(\begin{smallmatrix}\cdot\\ \cdot\end{smallmatrix})$ may be replaced by a suitable multiple of a polynomial which is symmetric in x_0^2, x_1^2, x_2^2, x_3^2. Lastly we note (for example, see van der Waerden [48] § 26) that any symmetric polynomial in x_0^2, x_1^2, x_2^2, x_3^2 can be expressed in a unique manner as a polynomial in X_2, X_4, X_6, X_8. The result has thus been proved. We say that P and Q are equivalent and write $P \sim Q$. Similar results were proved by Rankin [44] for Π_0 and J_0.

Identities of the form

$$\sum_{\gamma,m} F(\begin{smallmatrix}\cdot\\ \cdot\end{smallmatrix}) = 0 \tag{7.4}$$

where $F(\begin{smallmatrix}\cdot\\ \cdot\end{smallmatrix})$ is a polynomial in x_0, x_1, x_2, x_3 are now obtained.

By Theorem 7.1, F may be assumed to be a polynomial in X_2, X_4, X_6, X_8. Also since X_2 is the same for every representation of m we may obtain new identities from any known identity by multiplying by powers of X_2 inside the summation sign. Such identities are not essentially different from the original identity from which they were derived and consequently we may confine our attention to identities of the form (7.4) where F does not contain X_2 as a factor.

F is then called reduced and (7.4) is a reduced identity.

A set of identities

$$\sum_{\xi,m} f_s(\xi) = 0 \qquad (s = 1, 2, \ldots r)$$

where the f_s are polynomials in x_0, x_1, x_2, x_3 is said to be linearly independent when no relation of the form

$$\sum_{s=1}^{r} h_s(X_s)\, f_s = 0$$

can exist for polynomials h_s which are not identically zero. Otherwise the identities are called linearly dependent. These terms are also applied to the polynomials f_s themselves.

We now prove

Theorem 7.2. For any rational integer t and element ρ of H of norm 1

$$\sum_{\xi,m} R^t(\xi) = \sum_{\xi,m} R^t(\xi\rho) \tag{7.5}$$

where, as before, $R(\xi)$ denotes the real part of ξ

Let ξ be any element of norm m in H. Then $\xi\rho$ is an element of norm m in H.

Further, if ξ takes all vector values of norm n in H then $\xi\rho$ takes the same set of values.

Clearly, this follows since

$$N(\xi\rho) = N(\xi).N(\rho) = N\xi$$

and

$$\xi_1\rho = \xi_2\rho$$

if and only if

$$\xi_1 = \xi_2 .$$

Theorem 7.2 is thus established.

Let $\xi = x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3$ and

$\rho = \frac{1}{2}(1 - i_1 - i_2 - i_3)$. Then

$R(\xi\rho) = \frac{1}{2}(x_0 + x_1 + x_2 + x_3)$.

By Theorem 7.1, we have for t an odd rational integer

$$R^t(\xi\rho) \sim 0.$$

Next let $t = 2$ in (7.5). Then, by Theorem 7.1,

$$R^2(\xi\rho) = \frac{1}{4}X_0 + \frac{1}{2}[x_0 x_1]$$

$$\sim \frac{1}{4}X_0$$

Thus (7.2) does not lead to an identity when $t = 2$.

Now put $t = 4$. Then, by Theorem 7.1,

$$R^4(\xi\rho) = \frac{1}{16}(x_0 + x_1 + x_2 + x_3)^4$$

$$\sim \frac{1}{16}(X_0 + 6[x_0^2 x_1^2]).$$

But

$$X_2^2 = X_4 + 2[x_0^2 x_1^2].$$

Thus, from Theorem 7.2, we have

$$\sum_{\xi,m} \tfrac{1}{4} X_4 = \sum_{\xi,m} \tfrac{1}{16}(X_4 + 3 X_2^2 - 3 X_4)$$

Hence

(i) $$\sum_{\xi,m} (2X_4 - X_2^2) = 0.$$

For $t = 6$, we have by Theorem 7.1

$$R^6(\xi\rho) = \tfrac{1}{64}(x_0 + x_1 + x_2 + x_3)^6$$

$$\sim \tfrac{1}{64}\{X_6 + 15[x_0^4 x_1^2] + 90[x_0^2 x_1^2 x_2^2]\}.$$

But

$$[x_0^4 x_1^2] = -X_6 + X_4 X_2$$

and

$$6[x_0^2 x_1^2 x_2^2] = 2X_6 - 3X_4 X_2 + X_2^3.$$

Thus from Theorem 7.2

$$\sum_{\xi,m} 2X_4 X_2 = \sum_{\xi,m} X_2^3$$

Clearly this identity and identity (i) are linearly dependent.

Now when $t = 8$ we have, again by Theorem 7.1,

$$R^8(\xi\rho) = \tfrac{1}{256}\{X_8 + 28[x_0^6 x_1^2] + 70[x_0^4 x_1^4] + 420[x_0^4 x_1^2 x_2^2] + 28.90[x_0^2 x_1^2 x_2^2 x_3^2]\}.$$

Also

$$[x_0^6\ x_1^2] = X_6X_2 - X_8$$

$$2[x_0^4\ x_1^4] = X_4^2 - X_8$$

$$2[x_0^4\ x_1^2\ x_2^2] = X_4X_2^2 - X_4^2 - 2X_6X_2 + 2X_8$$

and

$$24[x_0^2\ x_1^2\ x_2^2\ x_3^2] = X_2^4 - 6X_4X_2^2 + 3X_4^2 + 8X_6X_2 - 6X_8.$$

But from (i)

$$X_4 \sim \tfrac{1}{3}X_2^2$$

Thus from Theorem 7.2 with $t = 8$ we have

$$(ii)\quad \sum_{\xi_i,m} (48X_8 - 20X_4^2 - 64X_6X_2 + 15X_2^4) \equiv 0$$

For $t = 10$ we have

$$H^{10}(\xi\rho) = \frac{1}{1024}(x_0 + x_1 + x_2 + x_3)^{10}$$

$$\sim \frac{1}{1024}\{X_{10} + 45[x_0^8x_1^2] + 210[x_0^6x_1^4] + 1260[x_0^6x_1^2x_2^2] + 210.15[x_0^4x_1^4x_2^2] + 210.90[x_0^4x_1^2x_2^2x_3^2]\}.$$

Also

$$[x_0^8x_1^2] = X_8X_2 - X_{10}$$

$$[x_0^6x_1^4] = X_6X_4 - X_{10}$$

$$2[x_0^6x_1^2x_2^2] = 2X_{10} - 2X_8X_2 - X_6X_4 + X_6X_2^2$$

$$2[x_0^4x_1^4x_2^2] = 2X_{10} - X_8X_2 - 2X_6X_4 + X_4^2X_2$$

and

$$60[x_0^4x_1^2x_2^2x_3^2] = -36X_{10} + 30X_8X_2 + 30X_6X_4 - 10X_6X_2^2 - 15X_4^2X_2 + X_2^5.$$

By substituting in

$$X_4 X_2^3 = X_{10} + 3[x_0^8 x_1^2] + 4[x_0^6 x_1^4] + 6[x_0^6 x_1^2 x_2^2] + 6[x_0^4 x_1^4 x_2^2] + 6[x_0^4 x_1^2 x_2^2 x_3^2]$$

we obtain

$$4X_{10} = 5X_6 X_2 + \tfrac{12}{7} X_6 X_4 - \tfrac{12}{7} X_6 X_2^2 - \tfrac{5}{2} X_4^2 X_2 + \tfrac{8}{7} X_2^5$$

Hence from Theorem 7.2 with t = 10 we have

$$\text{(iii)} \sum_{\xi,m} \left(96X_8 X_2 - 80X_6 X_4 - 88X_6 X_2^2 + 60X_4 X_2^2 + 5X_2^5\right) = 0.$$

A simpler form of identity (iii) can be obtained by using (ii) to substitute for $X_8 X_2$ say in (iii).

A similar discussion for t = 12 shows that

$$\text{(iv)} \sum_{\xi,m} (96X_6 X_4 - 48X_8 X_2^2 - 128X_6 X_4 X_2 + 64X_6 X_2^3 - 56X_4^3 + 132X_4^2 X_2^2 - 26X_2^6) = 0.$$

We have proved

Theorem 7.3. For any positive rational integer m and polynomial function $h(X_2)$ of X_2

$$\sum_{\xi,\mathrm{H},m} h(X_2) \cdot F_s\left(\tfrac{\xi}{\eta}\right) = 0$$

when /

when

(i) $F_4(\xi) = 2X_4 - X_2^2$

(ii) $F_8(\xi) = 48X_8 - 20X_4^2 - 64X_6X_2 + 15X_2^4$

(iii) $F_{10}(\xi) = 96X_8X_2 - 80X_6X_4 - 88X_6X_2^2 + 60X_4^2X_2 + 5X_2^5$

(iv) $F_{12}(\xi) = 96X_8X_4 - 48X_8X_2^2 - 128X_6X_4X_2 + 64X_6X_2^3 - 56X_4^3 + 132X_4^2X_2^2 - 26X_2^6$.

Also,

$$F_4(\xi),\ F_8(\xi),\ F_{10}(\xi) \text{ and } F_{12}(\xi)$$

are linearly independent. For m an even positive rational integer Theorem 7.3 holds in H_0. This was proved by Rankin [44] without explicit use of quaternion multiplication. Theorem 7.3 as stated for H is in fact equivalent to Rankin's result for H_0. This follows since if m is even then the set of all elements ξ of H for which $N\xi = m$ is the same as the set of all elements of norm m in H_0, while for m odd or even the set of elements of H of norm m is the same as the set of elements $\frac{1}{2}\eta$ where η is any element of H_0 of norm 4m. Also the polynomials are homogeneous in x_0, x_1, x_2, x_3 Rankin also explains (1.c) how identities of these forms may be derived by equating coefficients in elliptic function expansions.

Finally, we note that in Theorem 7.2 above we chose $\rho = \frac{1}{4}(1 - i_1 - i_2 - i_3)$. Now ρ must be an element of H of norm 1. If we choose ρ equal to a unit of C then Theorem 7.2 gives a trivial result. Clearly, any other ρ, not a unit of C, gives the identities stated in Theorem 7.3.

8. Multiplicative Functions related to Representations in H.

We now wish to find multiplicative functions of the form

$$\sum_{\xi,H,m} P_r(\xi) \tag{8.1}$$

where $P_r(\xi)$ is a homogeneous polynomial of weight r in the coordinates x_0, x_1, x_2, x_3 of ξ and summation is over all ξ of norm m in maximal quaternion arithmetic H. Before carrying out the construction we must first give results on the number of representations of a positive rational integer as the norm of an element of H and then prove results on the number of factorizations of a given element of H into factors of prescribed norm in H. As already stated in § 6, Rankin gives a similar discussion for quaternion arithmetic H_0 in his paper [45].

For any positive rational integer m, let $r_H(m)$ be the number of distinct elements ξ belonging to H for which $N\xi = m$. We call $r_H(m)$ the number of representations of m in H. It is noted that $r_H(n) = \sum_{\xi,H,m} 1$. Thus for the non maximal quaternion arithmetic H_0 we define $r_{H_0}(m)$ to be

$$\sum_{\xi,H_0,m} 1.$$

We state

Theorem 8.1.

For l, m, n positive rational integers and p an odd positive rational prime

(i) $24\, r_H(mn) = r_H(m)\, r_H(n)$

whenever $(m,n) = 1$

(ii) $24\, r_H(p^{l+1}) = r_H(p) r_H(p^l) - 24p r_H(p^{l-1})$

$r_H(p) = 24(1 + p)$ if $l > 0$.

(iii) $r_H(2^l) = 24$ if $l > 0$.

The theorem can be deduced at once from the corresponding results for H_0 given in Rankin [45], for it is easy to show that

(8.2) $r_H(m) = r_{H_0}(4m)$

The relation (8.2) follows from the fact that the set of all elements of H of norm n is the same as the set of all elements of the form $\pm\eta$ for which η is an element of H_0 of norm $4m$.

We now wish to prove some results on the number of factorizations of a given element of H into factors of prescribed norm in H. We therefore adopt the following notation. Let ξ be a given element of H of norm mn where m, n are positive rational integers.

Let $\mathfrak{S}_H(\zeta;\ m,n) = \mathfrak{S}_H(\zeta)$ denote the set of all pairs of factors (ξ, η) of ζ in H for which $N\xi = m$ and $N\eta = n$. Let $S_H(\zeta;\ m,n) = S_H(\zeta)$ be the number of such pairs (ξ, η). Similar definitions can be given for H_0.

We first prove

Theorem 8.2.

$$S_H(\zeta;\ m,n) = 24 \quad \text{whenever } (m,n) = 1.$$

In order to prove this result we can use the method described in § 4 to prove the corresponding result for maximal arithmetic $\mathfrak{J}_w$ of C. However, since the associative law holds in H, we can simplify the method as follows. Let (ξ_1, η_1) and (ξ_2, η_2) be any two elements of $\mathfrak{S}_H(\zeta)$. Then

$$\xi_1\eta_1 = \xi_2\eta_2 = \zeta.$$

Hence

$$\bar{\xi}_1\zeta\bar{\eta}_2 = m\eta_1\bar{\eta}_2 = n\,\bar{\xi}_1\xi_2.$$

Thus since $(m,n) = 1$

$$\bar{\xi}_1\xi_2 = n\rho, \qquad \eta_1\bar{\eta}_2 = m\rho$$

where ρ is an element of H of norm 1.

There are exactly 24 such elements in H. This implies that $S_\mu(\xi)$ is 0 or 24.

Suppose there exists a ξ for which $S_\mu(\xi) = 0$. Then

$$r_\mu(m)r_\mu(n) = \sum_{\xi,mn} S_\mu(\xi) < 24 \sum_{\xi,mn} 1 = 24 r_\mu(mn).$$

This contradicts Theorem 8.1 (i). Thus $S_\mu(\xi) = 24$ and any solution (ξ, η) of $G_\mu(\xi)$ is given in terms of any one solution (ξ_1, η_1) by the relations

$$\xi = \xi_1 \pi, \qquad \eta = \nu \eta_1.$$

where ν is an element of H of norm 1.

Next we prove

Theorem 8.3. *For p an odd positive rational prime and $\beta > 0$.*

$S_\mu(\xi ; p, p^\beta) = 24(1 + p)$ if $p \mid \xi$ in H

$S_\mu(\xi ; p, p^\beta) = 24$ if $p \nmid \xi$ in H.

If p divides ξ in H, the result follows at once from Theorem 8.1(ii).

Now suppose that p does not divide ξ in H. Then, for a any unit of Q_p by (1.4), (1.7) and (1.9) applied to Q_p we have

$$p.R(\xi_1 u \eta_1 + \bar{\eta}_1 u \bar{\xi}_2) = R(\xi_1 u \bar{\xi}_2 \zeta + \bar{\zeta} \xi_1 u \bar{\xi}_2)$$
$$= R(\zeta).2R(\xi_1 u \bar{\xi}_2).$$
$$= R(\zeta).2R(\bar{\xi}_2 \xi_1 u).$$

Hence, as in Theorem 4.8, p divides $\bar{\xi}_2 \xi_1$ in H.

Thus $\bar{\xi}_2 \xi_1 = p\rho$ where ρ is an element of norm 1 in H. Hence $S_H(\zeta)$ is 0 or 24. Suppose that there exists a ζ for which $S_H(\zeta)$ is 0. Then, by Theorem 8.1 (ii), we have

$$r_H(p)\, r_H(p^\ell) = \sum_{\zeta, p^{\ell+1}} S_H(\zeta)$$
$$< 24 \sum_{\substack{\zeta, p^{\ell+1} \\ p \nmid \zeta}} 1 + 24(1+p) \sum_{\substack{\zeta, p^{\ell+1} \\ p \mid \zeta}} 1$$
$$= 24\, r_H(p^{\ell+1}) - r_H(p^{\ell-1}) + 24(1+p)\, r_H(p^{\ell-1})$$
$$= 24\, r_H(p^{\ell+1}) + 24\, p\, r_H(p^{\ell-1})$$
$$= r_H(p)\, r_H(p^\ell).$$

This is a contradiction. Thus

$$S_H(\zeta) = 24$$

for all ζ for which p does not divide ζ. Also, the 24 solutions (ξ, η) are given in terms of any one of them (ξ_1, η_1) by

$$\xi = \xi_1 \bar{\tau} \qquad \eta = \tau \eta_1$$

where τ takes the 24 quaternion values of norm 1 in H.

Next we have

Theorem 8.4. For $\ell > 0$,

$$S_H(\zeta\,;\, 2, 2^\ell) = 24.$$

Let (ξ, η) be any solution of $G_H(\zeta; 2, 2^l)$. We note that 2 divides ζ in H for all ζ of norm 2^{l+1} $(l > 0)$ since either all the coordinates of ζ are odd or all are even rational integers. Thus

$$\zeta = 2\zeta'$$

where ζ' belongs to H. Hence

$$\eta = \bar{\xi}\zeta'$$

Thus every solution of $N\xi = 2$ in H produces a solution of $G_H(\zeta)$. The result follows by Theorem 8.1 (iii).

From Theorems 8.2, 8.3 and 8.4 we deduce the following three theorems for $P_r(\zeta)$ a homogeneous polynomial of weight r in the coordinates z_0, z_1, z_2, z_3 of ζ.

Theorem 8.5. If $(m, n) = 1$,

$$24 \sum_{\zeta, H, mn} P_r(\zeta) = \sum_{\xi, H, m} \sum_{\eta, H, n} P_r(\xi\eta).$$

Theorem 8.6. If p is a rational prime and $l > 0$

$$24 \sum_{\zeta, H, p^{l+1}} P_r(\zeta) = \sum_{\xi, H, p} \sum_{\eta, H, p^l} P_r(\xi\eta) - 24\, p^{r+1} \sum_{\zeta, H, p^{l-1}} P_r(\zeta').$$

Theorem 8.7. If $l > 0$,

$$24 \sum_{\zeta, H, 2^{l+1}} P_r(\zeta) = \sum_{\xi, H, 2} \sum_{\eta, H, 2^l} P_r(\xi\eta).$$

We now use Theorems 8.5, 8.6 and 8.7 to construct multiplicative functions related to the representations of m as the norm of an element of H.

Since

$$Z_2 = X_2 Y_2 = mn$$

is a constant for each member of $G_N(\zeta ; m, n)$ it is clear that we need only consider polynomials $P_r(\zeta)$ in Theorems 8.5, 8.6 and 8.7 which do not contain Z_2 as a factor. For example, when $r = 0$ or 2 Theorem 8.5 leads to a restatement of Theorem 8.1 (i). Also in the case when $r = 4$, $P_4(\zeta)$ must be a linear combination of Z_4 and Z_2^2. But by Theorem 7.3 (i) we have

$$Z_4 \sim \tfrac{1}{2} Z_2^2 .$$

Thus this case also leads to a restatement of Theorem 8.1 (i).

We now consider Theorem 8.5 with $r = 6$. We obtain a function which is not merely a multiple of $r_N(n)$. $P_6(\zeta)$ must be a linear combination of Z_6, $Z_4 Z_2$ and Z_2^3. Again by Theorem 7.3 (i)

$$Z_4 Z_2 \sim \tfrac{1}{2} Z_2^3 .$$

Therefore, we write

$$P_6(\zeta) = a Z_6 + b Z_2^3 \tag{8.3}$$

for arbitrary real numbers a and b. Now from Theorem 8.5 for $(m,n) = 1$ we have

$$\sum_{\zeta, mn} Z_6 = \frac{1}{24} \sum_{\zeta, mn} 4 z_0^6 = \frac{1}{6} \sum_{\xi, m} \sum_{\eta, n} \{R(\xi\eta)\}^6 .$$

But

$$R(\xi\eta) = x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3 .$$

When this is raised to the sixth power all those terms which are not even functions of each x_s and y_s $(0 \leq s \leq 3)$ may be omitted as they contribute nothing to the double sum. There remain terms of the type
(i) $x_0^6y_0^6$ (4 such) each with coefficient 1,
(ii) $x_0^4x_1^2y_0^4y_1^2$ (12 such) each with coefficient 15
and
(iii) $x_0^2x_1^2x_2^2y_0^2y_1^2y_2^2$(4 such) each with coefficient 90.
But $[x_0^6Iy_0^6]$ contains 16 terms, $[x_0^4x_1^2Iy_0^4y_1^2]$contains 144 terms and $[x_0^2x_1^2x_2^2][y_0^2y_1^2y_2^2]$ contains 16 terms.
Hence

$$\sum_{\xi,mn} Z_6 = \frac{1}{24}\sum_{\xi,m}\sum_{\eta,n}\left\{X_6Y_6 + 5[x_0^4x_1^2Iy_0^4y_1^2] + 90[x_0^2x_1^2x_2^2Iy_0^2y_1^2y_2^2]\right\}.$$

Now

$$[x_0^4x_1^2] = X_4X_2 - X_6 \sim \tfrac{1}{2}X_2^3 - X_6$$

and

$$6[x_0^2x_1^2x_2^2] = 2X_6 - 3X_4X_2 + X_2^3$$
$$\sim 2X_6 + \tfrac{1}{2}X_2^3 .$$

Hence

$$(8.4)\quad \sum_{\xi,mn} Z_6 = \frac{1}{24}\sum_{\xi,m}\sum_{\eta,n}\left\{16\,X_6Y_6 - 5\,(X_6Y_2^3 + X_2^3Y_6) + \tfrac{15}{8}X_2^3Y_2^3\right\}.$$

Again we have

$$(8.5)\quad \sum_{\xi,mn} Z_2^3 = \frac{1}{24}\sum_{\xi,m}\sum_{\eta,n} X_2^3Y_2^3 .$$

Now we require

$$(8.6)\quad \sum_{\zeta,mn} P_6(\zeta) = \sum_{\xi,m}\sum_{\eta,n}\{P_6(\xi)\,P_6(\eta) + F_4(\xi)\,X_2T_6(\eta) + T_6'(\xi)\,F_4(\eta)\,X_2\}$$

where $F_4(\xi) = 2X_4 - X_2^2$ and where $T_6(\eta)$ and $T_6'(\xi)$ are any homogeneous polynomials of weight 6 in the coordinates of η and ξ respectively. We can therefore write

$$T_6(\eta) \sim A\,Y_6 + B\,Y_2^3,$$

$$T_6'(\xi) \sim A'X_6 + B'X_2^3$$

for real A, B, A', B'.

From (8.3), (8.4) and (8.5) we have

$$\sum_{\zeta,mn} P_6(\zeta) = \tfrac{1}{24}\sum_{\xi,m}\sum_{\eta,n}\{16aX_6Y_6 - 5a(X_6Y_2^3 + X_2^3Y_6) + (\tfrac{15}{8}a + b)\,X_2^3Y_2^3\}.$$

while for the right hand side of (8.6), omitting some rather lengthy working, the terms needed are

$$\sum_{\xi,m}\sum_{\eta,n}\{a^2X_6Y_6 + ab\,(X_6Y_2^3 + X_2^3Y_6) + b^2X_2^3Y_2^3\}.$$

Hence equating coefficients in (8.6) gives

$$\tfrac{2}{3}a = a^2, \qquad -\tfrac{5}{24}a = ab \qquad \text{and} \qquad \tfrac{15}{8}a + b = 24\,b^2.$$

If $a = 0$, $b = \frac{1}{24}$ and we have $P_6(\zeta) = \frac{1}{24}Z_2^3$ which gives $\frac{1}{24}\,m^3r_4(m)$ as a multiplicative function. This, of course, follows at once from Theorem 8.1 (i). If $a \neq 0$, we have $a = \frac{2}{3}$ and $b = -\frac{5}{24}$. Then

$$(8.7)\qquad P_6(\zeta) = \tfrac{1}{24}(16Z_6 - 5Z_2^3).$$

Write

$$g_6^*(n) = \sum_{\xi,n} P_6(\xi).$$

Then $g_6^*(n)$ is a multiplicative function defined by using H. In addition, it follows from Theorems 8.6 and 8.7 that $g_6^*(n)$ satisfies (6.2) and (6.3).

For r = 8 the numerical working for a construction of the above type is long. We therefore omit some of the details. $P_8(\zeta)$ must be a linear combination of Z_8, Z_6Z_2, Z_4^2, $Z_4Z_2^2$ and Z_2^4. Again by Theorem 7.3 (i) and (ii) we have

$$Z_4Z_2^2 \sim \tfrac{1}{2} Z_2^4 \tag{8.8}$$

and

$$20\, Z_4^2 \sim 48\, Z_8 - 64\, Z_6Z_2 + 15\, Z_2^4. \tag{8.9}$$

Therefore we write

$$P_8(\zeta) = a\, Z_8 + b\, Z_6Z_2 + c\, Z_2^4$$

where a, b and c are real numbers. Now from Theorem 8.5 for $(m,n) = 1$ we have

$$\sum_{\xi,mn} Z_8 = \frac{1}{6} \sum_{\xi,m} \sum_{\eta,n} R^8(\xi\eta).$$

By raising $R(\xi\eta)$ to the eighth power and expressing the summands obtained in terms of symmetric functions we have

(8.10)
$$\sum_{\xi,mn} Z_8 = \frac{1}{72}\sum_{\xi,m}\sum_{\eta,n}\{3X_8Y_8 + 28[x_0^6x_1^2][y_0^6y_1^2] + 140[x_0^4x_1^4][y_0^4y_1^4] + 420[x_0^4x_1^2x_2^2][y_0^4y_1^2y_2^2] + 28.90[x_0^2x_1^2x_2^2x_3^2][y_0^2y_1^2y_2^2y_3^2]\}.$$

Now we have using (8.8) and (8.9)

$$[x_0^6x_1^2] = X_6X_2 - X_8$$

$$2[x_0^4x_1^4] = X_4^2 - X_8$$
$$\sim \tfrac{7}{5}X_8 - \tfrac{14}{5}X_6X_2 + \tfrac{3}{4}X_2^4$$

$$2[x_0^4x_1^2x_2^2] = X_4X_2^2 - X_4^2 - 2X_6X_2 + 2X_8$$
$$\sim -\tfrac{2}{5}X_8 + \tfrac{6}{5}X_6X_2 - \tfrac{1}{4}X_2^4$$

$$24x_0^2x_1^2x_2^2x_3^2 = X_2^4 - 6X_4X_2^2 + 3X_4^2 + 8X_6X_2 - 6X_8$$
$$\sim \tfrac{6}{5}X_8 - \tfrac{3}{5}X_6X_2 + \tfrac{1}{4}X_2^4.$$

We now substitute these relations in (8.10) and thus obtain a double sum for

$$\sum_{\xi,mn} Z_8$$

in terms of X_8, X_6X_2, X_2^4, X_8, X_6Y_2, and X_2^4.

Similar relations for

$$\sum_{\xi,mn} Z_6Z_2 \qquad \text{and} \qquad \sum_{\xi,mn} Z_2^4$$

are obtained as in (8.4) and (8.5) above. Then continuing as in the previous case we find that the polynomial

(8.11) $$P_8(\xi) = \frac{1}{24}(64X_8 - 112X_6X_2 + 21X_2^4)$$

gives rise to the multiplicative function

$$g_8^*(m) = \sum_{\xi,m} P_8(\xi).$$

Thus $g_8^*(m)$ is a multiplicative function defined by using H. Also it follows from Theorems 8.6 and 8.7 that $g_8^*(m)$ satisfies (6.2) and (6.3).

We now relate multiplicative functions defined by means of H to those defined by means of H_o. Let $g_r(m)$ be any multiplicative function of the form

$$g_r(m) = \sum_{\xi, H_o, m} T_r(\xi) \tag{8.12}$$

for $T_r(\xi)$ a homogeneous polynomial of weight r in the coordinates of ξ. Then

$$g_r(4m) = \sum_{\xi, H_o, 4m} T_r(\xi) = 2^r \sum_{\xi, H, m} T_r(\xi).$$

The final summation depends on H. Now

$$\frac{1}{g_r(4)}\ g_r(4m)$$

is multiplicative provided that $g_r(4) \neq 0$. Hence

$$g_r^*(m) = \frac{1}{g_r(4)}\ g_r(4m)$$

is a multiplicative function depending on H provided that the function $g_r(m)$ does not vanish for even m. We have thus related the multiplicative functions defined by Rankin [45] using H_o to those defined by means of H. In fact

$$g_6^*(m) = \frac{1}{g_6(4)}\ g_6(4m)$$

and

$$C_8^*(n) = \frac{1}{C_8'(4)} C_8'(4n)$$

where

$$C_6(n) = \frac{1}{3}\sum_{\xi, H_0, n} (16 X_6 - 20 X_4 X_2 + 5 X_2^3)$$

and

$$C_8'(n) = \frac{1}{24}\sum_{\xi, H_0, n} (-480 X_8 + 560 X_6 X_2 + 280 X_4^2 - 420 X_4 X_2^2 + 63 X_2^4).$$

The remaining multiplicative functions of the form (8.12) found by Rankin are zero for all even values of n. It is easy to verify that they correspond to the identities depending on H stated in Theorem 7.3 above.

9. Identities related to Representations in Maximal and Non Maximal Arithmetics strictly containing J_0.

In order to construct identities depending on maximal arithmetic J_w of C, for w any basic unit of C other than 1, we consider summations written as

$$\sum_{\xi, J_w, m} P_r(\xi).$$

Here $P_r(\xi)$ is a homogeneous polynomial of weight r in the coordinates x_s $(0 \leq s \leq 7)$ of element ξ of C. The summation is over all elements ξ of J_w of norm some fixed positive rational integer m. When no confusion can arise we write the summation as

$$\sum_{\xi, m} P_r(\xi).$$

If, for any other homogeneous polynomial of weight r,

$$\sum_{\xi, m} P_r(\xi) = \sum_{\xi, m} Q_r(\xi),$$

for all rational integers m considered, we say that $P_r(\xi)$ and $Q_r(\xi)$ are equivalent and write

$$P_r(\xi) \sim Q_r(\xi).$$

The expression $[x_0^{l_0} x_1^{l_1} x_2^{l_2} \ldots x_7^{l_7}]$ is used to denote the symmetric function of the eight variables $x_0, x_1, \ldots x_7$. The function consists of all terms of the type $x_{s_0}^{l_0} x_{s_1}^{l_1} \ldots x_{s_7}^{l_7}$ each term occuring only once. We denote the symmetric functions

$$\sum_{s=0}^{7} x_s^r, \quad \sum_{s=0}^{7} y_s^r \quad \text{and} \quad \sum_{s=0}^{7} z_s^r$$

by X_r, Y_r and Z_r respectively.

Again we consider

$$\sum_{\xi, J_w, m} P_r(\xi).$$

If ξ_1 is obtained from an element ξ of norm m of J_w by any set of sign changes on the coordinates of ξ, then ξ_1 also belongs to J_w and has norm m. Thus any term of polynomial $P_r(\xi)$ which is an odd function of any coordinate x_s, $(0 \leq s \leq 7)$, of ξ is equivalent to 0 and may therefore be omitted from the summation. Now any element ξ_2 obtained by permu ting the coordinates of an element ξ of J_w of norm m with coordinates all integers or all half odd integers belongs to J_w and has norm m. Hence, by Lemma 3.10, each term of $P_r(\xi)$ involving one, two or three variables may be replaced by a polynomial which is symmetric in $x_0^2, x_1^2 \ldots x_7^2$.

Clearly, for four variables, we have

$$\sum_{\xi, J_{i_3}, m} x_0^2 x_1^2 x_2^2 x_3^2 \quad \text{and} \quad \sum_{\xi, J_{i_3}, m} x_0^2 x_1^2 x_2^2 x_4^2$$

since $(1, i_1, i_2, i_3)$ is a basic defining set for J_{i_3} while $(1, i_1, i_2, i_4)$ is not. The two sets of basic units are therefore not replaceable for J_{i_3} in the sense defined in § 3. For J_w, by the previous cases, we need only consider

$$\sum x_{s_0}^2 x_{s_1}^2 x_{s_2}^2 x_{s_3}^2$$

where the summation is over all sets (s_0, s_1, s_2, s_3) for which $(i_{s_0}, i_{s_1}, i_{s_2}, i_{s_3})$ is a basic defining

set of units for J_W and

$$\sum x_{\ell_0}^2 x_{\ell_1}^2 x_{\ell_2}^2 x_{\ell_3}^2$$

where the summation is over all sets $(\ell_0, \ell_1, \ell_2, \ell_3)$ for which $(i_{\ell_0}, i_{\ell_1}, i_{\ell_2}, i_{\ell_3})$ is not a basic defining set of units for J_W. The functions are denoted by

$$[x_{s_0}^2 x_{s_1}^2 x_{s_2}^2 x_{s_3}^2]_W \quad \text{and} \quad [x_{\ell_0}^2 x_{\ell_1}^2 x_{\ell_2}^2 x_{\ell_3}^2]'_W$$

respectively. Then $[x_{s_0}^2 x_{s_1}^2 x_{s_2}^2 x_{s_3}^2]_W$ contains 14 terms and $[x_{\ell_0}^2 x_{\ell_1}^2 x_{\ell_2}^2 x_{\ell_3}^2]'_W$ contains 56 terms. We have

$$(9.1) \quad [x_0^2 x_1^2 x_2^2 x_3^2] = [x_{s_0}^2 x_{s_1}^2 x_{s_2}^2 x_{s_3}^2]_W + [x_{\ell_0}^2 x_{\ell_1}^2 x_{\ell_2}^2 x_{\ell_3}^2]'_W .$$

Similar arguments can be applied to polynomials of weight greater than 8. Thus we can define

$$[x_{s_0}^4 x_{s_1}^2 x_{s_2}^2 x_{s_3}^2]_W \quad \text{and} \quad [x_{\ell_0}^4 x_{\ell_1}^2 x_{\ell_2}^2 x_{\ell_3}^2]'_W$$

in the above way. Further arguments are not needed as we do not deal with polynomials of weight greater than 10.

We have proved

<u>Theorem 9.1.</u> <u>For any homogeneous polynomial</u> $P_r(\xi)$ <u>of weight</u> $r \leq 8$ <u>in the coordinates</u> x_s $(0 \leq s \leq 7)$ <u>of</u> ξ, <u>there exists a homogeneous polynomial</u> $Q_r(\xi)$ <u>in the symmetric functions</u> X_2, X_4, X_6, X_8 <u>and in</u> $[x_{s_0}^2 x_{s_1}^2 x_{s_2}^2 x_{s_3}^2]_W$ <u>for which</u>

$$\sum_{\xi, J_W, m} Q_r(\xi) = \sum_{\xi, J_W, m} P_r(\xi).$$

Let ρ be any element of norm 1 in J_n. Then as ξ runs through all elements of J_w of norm m, $\xi\rho$ runs through the same subset of J_w in a different order for $\rho \neq 1$.

We thus have

Theorem 9.2. For any rational integer t and element ρ of J_w of norm 1

$$\sum_{\xi,m} R^t(\xi) = \sum_{\xi,m} R^t(\xi\rho)$$

where as before $R(\xi)$ is the real part of ξ.

By Theorem 9.1, we see that for t an odd rational integer

$$R^t(\xi\rho) \sim 0.$$

Thus we need only consider even values of t in the above theorem.

We admit the definitions of linear dependence and independence given in § 7 without restatement as they are easily modified for J_w.

In Theorem 9.2, let

$$\rho = \tfrac{1}{2}(1 - i_{s_1} - i_{s_2} - i_{s_3})$$

where s_1, s_2, s_3 are distinct integers such that ρ is contained in J_w. Then

$$R(\xi\rho) = \tfrac{1}{2}(x_0 + x_{s_1} + x_{s_2} + x_{s_3}).$$

The first useful result is given by taking $t = 4$. We have

$$R^4(\xi\rho) = \frac{1}{16}\left(x_0 + x_{s_1} + x_{s_2} + x_{s_3} \right)^4$$
$$\sim \frac{1}{16}\left(\frac{1}{2} X_4 + \frac{36}{28}[x_0^2 x_1^2] \right)$$
$$= \frac{1}{16}\left(\frac{1}{2} X_4 + \frac{9}{7}[x_0^2 x_1^2] \right).$$

Now

$$2\,[x_0^2 x_1^2] = X_2^2 - X_4.$$

Hence we have

$$\sum_{\xi,m} 2\, X_4 = \sum_{\xi,m} \left(-\frac{1}{7} X_4 + \frac{9}{14} X_2^2 \right).$$

It follows that

$$\sum_{\xi,m} \left(10\, X_4 - 3\, X_2^2 \right) = 0 \tag{9.2}$$

Now in Theorem 9.2 put

$$\bar{\rho} = \frac{1}{4}\left(u_1 + u_2 + u_3 + u_4 \right)$$

where (u_1, u_2, u_3, u_4) takes each of the 14 values of the basic defining sets for J_w in turn. On adding the identities obtained we have

$$7.2^{t-2} \sum_{\xi,m} X_t = \sum_{\xi,m} \sum \left(x_{s_0} + x_{s_1} + x_{s_2} + x_{s_3} \right)^t \tag{9.3}$$

where the inner summation is over the 14 sets of suffixes (s_0, s_1, s_2, s_3) of the basic defining sets for J_w.

Thus from (9.3) with $t = 6$ we have

$$4.28 \sum_{\xi,m} X_6 = \sum_{\xi,m} \left\{ 7\, X_6 + 3.15\, [x_0^4 x_1^2] + 90\, [x_0^2 x_1^2 x_2^2] \right\}.$$

Now

$$[x_0^4 x_1^2] = - X_6 + X_4 X_2$$

and

$$6[x_0^2 x_1^2 x_2^2] = 2 X_6 - 3 X_4 X_2 + X_2^3 .$$

Hence using (9.2) we have

$$(9.4) \qquad 8 \sum_{\xi,m} X_6 = \sum_{\xi,m} X_2^3 .$$

Next we put $t = 8$ in (9.3) and use

$$[x_0^6 x_1^2] = - X_8 + X_6 X_2$$

$$2[x_0^4 x_1^4] = - X_8 + X_4^2$$

$$2[x_0^4 x_1^2 x_2^2] = 2 X_8 - 2 X_6 X_2 - X_4^2 + X_4 X_2^2$$

and (9.2) and (9.4) to obtain

$$(9.5) \qquad \sum_{\xi,m} (10 X_8 + 5 X_4^2 - 120[x_0^2 x_1^2 x_2^2 x_3^2]_W - X_2^4) = 0 .$$

Thus in (9.2), (9.4) and (9.5) we have proved

<u>Theorem 9.3.</u> <u>For any positive rational integer</u> m <u>and polynomial function</u> $h(X_2)$ <u>of</u> X_2

$$\sum_{\xi,J_w,m} h(X_2) F_r(\xi) = 0$$

<u>when</u>

(i) $F_4(\xi) = 10 X_4 - 3 X_2^2$

(ii) $F_6(\xi) = 8 X_6 - X_2^3$

(iii) $F_8(\xi) = 10 X_8 + 5 X_4^2 - X_2^4 - 120[x_0^2 x_1^2 x_2^2 x_3^2]_W .$

Also F_4, F_6, F_8 are linearly independent and are the only polynomials of weight less than 10 which give identities which can be obtained by this method.

We now consider summations of the form

$$\sum_{\xi, J_s, m} P_r(\xi)$$

where J_s $(1 \leq s \leq 7)$ is one of the seven non maximal arithmetics of C which strictly contain J_0. We define the basic characteristic sets of units for J_s to be

$$(1, i_1', i_2', i_3')$$

and

$$(i_s, i_1' i_s, i_2' i_s, i_3' i_s)$$

where (i_1', i_2', i_3') is the unique proper associative triad of basic units of C with assigned unit i_s. Then the only elements of J_s of norm 1 which do not belong to J_0 are

$$\tfrac{1}{2}(\pm 1 \pm i_1' \pm i_2' \pm i_3')$$

and

$$\tfrac{1}{2}(\pm i_s \pm i_1' i_s \pm i_2' i_s \pm i_3' i_s).$$

For simplicity of notation we consider J_4 for which (i_1', i_2', i_3') equals (i_1, i_2, i_3).

We consider

$$\sum_{\xi,\, J_4,\, m} P_r(\xi).$$

As before, any term of $P_r(\xi)$ which is an odd function of any of the coordinates x_s $(0 \leq s \leq 7)$ of ξ is equivalent to 0 and may therefore be omitted. Now consider any permutation θ with possible sign changes on the units of C for which, if ξ is contained in J_4, $\theta\xi$ is also contained in J_4. Clearly, for all such permutations θ, $N(\theta\xi) = N\xi$. For example, for any unit u of C and element ξ of J_4, we have $u\xi$ contained in J_4. Thus any term x_ℓ^r, $0 \leq \ell \leq 7$, of $P_r(\xi)$ may be replaced by $\frac{1}{8} X_r$ where as before

$$X_r = \sum_{\ell=0}^{7} x_\ell^r.$$

It also follows that any term $x_{\ell_1}^{r_1} x_{\ell_2}^{r_2}$, $\ell_1 \neq \ell_2$, $r_1 + r_2 = r$, of $P_r(\xi)$ is equivalent under summation in J_4 to $x_0^r x_1^{r_2}$ or to $x_0^r x_4^{r_2}$ according as i_{ℓ_1} and i_{ℓ_2} both belong to the same characteristic set for J_4 or not. We define $[x_0^{r_1} x_1^{r_2}]_4$ to be the sum of all terms of the form $x_{\ell_1}^{r_1} x_{\ell_2}^{r_2}$ for which i_{ℓ_1} and i_{ℓ_2} belong to the same characteristic set for J_4 and $[x_0^{r_1} x_4^{r_2}]_4'$ to be the sum of all terms of the form $x_{\ell_1}^{r_1} x_{\ell_2}^{r_2}$ for which i_{ℓ_1} and i_{ℓ_2} belong to different characteristic sets for J_4. Then

$$(9.6) \qquad [x_0^{r_1} x_1^{r_2}] = [x_0^{r_1} x_1^{r_2}]_4 + [x_0^{r_1} x_4^{r_2}]_4'.$$

Similarly we define $[x_0^{r_1} x_1^{r_2} x_2^{r_3}]_4$ and $[x_0^{r_1} x_1^{r_2} x_4^{r_3}]_4'$.

We note that

$$(9.7)\quad [x_0^{r_1} x_1^{r_2} x_2^{r_3}]_4 + [x_0^{r_1} x_1^{r_2} x_4^{r_3}]'_4 = [x_0^{r_1} x_1^{r_2} x_2^{r_3}].$$

For summands involving four variables, we have $[x_0^{r_1}x_1^{r_2}x_2^{r_3}x_3^{r_4}]_4$, $[x_0^{r_1}x_1^{r_2}x_2^{r_3}x_3^{r_4}]'_4$ and $[x_0^{r_1}x_1^{r_2}x_2^{r_3}x_3^{r_4}]''_4$. In the first case all the corresponding units belong to the same characteristic set for J_4, in the second case three units belong to one characteristic set and one to the other and in the third case two belong to each of the characteristic sets. We have

$$(9.8)\quad [x_0^{r_1}x_1^{r_2}x_2^{r_3}x_3^{r_4}]_4 + [x_0^{r_1}x_1^{r_2}x_2^{r_3}x_4^{r_4}]'_4 + [x_0^{r_1}x_1^{r_2}x_4^{r_3}x_5^{r_4}]''_4 = [x_0^{r_1}x_1^{r_2}x_2^{r_3}x_3^{r_4}].$$

We do not proceed further with this argument.

As before we have

<u>Theorem 9.4.</u> <u>For any rational integer</u> t <u>and element</u> ρ <u>of</u> J_s, $(1 \leq s < 7)$, <u>of norm</u> 1

$$\sum_{\xi, J_s, m} R^t(\xi) = \sum_{\xi, J_s, m} R^t(\xi\rho)$$

<u>when</u> $R(\xi)$ <u>denotes the real part of</u> ξ.

Let $n = 4$ and

$$\rho = \tfrac{1}{2}(1 - i_1 - i_2 - i_3).$$

Then

$$R(\xi\rho) = \tfrac{1}{2}(x_0 + x_1 + x_2 + x_3).$$

Similarly if we take

$$\rho_1 = -\tfrac{1}{2}(i_4 + i_5 + i_6 + i_7)$$

we obtain

$$R(\xi \rho_1) = \tfrac{1}{2}(x_4 + x_5 + x_6 + x_7).$$

On adding the corresponding identities of Theorem 9.4 we have

$$(9.9)\quad 2^{t-2}\sum_{\xi, J_4, m} X_t = \sum_{\xi, J_4, m}\{(x_0 + x_1 + x_2 + x_3)^t + (x_4 + x_5 + x_6 + x_7)^t\}.$$

Let $t = 4$ in (9.9) and we obtain

$$\sum_{\xi, J_4, m}\{ X_4 - 2\,[x_0^2 x_1^2]_4\} = 0.$$

When we put $t = 6$, we have

$$16\sum_{\xi, J_4, m} X_6 = \sum_{\xi, J_4, m}\{(x_0 + x_1 + x_2 + x_3)^6 + (x_4 + x_5 + x_6 + x_7)^6\}.$$

Thus

$$\sum_{\xi, J_4, m}\{ X_6 - [x_0^4 x_1^2]_4 - 6\,[x_0^2 x_1^2 x_2^2]_4\} = 0.$$

Finally we let $t = 8$ in (9.9). We then have

$$\sum_{\xi, J_4, m}\{\tfrac{9}{2} X_8 - 2\,[x_0^6 x_1^2]_4 - 5\,[x_0^4 x_1^4]_4 - 30\,[x_0^4 x_1^2 x_2^2]_4 - 180\,[x_0^2 x_1^2 x_2^2 x_3^2]_4\} = 0.$$

Similar arguments hold for any one of the non maximal arithmetics J_s $(1 \leq s \leq 7)$ which strictly contains J_0.

We have therefore proved the following theorem.

Theorem 9.5. For any positive rational integer n and polynomial function $h(X_2)$ of X_2

$$\sum_{\xi, J_3, m} h(X_2)\, F_n(\xi) = 0$$

when

(i) $F_4(\xi) = X_4 - 2\,[x_{l_0}^2 x_{l_1}^2]_S$

(ii) $F_6(\xi) = X_6 - [x_{l_0}^4 x_{l_1}^2]_S - 6\,[x_{l_0}^2 x_{l_1}^2 x_{l_2}^2]_S$

(iii) $F_8(\xi) = 9X_8 - 4[x_{l_0}^4 x_{l_1}^4]_S - 10[x_{l_0}^4 x_{l_1}^2]_S$
$- 60\,[x_{l_0}^4 x_{l_1}^2 x_{l_2}^2]_S - 360\,[x_{l_0}^2 x_{l_1}^2 x_{l_2}^2 x_{l_3}^2]_S$

The square bracket functions are sums of all those terms with suffixes those of units which appear at the same time in one or other of the two basic characteristic sets of units for non maximal arithmetic J_S $(1 \leq s < 7)$.

10. Multiplicative Functions related to Representations in Maximal and Non Maximal Arithmetics strictly containing J_0.

Our object now is to find multiplicative functions of the form

$$f(m) = \sum_{\xi, J_h, m} P_r(\xi) \tag{10.1}$$

where $P_r(\xi)$ is a homogeneous polynomial of weight r in the coordinates $x_0, x_1 \ldots x_7$ of ξ and the summation is over all ξ of norm m in maximal arithmetic $J_h = J_w$ of C $(w = i_1, i_2, \ldots i_7)$ or non maximal arithmetic $J_h = J_s$ of C $(1 \leq s \leq 7)$. We use the results of Theorem 4.6 on the number of representations of a positive rational integer as the norm of an element of J_h. Also we use Theorems 4.7, 4.8, 4.11 and 4.12. It has already been noted in § 6 that Rankin gives a similar discussion for J_0 in his paper [45]. We have seen that the multiplicative functions depending on H derived § 8 are simply related to those depending on H_0 which were constructed by Rankin (l.c.). A simple relation of this type does not exist between the multiplicative functions of the form (10.1) and those depending on J_0.

We deduce from Theorem 4.7, for maximal arithmetic J_w of C,

Theorem 10.1. If $(n,n) = 1$,

$$240 \sum_{\zeta, J_w, n} P_r(\zeta) = \sum_{\xi, J_w, m} \sum_{\eta, J_w, n} P_r(\xi\eta).$$

From Theorem 4.8 we have

Theorem 10.2. If p is an odd rational prime and $\ell > 0$

$$240\sum_{\zeta, J_w, p^{\ell+1}} P_r(\zeta) = \sum_{\xi, J_w p} \sum_{\eta, J_w p^{\ell}} P_r(\xi\eta) - 240\, p^{r+3}\sum_{\zeta', J_w, p^{\ell-1}} P_r(\zeta').$$

For J_s a non maximal arithmetic which strictly contains J_o, we have from Theorem 4.11,

Theorem 10.3. If $(m,n) = 1$

$$48\sum_{\zeta, J_s, mn} P_r(\zeta) = \sum_{\xi, J_s, m} \sum_{\eta, J_s, n} P_r(\xi\eta).$$

Also from Theorem 4.12 it follows that

Theorem 10.4. If p is an odd rational prime and $\ell > 0$

$$48\sum_{\zeta, J_s, p^{\ell+1}} P_r(\zeta) = \sum_{\xi, J_s, p} \sum_{\eta, J_s, p^{\ell}} P_r(\xi\eta) - 48\, p^{r+3}\sum_{\zeta', J_s, p^{\ell-1}} P_r(\zeta').$$

We use Theorems 10.1 and 10.3 to investigate the existence of multiplicative functions of the form (10.1). We must use the identities stated in Theorems 9.3 and 9.5.

First we construct multiplicative functions depending on maximal arithmetic J_w of C. If we put $r = 6$ in Theorem 10.1, $P_6(\xi)$ must be a linear combination of X_6, X_4X_2 and X_2^3. But by (i) and (ii) of Theorem 9.3 we have

$$X_4X_2 \sim \frac{3}{10} X_2^3$$

and

$$X_6 \sim \frac{1}{3} X_2^3.$$

Thus for

$$f(n) = \sum_{s,J_m,m} P_s(\underline{x})$$

to be multiplicative it must be of the form

$$\tfrac{1}{240} n^3 r_w(n).$$

Similarly, for $r = 2,4$, Theorem 10.1 leads to a restatement of the relation

$$240\, r_w(mn) = r_w(n)\, r_w(n) \qquad \text{for} \qquad (m,n) = 1$$

given in Theorem 4.6 (ii).

Since the working involved in constructions involving polynomials of larger weight is prohibitive, we now turn to the case of functions of the form (10.1) for which $J_1 = J_s$ $(1 < s < 7)$. We show that

$$f_4(n) = \tfrac{1}{65} \sum_{s,J_s,m} (10 X_4 - 3 X_2^2) \tag{10.2}$$

is a new definition of a multiplicative function and that it is the only multiplicative function, obtainable by this method by summation of a homogeneous polynomial of weight four, other than

$$\tfrac{1}{48} n^2 r_s(n).$$

To carry out the construction we apply Theorem 10.3 in the case when $r = 4$. First we note that $P_4(\underline{x})$ must be a linear combination of X_4, X_2^2 and $[x_{l_0}^2 x_{l_1}^2]_s$ since as in (9.6)

$$[x_{l_0}^2 x_{l_1}^2]_s + [x_{l_0}^2 x_{l_1}^2]'_s = [x_{l_0}^2]\,[x_{l_1}^2].$$

But by Theorem 9.5 (i)

$$X_4 \equiv 2\,[x_{l_0}^2\, x_{l_1}^2]_5 .$$

Hence

$$[x_{l_0}^2\, x_{l_1}^2]_5' \equiv \tfrac{1}{2} X_2^2 - X_4 .$$

Thus we can write

$$P_4(\xi_5) = a X_4 + b X_2^2$$

for real numbers a and b.

Let

$$f_4(n) = \sum_{x_5, y_5, n} (a X_4 + b X_2^2).$$

Then it is easy to deduce that when $(m,n) = 1$

$$(10.3)\quad f_4(mn) = \frac{1}{r_5} \sum_{\xi_5, x_5, m} \sum_{\eta_5, y_5, n} \Big\{ \tfrac{5}{8} a^2 X_4 Y_4 - \tfrac{3}{16} a\,(X_4 Y_2^2 + X_2^2 Y_4) + (\tfrac{3}{4} a + b)\, X_2^2 Y_2^2 \Big\}.$$

We require that when $(m,n) = 1$

$$f_4(mn) = f_4(m)\, f_4(n).$$

That is

$$(10.4)\quad f_4(mn) = \sum_{\xi_5, x_5, m} \sum_{\eta_5, y_5, n} \Big\{ a^2 X_4 Y_4 + ab\,(X_4 Y_2^2 + X_2^2 Y_4) + b^2 X_2^2 Y_2^2 \Big\}.$$

Hence equating coefficients in (10.3) and (10.4) we have

$$\tfrac{5}{8} a = a^2, \qquad -\tfrac{3}{16} a = ab \qquad \text{and} \qquad \tfrac{1}{32}(\tfrac{3}{4} a + b) = b^2 .$$

Thus

$$a = 0 \text{ and } b = \tfrac{1}{4} \qquad \text{or} \qquad a = \tfrac{5}{4} \text{ and } b = -\tfrac{1}{32}.$$

From the first pair of solutions we get the function

$$\tfrac{1}{48} n^2 r_8(n)$$

while from the second we get (10.2). i.e.

$$r_4(n) = \tfrac{1}{96} \sum_{x,y,z,w} \{10 X_4 - 5 X_2^2\} .$$

We have already noted in Theorem 4.6 (ii) that $\frac{1}{48} n^2 r_8(n)$ is multiplicative. We must now check that X_4, X_2^2 are in fact linearly independent. From this we deduce that (10.2) is a new definition of a multiplicative function. If

$$\tfrac{1}{96} \sum_{x,y,z,w} X_2^2$$

and

$$\tfrac{1}{96} \sum_{x,y,z,w} (10 X_4 - 5 X_2^2)$$

are the same, we must have

$$2 X_4 \equiv X_2^2 .$$

This is certainly true for $n = 1$. But

$$\sum_{x,y,z,w}^{1} X_4 = 2^5 .21$$

while

$$\sum_{x,y,z,w}^{1} X_2^2 = 2^5 .39.$$

The result has thus been proved.

It is of interest to note that the polynomial involved in the identity of Theorem 9.3 (i) and the polynomial used in (10.2) are the same.

TABLE I.

(i)

Associative Triad of Basic Units.			Assigned Basic Unit.
6	5	3	1
1	7	6	2
7	2	5	3
1	2	3	4
6	2	4	5
7	3	4	6
1	4	5	7

(ii)

Associative Triad of Basic Units.			Assigned Basic Unit
je	ie	k	i
i	ke	je	j
ke	j	ie	k
i	j	k	e
je	j	e	ie
ke	k	e	je
i	e	ie	ke

Here we tabulate the proper associative triads of basic units with their corresponding assigned units. In (i) Cayley's notation is used and the basic units are denoted by their suffixes. In (ii) the same table is given using Dickson's notation.

TABLE II.

(i)

0	1	2	3
0	1	4	5
0	1	6	7
0	2	4	7
0	3	4	6
0	2	5	6
0	3	5	7

4	5	6	7
2	3	6	7
2	3	4	5
1	3	5	6
1	2	5	7
1	3	4	7
1	2	4	6

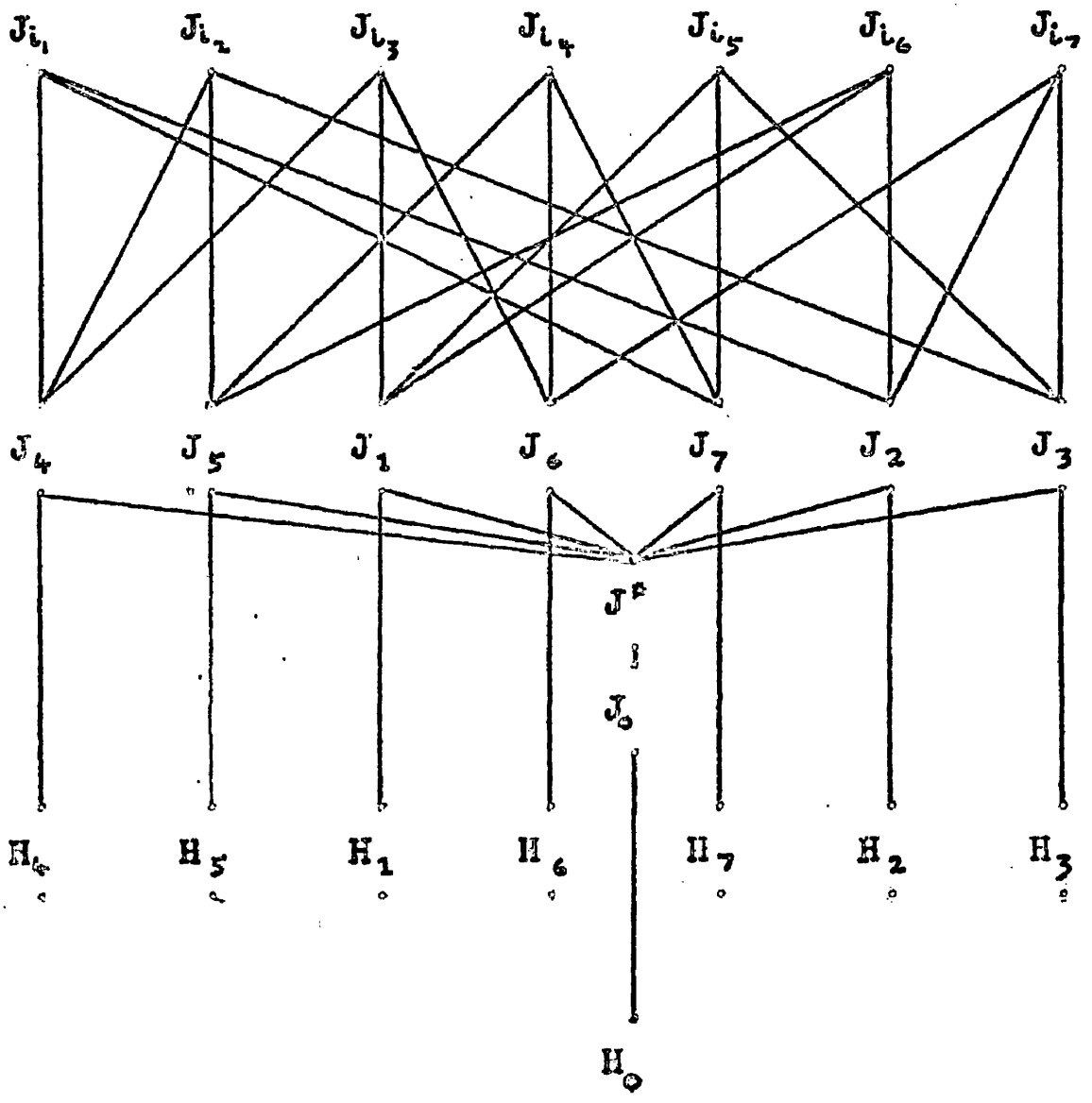
(ii)

1	i	j	k
1	i	e	ie
1	i	je	ke
1	j	e	ke
1	k	e	je
1	j	ie	je
1	k	ie	ke

e	ie	je	ke
j	k	je	ke
j	k	e	ie
i	k	ie	je
i	j	ie	ke
i	k	e	ke
i	j	e	je

Here we tabulate the basic defining sets of units for $J_{i_1} = J_i$. In (i) we use Cayley's notation and write s for i_s $(0 \leq s \leq 7)$ while in (ii) we use Dickson's notation.

TABLE III.


J_{i_1} J_{i_2} J_{i_3} J_{i_4} J_{i_5} J_{i_6} J_{i_7}
J_4 J_5 J_1 J_6 J_7 J_2 J_3
J^p
J_0
H_4 H_5 H_1 H_6 H_7 H_2 H_3
H_0

In Table III we have tabulated the sixteen arithmetics of C which contain J_0 along with the seven isomorphs H_s $(1 \leq s \leq 7)$ of Hurwitz quaternion arithmetic H and H_0. Arithmetics printed in the same line are isomorphic. Two arithmetics are connected by a straight line if and only if the arithmetic below is contained in the one above. We note that each maximal arithmetic J_w contains three isomorphic non maximal arithmetics J_s $(1 \leq s \leq 7)$ while each of the arithmetics J_s is contained in three of the maximal arithmetics J_w.

Bibliography.

1. A. A. Albert, On a certain algebra of quantum mechanics, Annals of Mathematics, (2), vol. 35 (1934), pp. 65 - 73.

2. H. Brandt, Über die Zerlegungsgesetze der rationalen Zahlen in Quaternionen-Körpern, Mathematische Annalen, vol. 117 (1941), pp. 758 - 763.

3. H. Brandt, Zur Zahlentheorie der Quaternionen, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 53 (1943), pp. 23 - 57.

4. R. H. Bruck, Some results in the theory of quasigroups, Transactions of the American Mathematical Society, vol. 55 (1944), pp. 19 - 52.

5. R. H. Bruck, A Survey of Binary Systems, Berlin (1958), pp. 1 - 23, 56 - 59.

6. A. Cayley, Note on a system of imaginaries, Phil. Mag. London, (3), vol.26(1845), p.210. Collected Mathematical Papers, vol. 1, p. 127.

7. A. Cayley, On the eight - square imaginaries, American Journal of Mathematics, vol. 4 (1881), pp. 293 - 296. Collected Mathematical Papers, vol. 11, pp. 368 - 371.

8. H. S. M. Coxeter, Integral Cayley numbers, Duke Mathematical Journal, vol. 13 (1946), pp. 561 - 578.

9. L. E. Dickson, Linear Algebras, Cambridge Tracts in Mathematics and Physics, 16 (1914).

10. L. E. Dickson, On quaternions and their generalization and the history of the eight square theorem, Annals of Mathematics, (2), vol. 20 (1919), pp. 155 - 171, 297.

11. L. E. Dickson, Arithmetic of quaternions, Proceedings of the London Mathematical Society, (2), vol. 20 (1921), pp. 225 - 232.

12. L. E. Dickson, Algebras and Their Arithmetics, Chicago, (1923).

13. L. E. Dickson, A new simple theory of hypercomplex integers, Journal de Mathématiques Pures et Appliquées, (9), vol. 2 (1923), pp. 281 - 326.

14. L. E. Dickson, History of the Theory of Numbers, vol. 2, New York, (1934).

15. M. Eichler, Zur Zahlentheorie der Quaternionen - Algebren, Journal für die reine und angewandte Mathematik, vol. 195 (1956), pp. 127 - 151.

16. J. W. L. Glaisher, Representations of a number as a sum of four squares and on some allied arithmetical functions, Quarterly Journal of Mathmatics, vol. 36 (1905), pp. 305 - 358.

17. J. W. L. Glaisher, The arithmetical functions P(n), Q(n), Ω(n), Quarterly Journal of Mathematics, vol. 37 (1906), pp. 36 - 48.

18. J. W. L. Glaisher, On the representations of a number as the sum of two, four, six, eight, ten and twelve squares, Quarterly Journal of Mathematics, vol. 38 (1907), pp. 1 - 62.

19. J. W. L. Glaisher, On the representations of a number as the sum of fourteen and sixteen squares, Quarterly Journal of Mathematics, vol. 38 (1907), pp. 178 - 236.

20. J. W. L. Glaisher, On the representations of a number as the sum of eighteen squares, Quarterly Journal of Mathematics, vol. 38 (1907), pp.289-351.

21. J. W. L. Glaisher, On elliptic-function expansions in which the coefficients are powers of the complex numbers having n as norm, Quarterly Journal of Mathematics, vol. 39 (1908), pp.266-300.

22. J. W. L. Glaisher, On the number of representations of a number as a sum of 2r squares, where 2r does not exceed eighteen, Proceedings of the London Mathematical Society, (2), vol. 5 (1907), pp.479-490.

23. G. H. Hardy, Ramanujan, Cambridge,(1940).

24. G. H. Hardy and E. M. Wright, The Theory of Numbers, Oxford, (1938), Third Edition, (1954).

25. B. A. Hausmann and O. Ore, Theory of quasigroups, American Journal of Mathematics, vol. 59 (1937), pp. 983 - 1004.

26. A. Hurwitz, Über die Zahlentheorie der Quaternionen, Nachrichten der Gesellschaft der Wissenschaften Göttingen, (1896), pp. 313 - 340.

27. A. Hurwitz, Vorlesungen über die Zahlentheorie der Quaternionen, Berlin, (1919).

28. J. Kirmse, Über die Darstellbarkeit natürlicher ganzer Zahlen als Summen von acht Quadraten und über ein mit diesem Problem zusammenhängendes nicht--kommutatives und nichtassoziatives Zahlensystem, Berichte, Leipzig, vol. 76 (1924), pp. 63 - 82.

29. J. Kirmse, Zur Darstellbarkeit natürlicher ganzer Zahlen als Summen von acht Quadraten, Berichte, Leipzig, vol. 80 (1928), pp. 33 - 34.

30. F. Klein, Elementary Mathematics from an Advanced Standpoint, MacMillan, (1932).

31. D. H. Lehmer, Ramanujan's function $\tau(n)$, Duke Mathematical Journal, vol. 10 (1943), pp. 483-492.

32. Yu. V. Linnik and A. V. Malyšev, Applications of the arithmetic of quaternions to the theory of ternary quadratic forms and to the decomposition of numbers into cubes, American Mathematical Society Translations, (2), vol. 3 (1956), pp. 91 - 162.

33. K. Mahler, On ideals in the Cayley-Dickson algebra, Proceedings of the Royal Irish Academy, (A), vol. 48 (1942), pp. 122 - 133.

34. K. Mahler, A problem of Diophantine approximation in quaternions, Proceedings of the London Mathematical Society, (2), vol. 48 (1945), pp. 435 - 466.

35. A. V. Malyšev, Theory of ternary quadratic forms. I. Arithmetic of hermitions, Vestnik Leningrad. University, vol. 14 (1959), pp. 55 - 71.

36. L. J. Mordell, On the solutions of $x^2+y^2+z^2+t^2=4m_1m_2$, Messenger of Mathematics, vol. 47 (1918), pp. 142 - 144.

37. L. J. Mordell, On the representations of a number as a sum of 2r squares, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 93 - 104.

38. Ruth Moufang, Alternativkörper und der Satz vom vollständigen Vierseit (D_9), Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, vol. 9 (1933), pp. 207 - 222.

39. R. Moufang, Zur Struktur von Alternativkörpern, Mathematische Annalen, vol. 110 (1934), pp. 416 - 430.

40. I. Niven, Sums of fourth powers of Gaussian integers, Bulletin of the American Mathematical Society, vol. 47 (1941), pp. 923 - 926.

41. I. Niven and S. Eilenberg, The "fundamental theorem of algebra" for quaternions, Bulletin of the American Mathematical Society, vol. 50 (1944), pp. 246 - 248.

42. H. Petersson, Über die Entwicklungskoeffizienten der automorphen Formen, Acta Mathematica, vol. 58 (1932), pp. 169 - 215.

43. S. Ramanujan, On certain arithmetic functions, Transactions of the Cambridge Philosophical Society, vol. 22 (1916), pp. 159 - 184. Collected Papers, Cambridge, (1927), pp. 136 - 162.

44. R. A. Rankin, On representations of a number as a sum of squares and certain related identities, Proceedings of the Cambridge Philosophical Society, vol. 41 (1945), pp. 1 - 11.

45. R. A. Rankin, A certain class of multiplicative functions, Duke Mathematical Journal, vol. 13 (1946), pp. 281 - 306.

46. J. Tannery and J. Molk, Fonctions elliptiques, Paris, (1893 - 1902).

47. J. V. Uspensky and M. A. Heaslet, Elementary Number Theory, New York, (1939).

48. B. L. Van der Waerden, Moderne Algebra, Berlin, (1937); New York, (1943).

49. J. Williamson, Hadamard's determinant theorem and the sum of four squares, Duke Mathematical Journal, vol. 11 (1944), pp. 65 - 81.

50. M. Zorn, Theorie der alternativen Ringe, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, vol. 8 (1931), pp. 123-147.

51. A. Hurwitz, Über die Composition der quadratischen Formen von beliebig vielen Variabeln, Nachrichten der Gesellschaft der Wissenschaften Göttingen, (1898), pp. 309-316.

52. L. J. Mordell, On Mr. Ramanujan's empirical expansions of modular functions, Proceedings of the Cambridge Philosophical Society, vol. 19 (1920), pp. 117 - 124.

Index of Definitions.

The numbers opposite each entry refer to section and page respectively. Thus the entry "Prime, Cayley. 4,45" means that a definition of a Cayley prime may be found in §4, page 45. In the text all newly introduced terms are underlined.

On Arithmetics in Cayley's Algebra and Multiplicative Functions.

P. J. C. Lamont.

Summary. The aim of this thesis is to discuss fully the characterisation and basic properties of the arithmetics of Cayley's algebra C and to define certain multiplicative functions by summing homogeneous polynomials in four (or eight) indeterminates over the components of all elements of constant norm m of an arithmetic of C.

The algebra C is introduced by reviewing some of the relevant work by Cayley, Dickson, Artin, Zorn and others. A generalisation of Dickson's condensed law of multiplication is then used to obtain certain automorphisms of C.

The maximal and non maximal arithmetics of C are characterized. Isomorphisms and other relations between certain of the arithmetics are obtained. Treatments of the arithmetics by Coxeter, Dickson and Kirmse are reviewed.

Results on congruence modulo a rational integer in any maximal arithmetic of C are proved. For example, it is shown that

> Any element ξ of odd norm of a maximal arithmetic J_w of C is congruent modulo 2 in J_w to an element, unique apart from sign, of norm 1 of J_w.

This result is used, under certain conditions, to characterize and count the factors of an element of an arithmetic of C.

For example, it is proved that

> Any element ζ of maximal arithmetic J_w of C for which $N\zeta = mn$, where m, n are positive rational integers for which $(m,n) = 1$, has precisely 240 factorizations $\xi\eta$ in J_w such that $N\xi = m$ and $N\eta = n$.

Results on factorization in the arithmetics of C, needed for the construction of multiplicative functions are thus established.

The section on ideals in C contains some improvements on Mahler's results on the same subject. For example, we prove that the basis of any ideal in C is a rational integer.

Finally, a systematic account of identities and multiplicative functions defined as above by using the arithmetics of C not previously used by Rankin for this purpose is given. While the identities and multiplicative functions defined by using Hurwitz maximal quaternion arithmetic are easily related to those constructed by Rankin, the remaining arithmetics not considered by Rankin appear to give new identities and functions.