FACTORIZATION AND ARITHMETIC FUNCTIONS FOR ORDERS IN COMPOSITION ALGEBRAS

by P. J. C. LAMONT

(Received 2 August, 1971)

A well-known product, referred to as the Dirichlet convolution product, is generalized to arithmetic functions defined on an order in a Cayley division algebra. Factorization results for orders, multiplicative functions and analogues of the Moebius inversion formula are discussed.

1. Introduction. Let **C**, with nondegenerate quadratic form N, be a composition algebra over a field k of characteristic other than 2. Then N is a map of **C** into k such that

(i) $N(t\xi) = t^2N(\xi)$ for all $t \in k$ and $\xi \in \mathbf{C}$,
(ii) $(\xi, \eta) = \frac{1}{2}\{N(\xi+\eta)-N(\xi)-N(\eta)\}$ is a bilinear function,
(iii) $N(\xi\eta) = N(\xi)N(\eta)$,
(iv) $(\xi, \eta) = 0$ for all $\xi \in \mathbf{C}$ implies that $\eta = 0$.

An algebra over k satisfying the conditions

$$\xi^2\eta = \xi(\xi\eta) \quad \text{and} \quad \xi\eta^2 = (\xi\eta)\eta \tag{1.1}$$

for all elements ξ, η in the algebra is called alternative. It follows that $\xi(\eta\xi) = (\xi\eta)\xi$. **C** is simultaneously an alternative algebra with an involution $\xi \to \bar{\xi}$ such that

$$\xi\bar{\xi} = N(\xi)1 \quad \text{and} \quad \xi+\bar{\xi} = 2T(\xi)1, \quad \text{where} \quad N(\xi), T(\xi) \in k, \tag{1.2}$$

and a quadratic algebra, since every element ξ of **C** satisfies

$$\xi^2 - 2T(\xi)\xi + N(\xi)1 = 0. \tag{1.3}$$

Since **C** is alternative, the Moufang identities hold:

$$(\xi\alpha)(\beta\xi) = \xi(\alpha\beta)\xi, \tag{1.4}$$

$$(\xi\alpha\xi)\eta = \xi[\alpha(\xi\eta)], \tag{1.5}$$

$$\eta(\xi\alpha\xi) = [(\eta\xi)\alpha]\xi. \tag{1.6}$$

I shall also use

$$T(\xi\eta) = T(\eta\xi), \tag{1.7}$$

$$T[\xi(\eta\zeta)] = T[(\xi\eta)\zeta]. \tag{1.8}$$

Any alternative algebra with an identity and an involution that satisfies (1.2) is a composition algebra.

https://doi.org/10.1017/S0017089500001786 Published online by Cambridge University Press

Given a composition algebra **K**. Take **H** to be the direct sum $\mathbf{K}\oplus\mathbf{K}e$, where $\mathbf{K}e$ is isomorphic to **K** under $\xi\to\xi e$. Define multiplication in **H** by

$$(\xi_1+\xi_2 e)(\eta_1+\eta_2 e)=(\xi_1\eta_1+a\bar{\eta}_2\xi_2)+(\eta_2\xi_1+\xi_2\bar{\eta}_1)e \tag{1.9}$$

for $0\neq a\in k$. Then **H** is a composition algebra if and only if **K** is associative. Also, any composition algebra over a field k may be obtained from $k1$ by applying this Dickson doubling process at most three times. Then **C** is one of the following: $k1$; an algebra $k[e]$ with $e^2=a$; a generalized quaternion algebra; or a generalized Cayley algebra. **C** is a division algebra if and only if the norm N is anisotropic.

Let the ground field be the rationals and take $i_0=1$. By letting $e=i_1$, i_2 and then i_4 with $a=-1$ each time and setting $i_1i_2=i_3$, $i_1i_4=i_5$, $i_2i_4=i_6$ and $i_3i_4=i_7$, we obtain a basis $\{i_s\}_0^7$ for the classical Cayley division algebra **D**.

An order or arithmetic of a composition algebra **C** over a field with a ring of integers is, by definition, a not necessarily associative ring, consists of integral elements only and contains 1. Orders of **C** have been discussed for local and global fields by van der Blij and Springer [**5**]. To introduce composition algebras they allow a ground field of characteristic 2.

If $\mathfrak{o}$ is an order of **D** and if $\mathfrak{o}$ contains a subset of $\{i_s\}$, then by closure of multiplication in $\mathfrak{o}$ the subset has cardinality 1, 2, 4, or 8. Examples of such orders, maximal in the algebra which they span, are: the rational integers **Z**; the Gaussian integers $\mathbf{Z}[i]$; the Hurwitz quaternion order $\mathbf{Z}[i_1,i_2,\rho]$ where $\rho=\frac{1}{2}(1+i_1+i_2+i_3)$; and the isomorphic maximal Cayley arithmetics [**3**]. The orders of **D** used below span the same algebra as does the subset of $\{i_s\}$ that they contain.

Let $\mathfrak{o}$ be an order of **C** in which the number of representations of any integer by norms of elements of $\mathfrak{o}$ is finite. For ξ and $\alpha\in\mathfrak{o}$, α is said to be a left divisor of ξ if ξ has a factorization $\alpha\beta$ in $\mathfrak{o}$, and we write $\alpha\,|\,\xi$. Right divisibility is similarly defined. Next one defines $r_{\mathfrak{o}}(m)$ to be the number of elements of norm m in $\mathfrak{o}$. For $\zeta\in\mathfrak{o}$ and $N\zeta=mn$, $s_{\mathfrak{o}}(\zeta,m,n)$ denotes the number of distinct factorizations $\delta\gamma$ of ζ in $\mathfrak{o}$ with $N\delta=m$ and $N\gamma=n$. When no confusion can arise we omit the suffix $\mathfrak{o}$ and write $r(1)=r$. Formulae for the values of the functions r and s on certain orders of **D** are given in Rankin [**4**] and in [**2**]. The methods of proof used in [**2**] are reviewed in the next section.

2. Factorization.

2. Factorization. Let $\mathfrak{o}$ be an order of **D** which possesses the following properties:

(i) $r(mn)r=r(m)r(n)$ if $(m,n)=1$, (2.1)

(ii) For any $\xi\in\mathfrak{o}$ of odd norm, there exists a unit $\varepsilon\in\mathfrak{o}$ such that $\xi\equiv\varepsilon(\text{mod }2)$. (2.2)

Then we are able to prove the theorem:

(2.3) *Any element $\zeta\in\mathfrak{o}$ with $N\zeta=mn$ has precisely r different factorizations $\xi\eta$ in $\mathfrak{o}$ with $N\xi=m$ and $N\eta=n$, if $(m,n)=1$. Moreover, for m odd, the factorization is unique apart from signs if a unit ε is prescribed to which ξ is congruent modulo 2.*

Proof. Suppose that $\zeta=\xi_1\eta_1=\xi_2\eta_2$, where $\xi_1\neq\pm\xi_2$ and $N\xi_1=N\xi_2=m$ is odd.

https://doi.org/10.1017/S0017089500001786 Published online by Cambridge University Press

Then $|T(\bar{\xi}_1 \xi_2)| < m$. By (1.1), $\zeta\bar{\eta}_1 = n\xi_1$ and $\zeta\bar{\eta}_2 = n\xi_2$. Hence $(\eta_1 \bar{\zeta})(\zeta\bar{\eta}_2) = n^2\bar{\xi}_1 \xi_2$. By (1.8), $mT(\eta_1 \bar{\eta}_2) = nT(\bar{\xi}_1 \xi_2)$.

Assume that $\xi_1 \equiv \xi_2 \pmod 2$. Then $\xi_1 \bar{\xi}_2 \equiv 1 \pmod 2$. Hence $\bar{\xi}_1 \xi_2$ has integral coefficients with respect to $\{i_s\}_0^7$. Thus, since $m \mid T(\bar{\xi}_1 \xi_2)$, we have that $T(\bar{\xi}_1 \xi_2) = 0$.

Again, since $N(\bar{\xi}_1 \xi_2) = m^2$, it follows that $\bar{\xi}_1 \xi_2$ has precisely one or five odd rational integral coefficients. Hence, using (2.2), $\xi_1 \bar{\xi}_2 \equiv i_s \pmod 2$ for some s $(1 \leqq s \leqq 7)$. This is a contradiction. Therefore $\xi_1 \not\equiv \xi_2 \pmod 2$. Again by (2.2), ζ has at most r factorizations $\xi\eta$.

Now consider all $\zeta \in \mathfrak{o}$ with norm mn. Suppose that there is some $\zeta \in \mathfrak{o}$ with strictly less than r factorizations of the required form. Then

$$r(m)r(n) < r \sum_{N\zeta = mn} 1 = r(mn)r.$$

This contradicts (2.1). If m is even, apply the argument to $s(\zeta, n, m)$. The theorem is thus proved.

Use of the alternative laws and the Moufang identities yields results of the following form.

(2.4). *For* ε *any unit in* $\mathfrak{o}$, $s(\zeta, m, n) = s(\zeta\varepsilon, m, n)$.

Proof. If $\zeta = \xi\eta$, then $\zeta\varepsilon = \{[(\xi\bar{\varepsilon})\varepsilon]\eta\}\varepsilon = (\xi\bar{\varepsilon})(\varepsilon\eta\varepsilon)$.

An element $\zeta \in \mathfrak{o}$ of odd norm is called primitive if $\zeta \not\equiv 0 \pmod p$ for any rational prime p.

Suppose now that, for the order $\mathfrak{o}$,

$$r(p^{t+1})r = r(p)r(p^t) + r(p^{t-1})[r - r(p)] \tag{2.5}$$

when the integer $t > 0$. Then the following theorem holds:

(2.6). *Any element* $\zeta \in \mathfrak{o}$, *with* $N\zeta = p^{t+1}$, *where* p *is an odd rational prime and the integer* $t > 0$, *has precisely*

(i) $r(p)$ *distinct factorizations* $\xi\eta$ *with* $N\xi = p$ *and* $N\eta = p^t$, *if* $\zeta \equiv 0 \pmod p$,

(ii) r *such factorizations, if* ζ *is primitive.*

Proof. (i) $\zeta = p\zeta'$, where $\zeta' \in \mathfrak{o}$. Let ξ be any element of norm p in $\mathfrak{o}$ and let $\eta = \bar{\xi}\zeta'$. Then $\xi\eta = \zeta$. Thus ζ has precisely as many distinct factorizations $\xi\eta$ of the required form as there are elements of norm p in $\mathfrak{o}$.

(ii) Suppose that ζ has distinct factorizations $\xi_1\eta_1$ and $\xi_2\eta_2$ in $\mathfrak{o}$ with $N\xi_1 = N\xi_2 = p$ and $\xi_1 \neq \pm\xi_2$. Assume that $\xi_1 \equiv \xi_2 \pmod 2$. Then $\xi_1 \bar{\xi}_2 \equiv 1 \pmod 2$. Hence $\xi_1 \bar{\xi}_2$ has integral coefficients with respect to the basis $\{i_s\}_0^7$.

Now, by (1.7) and (1.8),

$$T\{\xi_1(\bar{\xi}_2\zeta) + (\bar{\zeta}\xi_1)\bar{\xi}_2\} = 2T(\zeta)T(\xi_1 \bar{\xi}_2).$$

Also $\xi_1(\bar{\xi}_2\zeta) = p\xi_1\eta_2$ and $(\bar{\zeta}\xi_1)\bar{\xi}_2 = p\bar{\eta}_1 \bar{\xi}_2$. Hence, using (2.4), p divides $T(\xi_1 \bar{\xi}_2)$. Since $\xi_1 \neq \pm\xi_2$, $\xi_1 \bar{\xi}_2 \neq \pm p$. But $N(\xi_1 \bar{\xi}_2) = p^2$. Hence $T(\xi_1 \bar{\xi}_2) = 0$ and $\xi_1 \bar{\xi}_2$ has precisely one or five odd rational integral coefficients. Thus $\xi_1 \bar{\xi}_2$ is congruent modulo 2 to one of $\{i_s\}_1^7$. This contradicts the fact that $\xi_1 \bar{\xi}_2 \equiv 1 \pmod 2$. Therefore $\xi_1 \not\equiv \xi_2 \pmod 2$.

https://doi.org/10.1017/S0017089500001786 Published online by Cambridge University Press

We have proved that there are at most r distinct factorizations $\xi\eta$ of ζ in $\mathfrak{o}$ with $N\xi = p$. Suppose that, for some ζ of norm p^{t+1}, there are less than r such factorizations. Then

$$\begin{aligned} r(p)r(p^t) &< r \sum_{\substack{N\zeta = p^{t+1} \\ p \nmid \zeta}} 1 + r(p) \sum_{\substack{N\zeta = p^{t+1} \\ p \mid \zeta}} 1 \\ &= r(p^{t+1})r - r(p^{t-1})r + r(p)r(p^{t-1}) \\ &= r(p^{t+1})r + r(p^{t-1})[r(p) - r]. \end{aligned}$$

This contradicts (2.5) and completes the proof of the theorem.

An element $\xi \in \mathfrak{o}$ with $N\xi \neq 1$ is called irreducible if $\xi = \gamma\delta$ in $\mathfrak{o}$ implies that one of γ and δ is a unit of $\mathfrak{o}$. If ξ has norm a prime, then ξ is irreducible.

Theorems (2.3) and (2.6) show that in, for example, the maximal Cayley arithmetics of **D**, unique factorization, apart from signs, order and parentheses, holds for primitive elements, provided that units are prescribed to which the irreducible factors are congruent modulo 2 and provided that parentheses are used in such a way that Theorem (2.6) is applicable.

Axiom (2.2) fails in the nonmaximal orders $\mathbf{J}_1 = \mathbf{Z}[i_1, i_2, i_3]$ and $\mathbf{J}_2 = \mathbf{Z}[i_1, \ldots, i_7]$. Factorization results for $\mathbf{J}_s (s = 1, 2)$ may be deduced from (2.3) and (2.6). Consider congruence modulo 2 in corresponding maximal quaternion and Cayley orders. Note that, if $\xi \equiv \varepsilon \pmod 2$, then $\xi \in \mathbf{J}_s$ if and only if $\varepsilon \in \mathbf{J}_s$. Thus we need only consider factorizations corresponding to units of the orders $\mathbf{J}_s$.

3. Arithmetic functions. Here the composition algebra **C**, defined over the field of rational numbers, is assumed to be a division algebra. Again $\mathfrak{o}$ is an order in **C** and $r_{\mathfrak{o}}(m)$ is finite for all integers m.

A function f with domain $\mathfrak{o}$ and codomain the field of complex numbers is called arithmetic. Let $\mathfrak{A}$ denote the set of all arithmetic functions on $\mathfrak{o}$.

Suppose that f and $g \in \mathfrak{A}$. A product $f \cdot g$ is defined by

$$f \cdot g(\xi) = \frac{1}{r} \sum_{\delta \mid \xi} f(\delta) g(\delta^{-1}\xi), \tag{3.1}$$

where the sum extends over all left divisors δ of ξ in $\mathfrak{o}$. Then $f \cdot g \in \mathfrak{A}$. Also

$$f \cdot g(\xi) = \frac{1}{r} \sum_{\alpha\beta = \xi} f(\alpha) g(\beta), \tag{3.2}$$

where the summation is over all ordered pairs α, β of elements of $\mathfrak{o}$ with the product $\alpha\beta$ equal to ξ.

First we consider the following symmetry properties:

$$f(\varepsilon\xi) = f(\xi\varepsilon) = f(\xi) \quad \text{for all} \quad \xi \quad \text{and units} \quad \varepsilon \in \mathfrak{o}, \tag{3.3}$$

$$f(\xi) = f(\bar{\xi}) \quad \text{for all} \quad \xi \in \mathfrak{o}. \tag{3.4}$$

Let $\mathfrak{A}_1$ be the set of all elements in $\mathfrak{A}$ satisfying (3.3).

(3.5). $\mathfrak{A}_1$ *is closed.*

Proof. Take $f, g\in\mathfrak{A}_1$ and $\xi, \varepsilon\in\mathfrak{o}$ with ε a unit. Using the Moufang identity (1.5), we have

$$f\cdot g(\varepsilon\xi)=\frac{1}{r}\sum_{\alpha\beta=\varepsilon\xi}f(\alpha)g(\beta)=\frac{1}{r}\sum_{\bar\varepsilon\{\alpha[\bar\varepsilon(\varepsilon\beta)]\}=\xi}f(\alpha)g(\beta)=\frac{1}{r}\sum_{(\bar\varepsilon\alpha\bar\varepsilon)(\varepsilon\beta)=\xi}f(\bar\varepsilon\alpha\bar\varepsilon)g(\varepsilon\beta)=f\cdot g(\xi).$$

Now from (1.4) we deduce that

$$f\cdot g(\varepsilon\xi)=\frac{1}{r}\sum_{(\bar\varepsilon\alpha)(\beta\bar\varepsilon)=\xi\bar\varepsilon}f(\bar\varepsilon\alpha)g(\beta\bar\varepsilon)=f\cdot g(\xi\bar\varepsilon).$$

Thus $f\cdot g\in\mathfrak{A}_1$.

Now suppose that functions f and $g\in\mathfrak{A}$ satisfy (3.4). Then

$$f\cdot g(\xi)=\frac{1}{r}\sum_{\gamma\delta=\bar\xi}f(\gamma)g(\delta)=\frac{1}{r}\sum_{\alpha\beta=\xi}g(\alpha)f(\beta)=g\cdot f(\xi).$$

For an arithmetic function f, f^* is defined to be the restriction of f to the integers $\mathbf{Z}$. For f, g and $h\in\mathfrak{A}$ we have $f\cdot g^*=g\cdot f^*$ and $(f\cdot g)\cdot h^*=f\cdot(g\cdot h)^*$.

Now define a function e by

$$e(\xi)=\begin{cases}1 & \text{if } \xi \text{ is a unit}\\ 0 & \text{otherwise.}\end{cases}\tag{3.6}$$

Clearly $e\in\mathfrak{A}_1$ and e satisfies (3.4). Now for $f\in\mathfrak{A}_1$ we have

$$f\cdot e(\xi)=\frac{1}{r}\sum_{\alpha\beta=\xi}f(\alpha)e(\beta)=\frac{1}{r}\sum_{N\varepsilon=1}f(\xi\bar\varepsilon)=f(\xi).$$

Similarly $e\cdot f=f$. Hence e is the unique identity for $\mathfrak{A}_1$.

(3.7). *For $f\in\mathfrak{A}_1$, a right inverse $f'\in\mathfrak{A}_1$ exists if and only if $f(1)\neq 0$.*

Proof. Note that, if $f\in\mathfrak{A}_1$, then $f(\varepsilon)=f(1)$ for all units $\varepsilon\in\mathfrak{o}$. Suppose that $f'\in\mathfrak{A}_1$ exists. Then $1=e(1)=f\cdot f'(1)=f(1)f'(1)$, by (3.2) and (3.3). Therefore $f(1)\neq 0$.

Now assume that $f(1)\neq 0$. Define f' inductively as follows.

$$f'(\xi)=\begin{cases}[f(1)]^{-1}, & \text{if } \xi \text{ is a unit,}\\ -[rf(1)]^{-1}\displaystyle\sum_{\substack{\alpha\beta=\xi\\ N\alpha\neq 1}}f(\alpha)f'(\beta), & \text{otherwise.}\end{cases}\tag{3.8}$$

An induction argument using the Moufang identities (1.5) and (1.6) shows that $f'\in\mathfrak{A}_1$. Next, for ε a unit,

$$f\cdot f'(\varepsilon)=\frac{1}{r}\sum_{N\varepsilon_1=1}f(\varepsilon_1)f'(\bar\varepsilon_1\varepsilon)=\frac{1}{r}\sum_{N\varepsilon_1=1}f(1)f'(1)=1.$$

https://doi.org/10.1017/S0017089500001786 Published online by Cambridge University Press

For ξ with $N\xi \neq 1$, we have

$$\begin{aligned} f\cdot f'(\xi) &= \frac{1}{r}\sum_{\alpha\beta=\xi} f(\alpha)f'(\beta) \\ &= \frac{1}{r}\sum_{N\varepsilon=1} f(\varepsilon)f'(\xi)+\frac{1}{r}\sum_{\substack{\alpha\beta=\xi\\ N\alpha\neq 1}} f(\alpha)f'(\beta) \\ &= f(1)f'(\xi)-f(1)f'(\xi) = 0. \end{aligned}$$

Hence $f\cdot f' = e$ and f' is a right inverse for f.

If $f\in\mathfrak{A}_1$ satisfies (3.4), then f' is a left inverse for f under the convolution product defined by

$$f\times g(\xi) = \frac{1}{r}\sum_{\alpha\beta=\xi} f(\beta)g(\alpha)$$

with summation as before. If $f\in\mathfrak{A}_1$ and both f and f' satisfy (3.4), then

$$f'\cdot f(\xi) = f\cdot f'(\bar{\xi}) = e(\bar{\xi}) = e(\xi).$$

Hence $f'\cdot f = e$ and f' is also a left inverse.

4. Multiplicative functions. Let $\mathfrak{o}$ again be an order of the Cayley division algebra over the rationals. We consider orders $\mathfrak{o}$ in which, for $N\zeta = uv$, $s(\zeta, u, v) = r$ if $(u, v) = 1$ or if ζ is primitive.

An arithmetic function f on $\mathfrak{o}$ is said to be multiplicative if it possesses the property

$$f(\xi\eta) = f(\xi)f(\eta) \tag{4.1}$$

when $\xi, \eta\in\mathfrak{o}$ and $(N\xi, N\eta) = 1$. Let $\mathfrak{M}$ denote the set of all nonzero multiplicative functions in $\mathfrak{A}_1$.

(4.2). *If f and $g\in\mathfrak{M}$, then $f\cdot g^*\in\mathfrak{M}$.*

Proof.

$$f\cdot g(1) = \frac{1}{r}\sum_{N\varepsilon=1} f(\varepsilon)g(\bar{\varepsilon}) = 1.$$

Now take positive integers m and n with $(m, n) = 1$.

$$f\cdot g(mn) = \frac{1}{r}\sum_{\xi\mid mn} f(\xi)g(\xi^{-1}mn).$$

We may write $\xi = \xi_1\xi_2$ in any one of r ways where $\xi_1\mid m$ and $\xi_2\mid n$ and $N\xi_1$ and $N\xi_2$ are fixed. Conversely, by (1.7) and (1.8), if $\xi_1\mid m$ and $\xi_2\mid n$, then $\xi_1\xi_2\mid mn$. Hence

$$f\cdot g(mn) = \frac{1}{r^2}\sum_{\substack{\xi_1\mid m\\ \xi_2\mid n}} f(\xi_1\xi_2)g(\xi_2^{-1}n\xi_1^{-1}m) = f\cdot g(m)f\cdot g(n).$$

For $\xi, \eta \in \mathfrak{o}$, $\xi \sim \eta$ means that $N\xi = N\eta$ and, for $p \in Z$, $p^m | \xi$ if and only if $p^m | \eta$. Take $\xi \sim \eta$ in $\mathfrak{o}$. Let β, γ be any left (or right) divisors of ξ, η, respectively, in $\mathfrak{o}$, such that $\beta \sim \gamma$. If $s(\beta, u, v) = s(\gamma, u, v)$ for all positive integers u, v with uv equal to the common norm, we shall write $s(\xi) = s(\eta)$. Henceforth it is assumed that, in $\mathfrak{o}$, $\xi \sim \eta$ implies that $s(\xi) = s(\eta)$.

I shall consider functions f satisfying the condition

$$f(\xi_1) = f(\xi_2) \quad \text{if} \quad \xi_1 \sim \xi_2. \tag{4.3}$$

(4.4). *If arithmetic functions f and g satisfy* (4.3), *then so does $f \cdot g$.*

Proof. Take $\xi_1 \sim \xi_2$. Let there be t integral elements β of fixed norm n such that $\beta | \xi_1$. Then

$$s(\xi_1, n, n^{-1}N\xi_1) = s(\xi_2, n, n^{-1}N\xi_2).$$

Therefore there are t elements $\gamma \in \mathfrak{o}$ of norm n that are left divisors of ξ_2. Also, if $p^m | \beta$, then $p^m | \xi_1$, and hence $p^m | \xi_2$. Let $\xi_s = p^m \xi'_s$ $(s = 1, 2)$. Then

$$s(\xi'_1, np^{-2m}, n^{-1}N\xi_1) = s(\xi'_2, np^{-2m}, n^{-1}N\xi_2).$$

Hence there is a one-to-one correspondence between the elements β and the elements γ under which $\beta \sim \gamma$. A similar result holds for the corresponding right divisors.

$$f \cdot g(\xi_1) = \frac{1}{r} \sum_{\beta | \xi_1} f(\beta) g(\beta^{-1}\xi_1) = \frac{1}{r} \sum_{\gamma | \xi_2} f(\gamma) g(\gamma^{-1}\xi_2) = f \cdot g(\xi_2).$$

(4.5). *If an arithmetic function h satisfies* (4.3) *and if* $h(1) \neq 0$, *then $h' \in \mathfrak{A}_1$ exists and satisfies* (4.3).

Proof. For ε a unit of $\mathfrak{o}$, $h'(\varepsilon) = [1/h(1)] = h'(1)$. Assume that (4.3) holds for h' whenever $N\xi_1 = N\xi_2 < N\xi$. Take $\xi \sim \eta$. Then, as in the proof of (4.4),

$$h'(\xi) = \frac{-1}{rh(1)} \sum_{\substack{\alpha\beta = \xi \\ N\alpha \neq 1}} h(\alpha) h'(\beta) = \frac{-1}{rh(1)} \sum_{\substack{\gamma\delta = \eta \\ N\gamma \neq 1}} h(\gamma) h'(\delta) = h'(\eta).$$

Let $\mathfrak{M}_1$ be the set of all functions $f \in \mathfrak{M}$ satisfying (4.3).

(4.6). *If f and $g \in \mathfrak{M}_1$, then*

$$f \cdot g(\xi\eta) = f \cdot g(\xi) f \cdot g(\eta)$$

if ξ and η are primitive in $\mathfrak{o}$ and if $(N\xi, N\eta) = 1$.

$f \cdot g$ is then said to be multiplicative on primitive elements.

Proof: $f \cdot g(\xi\eta) = \frac{1}{r} \sum_{\delta | \xi\eta} f(\delta) g[\delta^{-1}(\xi\eta)]$.

Suppose that $\xi, \eta \in \mathfrak{o}$ are primitive and that $(N\xi, N\eta) = 1$. For fixed norm n there are r left divisors δ of $\xi\eta$ with $N\delta = n$ provided that $n | N(\xi\eta)$. Let $\delta = \alpha\beta$, where $N\alpha | N\xi$ and

$N\beta \mid N\eta$. There are r such factorizations of each δ for fixed $N\alpha$ and $N\beta$. Now $\xi = \alpha_1\xi_1$ and $\eta = \beta_1\eta_1$ each in any one of r ways where $N\alpha_1 = N\alpha$, $N\beta_1 = N\beta$. Then $\alpha_1 \sim \alpha$ and $\beta_1 \sim \beta$. Also $(\alpha\beta)^{-1}(\xi\eta) \sim (\alpha_1^{-1}\xi)(\beta_1^{-1}\eta)$.

$$f\cdot g(\xi\eta) = \frac{1}{r^2}\sum_{\alpha\beta \mid \xi\eta} f(\alpha\beta)g[(\alpha\beta)^{-1}(\xi\eta)] = \frac{1}{r^2}\sum_{\substack{\alpha_1 \mid \xi \\ \beta_1 \mid \eta}} f(\alpha_1\beta_1)g[(\alpha_1^{-1}\xi)(\beta_1^{-1}\eta)] = f\cdot g(\xi)f\cdot g(\eta).$$

For any complex number x, arithmetic functions n_x are defined by $n_x(\xi) = (N\xi)^x$. Then $n_x \in \mathfrak{M}_1 \subseteq \mathfrak{M}$.

(4.7) *Let* $g(\xi) = \frac{1}{r}\sum_{\delta \mid \xi} f(\delta)$.

(i) *If* $f \in \mathfrak{M}$, *then* $g^* \in \mathfrak{M}$.

(ii) *If* $f \in \mathfrak{M}_1$, *then* g *is multiplicative on primitive elements.*

Proof. $g = f\cdot n_0$. The results follow by (4.2) and (4.6) respectively.

(4.8). *If* $f \in \mathfrak{M}_1$, *then* f' *is multiplicative on primitive elements.*

Proof. f' exists and satisfies (4.3). $f'(\varepsilon) = 1$ for any unit $\varepsilon \in \mathfrak{o}$.

Assume that $f'(\alpha\beta) = f'(\alpha)f'(\beta)$ for all primitive $\alpha, \beta \in \mathfrak{o}$ with $(N\alpha, N\beta) = 1$ and $N(\alpha\beta) < b$. Choose primitive $\xi, \eta \in \mathfrak{o}$ with $(N\xi, N\eta) = 1$ and $N\xi N\eta = b$. Then

$$\begin{aligned} 0 = e(\xi\eta) &= f\cdot f'(\xi\eta) \\ &= \frac{1}{r}\sum_{\delta \mid \xi\eta} f(\delta)f'[\delta^{-1}(\xi\eta)] \\ &= \frac{1}{r^2}\sum_{\substack{\alpha \mid \xi \\ \beta \mid \eta \\ N\alpha\beta \neq 1}} f(\alpha\beta)f'[(\alpha^{-1}\xi)(\beta^{-1}\eta)] + \frac{1}{r^2}\sum_{N\varepsilon_1\varepsilon_2 = 1} f'(\xi\eta) \\ &= \frac{1}{r^2}\sum_{\alpha \mid \xi} f(\alpha)f'(\alpha^{-1}\xi)\sum_{\beta \mid \eta} f(\beta)f'(\beta^{-1}\eta) - f'(\xi)f'(\eta) + f'(\xi\eta) \\ &= f\cdot f'(\xi)f\cdot f'(\eta) - f'(\xi)f'(\eta) + f'(\xi\eta). \end{aligned}$$

Thus $f'(\xi\eta) = f'(\xi)f'(\eta)$.

5. Moebius inversion. Let $\mu = n_0'$. Then μ is multiplicative on primitive elements and on $\mathbf{Z}$.

(5.1). *If* $\xi \in \mathfrak{o}$ *and* $N\xi > 1$, *then* $\sum_{\eta \mid \xi} \mu(\eta^{-1}\xi) = 0$.

Proof. $\frac{1}{r}\sum_{\eta \mid \xi} \mu(\eta^{-1}\xi) = \frac{1}{r}\sum_{\eta \mid \xi} n_0(\eta)\mu(\eta^{-1}\xi) = n_0\cdot\mu(\xi) = e(\xi) = 0.$

https://doi.org/10.1017/S0017089500001786 Published online by Cambridge University Press

(5.2). *$\mu(\xi) = -1$, if ξ is irreducible in $\mathfrak{o}$.*

Proof. $0 = \frac{1}{r}\sum_{\delta \mid \xi} \mu(\delta^{-1}\xi) = \frac{1}{r}\sum_{N\varepsilon=1} \mu(\xi) + \frac{1}{r}\sum_{N\varepsilon=1} \mu(\varepsilon) = \mu(\xi)+1.$

Hence

(5.3). *If η is any product of t primitive irreducible elements of $\mathfrak{o}$ with distinct norms, then $\mu(\eta) = (-1)^t$.*

Now it is easy to prove

(5.4). *For rational prime p, $\mu(p) = (1/r)r(p)-1$.*

Proof. $0 = \frac{1}{r}\sum_{\delta \mid p} \mu(\delta) = \frac{1}{r}\sum_{N\varepsilon=1} \mu(\varepsilon) + \frac{1}{r}\sum_{N\delta=p} \mu(\delta) + \frac{1}{r}\sum_{N\varepsilon=1} \mu(p) = 1 - \frac{1}{r}r(p) + \mu(p).$

We recall that, in $\mathbf{Z}$, $r(p) = 0$ and, in the Gaussian integers, for odd p,

$$r(p) = 4\{1+(-1)^{\frac{1}{2}(p-1)}\}.$$

(5.5). *If $N\zeta = p^2$, then $\mu(\zeta) = (1/r)s(\zeta, p, p)-1$.*

Proof. $0 = \frac{1}{r}\sum_{N\varepsilon=1} \mu(\zeta) + \frac{1}{r}\sum_{\substack{N\delta=p \\ \delta \mid \zeta}} \mu(\bar{\delta}) + \frac{1}{r}\sum_{N\varepsilon=1} \mu(\varepsilon) = \mu(\zeta) - \frac{1}{r}s(\zeta, p, p) + \mu(1).$

(5.6). *If $N\zeta = p^k$, where ζ is primitive, p is a prime and $k \geqq 2$, then $\mu(\zeta) = 0$.*

Proof. For $k = 2$, $\mu(\zeta) = 0$ by (5.5). The result follows by induction.

μ defined on $\mathbf{Z}$ is the well-known Moebius function. For μ defined on $\mathfrak{o}$, the following inversion formula holds.

(5.7). *Under any condition or restriction that makes the convolution product associative and for any arithmetic functions f and $g \in \mathfrak{A}_1$,*

$$g(\xi) = \frac{1}{r}\sum_{\eta \mid \xi} f(\eta) \quad \textit{if and only if} \quad f(\xi) = \frac{1}{r}\sum_{\eta \mid \xi} g(\eta)\mu(\eta^{-1}\xi).$$

Proof. $g = f \cdot n_0$. Thus $g \cdot \mu = f$. Conversely, by (4.5), μ satisfies (3.4) and is therefore a left inverse for n_0.

The theorem may be generalized by replacing n_0 by any function $h \in \mathfrak{A}_1$ with an inverse h', provided that the function and the inverse satisfy (3.4). Any $h \in \mathfrak{A}_1$ that satisfies (4.3) and has $h(1) \neq 0$ would be suitable.

REFERENCES

1. N. Jacobson, Composition algebras and their automorphisms, *Rend. Circ. Mat. Palermo* **7** (1958), 55–80.

2. P. J. C. Lamont, *On arithmetics in Cayley's algebra and multiplicative functions*, Thesis, Glasgow (1962).

https://doi.org/10.1017/S0017089500001786 Published online by Cambridge University Press

3. P. J. C. Lamont, Arithmetics in Cayley's algebra, *Proc. Glasgow Math. Assoc.* **6** (1963), 99–106.

4. R. A. Rankin, A certain class of multiplicative functions, *Duke Math. J.* **13** (1946), 281–306.

5. F. van de Blij and T. A. Springer, The arithmetics of the octaves and of the group G_2, *Nederl. Akad. Wetensch. Proc.* **62** A (1959), 406–418.

St. Mary's College
and
University of Notre Dame
Notre Dame, Indiana 46556