RINGS OF ARITHMETIC FUNCTIONS

L. CARLITZ

1. Introduction. Let F denote a fixed but arbitrary field and let Z denote the set of positive integers. By an *arithmetic function* f is meant a function from Z to F, that is to say $f(n) \in F$ for all $n \in Z$. If f, g are two arithmetic functions, the sum $h = f + g$ is defined by means of

$$h(n) = f(n) + g(n) \qquad (n \in Z) . \tag{1}$$

There are two products that are of interest, the *ordinary* product defined by

$$h(n) = f(n)g(n) \qquad (n \in Z) , \tag{2}$$

and the Dirichlet product defined by

$$h(n) = \sum_{rs=n} f(r)g(s) \qquad (n \in Z) , \tag{3}$$

where the summation on the right is extended over all factorizations $rs = n$. We shall denote the ordinary product by $f \circ g$ and the Dirichlet product by $f * g$.

Let S denote the set of arithmetic functions as defined above. It is well known and easy to prove that the system

$$\Omega = (S, f, \circ) \tag{4}$$

is a commutative ring. The multiplicative identity of Ω is defined by

$$v(n) = 1 \qquad (n \in Z) . \tag{5}$$

Clearly Ω is not a domain of integrity; note however that there are no nilpotent elements in Ω. On the other hand the system

$$\Delta = (S, f, *) \tag{6}$$

is a domain of integrity. The multiplicative identity of Δ is given by

$$u(n) = \begin{cases} 1 & (n = 1) \\ 0 & (n > 1) . \end{cases} \tag{7}$$

Moreover the function f has an inverse (relative to $*$) if and only if

$$f(1) \neq 0 ; \tag{8}$$

Received September 15, 1963, and in revised form November 12, 1963. Supported in part by NSF grant G16485.

the set of functions that satisfy (8) evidently constitute an abelian group with respect to $*$.

If $\lambda \in F$ we define the function λf by means of

$$(9) \qquad (\lambda f)(n) = \lambda \cdot f(n) \qquad (n \in Z) .$$

It follows at once that S is a vector space over F of infinite dimension. Also we have

$$\lambda(f \circ g) = (\lambda f) \circ g = f \circ (\lambda g) , \qquad \lambda(f * g) = (\lambda f) * g = f * (\lambda g) .$$

If in place of Z we employ a semigroup J that has no units except the identity, a countable infinity of primes, and which has the unique factorization property, the resulting systems Ω and Δ are not essentially different. Indeed if $\overline{p}_1, \overline{p}_2, \overline{p}_3, \cdots$ denote the primes of J we may set up the correspondence $f \rightleftarrows \overline{f}$ by means of $f(n) = \overline{f}(\overline{n})$, where

$$(10) \qquad n = \Pi p_j^{e_j} , \qquad \overline{n} = \Pi \overline{p}_j^{e_j} ,$$

where the first half of (10) is the usual factorization of n into primes. There is therefore little loss in generality in restricting the discussion to Z.

In view of the above it is of interest to consider the system

$$(11) \qquad \Phi = (S, +, \circ, *)$$

with three binary operations and in particular to attempt to give an abstract formulation of such systems. Since $\circ$ and $*$ do not combine in any very obvious way, it is perhaps not clear how this can be done. We shall obtain such a characterization by making use of *minimal* functions. A function f is minimal provided there exists an integer k (depending on f) such that

$$(12) \qquad f(n) = 0 \ (n \neq k) ; \qquad f(k) \neq 0 .$$

We remark that Cashwell and Everett [1] have proved that Δ is a unique factorization domain. However this result will not be required in what follows.

2. As above let F denote a fixed but arbitrary field. Let $\overline{S}$ denote a vector space over F. The elements of $\overline{S}$ will be denoted by small italic letters, the elements of F by small Greek letters; addition in $\overline{S}$ will be denoted by $+$. Moreover we have two "multiplications" denoted by $\circ$ and $*$. The following assumptions will be made.

S1. The system

$$(13) \qquad \Omega = (\overline{S}, +, \circ)$$

is a commutative ring with multiplicative identity $\bar{v}$. Moreover

$$\alpha(\bar{f}\circ\bar{g}) = (\alpha\bar{f})\circ\bar{g} = \bar{f}\circ(\alpha\bar{g}) \qquad (\bar{f}, \bar{g}\in\bar{S}, \alpha\in F) .$$

S2. The system

$$\bar{\Delta} = (\bar{S}, +, *) \tag{14}$$

is a domain of integrity with multiplicative *identity* $\bar{u}$. Moreover

$$\alpha(\bar{f}*\bar{g}) = (\alpha\bar{f})*\bar{g} = \bar{f}*(\alpha\bar{g}) \qquad (\bar{f}, \bar{g}\in\bar{S}, \alpha\in F) .$$

DEFINITION. Two elements $\bar{f}, \bar{g}\in\bar{S}$ are *associates* provided $\bar{f} = \lambda\bar{g}$, where $\lambda\in F$, $\lambda\neq 0$.

DEFINITION. An element $\bar{f}\in\bar{S}$, $\bar{f}\neq 0$, is *minimal* provided

$$\bar{f}\circ\bar{g} = \lambda(\bar{f}, \bar{g})\bar{f} \qquad (\bar{g}\in\bar{S}) \tag{15}$$

where $\bar{g}$ is any element of $\bar{S}$ and $\lambda(\bar{f}, \bar{g})$ is a number of F. It is evident that $\lambda(\bar{f}, \bar{g})$ is unique.

Clearly the associate of a minimal element is also minimal. Also it is evident that if $\bar{f}, \bar{g}$ are two minimal elements that are not associates then

$$\bar{f}\circ\bar{g} = 0 . \tag{16}$$

S3. For each minimal element $\bar{f}$ there exists a nonzero number $\lambda(\bar{f})$ of F such that

$$\bar{f}\circ\bar{f} = \lambda(\bar{f})\bar{f} . \tag{17}$$

DEFINITION. A minimal element $\bar{f}\in\bar{S}$ is *normalized* provided

$$\bar{f}\circ\bar{f} = \bar{f} . \tag{18}$$

S4. If $\bar{g}$ is an arbitrary nonzero element of $\bar{S}$ there exists at least one minimal element $\bar{f}$ such that $\lambda(\bar{f}, \bar{g})\neq 0$, where $\lambda(\bar{f}, \bar{g})$ is defined by (15).

Let M denote the set of normalized minimal elements.

S5. M is a semigroup with respect to $*$; the identity element of M coincides with $\bar{u}$, the multiplicative identity of $\bar{\Delta}$. Moreover M contains no units except the identity.

DEFINITION. An element $\bar{f}$ of M, $\bar{f}\neq\bar{u}$, is prime provided $\bar{f}=\bar{g}*\bar{h}$ implies $\bar{g} = \bar{u}$ or $\bar{h} = \bar{u}$.

S6. M contains a countable number of primes. Any element of M, different from $\bar{u}$, can be expressed as a product of primes in essentially only one way.

DEFINITION. Let $\bar{f}_1, \bar{f}_2, \bar{f}_3, \cdots$ denote the elements of M. If $\bar{g}$ is an arbitrary element of $\bar{S}$ the numbers

$$\lambda_j(\bar{g}) = \lambda(\bar{f}_j, \bar{g})$$

defined by

$$\bar{f}_j \circ \bar{g} = \lambda(\bar{f}_j, \bar{g})\bar{f}_j \tag{19}$$

may be called the (Dirichlet) coefficients of $\bar{g}$.

S7. If $\bar{g} \neq \bar{h}$ then for at least one value of j we have $\lambda_j(\bar{g}) \neq \lambda_j(\bar{h})$.

It evidently follows that two elements of $\bar{S}$ are equal if and only if the respective sets of coefficients are equal.

S8. If $\bar{g}$ and $\bar{h}$ are arbitrary elements of $\bar{S}$ while $\bar{f}$ is an element of M, then

$$\bar{f} \circ (\bar{g} * \bar{h}) = \Sigma(\bar{f}_r \circ \bar{g}) * (\bar{f}_s \circ \bar{h})$$

where the summation is over all $\bar{f}_r, \bar{f}_s \in M$ such that $\bar{f}_r * \bar{f}_s = \bar{f}$.

Finally we have

S9. For every sequence $\lambda_1, \lambda_2, \lambda_3, \cdots, \lambda_j \in F$, there exists a $\bar{g} \in \bar{S}$ such that

$$\bar{f}_j \circ \bar{g} = \lambda_j \bar{f}_j \qquad (j = 1, 2, 3, \cdots) .$$

3. LEMMA 1. *If $\bar{f}_i, \bar{f}_j$ are distinct elements of M then*

$$\bar{f}_i \circ \bar{f}_j = 0 \qquad (i \neq j) . \tag{20}$$

This is immediate from (16).

LEMMA 2. *Let $\bar{g}, \bar{h}$ be two arbitrary elements of $\bar{S}$ and let $\lambda_j(\bar{g})$, $\lambda_j(\bar{h})$ denote the respective sets of coefficients of $\bar{g}$ and $\bar{h}$. Then*

$$\lambda_j(\bar{g} \circ \bar{h}) = \lambda_j(\bar{g})\lambda_j(\bar{h}) \qquad (j = 1, 2, 3, \cdots) . \tag{21}$$

Indeed we have by (18) and (19)

$$\begin{aligned}\lambda_j(\bar{g} \circ \bar{h})\bar{f}_j &= \bar{f}_j \circ (\bar{g} \circ \bar{h}) = (\bar{f}_j \circ \bar{g}) \circ (\bar{f}_j \circ \bar{h}) = (\lambda_j(\bar{g})\bar{f}_j) \circ (\lambda_j(\bar{h})\bar{f}_j) \\ &= \lambda_j(\bar{g})\lambda_j(\bar{h})(\bar{f}_j \circ \bar{f}_j) = \lambda_j(\bar{g})\lambda_j(\bar{h})\bar{f}_j\end{aligned}$$

and (21) follows at once.

LEMMA 3. *Let $\bar{g}, \bar{h}$ be two arbitrary elements of $\bar{S}$ and let $\lambda_j(\bar{g})$, $\lambda_j(\bar{h})$ denote the respective sets of coefficients of $\bar{g}$ and $\bar{h}$. Then*

$$\lambda_j(\bar{g}*\bar{h}) = \Sigma\lambda_r(\bar{g})\lambda_s(\bar{h}) \qquad (j = 1, 2, 3, \cdots), \tag{22}$$

where the summation is over all pairs r, s such that

$$\bar{f}_r*\bar{f}_s = \bar{f}_j . \tag{23}$$

Proof. We have by S8

$$\begin{aligned}\lambda_j(\bar{g}*\bar{h})\bar{f}_j = \bar{f}_j\circ(\bar{g}*\bar{h}) &= \sum_{\bar{f}_r*\bar{f}_s=\bar{f}_j}(\bar{f}_r\circ\bar{g})*(\bar{f}_s\circ\bar{h}) \\ &= \sum_{\bar{f}_r*\bar{f}_s=\bar{f}_j}(\lambda_r(\bar{g})\bar{f}_r)*(\lambda_s(\bar{h})\bar{f}_s) \\ &= \Big\{\sum_{\bar{f}_r*\bar{f}_s=\bar{f}_j}\lambda_r(\bar{g})\lambda_s(\bar{h})\Big\}\bar{f} .\end{aligned}$$

This evidently implies (22).

Let $\bar{p}_1, \bar{p}_2, \bar{p}_3, \cdots$ denote the primes of M and let $p_1, p_2, p_3, \cdots$ denote the ordinary primes. We assume to begin with that the number of primes in M is infinite and set up the correspondence

$$p_j \rightleftarrows \bar{p}_j \qquad (j = 1, 2, 3, \cdots) . \tag{24}$$

If

$$n = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$$

is an arbitrary positive integer, we put

$$\bar{f}_n = \bar{p}_1^{e_1}*\bar{p}_2^{e_2}*\cdots*\bar{p}_r^{e_r} , \tag{25}$$

where

$$\bar{g}^e = \bar{g}*\cdots*\bar{g} ,$$

with e factors on the right. By means of (25) we have the one-to-one correspondence between Z and M

$$n \rightleftarrows \bar{f}_n \qquad (n = 1, 2, 3, \cdots) . \tag{26}$$

Let $\bar{g}$ be an arbitrary element of $\bar{S}$ and let $\lambda_j(\bar{g})$ denote the set of coefficients of $\bar{g}$. Corresponding to $\bar{g}$ we have the function g in S defined by

$$g(n) = \lambda_n(\bar{g}) . \tag{27}$$

Conversely if g is any function in S then by S9 and S7 the element $\bar{g}$ of $\bar{S}$ is uniquely determined by means of (27), so that we have obtained a one-to-one correspondence between S and $\bar{S}$.

Now if $\alpha \in F$ it follows at once from (27) that

$$\alpha g(n) = \lambda_n(\alpha \bar{g}) , \tag{28}$$

so that scalar multiplication is consistent with the correspondence defined by (27). Again if $h \in S$ and $\bar{h} \in \bar{S}$ satisfy

$$h(n) = \lambda_n(\bar{h}) \tag{29}$$

it is clear that

$$g(n) + h(n) = \lambda_n(\bar{g} + \bar{h}) . \tag{30}$$

In the next place, if (27) and (29) hold, it follows from Lemma 2 that

$$g(n)h(n) = \lambda_n(\bar{g})\lambda_n(\bar{h}) = \lambda_n(\bar{g} \circ \bar{h}) . \tag{31}$$

Thus if $\bar{g}$ corresponds to g and $\bar{h}$ corresponds to h then $\bar{g} \circ \bar{h}$ corresponds to the "ordinary" product of g and h.

Next we observe that if

$$r \rightleftarrows \bar{f}_r , \qquad s \rightleftarrows \bar{f}_s$$

under the correspondence (26), then

$$rs \rightleftarrows \bar{f}_r * \bar{f}_s . \tag{32}$$

Thus, assuming (27) and (29), we get

$$\sum_{rs=n} g(r)h(s) = \sum_{rs=n} \lambda_r(\bar{g})\lambda_s(\bar{h}) = \sum_{\bar{f}_r * \bar{f}_s = \bar{f}_n} \lambda_r(\bar{g})\lambda_s(\bar{h}) .$$

Therefore, by Lemma 3,

$$\sum_{rs=n} g(r)h(s) = \lambda_n(\bar{g} * \bar{h}) . \tag{33}$$

Thus if $\bar{g}$ corresponds to g and $\bar{h}$ corresponds to h then $\bar{g} * \bar{h}$ corresponds to the Dirichlet product of g and h.

Combining (27), (28), (29), (30), (31), (32) and (33) we have the following result.

THEOREM 1. *Let Φ denote the system of arithmetic functions from the integers to an arbitrary but fixed field F as defined in* § 1. *Let $\bar{\Phi}$ be a structure with the three binary operations $+$, $\circ$, $*$ that satisfies the assumptions* S1–S9 *of* § 2. *Also let the number of primes in M be infinite. Then $\bar{\Phi}$ is isomorphic to Φ, all operations being preserved under the isomorphism.*

4. We have assumed in the above result that the number of

prime elements in M is infinite. The conclusion of the theorem is no longer valid when the number of primes is finite. However it is easily verified that in this case $\bar{\Phi}$ is isomorphic to a subset of Φ. More precisely, we have the following result.

Let $\bar{p}_1, \bar{p}_2, \cdots, \bar{p}_k$ denote the primes of M and let $p_1, p_2, \cdots, p_k$ be a set of k distinct primes, for example the first k primes. Then the correspondence (26) holds except that n is now restricted to the set of integers Z_k whose prime divisors are in the set $p_1, p_2 \cdots, p_k$. Consider the set of functions g such that

$$g(n) = 0 \qquad (n \in Z - Z_k) , \tag{34}$$

while $g(n)$ is an arbitrary number of F when $n \in Z_k$. It is easily verified that the set of functions satisfying (34) is closed under scalar, ordinary and Dirichlet multiplication. We denote the system by Φ_k. Then we have

THEOREM 2. *Let Φ_k denote the system of arithmetic functions that satisfy* (34). *Let $\bar{\Phi}$ be a structure with three binary operations* $+, \circ, *$ *that satisfies the assumptions* S1–S9 *of* § 2 *but let the number of primes in M equal k. Then $\bar{\Phi}$ is isomorphic to Φ_k.*

It is evident that Φ_k is isomorphic to $F\{x_1, x_2, \cdots, x_k\}$, the ring of formal power series in k indeterminates with coefficients in F.

REMARK. The referee has pointed out that S4 and S7 are equivalent, in the presence of the other assumptions. First, S7 implies S4. For $\bar{g} \neq 0$, by S7 there exists a j such that $\lambda_j(\bar{g}) \neq \lambda_j(0) = 0$. Hence S4 holds with $\bar{f} = \bar{f}_j$.

Conversely, S4 implies S7. For if $\bar{g} \neq \bar{h}$, then $\bar{d} = \bar{g} - \bar{h} \neq 0$. By S4 there exists a minimal $\bar{f}$ such that $\bar{f} \circ \bar{d} = \lambda(\bar{f}, \bar{d})\bar{f}$, where $\lambda(\bar{f}, \bar{d}) \neq 0$. Since $\bar{f}$ is minimal, $\bar{f} \circ \bar{f} = \lambda(\bar{f})\bar{f}$, where $\lambda(\bar{f}) \neq 0$ by S3. Hence there exists a minimal

$$\bar{f} = (\lambda(\bar{f}))^{-1}\bar{f}$$

(an associate of the minimal element $\bar{f}$) which is also normalized. Thus

$$\begin{aligned} \bar{f}_j \circ \bar{d} = \lambda(\bar{f}, \bar{d})\bar{f}_j &= \bar{f}_j \circ (\bar{g} - \bar{h}) = \bar{f}_j \circ \bar{g} - \bar{f}_j \circ \bar{h} \\ &= \lambda_j(\bar{g})\bar{f}_j - \lambda_j(\bar{h})\bar{f}_j = [\lambda_j(\bar{g}) - \lambda_j(\bar{h})]\bar{f}_j . \end{aligned}$$

Hence

$$\lambda_j(\bar{g}) - \lambda_j(\bar{h}) = \lambda(\bar{f}, \bar{d}) \neq 0 .$$

REFERENCE

1. E. D. Cashwell and C. J. Everett, *The ring of number-theoretic functions*, Pacific J. Math., **9** (1959), 975–985.