ARITHMETIC FUNCTIONS IN AN ALGEBRAIC SETTING

By

Pentti Haukkanen (Tampere) and R. Sivaramakrishnan (Calicut)

1. Introduction

Let A (resp. $\tilde{A}$) denote the set of all arithmetic functions defined on N, the set of positive integers, (resp. $\tilde{N}$, the set of non-negative integers) with values in C, the field of complex numbers.

Various binary operations on A or $\tilde{A}$ are known. Addition and multiplication of two functions of A or $\tilde{A}$ defined as ordinary addition and multiplication of function values are standard examples, and under these operations A or $\tilde{A}$ forms a commutative ring.

A or $\tilde{A}$ also forms a commutative ring (with or without zero divisors) under addition and other kinds of multiplication. The aim of this paper is to study algebraic structures arising from certain operations. Another objective is the study of algebraic structures of the subclass S, the set of functions f (called semi-multiplicative functions) such that

(1.1) $$f(r)f(s)=f((r, s))f(\{r, s\})$$

with (r, s) (resp. $\{r, s\}$) denoting the g.c.d (resp. l.c.m) of r and s, and such that $f\not\equiv 0$, the zero map. The functions $f\in S$ are characterized by D. Rearick [14] as those which are of the form

(1.2) $$f(r)=c_f f'(r/a_f),$$

where $c_f\in C^*$, the set of non-zero elements of C, $a_f=N(f)$ called the norm of f and defined by E.D. Cashwell and C.J. Everett [3] to be the least $r\in N$ for which $f(r)\neq 0$, and $f'\in M$, the subclass of S consisting of multiplicative functions to be defined right now.

If $a_f=1$, f is called a quasi-multiplicative function, or in other words, the subclass Q of S consists of those functions f satisfying the conditions that $f\not\equiv 0$ and there exists $q\in C^*$ such that

(1.3) $$f(r)f(s)=qf(rs)$$

whenever $(r, s)=1$. The subclass $M\subset Q$ of multiplicative functions consists of

those functions f for which $q=1$ in (1.3). We shall prove that Q is a quasi-field in the sense of P. Kesava Menon [11] and study Q using its Z-module structure.

We shall also construct structure-preserving transformations on A, M and S. In particular, the B-transform to be given in (4.2) is a vector space isomorphism of A viewed as a vector space over C, preserving the Dirichlet convolution which naturally arises from the product of the Dirichlet series of f, $g \in A$.

2. Rings with or without zero divisors

A forms a commutative ring under addition and Dirichlet convolution defined by

$$(2.1) \qquad (f \cdot g)(r) = \sum_{d \mid r} f(d)g(r/d),$$

where the summation is over all divisors d of r. As mentioned above this multiplication appears quite naturally if we consider the Dirichlet series $F(s)$ $= \sum_{r=1}^{\infty} f(r)r^{-s}$, $G(s) = \sum_{r=1}^{\infty} g(r)r^{-s}$ supposing they are absolutely convergent in some half-plane. The coefficient of r^{-s} in the product $F(s)G(s)$ is given precisely by (2.1).

Restricting the summation in (2.1) over 'unitary divisors' of r, i.e. those divisors d for which $(d, r/d)=1$, we obtain the notion of unitary convolution $f \oplus g$. Using the multiplicative property of norms, we conclude that $(A, +, \cdot)$ is an integral domain (which actually is a unique factorization domain as proved by Cashwell and Everett [3], see also H.N. Shapiro [15, Chapter 4] and R. Sivaramakrishnan [16, Part 1, Chapter I]), while the commutative ring $(A, +, \oplus)$ has divisors of zero.

On the other hand, $\tilde{A}$ forms an integral domain under addition and Cauchy multiplication defined by

$$(f \circ g)(r) = \sum_{i=0}^{r} f(i)g(r-i).$$

Cauchy multiplication also comes out naturally if we associate the formal power series

$$P_f(x) = \sum_{r=0}^{\infty} f(r)x^r, \qquad P_g(x) = \sum_{r=0}^{\infty} g(r)x^r$$

with f and g respectively and multiply $P_f(x)$ and $P_g(x)$. It can be shown that $\tilde{A}$ is isomorphic to the formal power series ring $C[[x]]$. For details of proof, see R. Sivaramakrishnan [16, Part 1, Chapter I].

3. Quasi-multiplicative functions

P. Kesava Menon [11] defines a non-empty set K with two binary operations $+$ and $\cdot$ to be a quasi-field when the following axioms are satisfied:

   (i) $(K, +)$ is an Abelian group,

  (ii) $(K, \cdot)$ is an Abelian group,

 (iii) for $a, b, c \in K$, the quasi-distributive law, viz.

$$a \cdot (b+c) + a = a \cdot b + a \cdot c,$$

      holds.

In this algebraic system the identity element under addition also serves as the identity element under multiplication.

In [11], the actual construction of a quasi-field is shown by considering functions defined over all finite subsets of a given set. For the construction of quasi-fields in the context of generalized Dirichlet convolutions one may refer to [6]. An example of a quasi-field relevant to the discussian is the set Q of quasi-multiplicative functions.

THEOREM 1. *The triple* $(Q, \oplus, \cdot)$ *is a quasi-field.*

Proof. It is easy to note that $(Q, \oplus)$ and $(Q, \cdot)$ are Abelian groups. The quasi-distributive law is known to hold for multiplicative functions [17, p. 607]. Thus it is easily seen to be valid for quasi-multiplicative functions, too. Hence $(Q, \oplus, \cdot)$ is a quasi-field.

Next we shall consider Q as a Z-module.

THEOREM 2. *The Abelian group* $(Q, \cdot)$ *of quasi-multiplicative functions considered as a* Z-*module is divisible and so injective.*

Proof. By Theorem 2 of [7] it can be seen that for every $g \in Q$ and $0 \neq n \in Z$ there exists $f \in Q$ such that $f^n = g$. That is, Q is divisible. Further, as Z is a principal ideal domain, by Theorem 7.1 of Chapter I in [8], Q is injective.

REMARK. Let U denote the set of units in $(A, +, \cdot)$, that is, the set of those functions f for which $f(1) \neq 0$. By Theorem 1 of [7] it can be seen that the Abelian group $(U, \cdot)$ considered as a Z-module is divisible, too.

REMARK. The sequence

$$0 \longrightarrow Q \overset{i}{\longrightarrow} U \overset{\pi}{\longrightarrow} U/Q \longrightarrow 0 \,,$$

where i is the inclusion map and π is the projection, is short exact.

Next we shall construct a partition of the set Q. For each $q \in C^*$, let M_q consist of those functions $f \in Q$ for which $f(1)=q$. For $f, g \in Q$, we say that f and g are equivalent, written $f \sim g$, if $f(1)=g(1)$. It is easy to verify that $\sim$ is an equivalence relation on Q and the equivalence class of f is $M_{f(1)}$. The equivalence classes form a partition of Q given by

(3.1) $$Q = \bigcup_{q \in C^*} M_q \,.$$

Here $M_1 = M$ and each of the sets M_q is in one-one correspondence with M. For, if we define $L_q : M_q \to M$ $(q \in C^*)$ by $L_q(f)=(1/q)f \in M$, then L_q is both injective and surjective. We can interpret (3.1) group-theoretically, since $(M, \cdot)$ is a subgroup of $(Q, \cdot)$.

THEOREM 3.   For each $q \in C^*$, M_q represents a coset of M in Q.

Proof.   We define

$$f \equiv g \pmod{M}, \qquad f, g \in Q$$

if and only if $f \cdot g^{-1} \in M$. In fact, the equivalence relation $\sim$ that gave (3.1) is suggested by the fact that $f \cdot g^{-1} \in M$ if and only if $f(1)=g(1)$ (since $f(1)g^{-1}(1) = f(1)/g(1)=1$). Therefore, the coset of M determined by $f \in Q$ is given by

$$f \cdot M = \{f \cdot g : g \in M\} = M_{f(1)} \,.$$

Thus,

$$Q/M = \{M_q : q \in C^*\} \,.$$

This proves Theorem 3.

REMARK.   The same kind of argument could be applied if the Dirichlet convolution is replaced by the unitary convolution and the unitary analogue of Theorem 3 is possible.

A similar kind of partitioning of the set of semi-multiplicative functions S could be carried out. For $f, g \in S$, we say $f \sim g$ if and only if $a_f = a_g$. This defines an equivalence relation on S. The equivalence class of $f \in S$ is the set of semi-multiplicative functions all of which have the same norm $N(f)$. Denoting by S_{a_f} the equivalence class of f we get

(3.2) $$S = \bigcup_{a_f \in N} S_{a_f}.$$

Here $S_1 = Q$ and each of the classes S_{a_f} is in one-one correspondence with Q. These one-one correspondences are exhibited by the maps $L_{a_f}: S_{a_f} \rightarrow Q$, $L_{a_f}(f)(r) = f(a_f r)$. The inverse maps are given by $L_{a_f}^{-1} = T_{a_f}$ (cf. (4.4)).

4. Transformations

Let

$$r = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}, \qquad a_i \geq 1, \qquad i = 1, 2, \cdots, t,$$

and

$$s = p_1^{b_1} p_2^{b_2} \cdots p_t^{b_t}, \qquad b_i \geq 1, \qquad i = 1, 2, \cdots, t.$$

Then we define

(4.1) $$B(r, s) = \begin{cases} \prod_{i=1}^{t} \binom{a_i - 1}{b_i - 1} & \text{if } s|r \text{ and } s \text{ contains all the prime factors of } r, \\ 0 & \text{otherwise} \end{cases}$$

(cf. [9]). Further, we define the transformation $B: A \rightarrow A$ by

(4.2) $$B(f)(r) = \sum_{d|r} B(r, d) f(d), \qquad f \in A,$$

where $B(r, s)$ is as defined in (4.1). It is easily seen that B is a linear operator on A when A is considered as a vector space over C.

THEOREM 4. *The B-transform preserves Dirichlet convolution. That is, for $f, g \in A$*

$$B(f \cdot g) = B(f) \cdot B(g).$$

Proof. By the definitions of the Dirichlet convolution and the B-transform we obtain

$$[B(f) \cdot B(g)](r) = \sum_{cus = r} f(c) g(u) \sum_{dv = s} B(cd, c) B(uv, u).$$

By the combinatorial identity

$$\sum_{k=0}^{n} \binom{x+k}{k} \binom{y+n-k}{n-k} = \binom{x+y+n+1}{n}$$

(see [5], p. 22) it can be verified that

$$\sum_{dv = s} B(cd, c) B(uv, u) = B(cus, cu).$$

Thus

$$[B(f) \cdot B(g)](r) = \sum_{cus=r} f(c)g(u)B(cus, cu)$$

$$= \sum_{ts=r} B(r, t) \sum_{cu=t} f(c)g(u) = \sum_{ts=r} B(r, t)(f \cdot g)(t).$$

This proves Theorem 4.

THEOREM 5.   *For each $g \in A$ there exists $f \in A$ such that $B(f)=g$.*

Proof.   The function f can be obtained inductively from the relations

$$f(r) = g(r) - \sum_{\substack{d \mid r \\ d \neq r}} B(r, d)f(d).$$

REMARK.   Theorem 5 shows that the transform $B: A \to A$ is surjective.   It can be verified that $B: A \to A$ is also injective.   Hence $B: A \to A$ is bijective and it preserves Dirichlet convolution.

THEOREM 6.   *The inverse of the B-transform of $f \in A$ is given by*

$$B^{-1}(f)(r) = \sum_{d \mid r} \lambda(r/d)B(r, d)f(d),$$

where λ is Liouville's function given by

(4.3) $$\lambda(r) = (-1)^{\Omega(r)},$$

$\Omega(r)$ representing the total number of prime factors of r, each being counted according to its multiplicity.

Proof.   We have, if $B(g)=f$,

$$\sum_{d \mid r} \lambda(r/d)B(r, d)f(d) = \sum_{ca=r} g(c) \sum_{e\delta=a} \lambda(\delta)B(r, ce)B(ce, c).$$

By the combinatorial identity

$$\sum_{k=j}^{n} (-1)^k \binom{n}{k}\binom{k}{j} = \begin{cases} 0 & \text{if } j \neq n, \\ (-1)^n & \text{if } j = n \end{cases}$$

(see [5, p. 36]), we see that

$$\sum_{e\delta=a} \lambda(\delta)B(r, ce)B(ce, c) = \begin{cases} 1 & \text{if } r = c, \\ 0 & \text{if } r \neq c. \end{cases}$$

This yields the desired result.

Next, we observe that the norm $\eta(f)$ of $f \in M$ defined by P. Kesava Menon [10] is also an example of a transformation.   It should not be confused with the norm $N(f)$ as defined by Cashwell and Everett in [3].   The norm $\eta(f)$ of $f \in M$ is the arithmetic function defined by

$$\eta(f)(r) = \sum_{d \mid r^2} f(r^2/d) f(d) \lambda(d).$$

The transformation $\eta : M \to M$ is an endomorphism of the Abelian group $(M, \cdot)$. In [13], C. Pomerance has obtained the kernel of the endomorphism. It is also known [10] that

$$\eta(f)_{(p)}(x) = f_{(p)}(\sqrt{x}) f_{(p)}(-\sqrt{x}),$$

where

$$f_{(p)}(x) = 1 + f(p)x + f(p^2)x^2 + \cdots + f(p^m)x^m + \cdots$$

Apostol [1] calls $f_{(p)}(x)$ the Bell-series of f to the base p.

Extending the definition of $\eta(f)$ to a k-fold Dirichlet convolution we define $\eta_k(f)$ to be the arithmetic function given by

$$\eta_k(f)(r) = \sum_{d_1 d_2 \cdots d_k = r^k} f(d_1) f(d_2) \cdots f(d_k) \lambda_k(d_2) \lambda_k^2(d_3) \cdots \lambda_k^{k-1}(d_k),$$

where

$$\lambda_k(r) = (\omega_k)^{\Omega(r)},$$

ω_k being a complex k^{th}-root of unity and $\Omega(r)$ being as given in (4.3).

It is easy to check that $\eta_k(f)$ is multiplicative whenever f is multiplicative. Also,

$$\eta_k(f \cdot g) = \eta_k(f) \cdot \eta_k(g) \qquad \text{whenever } f, g \in M.$$

That is, η_k preserves the Dirichlet convolution. The definition of the η_k-transform can be carried out in the class S as well. The details are omitted.

For $a \in N$ we define

$$e_a(r) = \begin{cases} 1 & \text{if } r = a, \\ 0 & \text{otherwise.} \end{cases}$$

Considering Dirichlet multiplication of f by e_a as a transformation of f, we define the right (or left) translation by e_a of $f \in A$ by

$$T_a(f)(r) = (f \cdot e_a)(r).$$

It is clear that

$$(4.4) \qquad T_a(f)(r) = \begin{cases} f(r/a) & \text{if } a \mid r, \\ 0 & \text{otherwise.} \end{cases}$$

Plainly $T_a : A \to A$ is a linear operator on the vector space A (over C). Also we note that the structure (1.2) of $f \in S$ can be written as

$$f(r) = f(a_f) T_{a_f}(f')(r).$$

References

[1]   Apostol, T. M.,   Introduction to analytic number theory, UTM, Springer-Verlag, 1976.

[2]   Carlitz, L.,   Arithmetic functions in an unusual setting, Amer. Math. Monthly **73** (1966), 582–590.

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

[4]   Cohen, E.,   Arithmetical functions associated with the unitary divisors of an integer, Math. Z. **74** (1960), 66–80.

[5]   Gould, H. W.,   Combinatorial identities, Printed by Morgantown Printing and Binding Co., 1972.

[6]   Haukkanen, P.,   Some classes of quasi-fields having isomorphic additive and multiplicative groups, Rend. Mat. Serie VII, Volume **7** (1987), 181–192 (1988).

[7]   Haukkanen, P.,   Arithmetical equations involving semi-multiplicative functions and the Dirichlet convolution, Rend. Mat. Serie VII, Volume **8** (1988), 511–517 (1989).

[8]   Hilton, P. J. and Stammbach, V.,   A course in homological algebra, GTM 4, Springer-Verlag, New York, 1970.

[9]   Kesava Menon, P.,   Transformations of arithmetic functions, J. Indian Math. Soc. **6** (1942), 143–152.

[10] Kesava Menon, P.,   Series associated with Ramanujan's function $\tau(n)$, J. Indian Math. Soc. **27** (1963), 57–65.

[11] Kesava Menon, P.,   A class of quasi-fields having isomorphic additive and multiplicative groups, J. Indian Math. Soc. **27** (1963), 71–90.

[12] Lahiri, D. B.,   Hypo-multiplicative number-theoretic functions, Aequations Math. **9** (1973), 184–192.

[13] Pomerance, C.,   Solution to Problem 5945, Amer. Math. Monthly **82** (1975), 410–411.

[14] Rearick, D.,   Semi-multiplicative functions, Duke Math. J. **33** (1966), 49–53.

[15] Shapiro, H. N.,   Introduction to the Theory of Numbers, Wiley Interscience, 1983.

[16] Sivaramakrishnan, R.,   Classical theory of arithmetic functions, Monographs & Textbooks in Pure and Applied Mathematics No. 126, Marcel Dekker, New York, 1989.

[17] Vaidyanathaswamy, R.,   The theory of multiplicative arithmetic functions, Trans. Amer. Math. Soc. **33** (1931), 579–662.

Pentti Haukkanen   R. Sivaramakrishnan
Department of Mathematical Sciences   Department of Mathematics
University of Tampere   University of Calicut
SF-33101 Tampere   Calicut 673 635
Finland   India