*ScienceAsia* 27 (2001) : **199-202**

# Arithmetic Functions and Operators

**Vichian Laohakosol[a], Nittiya Pabhapote[b,*] and Nalinee Wechwiriyakul[b]**
[a] Department of Mathematics, Kasetsart University, Bangkok 10900, Thailand.
[b] Department of Mathematics, The University of the Thai Chamber of Commerce, Bangkok 10400, Thailand
* Corresponding author, E-mail: anipa@mail.utcc.ac.th

*Received 22 Dec 1999*
*Accepted 1 May 2001*

**ABSTRACT** Basic results about arithmetic functions and their major operations, namely, valuation, derivation and operators, are collected. The logarithmic and related operators, introduced and applied in 1968 by D Rearick to establish isomorphisms among various groups of real-valued arithmetic functions are extended to complex-valued arithmetic functions along the original lines suggested by him.

KEYWORDS: arithmetic functions, operators.

## INTRODUCTION

An arithmetic function is a function whose domain is N and range is a subset of C.

Let $f$ and $g$ be arithmetic functions. The sum (or addition) of $f$ and $g$ is an arithmetic function $f+g$ defined by $(f+g)(n) = f(n) + g(n)$. The Dirichlet product ( or convolution or Dirichlet multiplication) of $f$ and $g$ is an arithmetic function $f * g$ defined by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

The set (A, +, ∗) of all arithmetic functions together with addition and convolution is a unique factorization domain but not a principal ideal domain.[1-3, 7-9] The function $Z(n) = 0$ ($\forall\, n \in$ N) is an additive identity, while the function

$$I(n) = \begin{cases} 1, & n=1 \\ 0, & \text{otherwise} \end{cases}$$ is a (Dirichlet) multiplicative

identity. Indeed, the so-called Möbius inversion formula[1-3, 7-9] states that for $f, g \in$ A, we have

$$f(n) = \sum_{d|n} g(d) \;\Leftrightarrow\; g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right),$$ which

is equivalent to stating that $f = g * u$ if and only if $g = f * \mu$, where u is the unit function defined for all $n \in$ N by $u(n) = 1$ and $\mu$ the Möbius function.

An arithmetic function $f$ is said to be multiplicative if $f(1) = 1$ and $f(mn) = f(m) f(n)$ for all relatively prime integers $m, n$. Let $f \in$ A. The (Dirichlet) inverse of $f$ is an arithmetic function $f^{-1}$ for which $I = f * f^{-1}$. It is known[1-3, 7-9] that $f^{-1}$ exists if and only if $f(1) \neq 0$.

A derivation over A[7] is a function D : A → A such that for all $f, g \in$ A, and for all a, b ∈ C , we have $D(f * g) = Df * g + f * Dg$, $D(af + bg) = aDf + bDg$. Three typical examples of derivation, which are often used, are

(i) log-derivation : $D_l f(n) := f(n) \log n$ ,
(ii) p-basic derivation (p prime) : $D_p f(n) := f(np)\, v_p(np)$, where $v_p(m)$ denotes the highest power of $p$ dividing $m$,
(iii) $D_h f(n) := f(n)\, h(n)$, where $h$ is a completely additive arithmetic function, ie, $h(mn) = h(m) + h(n)$.

In 1968, D. Rearick[5, 6] constructed a number of operators over A analogous to the classical logarithmic, exponential and trigonometric operators. He subsequently used them to show that various groups of real - valued arithmetic functions are isomorphic. That is, $(A_R, +)$, $(P_R, *)$, $(M_R, *)$, $(P_R, \text{x})$ and $(M_R, \text{x})$ are isomorphic, where

$A_R = \{ f : N \to R \}$ = set of real-valued arithmetic functions,
$P_R = \{ f \in A_R ; f(1) > 0 \}$,
$M_R = \{ f \in P_R ; f \text{ is multiplicative} \}$,

and x is the unitary product defined by $(f \text{ x } g)(n) = \Sigma' f(d)\, g(n/d)$, with $\Sigma'$ indicating that the sum is taken over the divisors d such that $(d, n/d) = 1$.

The objectives of this work are :

(i) to extend the definition of Rearick in order to embrace those arithmetic functions which assume complex values of all but one point, namely, at $n = 1$; this is indeed suggested at the end of Rearick paper,[5] and

(ii) to establish relevant isomorphisms among certain groups of arithmetic functions considered in (i) which encompass those in Rearick.[5, 6]

## Logarithmic Operators

The following notation will be standard throughout the whole paper:

$A_C := \{f\,; f: \mathbb{N} \to \mathbb{C}\}$ = set of all complex-valued arithmetic functions ,

$A'_C := \{f \in A_C\,; f(1) \in \mathbb{R}\}$ ,

$P_C := \{f \in A'_C\,; f(1) > 0\}$ ,

$M_C := \{f \in A_C\,; f$ is multiplicative $\}$.

We define the (complex) logarithmic operator $L_C : P_C \to A'_C$ by

$L_C f(1) = \log f(1)$ and

$$L_C f(n) = \sum_{d|n} f(d) f^{-1}\left(\frac{n}{d}\right) \log d = D_1 f * f^{-1}(n) \; (n > 1).$$

**Proposition 1.** For all $f, g \in P_C$, we have $L_C(f * g) = L_C f + L_C g$.

**Proof.** $L_C(f * g)(1) = \log(f * g)(1) = \log(f(1)g(1))$
$= \log f(1) + \log g(1)$
$= L_C f(1) + L_C g(1)$.

Since $L_C f = f^{-1} * D_1 f$, evaluating at $n > 1$, we see that

$$L_C(f * g)(n) = ((f * g)^{-1} * D_1(f * g))(n)$$
$$= (f^{-1} * g^{-1} * (f * D_1 g + g * D_1 f))(n)$$
$$= L_C g(n) + L_C f(n).$$

**Proposition 2.** For each $h \in A'_C$, there is a unique $f \in P_C$ such that $h = L_C f$.

**Proof.** Define $f(1) = \exp h(1)$. Let $n > 1$ and assume $f(k)$ has been defined for all $k < n$. The value $f^{-1}(k)$ are recursively determined by the relation $\sum_{d|k} f^{-1}(d) f(\frac{k}{d}) = I(k)$. This gives us a triangular system which can be solved for the unknowns $f^{-1}(k)$. Now given $h(n), f(k)$ and $f^{-1}(k)$ for all $k < n$, we define $f(n)$ by solving for the term corresponding to $d = n$ in the equation $h(n) = \sum_{d|n} f(d) f^{-1}(\frac{n}{d}) \log d$, noting that the term containing $f^{-1}(n)$ disappears because $\log 1 = 0$ and all other terms are known.

**Remark.** Proposition 1 and 2 show that the map $f \mapsto L_C f$ is an isomorphism of the groups $(P_C, *)$ and $(A'_C, +)$.

**Proposition 3.** Let $f \in P_C$. Then $f$ is multiplicative if and only if $L_C f(n) = 0$ whenever $n$ is not a prime power.

**Proof.** Assume $f$ is multiplicative. Then $f(1) = 1$ and so $L_C f(1) = 0$.
Let $N$ be a positive integer which is not a prime power. Then there are positive integers $m, n$ both $> 1$, $(m, n) = 1$ such that $N = mn$. Thus

$$L_C f(N) = \sum_{d|mn} f(d) f^{-1}\left(\frac{mn}{d}\right) \log d$$

$$= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) f^{-1}\left(\frac{m}{d_1}\right) f^{-1}\left(\frac{n}{d_2}\right)(\log d_1 + \log d_2)$$

$$= L_C f(m)\, I(n) + L_C f(n)\, I(m) = 0.$$

Next assume that $L_C f(n) = 0$ whenever n is not a prime power. Since $L_C f(1) = 0$, then $f(1) = 1$. For $n > 1$, define $g \in P_C$ by $g(1) = 1$ and $g(n) = \prod_{p|n} f(p^{\nu})$ where $p^{\nu} \| n$. Clearly, $g$ is multiplicative. We now show that $f = g$. Observe that $f(n) = g(n)$ and $f^{-1}(n) = g^{-1}(n)$ whenever $n$ is a prime power. From the definition of $L_C$, we thus get $L_C f(n) = L_C g(n)$ whenever $n$ is a prime power. Since $g \in P_C$, then the first half of the proof yields that $L_C g(m) = 0$ whenever m is not a prime power. Hence, $L_C f(n) = L_C g(n)$ for all $n \in \mathbb{N}$ and so $f = g$ by the isomorphism $L_C$.

**Remarks.** Proposition 3 implies that the groups $(M_C, *)$ and $(A''_C, +)$ are isomorphic, where $A''_C := \{h \in A'_C : h(n) = 0$ whenever $n$ is not a prime power $\}$. The group $(A''_C, +)$ is also isomorphic to the group $(A_C, +)$ via the map $h \leftrightarrow H$ where $H(n) = h(k_n)$ with $\{k_n\}$ being the sequence of prime powers arranged in ascending order.

Consequently, the groups $(M_C, *)$ and $(A_C, +)$ are isomorphic.

## Other Operators

Let $h \in A'_C$. Denote by $E_C h$, call the (complex) exponential of $h$, the unique element $f \in P_C$, justified by Proposition 2, such that $h = L_C f$. It follows easily from the definition and the properties of logarithmic operators that

(i) $E_C(h_1+h_2) = E_C h_1 * E_C h_2 \quad (\forall h_1, h_2 \in A'_C)$
(ii) $L_C(E_C h) = h \quad (\forall h \in A'_C)$
(iii) $E_C(L_C f) = f \quad (\forall f \in P_C)$
(iv) $E_C(Z) = I$.

For $f \in P_C$, and $r \in R$ define the r$^{th}$ power arithmetic function by $f^r := E_C(r L_C f)$.

It is easily checked that

(i) $(f^r)^s = f^{rs}$.
(ii) $f^{r+s} = f^r * f^s$.
(iii) $(f * g)^r = f^r * g^r$.
(iv) If $r$ is a positive interger, then $f^r = E_C(L_C f + ... + L_C f) = f * ... * f$ ($r$ factors), agreeing with our previous definition of positive integral power function.
(v) If $r = -1$, then $f^{-1} = E_C(-L_C f)$, and so $f * f^{-1} = E_C(L_C f) * E_C(-L_C f) = E_C(L_C f - L_C f) = I$ agreeing with the usual meaning of inverse.
(vi) If $r \in R - \{0\}$ and $f \in P_C$, it follows that the equation $g^r = f$ is uniquely solvable for $g \in P_C$; indeed, the solution is $g = f^{\frac{1}{r}}$, which amounts to saying that every $f \in P_C$ has a unique r$^{th}$ root in $P_C$.

Proposition 4. Let $r \in R$. If $f \in M_C$, then $f^r \in M_C$.

Proof. If $f \in P_C$, then by Proposition 3, $L_C f(n) = 0$ whenever n is not a prime power and so is $r L_C f(n)$. Therefore, Proposition 3 again yields that $f^r = E_C(r L_C f)$ is multiplicative.

Remark. It follows from the last proposition that for nonzero real $r$, the map $f \to f^r$ is an automorphism of the group $(P_C, *)$ which sends multiplicative elements onto themselves.

Let $f \in A'_C$. Define the hyperbolic sinh, cosh and tanh as follows:

$$S_c f = \frac{1}{2}\,(E_c f - E_c(-f)),$$

$$C_c f = \frac{1}{2}\,(E_c f + E_c(-f)),$$

$$T_c f = S_c f * (C_c f)^{-1}.$$

Since this definition mimics the classical one, it is clear that most elementary identities involving hyperbolic and/or trigonometric functions hold. We list some examples here.

(i) $S_C f + ((S_C f)^2 + I)^{1/2} = E_C f$.
(ii) If $S_C f = S_C g$, then $E_C f = E_C g$ and $f = g$, ie $S_C$ is injective.
(iii) For each $h \in A'_C$, there exists an $f \in A'_C$ such that $S_C f = h$, viz, $f = L_C(h + (h^2 + I)^{1/2})$. This shows that $S_C$ is surjective.
(iv) $S_C(f + g) = S_C f * ((S_C g)^2 + I)^{1/2} + S_C g * ((S_C f)^2 + I)^{1/2}$.

Proposition 5. The system $(A'_C, \square)$ forms a group which is isomorphic to $(A'_C, +)$, where

$$f \square g = f * (g^2 + I)^{1/2} + g * (f^2 + I)^{1/2}.$$

Proof. That $(A'_C, \square)$ is a group can be directly checked using the identities mentioned above. The map $(A'_C, +) \to (A'_C, \square)$ defined via $f \mapsto S_C f$ provides us with a desired isomorphism.

Let $V_C := \{f \in A'_C : -1 < f(1) < 1\}$ and let $\Delta$ be a binary operation defined over $V_C$ via $f \Delta g := (f + g) * (I + f * g)^{-1}$. It is easily checked that $(V_C, \Delta)$ forms a group with the zero function Z acting as the group identity.

Proposition 6. The groups $(V_C, \Delta)$ and $(A'_C, +)$ are isomorphic.

Proof. The hyperbolic tanh map $T_C : f \to T_C(f) = S_C f * (C_C f)^{-1}$ gives a desired isomorphism from $A'_C$ onto $V_C$.

Proposition 7. The groups $(A_C, +)$, $(A_R, +)$ and $(A'_C, +)$ are all isomorphic.

Proof. The map $\alpha : (A_R, +) \to (A_C, +)$ defined for each positive integer $n$ by

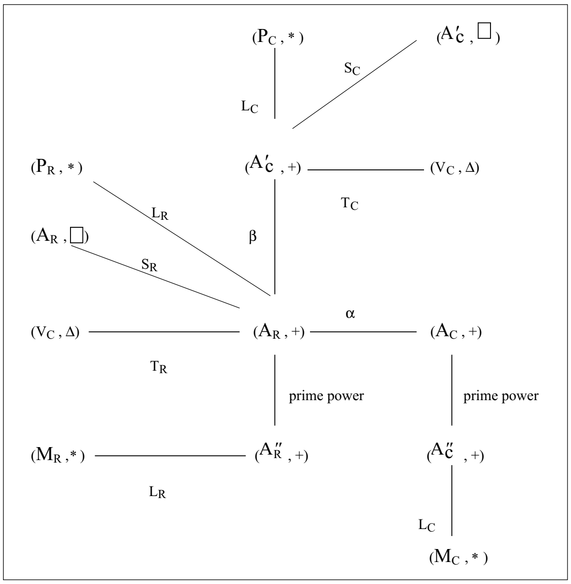
$$\alpha(f)(n) := f(2n-1) + i f(2n)$$

yields a desired isomorphism, while the map $\beta : (A_R, +) \to (A'_C, +)$ defined by

$$\beta(f)(1) = f(1),\ \beta(f)(n) = f(2n-2) + i f(2n-1)\ (n > 1),$$

yields the other desired isomorphism.

To sum up, we have the following isomorphisms diagram.





## Acknowledgements

This research is partially supported by a 1998-1999 research grant from the University of the Thai Chamber of Commerce.


## References


1. Apostol TM (1976) "Introduction to Analytic Number Theory," Springer-Verlag, New York.
2. Berberian SK (1962) Number-theoretic functions via convolution rings. *Math Magazine* 65, 75-92.
3. Carlitz L and Subbarao MV (1973) Transformation of arithmetic functions. *Duke Math J* 40, 949-58.
4. Cashwell ED and Everett CJ (1959) The ring of number-theoretic functions. *Pacific J Math* 9, 975-85.
5. McCarthy PJ (1986) "Introduction to Arithmetical Functions", Springer-Verlag, New York.
6. Rearick D (1968) Operators on algebras of arithmetic functions. *Duke Math J* 35, 761-6.
7. Rearick D (1968) The trigonometry of numbers. *Duke Math J* 35, 767-76.
8. Shapiro HN (1983) "Introduction to the Theory of Numbers," John Wiley & Sons, New York.
9. Sivaramakrishnan R (1989) "Classical Theory of Arithmetic Functions," Marcel Dekker, New York.