PACIFIC JOURNAL OF MATHEMATICS
Vol. 61, No. 1, 1975

GENERALIZED CONVOLUTION RING OF ARITHMETIC FUNCTIONS

INGRID POPA FOTINO

1. Introduction. The set of arithmetic functions has the structure of a unitary associative ring under functional addition and the convolution operation defined by

$$(1.1)\qquad (f^*g)(n)=\sum_{ab=n}f(a)g(b)\qquad a,b,n\in N\,.$$

It is also a unique factorization domain with respect to convolution.

The purpose of this paper is to determine the conditions under which this structure is preserved when the concept of convolution is generalized to include a weighting kernel γ:

$$(1.2)\qquad (f\overset{*}{_\gamma}g)(n)=\sum_{ab=n}f(a)g(b)\gamma(a,b)$$

The problem consists mainly in characterizing the kernels γ for which γ-convolution is associative. There have been several attempts to answer this question in certain special cases: A. A. Gioia [4] characterized those kernels γ which are functions of the greatest common divisor of pairs of natural integers (a, b) and for which γ-convolution is associative; T. M. K. Davison [2], defining γ-convolution by $(f\overset{*}{_\gamma}g)(n)=\sum_{ab=n}f(a)g(b)\gamma(ab, a)$, characterized those kernels $\gamma(ab, a)$ for which the subset of multiplicative arithmetic functions forms a group.

Actually, all weighting kernels γ can be fully characterized by the requirement that the set of arithmetic functions remain an associative, integral ring under γ-convolution and this is our aim (§3 and Theorem 4.2). The conditions under which unique factorization is preserved are a direct result of this characterization (§4).

Finally, the methods which yield this characterization will be applied to the more general case of the ring of functions defined on denumerably-generated abelian groups or semi-groups to obtain similar results (§5).

2. Preliminaries.

Let A denote the ring of arithmetic functions under the usual convolution (1.1) and A_γ the set of arithmetic functions together with the generalized γ-convolution (1.2).

We wish to examine first the nature of those kernels γ for which A_γ has the struture of an associative, integral ring.

It is immediate that γ-convolution is distributive with respect to functional addition for any kernel γ. The first condition imposed on

γ is due to the requiremet that A_γ be integral and is given by the following lemma whose proof is elementary:

LEMMA 2.1. *A_γ has no divisors of zero with respect to γ-convolution if and only if $\gamma(a, b) \neq 0$ for all $a, b \in N$.*

It will therefore be assumed henceforth that γ vanishes nowhere.

Given this assumption, the only requirement γ-convolution must satisfy in order that A_γ be an associative, integral ring is:

$$[(f_\gamma^* g)_\gamma^* h](n) = [f_\gamma^*(g_\gamma^* h)](n) \qquad \text{for all } n \in N . \tag{2.1}$$

Recalling definition (1.2), equation (2.1) is easily seen to be equivalent to

$$\gamma(a, b)\gamma(ab, c) = \gamma(a, bc)\gamma(b, c) \quad \text{for all } a, b, c \in N . \tag{2.2}$$

The nonvanishing solutions of this "associativity equation" (2.2) will therefore be those weighting functions γ for which A_γ has the desired structure. They are analyzed in the next section.

REMARK. 1. γ-convolution is commutative if and only if γ is symmetric i.e.

$$\gamma(a, b) = \gamma(b, a) \qquad \text{for all } a, b \in N . \tag{2.3}$$

2. If γ is a nonvanishing solution of the associativity equation (2.2) then, for all $n \in N$,

$$\begin{gathered}\gamma(1, n) = \gamma(n, 1) = \gamma(1, 1) = k \neq 0 \\ k \text{ a constant depending on } \gamma .\end{gathered} \tag{2.4}$$

Proof. Let first $a = b = 1$, then $b = c = 1$ in equation (2.2).

3. From Remark 2 and Lemma 2.1 it follows that if A_γ is an associative, integral ring then γ satisfies condition (2.4). Thus A_γ has both a left and a right identity defined by

$$e_\gamma(n) = \begin{cases} \dfrac{1}{\gamma(1, 1)} & \text{for } n = 1 . \\ 0 & \text{otherwise} \end{cases} \tag{2.5}$$

Therefore if A_γ is an associative, integral ring it is necessarily unitary.

3. **Characterization of the non-vanishing solutions of the associativity equation.** Consider a given ordering $p_1, p_2, \cdots$ of the prime numbers of N. Any integer $a \in N$ has then a prime factor

decomposition $a = \prod_i^\infty p_i^{\alpha_i}$ where the α_i's are positive integers or zero. Whithin this setting one can state:

THEOREM 3.1. *A nonvanishing function $\gamma(a, b)$ is a solution of the associativity equation* (2.2) *if and only if*

$$\gamma(a, b) = \frac{\omega(ab)}{\omega(a)\omega(b)}\mu(a, b) \qquad a, b \in N \tag{3.1}$$

where ω and μ are nonvanishing functions and μ is bi-multiplicative; γ is symmetric if and only if $\mu \equiv 1$. Furthermore, letting $a = \prod_i^\infty p_i^{\alpha_i}$ and $b = \prod_i^\infty p_i^{\beta_i}$ be the prime factor decompositions of a and b, ω and μ can be expressed in terms of γ respectively by

$$\omega(a) = \prod_{i=1}^{\infty} \prod_{j=0}^{\max(0,\alpha_i-1)} d_i c_i^{\alpha_i} \gamma(p_i, p_i^j)\gamma(p_i^{\alpha_i}, p_{i+1}^{\alpha_{i+1}} \cdots) \tag{3.2}$$

where $\{c_i\}$ is a sequence of arbitrary nonzero real numbers,

$$d_j = \begin{cases} \dfrac{1}{\gamma^3(1, 1)} & \textit{when } \alpha_i = 0 \\[2ex] \dfrac{c_i}{\gamma^2(1, 1)} & \textit{otherwise} \end{cases}$$

and

$$\mu(a) = \prod_{j=1}^{\infty} \prod_{i=j}^{\infty} \left[\frac{\gamma(p_i, p_j)}{\gamma(p_j, p_i)}\right]^{\alpha_i \beta_j} . \tag{3.3}$$

REMARK. In algebraic topology, solutions of the associativity equation (2.2) are viewed as cocycles and symmetric functions of the type (3.1), with $\mu \equiv 1$, as coboundaries. Part of Theorem 3.1 can thus be restated as follows: "a symmetric cocycle is a coboundary". This result can be proved in several ways,[1] but only in the case of symmetric cocycles. We propose to give here an elementary arithmetic proof which extends to the nonsymmetric case as well.

Proof of Theorem 3.1. One can easily verify that any function of the type (3.1) is a solution of the associativity equation (2.2).

To show the converse, consider first the symmetric solutions γ: (a) *symmetric case*. The proof will consist in the repeated application of the associativity equation (2.2). As an example, let first $a = p_1^{\alpha_1} p_2^{\alpha_2}$ and $b = p_1^{\beta_1} p_2^{\beta_2}$ or, for simplicity, $a = a_1 a_2$ and $b = b_1 b_2$. The following three expressions are a direct result of the associativity equation:

[1] For example using group extensions [3] or the Künneth formula.

$$\text{(i)} \qquad \gamma(b_1b_2, a_2) = \frac{\gamma(b_1, a_2b_2)\gamma(b_2, a_2)}{\gamma(b_1, b_2)}$$

$$\text{(ii)} \qquad \gamma(a_1, a_2b_1b_2) = \frac{\gamma(a_1, b_1)\gamma(a_1b_1, a_2b_2)}{\gamma(b_1, a_2b_2)}$$

$$\text{(iii)} \qquad \gamma(a, b) = \gamma(a_1a_2, b_1b_2) = \frac{\gamma(a_1, a_2b_1b_2)\gamma(a_2, b_1b_2)}{\gamma(a_1, a_2)}$$

Since γ is symmetric in this example, $\gamma(b_1b_2, a_2) = \gamma(a_2, b_1b_2)$ and we can therefore make in (iii) the substitutions (i) and (ii) to obtain:

$$\begin{aligned}\gamma(a, b) = \gamma(a_1a_2, b_1b_2) &= \frac{1}{\gamma(a_1, a_2)} \frac{\gamma(a_1, b_1)\gamma(a_1b_1, a_2b_2)\gamma(b_1, a_2b_2)\gamma(b_2, a_2)}{\gamma(b_1, a_2b_2)\gamma(b_1, b_2)} \\ &= \gamma(a_1, b_1)\gamma(a_2, b_2)\frac{\gamma(a_1b_1, a_2b_2)}{\gamma(a_1, a_2)\gamma(b_1, b_2)}\end{aligned}$$

or

$$\text{(iv)} \qquad \gamma(a, b) = \gamma(p_1^{\alpha_1}, p_1^{\beta_1})\gamma(p_2^{\alpha_2}, p_2^{\beta_2})\frac{\gamma(p_1^{\alpha_1+\beta_1}, p_2^{\alpha_2+\beta_2})}{\gamma(p_1^{\alpha_1}, p_2^{\alpha_2})\gamma(p_1^{\beta_1}, p_2^{\beta_2})}$$

Note that the desired form $\omega_1(ab)/\omega_1(a)\omega_1(b)$ already emerges in the last factor of equation (iv) provided we define

$$\omega_1(p_1^{\delta_1}p_2^{\delta_2}) = \omega_1(p_2^{\delta_2}p_1^{\delta_1}) \equiv \gamma(p_1^{\delta_1}, p_2^{\delta_2}) .$$

The first two factors, which involve only one prime each, can also be reduced to a similar form: let

$$\text{(3.4)} \qquad \begin{aligned}\omega_0(p^\alpha) &\equiv \prod_{j=1}^{\alpha-1} \gamma(p, p^j) \text{ for } \alpha > 1 \\ \omega_0(p) &\equiv 1 \\ \omega_0(1) &\equiv \frac{1}{k} \quad k \neq 0 \text{ the common value of } \gamma(1, n) = \gamma(n, 1) .\end{aligned}$$

It is proved in the Appendix (Lemma 6.1), by induction on the exponents, that $\gamma(p^\alpha, p^\beta)$ can then be expressed as:

$$\text{(3.5)} \qquad \gamma(p^\alpha, p^\beta) = \frac{\omega_0(p^{\alpha+\beta})}{\omega_0(p^\alpha)\omega_0(p^\beta)} .$$

It is now clear that a proper definition of ω would lead to the desired expression:

$$\gamma(p_1^{\alpha_1}p_2^{\alpha_2}, p_1^{\beta_1}p_2^{\beta_2}) = \frac{\omega(p_1^{\alpha_1+\beta_1}p_2^{\alpha_2+\beta_2})}{\omega(p_1^{\alpha_1}p_2^{\alpha_2})\omega(p_1^{\beta_1}p_2^{\beta_2})} .$$

The same procedure is followed in the general case: consider any two integers $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ where some of the exponents may be null. In exactly the same manner one can use the associativity equation to obtain

$$\begin{aligned}\gamma(a, b) &= \gamma(p_1^{\alpha_1} \cdots p_n^{\alpha_n}, p_1^{\beta_1} \cdots p_n^{\beta_n}) \\ &= \frac{\gamma(p_1^{\alpha_1}, p_1^{\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n})\gamma(p_2^{\alpha_2} \cdots p_n^{\alpha_n}, p_1^{\beta_1} \cdots p_n^{\beta_n})}{\gamma(p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p_n^{\alpha_n})} .\end{aligned} \tag{3.6}$$

Since γ is symmetric, the factor $\gamma(p_2^{\alpha_2} \cdots p_n^{\alpha_n}, p_1^{\beta_1} \cdots p_n^{\beta_n})$ can be replaced by $\gamma(p_1^{\beta_1} \cdots p_n^{\beta_n}, p_2^{\alpha_2} \cdots p_n^{\alpha_n})$ and substitutions similar to (i) and (ii) yield:

$$\begin{aligned}\gamma(a, b) = \frac{1}{\gamma(p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p_n^{\alpha_n})} & \frac{\gamma(p_1^{\alpha_1}, p_1^{\beta_1})\gamma(p_1^{\alpha_1+\beta_1}, p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n})}{\gamma(p_1^{\rho_1}, p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n})} \\ & \times \frac{\gamma(p_1^{\beta_1}, p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n})\gamma(p_2^{\beta_2} \cdots p_n^{\beta_n}, p_2^{\alpha_2} \cdots p_n^{\alpha_n})}{\gamma(p_1^{\beta_1}, p_2^{\beta_2} \cdots p_n^{\beta_n})} .\end{aligned} \tag{3.7}$$

After cancellation and rearrangement of terms one arrives at

$$\begin{aligned}\gamma(a, b) = \gamma(p_1^{\alpha_1}, p_1^{\beta_1})&\gamma(p_2^{\beta_2} \cdots p_n^{\beta_n}, p_2^{\alpha_2} \cdots p_n^{\alpha_n}) \\ &\times \frac{\gamma(p_1^{\alpha_1+\beta_1}, p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n})}{\gamma(p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p_n^{\alpha_n})\gamma(p_1^{\beta_1}, p_2^{\beta_2} \cdots p_n^{\beta_n})}\end{aligned} \tag{3.8}$$

The same procedure can now be followed starting with the middle factor $\gamma(p_1^{\alpha_2} \cdots p_n^{\alpha_n}, p_2^{\beta_2} \cdots p_n^{\beta_n})$. Repeated application of this procedure yields finally:

$$\begin{aligned}\gamma(a, b) &= \prod_{i=1}^{n} \gamma(p_i^{\alpha_i}, p_i^{\beta_i}) \prod_{i=1}^{n-1} \frac{\gamma(p_i^{\alpha_i+\beta_i}, p_{i+1}^{\alpha_{i+1}\beta_{i+1}} \cdots p_n^{\alpha_n+\beta_n}}{\gamma(p_i^{\alpha_i}, p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n})\gamma(p_i^{\beta_i}, p_{i+1}^{\beta+1} \cdots p_n^{\beta_n})} \\ &= k\prod_{i=1}^{n} \gamma(p_i^{\alpha_i}, p_i^{\beta_i}) \frac{\gamma(p_i^{\alpha_i+\beta_i}, p_{i+1}^{\alpha_{i+1}+\beta_{i+1}} \cdots p_n^{\alpha_n+\beta_n})}{\gamma(p_i^{\alpha_i}, p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n})\gamma(p_i^{\beta_i}, p_{i+1}^{\beta_{i+1}} \cdots p_n^{\beta_n})} \\ &\qquad \text{since } \alpha_{n+1} = \beta_{n+1} = 0 .\end{aligned} \tag{3.9}$$

Replacing now $\gamma(p_i^{\alpha_i}, p_i^{\beta_i})$ with the expression given by equation (3.5) and recalling definition (3.4) of ω_0 one can define ω as follows:

$$\omega(a) \equiv \frac{1}{k} \prod_{i=1}^{\infty} c_i^{\alpha_i} \omega_0(p_i^{\alpha_i})\gamma(p_i^{\alpha_i}, p_{i+1}^{\alpha_{i+1}} \cdots) \tag{3.10}$$

c^i a sequence of arbitary nonzero real numbers .

This definition is equivalent to the expression (3.2) given for ω in the statement of the theorem. Note that $\alpha_i = 0$ for those p_i which do not divide a and that the extra factors of the type $\gamma(p_i^0, p_j^{\alpha_j} \cdots p_r^{\alpha_r}) = k$ and $\omega_0(p_i^0) = 1/k$ introduced by taking infinite products cancel out for each i.

This definition of ω yields the desired expression in the symmetric case:

$$\gamma(a, b) = \frac{\omega(a)}{\omega(a)\omega(b)}$$

with $\omega(a) \neq 0$ for all a.

(b) *general case.* The proof in this case is only a slight modification of the previous one. Define

$$\sigma(a, b) \equiv \frac{\gamma(a, b)}{\gamma(b, a)} . \tag{3.12}$$

Obviously $\sigma \equiv 1$ if and only if γ is symmetric. The inclusion of σ in the previous development will suffice to carry through the differences due to nonsymmetry, after the following lemma will have specified the multiplicative nature of σ:

LEMMA 3.1. *The function $\sigma(a, b)$ is bi-multiplicative.*

Proof. From the associativity equation (2.2) one deduces:
(i) $\gamma(q, v)\gamma(qv, p) = \gamma(q, vp)\gamma(v, p)$.
(ii) $\gamma(q, p)\gamma(qp, v) = \gamma(q, pv)\gamma(p, v)$.
(iii) $\gamma(p, q)\gamma(qp, v) = \gamma(p, qv)\gamma(q, v)$.
Substituting in (ii) the expression given for $\gamma(qp, v)$ in (iii) and combining (i) and (ii) one obtains:

$$\gamma(q, pv) = \frac{\gamma(q, v)\gamma(qv, p)}{\gamma(v, p)} = \frac{\gamma(q, p)\gamma(p, qv)\gamma(q, v)}{\gamma(p, v)\gamma(p, q)} .$$

After cancellation of $\gamma(q, v)$ this yields:

$$\sigma(qv, p) = \sigma(q, p)\sigma(v, p) .$$

Since $\sigma(p, q) = 1/\sigma(q, p)$ this also implies:

$$\sigma(p, qv) = \sigma(p, q)\sigma(p, v)$$

and Lemma 3.1 is thus proved.

Repeating now the steps of the proof in the symmetric case, equation (3.6) becomes

$$\begin{aligned} \gamma(a, b) &= \frac{1}{\gamma(p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p_n^{\alpha_n})}\gamma(p_1^{\alpha_1}, p_1^{\beta_1}p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n}) \\ &\times \gamma(p_1^{\beta_1} \cdots p_n^{\beta_n}, p_2^{\alpha_2} \cdots p_n^{\alpha_n})\sigma(p_2^{\alpha_2} \cdots p_n^{\alpha_n}, p^{\beta_1} \cdots p_n^{\beta_n}) \end{aligned} \tag{3.6'}$$

where the last factor γ in (3.6) has been replaced by its symmetric in order to apply the substitutions which led to equation (3.7). After these substutitions and after cancellation one obtains:

$$\begin{aligned}\gamma(a, b) = {} & \frac{\gamma(p_1^{\alpha_1+\beta_1}, p_2^{\alpha_2+\beta_2} \cdots p_n^{\alpha_n+\beta_n})}{\gamma(p_1^{\alpha_1}, p_2^{\alpha_2} \cdots p_n^{\alpha_n})\gamma(p_1^{\beta_1}, p_2^{\beta_2} \cdots p_n^{\beta_n})}\gamma(p_1^{\alpha_1}, p_1^{\beta_1}) \\ & \times \gamma(p_2^{\alpha_2} \cdots p_n^{\alpha_n}, p_2^{\beta_2} \cdots p_n^{\beta_n})\sigma(p_2^{\beta_2} \cdots p_n^{\beta_n}, p_2^{\alpha_2} \cdots p_n^{\alpha_n}) \\ & \times \sigma(p_2^{\alpha_2} \cdots p_n^{\alpha_n}, p_1^{\beta_1} \cdots p_n^{\beta_n}) \,.\end{aligned} \tag{3.8'}$$

The product of the last two factors reduces to $\sigma(p_2^{\alpha_2} \cdots p_n^{\alpha_n}, p_1^{\beta_1})$. The final result is then:

$$\begin{aligned}\gamma(a, b) = {} & \prod_{i=1}^{n} \gamma(p_i^{\alpha_i}, p_i^{\beta_i}) \prod_{i=1}^{n-1} \frac{\gamma(p_i^{\alpha_i+\beta_i}, p_{i+1}^{\alpha_{i+1}+\beta_{i+1}} \cdots p_n^{\alpha_n+\beta_n})}{\gamma(p_i^{\alpha_i}, p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n})\gamma(p_i^{\beta_i}, p_{i+1}^{\beta_{i+1}} \cdots p_n^{\beta_n})} \\ & \times \prod_{j=1}^{n} \prod_{i=j}^{n} \sigma^{\alpha_i\beta_j}(p_i, p_j) = \frac{\omega(ab)}{\omega(a)\omega(b)}\mu(a, b)\end{aligned} \tag{3.9'}$$

where ω is defined as in the symmetric case and μ is defined in the statement of the theorem by (3.3). Note that if γ is symmetric, $\mu \equiv 1$. Theorem 3.1 is thereby proved in its most general form.

4. Unique factorization in A_γ. From §2 it results that A_γ is an associative, integral ring if and only if γ is a nonvanishing solution of the associativity equation (2.2). As a direct application of Theorem 3.1, one can now determine the conditions under which A_γ is also a unique factorization domain:

THEOREM 4.1. *The ring of arithmetic functions A_γ is a unique factorization domain with respect to γ-convolution if and only if A_γ is commutative, that is, if and only if γ is symmetric*:

$$\gamma(a, b) = \gamma(b, a) \qquad \textit{for all } a, b \in N\,.$$

Proof. The ring A of of arithmetic functions under the usual convolution operation is a unique factorization domain [1]. To prove that A_γ is a unique factorization domain when γ is symmetric it is therefore sufficient to establish that A_γ is isomorphic to $A \equiv A_1$. Since γ is symmetric one can write, by Theorem 3.1,

$$\gamma(a, b) = \frac{\omega(ab)}{\omega(a)\omega(b)}$$

where $\omega(a, b) \neq 0$ for all $a, b \in N$. The map $\alpha\colon A_1 \leftrightarrow A_\gamma$ defined by

$$\alpha(f) \equiv \omega f \quad f \in A_1$$

is the desired isomorphism.

If γ is not symmetric, a counterexample indicates that A_γ is not a unique factorization domain. In order to construct such a counterexample, note first that if γ is not symmetric, there exist three distinct elements a, b, c such that

$$\sigma(a, b) \neq \sigma(b, c)$$

where σ is defined by (3.12). For if not, one would have

$$\sigma(a, b) = \sigma(b, c) \qquad \text{for any } a, b, c \in N .$$

In particular, when $c = 1$, this would imply that $\sigma(a, b) = 1$ for all a, b contradicting the assumption that γ is not symmetric. Since σ is multiplicative in both variables, one can therefore consider three primes p, q, r such that

$$\sigma(q, p) \neq \sigma(r, p)$$

Define then

$$f(n) = \begin{cases} 1 & \text{if } n = p \\ 0 & \text{if } n \neq p \end{cases}$$

$$g_1(n) = \begin{cases} \gamma(q, p) & \text{if } n = q \\ \gamma(r, p) & \text{if } n = r \\ 0 & \text{otherwise} \end{cases}$$

$$g_2(n) = \begin{cases} \gamma(p, q) & \text{if } n = q \\ \gamma(p, r) & \text{if } n = r \\ 0 & \text{otherwise .} \end{cases}$$

The functions f, g_1, g_2 are prime and

$$f{}_\gamma^* g_1 = g_2{}^*_\gamma f \text{ .}$$

It remains to be ascertained that g_1, say, is not the γ-product of g_2 and a unit. If a unit u were to exist such that

$$g_1 = u{}_\gamma^* g_2$$

the following equations would have to be satisfied:

$$g_1(q) = u(1) g_2(q) \gamma(1, q) \tag{4.1}$$

$$g_1(r) = u(1) g_2(r) \gamma(1, r) \text{ .} \tag{4.2}$$

Equations (4.1) and (4.2) imply respectively that

$$ku(1) = \frac{g_1(q)}{g_2(q)} = \sigma(q, p)$$

and

$$ku(1) = \frac{g_1(r)}{g_2(r)} = \sigma(r, p)$$

$$\text{where } k = \gamma(1, q) = \gamma(1, r) \neq 0 \, .$$

But $\sigma(q, p) \neq (r, p)$, therefore no such unit can exist and A_γ is not a unique factorization domain.

The results of the previous three sections can be summarized in the following theorem, which answers the question initially formulated in the introduction:

THEOREM 4.2. *The set of all arithmetic functions A_γ has the structure of an associative, integral ring with respect to functional addition and γ-convolution if and only if*

$$\gamma(a, b) = \frac{\omega(ab)}{\omega(a)\omega(b)}\mu(a, b)$$

where ω and μ are nonvanishing functions and μ is bi-multiplicative. This ring is unitary. It is commutative if and only if $\mu \equiv 1$. Finally, it is a unique factorization domain if and only if it is commutative.

5. **Generalization to the set of functions over groups and semi-groups.** The methods used in the proof of Theorem 4.2 have been based solely on the semi-group properties of the natural integers N and, for the characterization of the solutions of the associativity equation, only on the group properties of the field of real or complex numbers. These methods can thus be easily extended to obtain the following generalized results:

THEOREM 5.1. (a) *Let G be a denumerably generated free abelian group or semi-group or a denumerably generated group with at least one presentation in which relations do not exceed in number the number of generators they involve. For any field F and a function $\gamma: G \times G \longrightarrow F$, the set of all functions $f: G \longrightarrow F$ is an associative, integral ring under functional addition and γ-convolution if and only if*

$$\gamma(a, b) = \frac{\omega^*(ab)}{\omega^*(a)\omega^*(b)}\mu(a, b) \tag{5.1}$$

where $\omega^*: G \longrightarrow F$ and $\mu: G \longrightarrow F$ are nonvanishing functions and μ is bi-multiplicative. This ring is commutative if and only if $\mu \equiv 1$. It is a unique factorization domain if and only if it is commutative.

(b) *Let G be as above, H any abelian group. Then a function $\gamma: G \times G \longrightarrow H$ is a solution of the associativity equation*

$$\gamma(a, b)\gamma(ab, c) = \gamma(a, bc)\gamma(b, c) \qquad a, b, c \in G$$

if and only if it is of the type (5.1)

(c) *In both previous cases, let*p_i, $i = 1, 2, \cdots$, *denote the generators of* G *and* $a = \prod_i^\infty p_i^{\alpha_i}$, $b = \prod_i^\infty p_i^{\beta_i}$ *be any two elements of* G. *Then* μ *and* ω^* *can be expressed in terms of* γ *respectively by*

$$\mu(a, b) = \prod_{j=1}^{\infty} \prod_{j=j}^{\infty} \left[\frac{\gamma(p_i, p_j)}{\gamma(p_j, p_i)}\right]^{\alpha_i\beta_j} \tag{5.2}$$

α_i, β_i *positive, negative or null integers*

and

$$\omega^*(a) = \prod_{i=1}^{\infty} \frac{1}{\gamma(1, 1)} x_i^{\alpha_i}\omega_0(p_i^{\alpha_i})\gamma(p_i^{\alpha_i}, p_{i+1}^{\alpha_{i+1}} \cdots) \tag{5.3}$$

where $\omega_0(p_i^{\alpha_i}) \equiv \prod_{j=1}^{\alpha_i-1} \gamma(p_i, p_i^j)$ *for* $\alpha_i > 1$, $\omega_0(p_i^{\alpha_i}) \equiv \prod_{j=0}^{\alpha_i} \gamma^{-1}(p_i, p_i^j)$ *for* $\alpha_i \leqq 0$, $\omega_0(p_i) = 1$ *and* x_i *is an undetermined constant if* p_i *appears in no relation of* G *or if* G *is free; otherwise* x_i *is determined in terms of values of* γ *on pairs of the type* $(p_i^{\alpha_i}, p_j^{\alpha_j} \cdots p_r^{\alpha_r})$ $i \leqq j \cdots r$, *by the relations of* G *which involve* p_i.

REMARK. Here again, part (b) of the the theorem has been proved, for symmetric γ only, by S. Eilenberg and S. MacLane [3] in the case of a free group G and by B. Jessen, J. Karpf and A. Thorup [5] in the case of any abelian group G and a divisible abelian group H. Our proof extends to nonsymmetric functions γ for any abelian group H and for the groups G indicated in the statement of the theorem.

Proof of Theorem 5.1. The proof of Theorem 4.2 applies here, unaltered in the case of a free semi-group G and with modifications, in the case of a free group or a group with relations, only in the characterization of the solutions of the associativity equation (2.2).

If G is free, definition (3.4) of ω_0 must simply be replaced by definition (6.5) of the appendix to include negative as well as positive exponents.

If G has relations, note that equalities (3.6′) through (3.9′) remain valid, as they are entirely based on the associativity equation (2.2) and only solutions γ of that equation are considered. The definition of ω however must be modified to ensure that it is well defined: if G has relations of the type

$$p_j^{\rho_j} \cdots p_r^{\rho_r} = 1$$

then one must have, for $\alpha_i = \eta_i\rho_i + \delta_i$, $i = j, \cdots, r$

$$\omega(p_j^{\alpha_j} \cdots p_r^{\alpha_r}) = \omega(p_j^{\delta_j} \cdots p_r^{\delta_r}) \tag{5.4}$$

Redefine then ω as follows:

$$\omega^*(p_1^{\alpha_1} \cdots p_n^{\alpha_n}) \equiv \prod_{i=1}^{n-1} x_i^{\alpha_i}\omega_0(p_i^{\alpha_i})\omega_0(p_i^{\alpha_i}, p_{i+1}^{\alpha_{i+1}} \cdots p_n^{\alpha_n})x_n^{\alpha_n}\omega_0(p_n^{\alpha_n}) \tag{5.5}$$

where ω_0 is defined by (6.5). (For the sake of clarity ω^* is defined in terms of finite n, but here again infinite products may be taken as the extra factors thus introduced cancel out.)

One can immediately see from equation (3.9′) that, with this definition of ω^*,

$$\gamma(a, b) = \frac{\omega^*(ab)}{\omega^*(a)\omega^*(b)}\mu(a, b) .$$

It is also a matter of verification, though much more elaborate, that ω^* is indeed well defined.

The x_i's are determined in terms of values of γ on pairs of the type $(p_j^{\alpha_j}, p_k^{\alpha_k} \cdots p_r^{\alpha_r})$, $i \leqq j, \cdots, r$, by the requirement (5.4) and by the relations of G which involve p_i, provided these relations do not exceed in number the number of generators they involve.

For example, in the special case of a finite cyclic group of order ρ, the requirement

$$\omega^*(p^{\eta\rho+\delta}) = \omega^*(p^\delta) \qquad 0 < \delta < \rho$$

implies

$$x^{\eta\rho+\delta} \prod_{j=1}^{\eta\rho+\delta-1} \gamma(p, p^j) = x^\delta \prod_{j=1}^{\delta-1} \gamma(p, p^j)$$

or

$$x^{\eta\rho} \prod_{j=\delta}^{\eta\rho+\delta-1} \gamma(p, p^j) = 1 .$$

Since

$$\prod_{j=\delta}^{\eta\delta+\delta-1} \gamma(p, p^j) = \left[\prod_{j=0}^{\rho-1} \gamma(p, p^j)\right]^\eta$$

one obtains

$$x^{\eta\rho} = \left[\prod_{j=0}^{\rho-1} \gamma(p, p^j)\right]^{-\eta}$$

and

$$x = \left[\prod_{j=0}^{p-1} \gamma(p, p^j)\right]^{-1/p} .$$

6. Appendix. For any given prime number or generator p and positive, negative or null exponents α, β, denote $\gamma(p^\alpha, p^\beta)$ by

$$\Gamma(\alpha, \beta) \equiv \gamma(p^\alpha, p^\beta) . \tag{6.1}$$

The associativity equation (2.2) then becomes:

$$\Gamma(\alpha, \beta)\Gamma(\alpha + \beta, \delta) = \Gamma(\alpha, \beta + \delta)\Gamma(\beta, \delta) \qquad \alpha, \beta, \delta \in \boldsymbol{Z} \tag{6.2}$$

LEMMA 6.1. *Any solution of the associativity equation* (6.2) *is symmetric and can be expressed as*

$$\Gamma(\alpha, \beta) = \Omega(\alpha + \beta)\Omega^{-1}(\alpha)\Omega^{-1}(\beta) \qquad \textit{for } \alpha, \beta \in \boldsymbol{Z} \tag{6.3}$$

where

$$\begin{aligned} \Omega(\alpha) &\equiv \prod_{j=1}^{\alpha-1} \Gamma(1, j)c^\alpha \quad \textit{for } \alpha > 1,\ c \textit{ a nonzero constant} \\ \Omega(\alpha) &\equiv \prod_{j=0}^{\alpha} \Gamma^{-1}(1, j)c^\alpha \qquad\qquad \textit{for } \alpha \leqq 0 \\ \Omega(1) &\equiv c . \end{aligned} \tag{6.4}$$

These results remain valid when the domain of Γ is limited to positive and null integers only.

REMARK. Reverting to the usual notation and letting $c = 1$, definition (6.4) can be rewritten as:

$$\begin{aligned} \omega_0(p^\alpha) &\equiv \prod_{j=1}^{\alpha-1} \gamma(p, p^j) \qquad \text{for } \alpha > 1 \\ \omega_0(p^\alpha) &\equiv \prod_{j=0}^{\alpha} \gamma^{-1}(p, p^j) \qquad \text{for } \alpha \leqq 0 \\ \omega_0(p) &\equiv 1 . \end{aligned} \tag{6.5}$$

Proof of Lemma 6.1. The symmetry of Γ is proved by repeated induction: it is already known from equation (2.4) that

$$\Gamma(0, \alpha) = \Gamma(\alpha, 0) = \Gamma(0, 0) = k \qquad \text{for all } \alpha \in \boldsymbol{Z}$$

Let $\alpha = \delta = 1$ in (6.2):

$$\Gamma(1, \beta)\Gamma(\beta + 1, 1) = \Gamma(1, \beta + 1)\Gamma(\beta, 1) .$$

Induction on β yields

$$\Gamma(\beta, 1) = \Gamma(1, \beta) . \qquad \text{for all } \beta \in \boldsymbol{Z}$$

Assume now that

$$\Gamma(\beta, \eta) = \Gamma(\eta, \beta) \tag{6.6}$$

for any $\beta \in \boldsymbol{Z}$ and $\eta = 0, \cdots, \eta_0$.

Then in particular

$$\Gamma(\varepsilon, \eta_0) = \Gamma(\eta_0, \varepsilon) \qquad \text{for } 0 \leqq |\varepsilon| \leqq |\eta_0| \tag{6.7}$$

and, from the associativity equation (6.2) with $\alpha = \delta = \eta_0$, $\beta = \varepsilon$:

$$\Gamma(\eta_0 + \varepsilon, \eta_0) = \Gamma(\eta_0, \eta_0 + \varepsilon)\ . \tag{6.8}$$

Thus, for $\mu = 1$,

$$\Gamma(\mu\eta_0 + \varepsilon, \eta_0) = \Gamma(\eta_0, \mu\eta_0 + \varepsilon)\ . \tag{6.9}$$

One can now apply induction on μ using the associativity equation (6.2) as follows:

$$\Gamma(\eta_0, \mu\eta_0 + \varepsilon)\Gamma((\mu + 1)\eta_0 + \varepsilon, \eta_0) = \Gamma(\eta_0, (\mu + 1)\eta_0 + \varepsilon)\Gamma(\mu\eta_0 + \varepsilon, \eta_0)$$

Therefore (6.6) is true for all $\eta = \mu\eta_0 + \varepsilon$ and Γ is symmetric.

To prove the rest of the lemma, define, for any solution Γ of the associativity equation (6.2):

$$\theta(\alpha) \equiv \Gamma(1, \alpha) = \Gamma(\alpha, 1)\ . \tag{6.10}$$

This definition is valid since Γ is symmetric. From the associativity equation (6.2) one deduces:

$$\Gamma(2, \beta) = \theta(\beta + 1)\theta(\beta)\theta^{-1}(1) \qquad \text{for all } \beta \in \boldsymbol{Z} \tag{6.11}$$

and

$$\Gamma(-1, \beta) = \theta(-1)\theta^{-1}(\beta - 1)\theta(0) \qquad \text{for all } \beta \in \boldsymbol{Z} \tag{6.12}$$

Applying induction one can now obtain, again from equation (6.2):

$$\Gamma(\alpha, \beta) = \prod_{j=0}^{\alpha-1} \theta(\beta + j)\theta^{-1}(j)\theta(0) \qquad \text{for } \alpha > 0,\ \beta \in \boldsymbol{Z} \tag{6.13}$$

and

$$\Gamma(\alpha, \beta) = \prod_{j=0}^{\alpha} \theta^{-1}(\beta + j)\theta(j)\theta(\beta) \qquad \text{for } \alpha \leqq 0,\ \beta \in \boldsymbol{Z}\ . \tag{6.14}$$

Given these expressions for Γ and definition (6.4) of Ω, it can be verified that equality (6.3) is true.

This proof is essentially unaltered if the domain of Γ is limited to the positive and null integers.

Remark. It is immediate that, conversely, any function Γ of the type (6.4) is symmetric and a solution of the associativity equation (6.2).

Acknowledgment. The author wishes to express her gratitutde to Professor Harold N. Shapiro for his constant and stimulating guidance throughout this work which originated in one of his articles [6].

References

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

2. T. M. K. Davison, *On arithmetic convolutions*, Canad. Math. Bull., **9** (1966), 287-296.

3. S. Eilenberg and S. MacLane, *Group extensions and homology*, Annals of Math. 2nd series, **43** (1942), 768.

4. A. A. Gioia, *The K-product of arithmetic functions*, Canad. J. Math., **17** (1965), 970-976.

5. Børge Jessen, Jørgen Karpf, Anders Thorup, *Some functional equations in groups and rings*, Math. Scand., **22** (1968), 257-265.

6. H. N. Shapiro, *On the convolution ring of arithmetic functions*, Communications on Pure and Applied Mathematics, **25** (1972), 287-336.

Received July 23, 1974 and in revised form September 3, 1975. This research was supported in part by NSF Grant #MPS 73-08659, Courant Institute of Mathematical Sciences.

Courant Institute of Mathematical Sciences, New York University, N. Y.