Characterization of regular convolutions

Sankar Sagi

 Communicated by V. V. Kirichenko

Abstract. A convolution is a mapping $C$ of the set $\mathbb{Z}^+$ of positive integers into the set $\mathcal{P}(\mathbb{Z}^+)$ of all subsets of $\mathbb{Z}^+$ such that, for any $n \in \mathbb{Z}^+$, each member of $C(n)$ is a divisor of $n$. If $D(n)$ is the set of all divisors of $n$, for any $n$, then $D$ is called the Dirichlet’s convolution [2]. If $U(n)$ is the set of all Unitary(square free) divisors of $n$, for any $n$, then $U$ is called unitary(square free) convolution. Corresponding to any general convolution $C$, we can define a binary relation $\leq_C$ on $\mathbb{Z}^+$ by ‘$m \leq_C n$ if and only if $m \in C(n)$’. In this paper, we present a characterization of regular convolution.

Introduction

A convolution is a mapping $C$ of the set $\mathbb{Z}^+$ of positive integers into the set $\mathcal{P}(\mathbb{Z}^+)$ of subsets of $\mathbb{Z}^+$ such that, for any $n \in \mathbb{Z}^+$, $C(n)$ is a nonempty set of divisors of $n$. If $C(n)$ is the set of all divisors of $n$, for each $n \in \mathbb{Z}^+$, then $C$ is the classical Dirichlet convolution [2]. If

$$C(n) = \{d / d|n \text{ and } \left\lfloor\frac{n}{d}\right\rfloor = 1\},$$

then $C$ is the Unitary convolution [1]. As another example if

$$C(n) = \{d / d|n \text{ and } m^k \text{ does not divide } d \text{ for any } m \in \mathbb{Z}^+\},$$

then $C$ is the $k$-free convolution. Corresponding to any convolution $C$, we can define a binary relation $\leq_C$ in a natural way by

$$m \leq_C n \quad \text{if and only if } \quad m \in C(n).$$

2010 MSC: 06B10, 11A99.

Key words and phrases: semilattice, lattice, convolution, multiplicative, co-maximal, prime filter, cover, regular convolution.
$\leq_{C}$ is a partial order on $Z^+$ and is called partial order induced by the convolution $C$ [11], [12]. W. Narkiewicz [2] first proposed the concept of a regular convolution, and in this paper we present a lattice theoretic characterization of regular convolution and prove that the Dirichlet’s convolution is the unique regular convolution that induces a lattice structure on $(Z^+, \leq_C)$.

1. Preliminaries

Let us recall that a partial order on a non-empty set $X$ is defined as a binary relation $\leq$ on $X$ which is reflexive ($a \leq a$), transitive ($a \leq b, b \leq c \implies a \leq c$) and antisymmetric ($a \leq b, b \leq a \implies a = b$) and that a pair $(X, \leq)$ is called a partially ordered set (poset) if $X$ is a non-empty set and $\leq$ is a partial order on $X$.

For any $A \subseteq X$ and $x \in X$, $x$ is called a lower (upper) bound of $A$ if $x \leq a$ (respectively $a \leq x$) for all $a \in A$. We have the usual notations of the greatest lower bound (glb) and least upper bound (lub) of $A$ in $X$. If $A$ is a finite subset $\{a_1, a_2, \ldots, a_n\}$, the glb of $A$ (lub of $A$) is denoted by $a_1 \land a_2 \land \cdots \land a_n$ or $\bigwedge_{i=1}^{n} a_i$ (respectively by $a_1 \lor a_2 \lor \cdots \lor a_n$ or $\bigvee_{i=1}^{n} a_i$).

A partially ordered set $(X, \leq)$ is called a meet semi lattice if $a \land b (=\text{glb}\{a, b\})$ exists for all $a$ and $b \in X$. $(X, \leq)$ is called a join semi lattice if $a \lor b (=\text{lub}\{a, b\})$ exists for all $a$ and $b \in X$. A poset $(X, \leq)$ is called a lattice if it is both a meet and join semi lattice. Equivalently, lattice can also be defined as an algebraic system $(X, \land, \lor)$, where $\land$ and $\lor$ are binary operations which are associative, commutative and idempotent and satisfying the absorption laws, namely $a \land (a \lor b) = a = a \lor (a \land b)$ for all $a, b \in X$; in this case the partial order $\leq$ on $X$ is such that $a \land b$ and $a \lor b$ are respectively the glb and lub of $\{a, b\}$. The algebraic operations $\land$ and $\lor$ and the partial order $\leq$ are related by

$$a = a \land b \iff a \leq b \iff a \lor b = b.$$  

Throughout the paper $Z^+$, $N$, and $P$ denote the set of positive integers, the set of non-negative integers, and set of prime numbers respectively.

**Theorem 1** ([12]). Let $\leq_{C}$ be the binary relation induced by convolution $C$. Then

1. $\leq_{C}$ is reflexive if and only if $n \in C(n)$.
2. $\leq_{C}$ is transitive if and only, for any $n \in Z^+$, $\bigcup_{m \in C(n)} C(m) \subseteq C(n)$.
3. $\leq_{C}$ is always antisymmetric.
Corollary 1 ([12]). The binary relation $\leq_C$ induced by convolution $C$ on $\mathbb{Z}^+$ is a partial order if and only if $n \in C(n)$ and $\bigcup_{m \in C(n)} C(m) \subseteq C(n)$ for all $n \in \mathbb{Z}^+$.

Definition 1 ([12]). Let $X$ and $Y$ be non-empty sets and $R$ and $S$ be binary relations on $X$ and $Y$ respectively. A bijection $f : X \to Y$ is said to be a relation isomorphism of $(X, R)$ into $(Y, S)$ if, for any elements $a$ and $b$ in $X$,

$$aRb \text{ in } X \text{ if and only if } f(a)Sf(b) \text{ in } Y.$$ 

Theorem 2 ([12]). Let $\theta : \mathbb{Z}^+ \to \sum_P N$ be the bijection defined by

$$\theta(n)(p) = \text{the largest } a \text{ in } N \text{ such that } p^a \text{ divides } n,$$

Then a convolution $C$ is multiplicative if and only if $\theta$ is a relation isomorphism of $(\mathbb{Z}^+, \leq_C)$ onto $(\sum_P N, \leq_C)$.

Theorem 3 ([9], [10]). For any multiplicative convolution $C$, $(\mathbb{Z}^+, \leq_C)$ is a lattice if and only if $(N, \leq^p_C)$ is a lattice for each prime $p$.

Now we state the following theorems on co-maximality and prime filters.

Theorem 4 ([5]). Let $(S, \wedge)$ be any meet semi lattice with smallest element $0$ satisfying the descending chain condition. Also, suppose that every proper filter of $S$ is prime. Then the following are equivalent to each other.

1. For any $x$ and $y \in S$, $x \parallel y \iff x \wedge y = 0$.
2. $S - \{0\}$ is a disjoint union of maximal chains.
3. Any two incomparable filters of $S$ are co-maximal.

Theorem 5 ([5]). Let $C$ be any multiplicative convolution such that $(\mathbb{Z}^+, \leq_C)$ is a meet semi lattice. Then any two incomparable prime filters of $(\mathbb{Z}^+, \leq_C)$ are co-maximal if and only if any two incomparable prime filters of $(N, \leq^p_C)$ are co-maximal, for each $p \in P$.

Theorem 6 ([3]). Let $p$ be a prime number. Then every proper filter in $(N, \leq^p_C)$ is prime if and only if $[p^a]$ is a prime filter in $(\mathbb{Z}^+, \leq_C)$ for all $n > 0$.

Theorem 7 ([3]). A filter $F$ of $(\mathbb{Z}^+, \leq_C)$ is prime if and only if there exists unique $p \in P$ such that $F^p$ is a prime filter of $(N, \leq^p_C)$ and $F^q = N$ for all $q \neq p$ in $P$ and, in this case,

$$F = \{ n \in \mathbb{Z}^+ \mid \theta(n)(p) \in F^p \}.$$
Theorem 8 ([3]). Let $F$ be a filter of $(Z^+, \leq_C)$. Then $F = [p^a]$ for some prime number $p$ and a positive integer $a$ which is join-irreducible in $(Z^+, \leq_C)$.

Definition 2. Any complex valued function defined on the set $Z^+$ of positive integers is called an arithmetical function. The set of all arithmetical functions is denoted by $\mathcal{A}$.

The following is a routine verification using the properties of addition and multiplication of complex numbers.

Theorem 9. For any arithmetical functions $f$ and $g$, define

$$(f + g)(n) = f(n) + g(n) \quad \text{and} \quad (f \cdot g)(n) = f(n)g(n)$$

for any $n \in Z^+$.

Then $+ \text{ and } \cdot$ are binary operations on the set $\mathcal{A}$ of arithmetical functions and $(\mathcal{A}, +, \cdot)$ is a commutative ring with unity in which the constant map $\overline{0}$ and $\overline{1}$ are the zero element and unity element respectively.

Definition 3. Let $C$ be a convolution and $f$ and $g$ arithmetical functions and $\mathcal{C}$ be the field of complex numbers. Define $fCg: Z^+ \rightarrow \mathcal{C}$ by

$$(fCg)(n) = \sum_{d \in C(n)} f(d)g\left(\frac{n}{d}\right).$$

We can consider $C$ as a binary operation, as defined above, on the set $\mathcal{A}$ of arithmetical functions. W.Narkiewicz proposed the following definition.

Definition 4 ([2]). A convolution $C$ is called regular if the following are satisfied.

1. $(\mathcal{A}, +, C)$ is a commutative ring with unity, where $+$ is the point-wise addition. This ring will be denoted by $\mathcal{A}_C$.
2. If $f$ and $g$ are multiplicative arithmetical functions, then so is the product $fCg$ (f is said to be multiplicative if $f(mn) = f(m)f(n)$.)
3. The constant function $\overline{1}$, defined by $\overline{1}(n) = 1$ for all $n \in Z^+$, is a unit in the ring $\mathcal{A}_C$.

It can be easily verified that the arithmetical function $e$, defined by

$$e(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1 \end{cases}$$

is the unity (the identity element with respect to the binary operation $C$).
W. Narkiewicz proved the following two theorems.

**Theorem 10 ([2]).** A convolution $C$ is regular if and only if the following conditions are satisfied for any $m, n$ and $d \in Z^+$.

1. $C$ is multiplicative convolution; i.e., $(m, n) = 1 \Rightarrow C(mn) = C(m)C(n)$.
2. $d \in C(m)$ and $m \in C(n) \Rightarrow d \in C(n)$ and $\frac{m}{d} \in C(\frac{n}{d})$.
3. $d \in C(n) \Rightarrow n \in C(\frac{n}{d})$.
4. $1 \in C(n)$ and $n \in C(n)$.
5. For any prime number $p$ and any $a \in Z^+$, $C(p^a) = \{1, p^t, p^{2t}, \cdots, p^{rt}\}$, $rt = a$ for some positive integer $t$ and $p^t \in C(p^{2t})$, $p^{2t} \in C(p^{3t})$, $\cdots$, $p^{(r-1)t} \in C(p^a)$.

**Theorem 11 ([2]).** Let $\mathcal{K}$ be the class of all decompositions of the set of non-negative integers into arithmetic progressions (finite or infinite) each containing 0 and no two progressions belonging to same decomposition have a positive integer in common. Let us associate with each $p \in P$, a member $\pi_p$ of $\mathcal{K}$. For any $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, where $p_1, p_2, \cdots, p_r$ are distinct primes and $a_1, a_2, \cdots, a_r \in N$, define

$$C(n) = \{p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r} | b_i \leq a_i, \text{ and } b_i \text{ and } a_i \text{ belong to the same progression in } \pi_{p_i}\}.$$  

Then $C$ is a regular convolution and, conversely every regular convolution can be obtained in this way.

From the above theorems, it is clear that any regular convolution $C$ is uniquely determined by a sequence $\{\pi_p\}_{p \in P}$ of decompositions of $N$ into arithmetical progressions (finite or infinite) and we denote this by expression $C \sim \{\pi_p\}_{p \in P}$.

**Definition 5.** For any two elements $a$ and $b$ in a partially ordered set $(X, \leq)$, $a$ is said to be covered by $b$ ($b$ is a cover of $a$) if $a < b$ and there is no $c \in X$ such that $a < c < b$. This is denoted by $a- < b$.

We note that $\theta : Z^+ \to \sum_P N$ defined by

$$\theta(a)(p) = \text{the largest } n \text{ in } N \text{ such that } p^n \text{ divides } a,$$

for any $a \in Z^+$ and $p \in P$

is a bijection.

2. **Main results**

In the following two theorems, we prove that any regular convolution $C$ gives a meet semi lattice structure on $(Z^+, \leq_C)$ and the convolution $C$ is
completely characterized by certain lattice theoretic properties of \((Z^+, \leq_C)\).

In particular Dirichlet’s convolution is the only regular convolution \(C\) which
gives a lattice structure on \((Z^+, \leq_C)\).

**Theorem 12.** Let \(C\) be a convolution and \(\leq_C\) the relation on \(Z^+\) induced
by \(C\). Then \(C\) is a regular convolution if and only if the following properties
are satisfied.

1. \(\theta: (Z^+, \leq_C) \to \sum_{p \in P} (N, \leq^p_C)\) is a relation isomorphism.
2. \((Z^+, \leq_C)\) is a meet semi lattice.
3. Any two incomparable prime filters of \((Z^+, \leq_C)\) are co-maximal.
4. \(F\) is a prime filter of \((Z^+, \leq_C)\) if and only if \(F = [p^a]\) for some
\(p \in P\) and \(a \in Z^+\).
5. For any \(m\) and \(n\) in \(Z^+\), \(m <_C n \implies 1 <_C \frac{n}{m} <_C n\).

**Proof.** Suppose that \(C\) is a regular convolution. By Theorem 11,
\(C \sim \{\pi_p\}_{p \in P}\), where each \(\pi_p\) is a decomposition of \(N\) into arithmetic
progressions (finite or infinite) in which each progression contains 0 and
no positive integer belongs to two distinct progressions. For any \(a, b \in N\)
and \(p \in P\), let us write for convenience,

\[\langle a < b \rangle \in \pi_p \iff a\text{ and }b\text{ belong to the same progression of }\pi_p.\]

Since \(C\) is regular, \(C\) satisfies properties (1)–(5) of Theorem 10. From
(2) and (4) of Theorem 10 and Corollary 1, it follows that \(\leq_C\) is a partial
order on \(Z^+\). Since \(C\) is multiplicative, it follows from Theorem 2 that
\(\theta: Z^+ \to \sum_{p \in P} N\) is an order isomorphism. Therefore the property (1) is
satisfied. For simplicity and convenience, we shall write \(\bar{n}\) for \(\theta(n)\). For
each \(n \in Z^+\), \(\bar{n}\) is the element in the direct sum \(\sum_{p \in P} N\) defined by

\[\bar{n}(p) = \text{the largest } a \text{ in } N \text{ such that } p^a \text{ divides } n.\]

\(n \mapsto \bar{n}\) is an order isomorphism of \((Z^+, \leq_C)\) onto \(\sum_{p \in P} (N, \leq^p_C)\), where for
each \(p \in P\), \(\leq^p_C\) is the partial order on \(N\) defined by

\[a \leq^p_C b \iff p^a \in C(p^b).\]

For any \(m\) and \(n\) in \(Z^+\), let \(m \wedge n\) be the element in \(Z^+\) defined by

\[\overline{m \wedge n}(p) = \begin{cases} 0 & \text{if } \langle \overline{m}(p), \overline{n}(p) \rangle \notin \pi_p, \\ \min\{\overline{m}(p), \overline{n}(p)\} & \text{otherwise.} \end{cases}\]

for all \(p \in P\). If \(\langle \overline{m}(p), \overline{n}(p) \rangle \in \pi_p\), then

\[\overline{m}(p) \leq^p_C \overline{n}(p) \text{ or } \overline{n}(p) \leq^p_C \overline{m}(p)\]
and hence $m \wedge \overline{n} \preceq \overline{m} \wedge \overline{n}$ for all $p \in P$. Therefore $m \wedge n$ is a lower bound of $m$ and $n$ in $(\mathbb{Z}^+, \preceq_C)$. Let $k$ be any other lower bound of $m$ and $n$. For any $p \in P$, if $(\overline{m}(p), \overline{n}(p)) \in \pi_p$, then, since

$$k(p) \preceq_C^p \overline{m}(p) \quad \text{and} \quad k(p) \preceq_C^p \overline{n}(p),$$

we have

$$k(p) \preceq_C^p m \wedge \overline{n}(p).$$

If $(\overline{m}(p), \overline{n}(p)) \notin \pi_p$, then

$$k(p) = 0 = m \wedge \overline{n}(p).$$

Thus $k \preceq m \wedge n$. Therefore, $m \wedge n$ is the greatest lower bound of $m$ and $n$ in $(\mathbb{Z}^+, \preceq_C)$. Thus $(\mathbb{Z}^+, \preceq_C)$ is a meet semi lattice and hence the property (2) is satisfied.

To prove (3), by Theorem 5, it is enough if we prove that any two incomparable prime filters of $(N, \preceq_C^p)$ are co-maximal for all $p \in P$. For any positive $a$ and $b$, if $a$ and $b$ are incomparable in $(N, \preceq_C^p)$, then $(a, b) \notin \pi_p$ and hence $a$ and $b$ have no upper bound and therefore $a \vee b$ does not exist in $(N, \preceq_C^p)$. Also, each progression in $\pi_p$ is a maximal chain in $(N, \preceq_C^p)$ and, for any $a$ and $b \in N$, $a$ and $b$ are comparable if and only if $(a, b) \in \pi_p$.

Therefore $(\mathbb{Z}^+, \preceq_C^p)$ is a disjoint union of maximal chains. Thus, by Theorem 4, any two incomparable prime filters of $(N, \preceq_C^p)$ are co-maximal. Therefore, by Theorem 5, any two incomparable prime filters of $(\mathbb{Z}^+, \preceq_C)$ are co-maximal. This proves (3).

(4) follows from Theorem 6 and Theorem 7 and from the discussion made above.

To prove (5), let $m$ and $n \in \mathbb{Z}^+$ such that $m <_C n$. By Theorem 10 (3), we get that $\frac{m}{n} \leq_C n$. Let us write

$$n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} \quad \text{and} \quad m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $p_1, p_2, \cdots, p_r$ are distinct primes and each $b_i > 0$ such that $0 \preceq_C^{p_i} a_i <_C^{p_i} b_i$. Since $m \neq n$, there exists $i$ such that $a_i \preceq_C^{p_i} b_i$. Now, if $a_j \preceq_C^{p_i} b_j$ for some $j \neq i$, then the element $k = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$, where

$$c_s = \begin{cases} a_s & \text{if } s \neq i, \\ b_s & \text{if } s = i. \end{cases}$$

will be between $m$ and $n$ (that is, $m <_C k <_C n$) which is a contradiction.

Therefore $a_j = b_j$ for all $j \neq i$ and hence $\frac{n}{m} = p_i^{a_i - b_i}$. 

Since \( \langle a_i, b_i \rangle \in \pi_i \), there exists \( t > 0 \) such that

\[
b_i = ut \quad \text{and} \quad a_i = vt
\]

for some \( u \) and \( v \) with \( v < u \). Also, \( vt, (v + 1)t, \cdots, ut \) are all in the same progression. Since \( m - \langle c n \rangle \), it follows that \( u = v + 1 \) and hence \( \frac{n}{m} = \pi_i \). Since \( 0 - \langle t \rangle \) in \( (N, \leq \pi_i^c) \), we get that

\[
1 - \langle c \rangle \pi_i^t = \frac{n}{m} \leq c n.
\]

This proves (5).

Conversely suppose that \( C \) satisfies properties (1)–(5), since \([p^a] \) is prime filter of \((Z^+, \leq_C)\) for all \( p \in P \) and \( a \in Z^+ \), by Theorem 6, every proper filter of \((N, \leq \pi_i^p)\) is prime, for any \( p \in P \). Since any two incomparable prime filters of \((Z^+, \leq_C)\) are co-maximal, by Theorem 8 and Theorem 5, we get that \((Z^+, \leq_C^p)\) is a disjoint union of maximal chains.

Fix \( p \in P \). Then

\[
Z^+ = \bigcap_{i \in I} Y_i
\]

where each \( Y_i \) is a maximal chain in \((Z^+, \leq_C^p)\) such that, for any \( i \neq j \in I \), \( Y_i \cap Y_j = \emptyset \) and each element of \( Y_i \) is incomparable with each element of \( Y_j \). Now, we shall prove that each \( Y_i \) is an arithmetical progression (finite or infinite).

Let \( i \in I \). Since \( N \) is countable, \( Y_i \) is at most countable. Also, since \((N, \leq \pi_i^p)\) satisfies the descending chain condition, we can express

\[
Y_i = \{ a_1 - \langle c \rangle a_2 - \langle c \rangle a_3 - < \ldots \}
\]

By using induction on \( r \), we shall prove that \( a_r = ra_1 \) for all \( r \).

Clearly, this is true for \( r = 1 \). Assume that \( r > 1 \) and \( a_s = sa_1 \) for all \( 1 \leq s < r \). Since \((r - 1)a_1 = a_{r-1} - < a_r \) in \((N, \leq \pi_i^p)\), we have

\[
p^{a_{r-1}} - \langle c \rangle p^{a_r} \text{ in } (Z^+, \leq_C^p)
\]

and hence, by condition (5),

\[
1 - \langle c \rangle p^{a_r - a_{r-1}} \leq_C p^{a_r}.
\]

Therefore, \( 0 \neq a_r - a_{r-1} \leq_C p a_r \) and hence \( a_r - a_{r-1} \in Y_i \) (since \( a_r \in Y_i \)).

Also, since \( 0 - \langle a_r - a_{r-1} \rangle \) in \((N, \leq \pi_i^p)\), we have \( a_r - a_{r-1} = a_1 \) and therefore \( a_r = a_{r-1} + a_1 = (r - 1)a_1 + a_1 = ra_1 \). Hence, for any prime \( p \)
and \( a \in \mathbb{Z}^+ \),
\[
\mathcal{C}(p^a) = \{1, p^t, p^{2t}, \ldots, p^{st}\} \quad \text{and} \quad st = a
\]
for some positive integers \( t \) and \( s \) and
\[
p^t \in \mathcal{C}(p^{2t}), p^{2t} \in \mathcal{C}(p^{3t}), \ldots, p^{(s-1)t} \in \mathcal{C}(p^a).
\]
The other conditions given in Theorem 10 are clearly satisfied. Thus, by Theorem 10, \( \mathcal{C} \) is a regular convolution.

\[ \square \]

**Theorem 13.** Let \( \mathcal{C} \) be a convolution, then the following conditions are equivalent to each other.
1. \((\mathbb{Z}^+, \leq_C)\) is a lattice.
2. \((\mathbb{N}, \leq^p_C)\) is a lattice for each \( p \in P \).
3. \((\mathbb{N}, \leq_C)\) is a totally ordered set for each \( p \in P \).
4. For any \( p \in P \) and \( a, b \in \mathbb{N} \), \( a \leq^p_C b \iff a \leq b \).
5. For any \( n \) and \( m \in \mathbb{Z}^+ \), \( n \leq_C m \iff n \text{ divides } m \).
6. \( \mathcal{C}(n) = \) The set of positive divisors of \( n \).

**Proof.** Since \( \mathcal{C} \) is regular, \( \mathcal{C} \sim \{\pi_p\}_{p \in P} \).

1. \( \implies \) (2) follows from Theorem 3.

2. \( \implies \) (3) Let \( p \in P \). Suppose that \((\mathbb{N}, \leq^p_C)\) is a lattice. If \( \pi_p \) contains two progressions, then choose an element \( a \) in one progression \( S \) and \( b \) in another progression \( T \) in \( \pi_p \). Since \( a \leq^p_C b \) and \( b \leq_C a \), \( a \lor b \in S \cap T \). A contradiction.

Therefore \( \pi_p \) contains only one progression, which must be
\[
N = \{0 <^p_C 1 <^p_C 2 <^p_C 3 <^p_C \ldots \}.
\]

Thus \((\mathbb{N}, \leq^p_C)\) is a totally ordered set.

3. \( \implies \) (4) It is trivial.

4. \( \implies \) (5) Let \( m \) and \( n \in \mathbb{Z}^+ \) and we write \( n = \prod_{i=1}^r P_i^a_i \) and \( m = \prod_{i=1}^r P_i^{b_i} \), where \( p_1, p_2, \ldots, p_r \) are distinct primes and \( a_i, b_i \in \mathbb{N} \). Now,
\[
n \text{ divides } m \iff a_i \leq b_i \text{ for all } 1 \leq i \leq r \\
\iff a_i \leq^p_C b_i \text{ for all } 1 \leq i \leq r \\
\iff n \leq_C m.
\]

5. \( \implies \) (6) For any \( n \in \mathbb{Z}^+ \),
\[
\mathcal{C}(n) = \{m \in \mathbb{Z}^+ \mid m \leq_C n\} = \{m \in \mathbb{Z}^+ \mid m \text{ divides } n\} = \mathcal{D}(n).
\]
(6) \implies (1) If \( C = D \), then \( \leq_C \leq_D \) and, for any \( n, m \in \mathbb{Z}^+ \),
\[
    n \wedge m = \gcd\{n, m\}
\]
and \( n \vee m = \text{lcm}\{n, m\} \) in \((\mathbb{Z}^+, \leq_C)\). \hfill \Box

The above Theorem implies that the Dirichlet’s convolution \( D \) is the only regular convolution for which \((\mathbb{Z}^+, \leq_C)\) is a lattice.

References


Contact Information

Sankar Sagi  
Assistant Professor of Mathematics, College of Applied Sciences, Sohar, Sultanate of Oman  
E-Mail(s): sagi_sankar@yahoo.co.in

Received by the editors: 09.10.2015  
and in final form 03.02.2018.