

# On the Structure of the Group of Multiplicative Arithmetical Functions

Paul-Olivier Dehaye

## Abstract

We analyze the structure of the group  $\mathbf{F}_{\mathbf{0}, \star}$  of non-zero multiplicative arithmetical functions, where  $\star$  is the usual Dirichlet product. In particular, we prove that  $\mathbf{F}_{\mathbf{0}, \star}$  is isomorphic to a complete direct product of certain subgroups of the multiplicative group of infinite upper-triangular matrices. We also show that the group  $\mathbf{F}_{\mathbf{0}, \star}$  is divisible.

## 1 Introduction

An **arithmetical function**, i.e. a function  $f : \mathbb{N}_0 \rightarrow \mathbb{R}$ , is called **multiplicative** if  $f(mn) = f(m)f(n)$  whenever  $(m, n) = 1$ . The Euler function  $\phi$  and the Moebius function  $\mu$  are classical examples of multiplicative functions. The arithmetical functions  $\mathbf{0}$  and  $\mathbf{I}$  defined for every  $n \in \mathbb{N}_0$  by  $\mathbf{0}(n) = 0$ ,  $\mathbf{I}(n) = 0$  or  $1$  according as  $n \neq 1$  or  $n = 1$ , are trivially multiplicative.

Let  $\mathbf{F}_{\mathbf{0}}$  denote the set of all multiplicative functions different from  $\mathbf{0}$ . Clearly,  $f(1) = 1$  for every  $f \in \mathbf{F}_{\mathbf{0}}$ . The **Dirichlet product** (or **convolution**) of two arithmetical functions  $f$  and  $g$  is defined as follows: for every  $n \in \mathbb{N}_0$ ,

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

For any given prime  $p$ , we will consider the following subset of  $\mathbf{F}_{\mathbf{0}}$ :

$$\mathbf{F}^p = \{f \in \mathbf{F}_{\mathbf{0}} : f(n) = 0 \text{ for every } n > 1 \text{ not divisible by } p\}$$

---

Received by the editors November 2000.

Communicated by J. Doyen.

It is well-known (see for example Apostol [1, chapter 2] or Niven and Zuckerman [5, section 4.4]) that  $\mathbf{F}_{\mathbf{0}, \star}$  is a commutative group.

The purpose of this paper is to analyze the structure of  $\mathbf{F}_{\mathbf{0}, \star}$ . We will prove the following result:

**Theorem:**

- (a) *The group  $\mathbf{F}_{\mathbf{0}, \star}$  is torsion-free (i.e. has no element of finite order).*
- (b)  *$\mathbf{F}^p, \star$  is a subgroup of  $\mathbf{F}_{\mathbf{0}, \star}$  for every prime  $p$ . All the subgroups  $\mathbf{F}^p, \star$  are isomorphic to the same multiplicative group of infinite upper-triangular matrices.*
- (c)  *$\mathbf{F}_{\mathbf{0}, \star}$  is isomorphic to the complete direct product of the subgroups  $\mathbf{F}^p, \star$ .*
- (d)  *$\mathbf{F}_{\mathbf{0}, \star}$  is divisible and has a natural structure of vector space over  $\mathbb{Q}$ .*

**Acknowledgements.** The author wishes to thank F. Buekenhout and J. Doyen for their help during the preparation of this paper.

## 2 Multiplicative functions

**Theorem 2.1:** *The group  $\mathbf{F}_{\mathbf{0}, \star}$  is torsion-free (i.e. has no element of finite order).*

*Proof.* Assume that the torsion subgroup of  $\mathbf{F}_{\mathbf{0}, \star}$  is non-trivial, and let  $q$  be the smallest prime power for which there is a function  $f$  in the torsion subgroup of  $\mathbf{F}_{\mathbf{0}, \star}$  such that  $f(q) \neq 0$ . If we denote by  $f^n$  the Dirichlet product of  $n$  copies of  $f$ , it is easily proved by induction that, for every  $n \in \mathbb{N}_0$ ,  $(f^n)(q) = nf(q) \neq 0$ , contradicting the fact that we should have  $f^n = \mathbf{0}$  for some  $n$ . ■

**Theorem 2.2:** *For any given prime  $p$ ,  $\mathbf{F}^p$  is a subgroup of  $\mathbf{F}_{\mathbf{0}, \star}$ .*

*Proof.* Clearly,  $\mathbf{I} \in \mathbf{F}^p$  for every prime  $p$ . If  $f, g \in \mathbf{F}^p$ , then  $(f \star g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = 0$  for every  $n > 1$  such that  $p \nmid n$ , because  $f(d)$  or  $g(\frac{n}{d})$  is equal to 0 for every  $d | n$ . Given an integer  $n > 1$  such that  $p \nmid n$ , assume that  $f^{-1}(m) = 0$  for every  $m \in \mathbb{N}$  such that  $p \nmid m$  and  $1 < m < n$ . Then  $f \star f^{-1} = \mathbf{I}$  implies that  $f^{-1}(n) = f^{-1}(n)f(1) = -\sum_{\substack{d|n \\ d>1}} f(d)f^{-1}(\frac{n}{d}) = -f(n)$ . But  $f(n) = 0$  since  $f \in \mathbf{F}^p$  and so  $f^{-1}(n) = 0$ . It follows that  $f^{-1} \in \mathbf{F}^p$ . ■

### 3 Infinite upper-triangular matrices

An **infinite matrix** is a map from  $\mathbb{N}_0 \times \mathbb{N}_0$  into  $\mathbb{R}$ . Intuitively, it is an array of real numbers with rows and columns indexed by the elements of  $\mathbb{N}_0$ . We denote by  $\mathbf{M}$  the set of infinite matrices, and by  $\mathbf{M}^+$  the set of **upper-triangular non-zero** infinite matrices, i.e.

$$\mathbf{M}^+ = \{m \in \mathbf{M} : m(a, a) \neq 0 \quad \forall a \in \mathbb{N}_0 \text{ and } m(a, b) = 0 \quad \forall a, b \in \mathbb{N}_0 \text{ s.t. } a > b\}.$$

Given two matrices  $m, n \in \mathbf{M}^+$ , their product  $m \cdot n$  defined by

$$(m \cdot n)(a, b) := \sum_{c \in \mathbb{N}_0} m(a, c)n(c, b)$$

is well-defined since  $n(c, b) = 0$  whenever  $c > b$ .

**Theorem 3.1:**  $\mathbf{M}^+, \cdot$  is a group whose identity element is the infinite identity matrix  $I$ .

*Proof.* The only non trivial fact to prove is that every  $m \in \mathbf{M}^+$  has an inverse  $m^{-1}$  for the product defined above. In order to find  $m^{-1}(a, b)$ , we first restrict  $m$  to a square matrix of size  $\max(a, b)$ . This restricted matrix has an inverse, which is a restricted  $m^{-1}$ . We find  $m^{-1}(a, b)$  by taking the corresponding entry in the restricted  $m^{-1}$ . The matrix constructed in this way is indeed an element of  $\mathbf{M}^+$ : the upper-triangular square matrices of given size form a group, and so the restricted inverse is also upper-triangular. Moreover, the product of the diagonal entries of any restriction of  $m^{-1}$  has to be non-zero, because these restrictions are invertible. Hence, all diagonal elements are non-zero. ■

Note that the group  $\mathbf{M}^+$  has an obvious subgroup, namely the group  $\mathbf{M}^1$  of upper-triangular infinite matrices all of whose diagonal entries are equal to 1.

### 4 Complete direct products

Many equivalent definitions can be found in the literature: Suzuki [6] gives a definition in terms of functions, Fuchs [2] and Kaplansky [3] use vectors and Kurosh [4] presents a more general concept.

**Definition:** A **word** over an infinite family of sets  $S_i$  ( $i \in \mathbb{N}_0$ ) is a set of elements of  $\cup S_i$  having exactly one element in each  $S_i$ .

**Definition:** The **complete** (or **Cartesian**) **direct product** of the groups  $H_i, \star_i$  ( $i \in \mathbb{N}_0$ ) is the set of words over the  $H_i$ 's, endowed with the component-wise product defined as follows: the component-wise product of two words  $w_1$  and  $w_2$  is the word  $w_3$  such that  $w_3 \cap H_i = (w_1 \cap H_i) \star_i (w_2 \cap H_i)$  for every  $i \in \mathbb{N}_0$ .

This construction is well-defined and indeed gives a group, denoted from now on by  $\overline{\prod}_{i \in \mathbb{N}_0} H_i, \star$ , where the product  $\star$  depends on the products  $\star_i$  in the subgroups  $H_i$ . If all the subgroups  $H_i, \star_i$  are equal to  $H, \star$ , we simply denote their complete direct product by  $\overline{\prod} H, \star$ .

**Theorem 4.1:** *If  $K_i, \star_i \cong L_i, \diamond_i$  for every  $i \in \mathbb{N}_0$ , then*

$$K, \star := \overline{\prod}_{i \in \mathbb{N}_0} K_i, \star \cong \overline{\prod}_{i \in \mathbb{N}_0} L_i, \diamond =: L, \diamond$$

*Proof.* Suppose that an isomorphism from  $K_i$  onto  $L_i$  is given by  $\phi_i : K_i \rightarrow L_i$ , where  $\phi_i(a \star_i b) = \phi_i(a) \diamond_i \phi_i(b)$  for every  $a, b \in K_i$ . We define a bijection  $\phi$  from the set of words over the  $K_i$ 's onto the set of words over the  $L_i$ 's by writing  $\phi(w) \cap L_i = \phi_i(w \cap K_i)$  for every  $i \in \mathbb{N}_0$ . This is of course well-defined for every  $w \in K$ . If two words  $w_1$  and  $w_2$  have the same image under  $\phi$ , then their intersection with  $L_i$  is the same for every  $i$ , and so  $\phi_i(w_1 \cap K_i) = \phi_i(w_2 \cap K_i)$  for every  $i \in \mathbb{N}_0$ ; since  $\phi_i$  is a bijection, it follows that  $w_1 \cap K_i = w_2 \cap K_i$  for every  $i \in \mathbb{N}_0$ . Therefore  $w_1 = w_2$  and  $\phi$  is injective.

We now define a function  $\psi$  from the set of words over the  $L_i$ 's onto the set of words over the  $K_i$ 's by  $\psi(w') \cap K_i = \psi_i(w' \cap L_i)$ . Since  $\psi$  is also injective and since  $\psi \circ \phi = \phi \circ \psi = Id$ ,  $\phi$  is a bijection and  $\phi^{-1} = \psi$ .

We just have to make sure that  $\phi$  is an isomorphism, i.e. that  $\phi(a \star b) = \phi(a) \diamond \phi(b)$  for every  $a, b \in K$ . It suffices to check that  $\phi(a \star b) \cap L_i = (\phi(a) \diamond \phi(b)) \cap L_i$  for every  $i \in \mathbb{N}_0$ . But

$$\begin{aligned} \phi(a \star b) \cap L_i &= \phi_i((a \star b) \cap K_i) && \text{(by def. of } \phi) \\ &= \phi_i((a \cap K_i) \star (b \cap K_i)) && \text{(by def. of the product on words)} \\ &= \phi_i(a \cap K_i) \diamond \phi_i(b \cap K_i) && \text{(because } \phi_i \text{ is an isomorphism)} \\ &= (\phi(a) \cap L_i) \diamond (\phi(b) \cap L_i) && \text{(by def. of } \phi) \\ &= (\phi(a) \diamond \phi(b)) \cap L_i && \text{(by def. of the product of words)} \end{aligned}$$

■

## 5 Isomorphism

We will now prove that the group  $\mathbf{F}_0, \star$  is isomorphic to a complete direct product of certain groups of upper-triangular matrices.

**Theorem 5.1:**  $\mathbf{F}_0, \star \cong \overline{\prod}_{i \in \mathbb{N}_0} \mathbf{F}^{p_i}, \diamond$ , where  $p_i$  is the  $i$ -th prime and  $\diamond$  denotes the product on the set of words.

*Proof.* We already know that every  $\mathbf{F}^{p_i}$  is a subgroup of  $\mathbf{F}_0, \star$ . We will construct a bijection  $\phi$  from the set  $W$  of words over the  $\mathbf{F}^{p_i}$ 's onto  $\mathbf{F}_0$ . Given a word  $w \in W$ , we define  $\phi(w)$  as follows: for every  $i, e \in \mathbb{N}_0$ ,

$$(\phi(w))(p_i^e) = (w \cap \mathbf{F}^{p_i})(p_i^e)$$

Since a multiplicative function is determined by its values on prime powers,  $\phi(w)$  is a multiplicative function. Trivially,  $\phi$  is injective. It is also surjective: for a given multiplicative function  $f$ , take the word  $w_f$  such that  $w_f \cap \mathbf{F}^{p_i}$  is equal to  $f$  on the powers of  $p_i$  and takes the value 0 on the powers of all the other primes. Its image under  $\phi$  is obviously  $f$ .

It remains to show that  $\phi$  is an isomorphism, i.e. that  $\phi(w_1 \diamond w_2) = \phi(w_1) \star \phi(w_2)$  for every  $w_1, w_2 \in W$ . For every  $e, i \in \mathbb{N}_0$ ,

$$\begin{aligned}
 (\phi(w_1 \diamond w_2))(p_i^e) &= ((w_1 \diamond w_2) \cap \mathbf{F}^{p_i})(p_i^e) \\
 &= ((w_1 \cap \mathbf{F}^{p_i}) \star (w_2 \cap \mathbf{F}^{p_i}))(p_i^e) \\
 &= \sum_{0 \leq t \leq e} ((w_1 \cap \mathbf{F}^{p_i})(p_i^t)) ((w_2 \cap \mathbf{F}^{p_i})(p_i^{e-t})) \\
 &= \sum_{0 \leq t \leq e} (\phi(w_1)(p_i^t)) (\phi(w_2)(p_i^{e-t})) \\
 &= (\phi(w_1) \star \phi(w_2))(p_i^e)
 \end{aligned}$$

and so these two multiplicative functions are equal since they take the same values on prime powers.  $\blacksquare$

In order to find an isomorphism between  $\mathbf{F}_0, \star$  and a group of infinite matrices, it is now sufficient to find such an isomorphism for each  $\mathbf{F}^{p_i}, \star$  and then use Theorem 4.1.

**Theorem 5.2:** *Every group  $\mathbf{F}^{p_i}, \star$  is isomorphic to the same subgroup of  $\mathbf{M}^1, \star$ .*

*Proof.* For any  $i \in \mathbb{N}_0$ , we define a bijection  $\phi$  from  $\mathbf{F}^{p_i}$  onto  $\phi(\mathbf{F}^{p_i})$  by

$$\phi(f) = \begin{pmatrix} 1 & f(p_i) & f(p_i^2) & f(p_i^3) & \cdots \\ 0 & 1 & f(p_i) & f(p_i^2) & \ddots \\ 0 & 0 & 1 & f(p_i) & \ddots \\ \vdots & \vdots & \ddots & \ddots & \ddots \end{pmatrix}$$

$\phi$  is an isomorphism because, if  $f, g \in \mathbf{F}^{p_i}$ , then

$$\begin{aligned}
 \phi(f) \cdot \phi(g) &= \begin{pmatrix} 1 & f(p_i) + g(p_i) & f(p_i^2) + f(p_i)g(p_i) + g(p_i^2) & \cdots \\ 0 & 1 & f(p_i) + g(p_i) & \ddots \\ 0 & 0 & 1 & \ddots \\ \vdots & \vdots & \ddots & \ddots \end{pmatrix} \\
 &= \begin{pmatrix} 1 & (f \star g)(p_i) & (f \star g)(p_i^2) & \cdots \\ 0 & 1 & (f \star g)(p_i) & \ddots \\ 0 & 0 & 1 & \ddots \\ \vdots & \vdots & \ddots & \ddots \end{pmatrix} \\
 &= \phi(f \star g).
 \end{aligned}$$

The image of  $\mathbf{F}^{p_i}$ , i.e. the subset of  $\mathbf{M}^1$  consisting of all matrices in which all the entries on a descending diagonal are equal, will be denoted by  $\mathbf{D}^1$ .

The function  $\phi$  immediately tells us that  $\mathbf{D}^1, \cdot$  is a group isomorphic to  $\mathbf{F}^{p_i}, \star$  for every  $i$ , hence also that all the groups  $\mathbf{F}^{p_i}, \star$  are pairwise isomorphic.  $\blacksquare$

The following result is now a consequence of Theorem 4.1:

**Theorem 5.3:**  $\mathbf{F}_0, \star \cong \prod \mathbf{D}^1$ .  $\blacksquare$

## 6 Divisibility

**Definition:** A group  $G$  is said to be **divisible** if for every  $x \in G$  and every integer  $n \in \mathbb{N}_0$ , there exists an element  $y \in G$  such that  $y^n = x$ .

**Lemma 6.1:** *If  $H, \star$  is divisible, then  $\overline{\prod}H, \diamond$  is also divisible.*

*Proof.* We denote the  $i$ -th copy of  $H$  by  $H_{(i)}$ . For a given  $w$  in  $\overline{\prod}H$ , define  $\sqrt[n]{w}$  by

$$(\sqrt[n]{w}) \cap H_{(i)} = \sqrt[n]{w \cap H_{(i)}}.$$

■

**Lemma 6.2:** *If a multiplicative group  $G, \star$  is divisible and torsion-free, then  $x, y \in G$  and  $x^n = y^n$  imply  $x = y$ .*

*Proof.*

$$x^n = y^n \Leftrightarrow (x \star y^{-1})^n = 1 \Leftrightarrow x \star y^{-1} = 1 \Leftrightarrow x = y$$

■

**Lemma 6.3:** *Every group  $\mathbf{F}^{p_i}, \star$  is divisible.*

*Proof:* For every  $n \in \mathbb{N}_0$  and every  $e \in \mathbb{N}$ ,

$$(f^n)(p_i^e) = \sum_{\substack{e_i \in \mathbb{N} \\ e_1 + \dots + e_n = e}} \prod_{t=1}^n f(p_i^{e_t}).$$

This yields the following recursive definition of  $\sqrt[n]{f}$ :

$$(\sqrt[n]{f})(p_i^e) = \frac{1}{n} \cdot \left\{ f(p_i^e) - \sum_{\substack{e_i \in \mathbb{N} \setminus \{e\} \\ e_1 + \dots + e_n = e}} \prod_{t=1}^n [(\sqrt[n]{f})(p_i^{e_t})] \right\}.$$

■

We are now able to conclude:

**Theorem 7.1:** *The group  $\mathbf{F}_0, \star$  is divisible.*

■

**Remark:** For any  $f \in \mathbf{F}_0$ , we may define  $\frac{f}{n}$  and  $nf$  in a unique way as  $\sqrt[n]{f}$  and  $f^n$ . It follows that  $\mathbf{F}_0$  has the structure of a vector space over  $\mathbb{Q}$ , the scalar product being defined by the convolution of multiplicative functions. It is an easy exercise to check all the required axioms (this is also explained in Kaplansky [3]).

## References

- [1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976
- [2] L. Fuchs, *Abelian Groups*, Pergamon Press, Oxford, 1960.
- [3] I. Kaplansky, *Infinite Abelian Groups*, University of Michigan Press, Ann Arbor, 1954.
- [4] A.G. Kurosh, *Theory of Groups*, Chelsea Publishing Company, New York, 1955.
- [5] I. Niven and H.S. Zuckerman, *An Introduction to the Theory of Numbers*, Wiley, New York, 1972
- [6] M. Suzuki, *Group Theory I*, Springer-Verlag, Berlin, 1982.

Département de Mathématiques  
Campus Plaine C.P. 216  
Université Libre de Bruxelles  
B-1050 Bruxelles  
Belgium

*Current address :*

Department of Mathematics  
Stanford University  
CA 94305 U.S.A.  
email : pdehaye@math.stanford.edu