Linear Algebra and its Applications 457 (2014) 383–399

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

The group of squarefree integers

Titus Hilberdink

Department of Mathematics, University of Reading, Whiteknights, P.O. Box 220, Reading RG6 6AX, UK

A R T I C L E I N F O

Article history:
Received 9 May 2014
Accepted 21 May 2014
Available online 11 June 2014
Submitted by R. Brualdi

MSC:
11A05
11A25
11C20
15A23
15B36

Keywords:
Squarefree numbers
Gcd and lcm
Character group

A B S T R A C T

We investigate the consequences of the elementary observation that the squarefree numbers form a group under the operation $\frac{\text{lcm}}{\text{gcd}}$. In particular, we discuss the characters on this group, one of which is the Möbius function, as well as the finite subgroups $D(k)$ formed from the divisors of a given squarefree integer k. We show further how a convolution, naturally based on this operation, leads to the factorization of various arithmetical matrices and the evaluation of the eigenvalues. We discuss briefly the associated L-functions. Finally, we generalize the operation to other subsets of $\mathbb{N}$.

1. The group of squarefree integers $\mathbb{N}^*$

1.1. Introduction

For $m, n \in \mathbb{N}$, define the (commutative) operation $\circ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by

$$m \circ n = \frac{[m, n]}{(m, n)}.$$

E-mail address: t.w.hilberdink@reading.ac.uk.

http://dx.doi.org/10.1016/j.laa.2014.05.037
0024-3795/

This simple and natural operation turns out, as we shall presently see, a group operation on the squarefree numbers. It is surprising that, apparently, this has not been observed. The closest that we have seen to this operation is in [7] (points 64, 65) regarding Boolean lattices, but here no groups are alluded to. The quantity $\frac{[m,n]}{(m,n)}$ does however appear in many papers in number theory and linear algebra especially with regard to certain arithmetical matrices (see for example [1,5,6,8,15,17] to name but a few).

Writing $m = \prod p^a$ and $n = \prod p^b$ for their prime decompositions, where $a, b \in \mathbb{N}_0$, one has $m \circ n = \prod p^{|a-b|}$. Thus $\mathbb{N}$ is closed under $\circ$. The operation $\circ$ has identity 1 since $n \circ 1 = n$, while every n is its own inverse as $n \circ n = 1$. However, $\circ$ is *not* associative. For example $(2 \circ 2) \circ 4 = 4$, while $2 \circ (2 \circ 4) = 1$. But $\circ$ is associative if we restrict to *squarefree* numbers.

Proposition 1.1. *Let* $\mathbb{N}^*$ *denote the set of squarefree numbers. Then* $(\mathbb{N}^*, \circ)$ *is an abelian group.*

Proof. First note that $m \circ n \in \mathbb{N}^*$ whenever $m, n \in \mathbb{N}^*$, since $|a - b| \in \{0, 1\}$ whenever $a, b \in \{0, 1\}$. We need therefore only check the associative law. Write $m = \prod p^a$, $n = \prod p^b$, and $r = \prod p^c$, for the prime decompositions, where $a, b, c \in \{0, 1\}$. Then $(m \circ n) \circ r = m \circ (n \circ r)$ follows on noticing that

$$\big||a - b| - c\big| = \big|a - |b - c|\big|$$

holds if $a, b, c = 0, 1$. □

Remarks 1.

(a) This group is isomorphic to a standard group – sometimes called the *Boolean group*. For a set X, let $F(X)$ denote the set of finite subsets of X and equip it with the symmetric difference operation $A \triangle B = (A \cup B) \setminus (A \cap B)$. Then $(F(X), \triangle)$ is a group, the *Boolean* group. Taking X to be the set of primes makes it isomorphic to $\mathbb{N}^*$ (see, for example, [13], p. 54 – thanks to Graham Williams for pointing this out).

(b) We mention a few more simple properties of $\circ$ the proofs of which can sometimes best be seen with a Venn diagram and noting that 'gcd' corresponds to intersection, 'lcm' corresponds to union while, as mentioned above, '$\circ$' corresponds to symmetric difference.

   (a) $(\mathbb{N}^*, \circ, \gcd)$ is a ring (without identity) with "addition" $\circ$ and "multiplication" $\gcd(\cdot, \cdot)$. It is a *Boolean ring* (as $(n, n) = n$) of characteristic 2 (as $n \circ n = 1$).

   (b) For $m, n, r \in \mathbb{N}^*$, we have

$$(m \circ n)(m \circ r)(n \circ r) = \frac{[m,n,r]^2}{(m,n,r)^2} \quad \text{and} \quad mnr(m \circ n \circ r) = [m,n,r]^2(m,n,r)^2.$$