L'Enseignement Mathématique, t. 49 (2003), p. 109–116

ADDITIVE NUMBER THEORY SHEDS EXTRA LIGHT ON THE HOPF-STIEFEL ○ FUNCTION

by Alain PLAGNE

ABSTRACT. The famous Hopf-Stiefel ○ function appears in several places in mathematics (linear and bilinear algebra, topology, intercalate matrices, ...). However, although the object of much study, this function kept a part of mystery since no simple formula was known for it. We shall derive a simple and practical explicit formula for ○ and more generally for β_p (p arbitrary prime), a generalized function due to Eliahou and Kervaire. The proof relies on a new result in combinatorial group theory which follows from additive number theoretical arguments. It is shown that this last result generalizes earlier ones by Eliahou and Kervaire and by Yuzvinsky.

1. INTRODUCTION

A *composition formula* of size $[r, s, n]$ over some field $\mathbf{F}$ (that we assume to be of characteristic different from 2) is an identity of the form

$$(x_1^2 + \cdots + x_r^2)(y_1^2 + \cdots + y_s^2) = (z_1^2 + \cdots + z_n^2)\,,$$

where $z_1, z_2, \ldots, z_n$ are n bilinear forms in the variables $(x_1, \ldots, x_r)$ and $(y_1, \ldots, y_s)$, with coefficients in $\mathbf{F}$. For example, the law of moduli for complex numbers provides the identity

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_2y_1 + x_1y_2)^2\,,$$

which is a composition formula of size $[2, 2, 2]$. The law of moduli for quaternions (respectively for octonions) provides a composition formula of size $[4, 4, 4]$ (respectively $[8, 8, 8]$) in a similar way. Conversely, Hurwitz's theorem [7] (see also [8]) states that the only possible values of n for which a composition formula of size $[n, n, n]$ exists are $1, 2, 4$ and 8.

In the late thirties, starting from the Hurwitz problem, Hopf [6] and Stiefel [15] began to study real division algebras. They introduced a function of an algebraic nature. The so-called Hopf-Stiefel function $\circ$ (which depends on two positive integral variables r and s) is defined by the formula

$$r \circ s = \min\{n \text{ such that } (x+y)^n = 0 \text{ in } \mathbf{F}_2[x,y]/(x^r, y^s)\}. \tag{1.1}$$

Hopf and Stiefel obtained a result which says that if a nonsingular bilinear map from $\mathbf{R}^r \times \mathbf{R}^s$ onto $\mathbf{R}^n$ exists over $\mathbf{R}$, then $n \geq r \circ s$ (Hopf-Stiefel theorem). The link between nonsingular bilinear maps and $\circ$ is realized by passing to projective spaces and their cohomology rings.

More generally, the $\circ$ function appears in different parts of mathematics. It allows a nice mathematical trip: starting from bilinear algebra (Hurwitz's problem, Pfister's quadratic forms [10, 11]) and algebra (its basic definition (1.1)), we pass through topology (Hopf-Stiefel theorem, real division algebras and Yuzvinsky's theorem [17]), visit the theory of intercalate matrices (Yuzvinsky's conjecture [17, 16]) and arrive at additive number theory ([5] and the present paper). The reader interested in the many applications of $\circ$ is mainly referred to the nice survey [13] by Shapiro, to his recent book [14, Chapters 12-15] and to the book by Rajwade [12], especially Chapter 13.

With the algebraic viewpoint (1.1), it is fairly natural to generalize, with Eliahou and Kervaire [5], the $\circ$ function in the following way. For any given prime p, we set

$$\beta_p(r,s) = \min\{n \text{ such that } (x+y)^n = 0 \text{ in } \mathbf{F}_p[x,y]/(x^r, y^s)\}.$$

Evidently, $\beta_2 = \circ$. It is a theorem of Eliahou and Kervaire [5] that this extension of (1.1) is still relevant in the additive number theoretical context.

Although many properties of $\circ$ and more generally of β_p were known (for instance recursion formulas or expression in terms of p-adic expansions), describing these functions efficiently appeared difficult, so that it is not rare to see tables giving the first values of $\circ$.

In this paper, perhaps surprisingly, we shall derive a simple and practical explicit formula for $\circ$ and more generally for β_p (p arbitrary prime).

THEOREM 1. *Let p be any prime number. The function β_p is given by the formula*

$$\beta_p(r,s) = \min_{t \in \mathbf{N}} \left(\lceil r/p^t \rceil + \lceil s/p^t \rceil - 1 \right) p^t .$$

Notice that clearly, the minimum involved is attained for a value of t satisfying $0 \leq t \leq \lceil \log(\max(r,s))/\log p \rceil$.

In particular, this result elucidates, in some sense, the Hopf-Stiefel function.

THEOREM 2. *The Hopf-Stiefel function is*

$$r \circ s = \min_{t \in \mathbf{N}} \left(\lceil r/2^t \rceil + \lceil s/2^t \rceil - 1 \right) 2^t .$$

With this formula, a large number of properties of $\circ$ follow immediately or admit a simplified proof.

In fact Theorem 1 follows from an additive number theoretical theorem (Theorem 3 below) which is of independent interest. Given a finite Abelian group G, we define (as in [5]) the function of two integral variables r and s $(1 \leq r, s \leq |G|)$

$$\mu_G(r,s) = \min\{|\mathcal{A} + \mathcal{B}|, \text{ with } \mathcal{A}, \mathcal{B} \subset G, \ |\mathcal{A}| = r, \ |\mathcal{B}| = s\}$$

where $\mathcal{A} + \mathcal{B}$ is the usual Minkowski sum of sets, namely

$$\mathcal{A} + \mathcal{B} = \{a + b \text{ with } a \in \mathcal{A}, \ b \in \mathcal{B}\} .$$

Given an arbitrary Abelian group G, determining the function μ_G is not easy: this is an open problem in general for G finite and Abelian. However, Eliahou and Kervaire [5] obtained such a result for finite groups of prime exponent, thus generalizing Yuzvinsky's result [17] for binary spaces.

Using a different approach (based on Kneser's theorem [9]), we shall obtain a result valid for any *cyclic* group.

THEOREM 3. *Let n be any integer. If $1 \leq r, s \leq n$, we have*

$$\mu_{\mathbf{Z}/n\mathbf{Z}}(r,s) = \min_{d|n} \left(\lceil r/d \rceil + \lceil s/d \rceil - 1 \right) d .$$

Taking $n = p$, a prime, gives exactly the Cauchy-Davenport theorem [2, 3, 4]. Moreover, as will be explained in Section 3, this result contains that of Eliahou and Kervaire.

Since cyclic groups are characterized by the equality $\exp G = |G|$, this theorem is a direct consequence of the following more general result.

THEOREM 4. *Let G be any finite Abelian group. Then, if $1 \leq r, s \leq |G|$, we have*

$$\min_{d \,||G|} \left(\lceil r/d \rceil + \lceil s/d \rceil - 1 \right) d \leq \mu_G(r,s) \leq \min_{\frac{|G|}{\exp G} \,|\, d \,||G|} \left(\lceil r/d \rceil + \lceil s/d \rceil - 1 \right) d .$$

With these results, we know the behaviour of μ_G at the two endpoints of the spectrum (cyclic groups and groups of prime exponent). What now remains to be done is to fill the gap between the upper bound and the lower bound for general finite Abelian groups.

2. Proof of Theorem 4

Let G be any given finite Abelian group and let $1 \leq r, s \leq |G|$.

2.1 The lower bound

If $\mu_G(r,s) \geq r+s-1$, the result is immediate (take $d=1$). We may thus assume that

$$\mu_G(r,s) \leq r+s-1\,. \tag{2.1}$$

Then, choosing two sets $\mathcal{A}$ and $\mathcal{B}$ in G with respective cardinalities r and s, such that $|\mathcal{A}+\mathcal{B}|$ attains $\mu_G(r,s)$, we get

$$|\mathcal{A}+\mathcal{B}| = \mu_G(r,s) \leq |\mathcal{A}|+|\mathcal{B}|-1\,.$$

We are in a position to apply Kneser's theorem [9] on the structure of sets with a small sumset. It follows that there exists a subgroup H of G (namely the stabilizer of $\mathcal{A}+\mathcal{B}$) such that

$$|\mathcal{A}+\mathcal{B}| = |\mathcal{A}+H|+|\mathcal{B}+H|-|H|\,.$$

Denoting by $(\mathcal{A}+H)/H$ (resp. $(\mathcal{B}+H)/H$) the H-cosets that $\mathcal{A}$ (resp. $\mathcal{B}$) intersects, we obtain

$$\begin{aligned} |\mathcal{A}+\mathcal{B}| &= \left(\left|\frac{\mathcal{A}+H}{H}\right|+\left|\frac{\mathcal{B}+H}{H}\right|-1\right)|H| \\ &\geq (\lceil r/f\rceil+\lceil s/f\rceil-1)f \end{aligned}$$

where f denotes the cardinality of H. Since Lagrange's theorem shows that f divides $|G|$, we get

$$|\mathcal{A}+\mathcal{B}| \geq \min_{d\,|\,|G|}(\lceil r/d\rceil+\lceil s/d\rceil-1)d\,.$$

From this it follows that, in any case,

$$\mu_G(r,s) \geq \min_{d\,|\,|G|}(\lceil r/d\rceil+\lceil s/d\rceil-1)d\,,$$

which is the desired lower bound.