Journal of Number Theory 133 (2013) 2999–3006

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A structure result for bricks in Heisenberg groups

Norbert Hegyvári [a,*], François Hennecart [b]

[a] ELTE TTK, Eötvös University, Institute of Mathematics, H-1117 Pázmány st. 1/c, Budapest, Hungary
[b] Université Jean-Monnet, Institut Camille Jordan, 23, rue du Docteur Paul Michelon, 42023 Saint-Etienne Cedex 02, France

ARTICLE INFO

Article history:
Received 14 February 2013
Revised 18 March 2013
Accepted 18 March 2013
Available online 13 May 2013
Communicated by David Goss

MSC:
primary 11B75
secondary 05D10

Keywords:
Bases
Heisenberg groups

ABSTRACT

We show that for a sufficiently big *brick* B of the $(2n+1)$-dimensional Heisenberg group H_n over the finite field $\mathbb{F}_p$, the product set $B \cdot B$ contains at least $|B|/p$ many cosets of some non-trivial subgroup of H_n.

1. Introduction

The notion of additive bases occupies a central position in Combinatorial Number Theory. In an additive semigroup G, a *basis* means a subset A of G such that there exists an integer h, depending only on A, for which any element of $x \in G$ can be written as a sum of h (or at most h) members of A. The idea has been widely investigated in different structures in which a number of results have been shown. One can quote the celebrated Lagrange theorem in the set of nonnegative integers but also such results in σ-finite abelian groups [HR].

In an additive structure we will use the notation $A+B=\{a+b:\ a\in A,\ b\in B\}$, its extension $hA = A+A+\cdots+A$ (h times) and also their counterparts $A\cdot B$, A^h in a multiplicative structure. In a group we also denote $-A$ (resp. A^{-1}) for the set of the inverses of elements of A. With this notation, A is a basis in G whenever for some integer h one has $hA=G$ or $A^h=G$ according to the underlying

* Corresponding author.
E-mail addresses: hegyvari@elte.hu (N. Hegyvári), francois.hennecart@univ-st-etienne.fr (F. Hennecart).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.03.011

structure. One also defines the notion of *doubling constant* (resp. *squaring constant*) of a finite set A that is $|A+A|/|A|$ (resp. $|A\cdot A|/|A|$).

Another aspect concerns inverse results in number theory in which the Freiman theorem has a central place. It asserts that a finite set A with a small doubling constant in an abelian (additive) group G has a sharp structure, namely it is included, as a rather dense subset, in a (generalized) arithmetic progression of cosets of some subgroup of G (cf. [GR]). An important tool for the proof, known as the Bogolyubov–Ruzsa Lemma, is the fact that $2A-2A$ contains a dense substructure.

According to the preceding discussion, one may consider the general problem of investigating in which conditions on a finite A, the sumset $A+A$ (or the product set $A\cdot A$) contains a *rich* substructure. In this paper we will focus on Heisenberg groups which give an interesting counterpoint to the commutative case.

Let p be a prime number and $\mathbb{F}$ the field with p elements. We denote by H_n the $(2n+1)$-dimensional Heisenberg linear group over $\mathbb{F}$ formed with the upper triangular square matrices of size $n+2$ of the following kind

$$[\underline{x},\underline{y},z]=\begin{pmatrix}1 & \underline{x} & z\\ 0 & I_n & {}^t\underline{y}\\ 0 & 0 & 1\end{pmatrix},$$

where $\underline{x}=(x_1,x_2,\dots,x_n)$, $\underline{y}=(y_1,y_2,\dots,y_n)$, $x_i,y_i,z\in\mathbb{F}$, $i=1,2,\dots,n$, and I_n is the $n\times n$ identity matrix. We have $|H_n|=p^{2n+1}$ and we recall the product rule in H_n:

$$[\underline{x},\underline{y},z]\big[\underline{x}',\underline{y}',z'\big]=\big[\underline{x}+\underline{x}',\underline{y}+\underline{y}',\langle\underline{x},\underline{y}'\rangle+z+z'\big],$$

where $\langle\cdot,\cdot\rangle$ is the inner product, that is $\langle\underline{x},\underline{y}\rangle=\sum_{i=1}^n x_iy_i$.

So this set of $(n+2)\times(n+2)$ matrices form a group whose unit is $e=[\underline{0},\underline{0},0]$. As group-theoretical properties of H_n, we recall that H_n is non-abelian and two-step nilpotent, that is the double commutator satisfies $aba^{-1}b^{-1}cbab^{-1}a^{-1}c^{-1}=e$ for any $a,b,c\in H_n$, where the commutator of a and b is defined as $aba^{-1}b^{-1}$.

The Heisenberg group possesses an interesting structure in which we can prove that in general there is no *good model* for a subset A with a small *squaring constant* $|A\cdot A|/|A|$ (see [G,HH] for more details), unlike for subsets of abelian groups. We should add that the situation is less unusual if we assume that A has a small *cubing constant* $|A\cdot A\cdot A|/|A|$ (see [T2]).

We now quote the following well-known results.

Lemma 1.1. *Let X and Y be subsets of a finite (multiplicative) group G. If $|X|+|Y|>|G|$ then $G=X\cdot Y$.*

The proof follows from the simplest case of the sieve formula:

$$\big|X\cap\big(\{x\}\cdot Y^{-1}\big)\big|=|X|+\big|\{x\}\cdot Y^{-1}\big|-\big|X\cup\big(\{x\}\cdot Y^{-1}\big)\big|\geqslant|X|+|Y|-|G|>0.$$

Lemma 1.2. *Let X and Y be subsets of $\mathbb{F}$. If $X+Y\neq\mathbb{F}$ then $|X+Y|\geqslant|X|+|Y|-1$.*

This general lower bound for the cardinality of sumsets in $\mathbb{F}$ is known as the Cauchy–Davenport Theorem (see e.g. [TV]).

We deduce from Lemma 1.1 that a sufficient condition ensuring that a subset $A\subseteq H_n$ is a basis is $|A|>|H_n|/2$. Moreover this condition is sharp if $p=2$ since in that case H_n has a subgroup of index 2. For $p>2$, any subset of H_n with cardinality bigger than $|H_n|/p$ is not contained in a coset of a proper subgroup of H_n, hence it is a basis for some order h bounded by a function depending only on p: indeed by a theorem of Freiman in arbitrary finite groups (see [T, paragraph 4.9]), it is known that if A is not included in some coset of some proper subgroup of H_n then $|A\cdot A|\geqslant 3|A|/2$.