ARTICLE IN PRESS YJNTH:5860

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A structure theorem for product sets in extra special groups

Thang Pham[a,1], Michael Tait[b,*,2], Le Anh Vinh[c], Robert Won[d]

[a] Department of Mathematics, EPFL, Lausanne, Switzerland
[b] Department of Mathematical Sciences, Carnegie Mellon University, United States
[c] University of Education, Vietnam National University, Viet Nam
[d] Department of Mathematics, Wake Forest University, United States

ARTICLE INFO

Article history:
Received 9 May 2017
Received in revised form 25 August 2017
Accepted 29 August 2017
Available online xxxx
Communicated by S.J. Miller

Keywords:
Extra special group
Quasigroup
Arithmetic combinatorics

ABSTRACT

Hegyvári and Hennecart showed that if B is a sufficiently large brick of a Heisenberg group, then the product set $B \cdot B$ contains many cosets of the center of the group. We give a new, robust proof of this theorem that extends to all extra special groups as well as to a large family of quasigroups.

1. Introduction

Let p be a prime. An extra special group G is a p-group whose center Z is cyclic of order p such that G/Z is an elementary abelian p-group (nice treatments of extra special

* Corresponding author.
E-mail addresses: thang.pham@epfl.ch (T. Pham), mtait@cmu.edu (M. Tait), vinhla@vnu.edu.vn (L.A. Vinh), wonrj@wfu.edu (R. Won).

[1] Thang Pham was partially supported by Swiss National Science Foundation grants no. 200020-162884 and 200021-175977.
[2] Michael Tait was supported by NSF grant DMS-1606350.

https://doi.org/10.1016/j.jnt.2017.08.031
0022-314X/© 2017 Published by Elsevier Inc.

Please cite this article in press as: T. Pham et al., A structure theorem for product sets in extra special groups, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.08.031

groups can be found in [2,6]). The extra special groups have order p^{2n+1} for some $n \geq 1$ and occur in two families. Denote by H_n and M_n the two non-isomorphic extra special groups of order p^{2n+1}. Presentations for these groups are given in [4]:

$$H_n = \langle a_1, b_1, \ldots, a_n, b_n, c \mid [a_i, a_j] = [b_i, b_j] = 1, [a_i, b_j] = 1 \text{ for } i \neq j,$$
$$[a_i, c] = [b_i, c] = 1, [a_i, b_i] = c, a_i^p = b_i^p = c_i^p = 1 \text{ for } 1 \leq i \leq n\rangle$$
$$M_n = \langle a_1, b_1, \ldots, a_n, b_n, c \mid [a_i, a_j] = [b_i, b_j] = 1, [a_i, b_j] = 1 \text{ for } i \neq j,$$
$$[a_i, c] = [b_i, c] = 1, [a_i, b_i] = c, a_i^p = c_i^p = 1, b_i^p = c \text{ for } 1 \leq i \leq n\rangle.$$

From these presentations, it is not hard to see that the center of each of these groups consists of the powers of c so are cyclic of order p. It is also clear that the quotient of both groups by their centers yield elementary abelian p-groups.

In this paper we consider the structure of products of subsets of extra special groups. The structure of sum or product sets of groups and other algebraic structures has a rich history in combinatorial number theory. One seminal result is Freiman's theorem [5], which asserts that if A is a subset of integers and $|A + A| = O(|A|)$, then A must be a subset of a small generalized arithmetic progression. Green and Ruzsa [7] showed that the same result is true in any abelian group. On the other hand, commutativity is important as the theorem is not true for general non-abelian groups [8]. With this in mind, Hegyvári and Hennecart were motivated to study what actually can be said about the structure of product sets in non-abelian groups.

The group H_1 is the classical Heisenberg group, so the groups H_n form natural generalizations of the Heisenberg group. The group H_n has a well-known representation as a subgroup of $\mathrm{GL}_{n+2}(\mathbb{F}_p)$ consisting of upper triangular matrices

$$[\underline{x}, \underline{y}, z] := \begin{bmatrix} 1 & \underline{x} & z \\ 0 & I_n & \underline{y} \\ 0 & 0 & 1 \end{bmatrix}$$

where $\underline{x}, \underline{y} \in \mathbb{F}_p^n$, $z \in \mathbb{F}_p$, and I_n is the $n \times n$ identity matrix. Let $\underline{e_i} \in \mathbb{F}_p^n$ be the i^{th} standard basis vector. In the presentation for H_n, a_i corresponds to $[\underline{e_i}, 0, 0]$, b_i corresponds to $[0, \underline{e_i}, 0]$ and c corresponds to $[0, 0, 1]$. By matrix multiplication, we have

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

where $\langle \, , \rangle$ denotes the usual dot product.

Let H_n be a Heisenberg group. A subset B of H_n is said to be a *brick* if

$$B = \{[\underline{x}, \underline{y}, z] \text{ such that } \underline{x} \in \underline{X}, \ \underline{y} \in \underline{Y}, \ z \in Z\}$$

where $\underline{X} = X_1 \times \cdots \times X_n$ and $\underline{Y} = Y_1 \times \cdots \times Y_n$ with non empty-subsets $X_i, Y_i, Z \subseteq \mathbb{F}_p$.

Please cite this article in press as: T. Pham et al., A structure theorem for product sets in extra special groups, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.08.031