Asia Pac. J. Math. 2023 **10**:23

A BRIEF ABOUT THE UNITS OF HEISENBERG GROUP ALGEBRA OF HIGHER DIMENSIONS

N. ABHILASH, E. NANDAKUMAR*

Department of Mathematics, College of Engineering and Technology, SRM Institute of Science & Technology, Kattankulathur - 603 203, Tamil Nadu, India

*Corresponding author: nanda1611@gmail.com

Received Jul. 7, 2023

Abstract. In this paper, the structure of the group formed by the unit elements of the group algebra corresponding to the finite Heisenberg group of higher dimensions is characterized. The characterization of the unit group is done for the semi simple case using the Wedderburn decomposition of the group algebra.

2020 Mathematics Subject Classification. 16U60, 20C05.

Key words and phrases. Heisenberg groups; group algebra; unit group.

1. Introduction

The Heisenberg group was named after the mathematician Werner Heisenberg. He introduced this special class of matrix group in [4]. The Heisenberg group is the set of all 3×3 upper triangular matrices with diagonal element 1 over a commutative ring R and is denoted by $H_3(R)$. The Heisenberg group has very important application in various fields like analysis and quantum mechanics.

The Heisenberg group possesses a unitary representation called the Segal-Bargmann transform, which maps functions on Heisenberg group to functions on Euclidean space. This transform has applications in signal processing, image analysis, and quantum mechanics (ref [10]). In the context of geometric quantization, the Heisenberg group plays a vital role in defining quantum observables and studying the quantization of symplectic manifolds. Pseudo-differential operators on Euclidean spaces can be extended to the Heisenberg group. The Heisenberg group serves as a framework for studying the properties and behavior of pseudo-differential operators as in [6]. Also, The Heisenberg group is a classical example of a sub-Riemannian manifold [9].

DOI: 10.28924/APJM/10-23

Due to the optimistic applications of the Heisenberg groups in various fields, the study of the corresponding group algebra and its unit group will help to use major algebraic properties which can be used in analysis and quantum mechanics. By extending the foundational concepts of the Heisenberg group to higher dimensions, researchers can make progress in addressing the challenges posed by real-world systems and exploring new frontiers in science and technology. In this paper, we generalize the Heisenberg group to higher dimensions which will be very much helpful for the researchers in new perspectives and offers tools to tackle complex problems, advance theoretical understanding, and develop practical applications across various domains. Also, we characterized the unit group $\mathcal{U}(KH_{2n+1}(C_p))$, $n \geq 1$ for the Heisenberg group algebra $KH_{2n+1}(C_p)$ over the finite field K and the characteristic of the field K does not divide the order of the Heisenbrg group p^{2n+1} in order to make the Heisenberg group algebra semi-simple.

The flow of the paper is as follows. Section 2 has the definition and basic properties of Heisenberg group is discussed and also, we introduced the Heisenberg group of higher dimension. In section 3, the definitions and results required to prove the main result is given. The main results are proved in section 4 and the final section concludes the paper.

2. Heisenberg groups and its generalization

Due to the enormous application in analysis and quantum mechanics as in [4], in this paper we consider only the finite Heisenberg groups over the cyclic group C_p, where p is any prime. Throughout this paper, the Heisenberg group means the following:

$$H_3(C_p) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in C_p \right\}$$

There must be p^3 possible matrices in $H_3(C_p)$. This p^3 matrices forms a group under matrix multiplication with identity element as identity matrix and is denoted by e. Every element of $H_3(C_p)$ is denoted by (a, b, c). Therefore, the multiplication can be viewed as $(a, b, c) \cdot (a', b', c') = (a + a', b + b' + ac', c + c')$. The inverse of (a, b, c) is given by $(a, b, c)^{-1} = (-a, -b + ac, -c)$.

Lemma 2.1. *i) For $x(\neq e) \in H_3(C_2)$, the order of x is either 2 or 4.*
ii) For $x(\neq e) \in H_3(C_p), p > 2$, the order of x is p.

Proof. i) We know that $x^2 = (a, b, c)^2 = (0, ac, 0)$. If the product $ac = 0$, then the order is 2. If not, the order is 4.
ii) The proof is direct from the fact that $x^m = (a, b, c)^m = (ma, mb + \frac{m(m-1)}{2} ac, mc)$. □

Lemma 2.2. *The number of conjugacy classes of $H_3(C_p)$ is $p^2 + p - 1$.*

Proof. The elements of the group $H_3(C_p)$ has any one of the following form (for $a, b, c \neq 0$):

$$(0,0,0),(a,0,0),(0,b,0),(0,0,c),(a,b,0),(0,b,c),(a,0,c),(a,b,c)$$

The conjugacy class of (a, o, c) is $C_{(a,0,c)} = \{(a, xc - az, c) | a, c \neq 0\}$, for any $(x, y, z) \in H_3(C_p)$. Both a and c has $p-1$ choices and so, $(p-1)^2$ conjugacy classes. Similarly, repeat the same procedure for other elements. □

Lemma 2.3. *For any $g(\neq e) \in H_3(C_p)$, the elements $g^2, \cdots, g^{p-1} \notin C_g$, where C_g denotes the conjugacy class of g.*

Proof. Let $g = (a, b, c) \in H_3(C_p)$. Then, $C_{(a,b,c)}$ has the elements of the form $(a, b + xc - az, c)$ for any $(x, y, z) \in H_3(C_p)$. On the other hand, for $2 \leq m \leq p-1$, $(a, b, c)^m = (ma, mb + \frac{m(m-1)}{2}ac, mc)$. If $(a, b, c)^m \in C_{(a,b,c)}$, then $a = ma \implies m = 1$ which is absurd. □

2.1. **Heisenberg group of higher dimension.** The Heisenberg group of higher dimension, denoted by $H_{2n+1}(C_p)$ is the $(n+2) \times (n+2)$ upper triangular matrix with entries from C_p, that is,

$$H_{2n+1}(C_p) = \left\{ \begin{pmatrix} 1 & \mathbf{x} & b \\ \mathbf{0} & I_n & \mathbf{y} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \mid b \in C_p \right\}$$

where $\mathbf{x}$ is the row vector of length n, $\mathbf{y}$ is the column vector of length n and the entries of $\mathbf{x}$ and $\mathbf{y}$ are taken from C_p.

3. Preliminaries

This section contains the prerequisite definitions and results required to prove the main result. The following notations holds throughout this paper.

K	finite field of order $\kappa = q^k$ with characteristic q and $k \in \mathbb{Z}^+$
K_d	extension field of K with degree of extension $d, d \in \mathbb{N}$
$\mathcal{G}$	finite group of order n with $q \nmid n$
$e_{\mathcal{G}}$	exponent of the group $\mathcal{G}$
ω	primitive $e_{\mathcal{G}}$-th root of unity over K
$\mathbb{G}$	Galois group of $K(\omega)$ over K, where $K(\omega)$ is the splitting field of K
$\mathcal{T}_{\mathcal{G},K}$	collection of all s such that $\sigma(\omega) = \omega^s$, where $\sigma \in \mathbb{G}$
$[x, y]$	denote the commutator $x^{-1}y^{-1}xy$ of $x, y \in \mathcal{G}$

The group algebra, denoted by $K\mathcal{G}$ over the field K is the linear combination of elements from $\mathcal{G}$ with coefficients from K. As a consequence of Maschke's theorem [7], the group algebra $K\mathcal{G}$ is semisimple.

Consequently, $K\mathcal{G}$ is isomorphic to the direct sum of matrix algebras over division rings by Wedderburn decomposition theorem [7], i.e.,

$$K\mathcal{G} \simeq M(n_1, D_1) \oplus \cdots M(n_t, D_t), n_i, t \in \mathbb{Z}^+$$

The structure of the unit group of $K\mathcal{G}$ can be obtained directly from the above isomorphism. The only tricky part is to find the dimension of the matrix algebra. We recall that the unit group consists of all invertible elements in $K\mathcal{G}$ and is denoted by, $\mathcal{U}(K\mathcal{G})$. The research in this direction becomes important because of the applications of units in number theory [3], coding theory [5], cryptography [8] etc.

Definition 3.1. [2] (i) *For any prime p, an element $x \in \mathcal{G}$ is said to be p-regular element if order of x is not divisible by p.*
(ii) *For any p-regular element $x \in \mathcal{G}$, the cyclotomic K-class of $\gamma_x = \sum_{h \in C_x} h$ is the set $S_K(\gamma_x) = \{\gamma_{x^s} \mid s \in \mathcal{T}_{\mathcal{G},K}\}$.*

The proposition given below discuss about the total count of cyclotomic K-classes, whereas lemma 2.1 discusses the number of elements in a particular cyclotomic class. These two results are given by Ferraz in [2].

Proposition 3.1. *The set of simple components of $K\mathcal{G}/J(K\mathcal{G})$ and the set of cyclotomic K-classes in $\mathcal{G}$, where $J(K\mathcal{G})$ is the Jacobson radical of $K\mathcal{G}$, are in 1-1 correspondence.*

Lemma 3.1. *Let l be the number of cyclotomic K-classes in $\mathcal{G}$. If $K^{(1)}, K^{(2)}, \cdots, K^{(l)}$ are the simple components of $Z\big(K\mathcal{G}/J(K\mathcal{G})\big)$ and $S_1, S_2, \cdots, S_l$ are the cyclotomic K-classes of $\mathcal{G}$, then $|S_i| = [K^{(i)} : K]$ with a suitable ordering of the indices, assuming that $\mathbb{G}$ is cyclic.*

Lemma 3.2. (i) *Let $K\mathcal{G}$ be a semi-simple group algebra and let $\mathcal{N} \trianglelefteq \mathcal{G}$. Then*

$$K\mathcal{G} \cong K\left(\mathcal{G}/\mathcal{N}\right) \oplus \Delta(\mathcal{G}, N),$$

where $\Delta(\mathcal{G}, N)$ is an ideal of $K\mathcal{G}$ generated by the set $\{n - 1 : n \in \mathcal{N}\}$.
(ii) *If $\mathcal{N} = \mathcal{G}'$ in part (i), then $K\left(\mathcal{G}/\mathcal{G}'\right)$ is the sum of all commutative simple components of $K\mathcal{G}$ and $\Delta(\mathcal{G}, \mathcal{G}')$ is the sum of all others.*

Proposition 3.2. *The number of irreducible representation of $K\mathcal{G}$ is equal to the number of conjugacy classes of $\mathcal{G}$.*

4. Main results

The group algebra $KH_{2n+1}(C_p)$ is semi-simple, by Maschke's theorem. Equivalently, $J(KH_{2n+1}(C_p)) = 0$. Observe that the order of the Heisenberg group $H_{2n+1}(C_p)$ is p^{2n+1} and it has $2n + 1$ generators each of order p.

Lemma 4.1. *The number of conjugacy classes of $H_{2n+1}(C_p)$ is $p^{2n}+p-1$.*

Proof. The proof follows from lemma-2.2. □

Lemma 4.2. *The commutator subgroup of $H_{2n+1}(C_p)$ is C_p.*

Proof. The commutator subgroup is generated by the commutators of the group. The commutator of the group has the following form.

$$\left[\begin{pmatrix}1 & \mathbf{x} & b\\ \mathbf{0} & I_n & \mathbf{y}\\ 0 & \mathbf{0} & 1\end{pmatrix}, \begin{pmatrix}1 & \mathbf{x}' & b'\\ \mathbf{0} & I_n & \mathbf{y}'\\ 0 & \mathbf{0} & 1\end{pmatrix}\right] = \begin{pmatrix}1 & \mathbf{0} & \mathbf{x}\mathbf{y}'-\mathbf{x}'\mathbf{y}\\ \mathbf{0} & I_n & \mathbf{0}\\ 0 & \mathbf{0} & 1\end{pmatrix}$$

Thus, every commutator belongs to the $Z(H_{2n+1}(C_p))$. Also, there are p elements in the center of the Heisenberg group and hence, the result. □

The unit group of the semi simple group algebras corresponding to the group $H_{2n+1}(C_2)$ and $H_{2n+1}(C_p)$, for $p>2$ are discussed in the subsequent sections.

4.1. **Unit group of $KH_{2n+1}(C_2)$.** The group $H_{2n+1}(C_2)$ has $2^{2n}+1$ conjugacy classes by lemma-4.1. The representatives(R), size(S) and order(O) of the conjugacy classes are given below.

R	e	$\mathbf{x_1}$	$\cdots$	$\mathbf{x_n}$	b	$\mathbf{y_1}$	$\cdots$	$\mathbf{y_n}$	$\mathbf{x_1x_2}$	$\mathbf{x_1y_1}$	$\cdots$	$\prod_{i,j=1}^{n}\mathbf{x_iy_j}$
S	1	2	$\cdots$	2	1	2	$\cdots$	2	2	2	$\cdots$	2
O	1	2	$\cdots$	2	2	2	$\cdots$	2	2	4	$\cdots$	2

The exponent of the group is 4.

Theorem 4.1. *Let $\mathcal{G}=H_{2n+1}(C_2)$ be the Heisenberg group and K be the finite field of characteristic q not equal to 2. Then,*

$$K\mathcal{G} \simeq K^{2^{2n}} \oplus M_{2^n}(K)$$

Proof. The group algebra $K\mathcal{G}$ is finite and so, Artinian. Therefore, by Wedderburn's theorem,

$$K\mathcal{G} \simeq M_{n_1}(D_1)\oplus M_{n_2}(D_2)\oplus\cdots\oplus M_{n_r}(D_r)$$

$$K\mathcal{G} \simeq M_{n_1}(K_{m_1})\oplus M_{n_2}(K_{m_2})\oplus\cdots\oplus M_{n_r}(K_{m_r})$$

In the above decomposition, each component is pairwise inequivalent simple components of the group algebra. Use lemma 4.2, $\frac{\mathcal{G}}{\mathcal{G}'}\simeq (C_2)^{2n}$, where C_2 is the cyclic group of order 2.
Therefore, by lemma 3.2,

$$K\mathcal{G} \simeq K^{2^{2n}} \oplus_{i=1}^{r-2^{2n}} M_{n_i}(K_{m_i})$$

Here, $r=2^{2n}+1$ by proposition 3.2. Since $q^k\equiv \pm1 \bmod 4$ for all prime q, $|S_K(\gamma_g)|=1, \forall g\in\mathcal{G}$. Therefore, by lemma 3.1, $m_1=m_2=\cdots=m_r=1$. Hence,

$$K\mathcal{G} \simeq K^{2^{2n}} \oplus M_{n_1}(K)$$

Equate the dimensions both the sides.

$$2^{2n+1} = 2^{2n} + n_1^2$$

$$2^{2n} = n_1^2$$

$$n_1 = 2^n$$

$$\therefore K\mathcal{G} \simeq K^{2^{2n}} \oplus M_{2^n}(K)$$

□

Corollary 4.1. *Notations as above. Let $\mathcal{U}(K\mathcal{G})$ denotes the unit group of the Heisenberg group algebra. Then,*

$$\mathcal{U}(K\mathcal{G}) \simeq (K^*)^{2^{2n}} \oplus GL_{2^n}(K)$$

Corollary 4.2. *Notations as above. The order of $\mathcal{U}(K\mathcal{G})$ is given by,*

$$|\mathcal{U}(K\mathcal{G})| = (\kappa - 1)^{2^{2n}} \times (\kappa^{2^n} - \kappa^{2^n - 1})(\kappa^{2^n} - \kappa^{2^n - 2}) \cdots (\kappa^{2^n} - 1)$$

4.2. **Unit group of $KH_{2n+1}(C_p)$; $p > 2$.** The Heisenberg group $H_{2n+1}(C_p)$ has $p^{2n} + p - 1$ conjugacy classes(by lemma-4.1) as given below.

R	e	$\mathbf{x_1}$	$\cdots$	$\mathbf{x_n}$	b	$\cdots$	b^{p-1}	$\mathbf{y_1}$	$\cdots$	$\mathbf{y_n}$	$\mathbf{x_1x_2}$	$\cdots$	$\prod_{i,j=1}^{n} \mathbf{x_i^{p-1}y_j^{p-1}}$
S	1	p	$\cdots$	p	1	$\cdots$	1	p	$\cdots$	p	p	$\cdots$	p
O	1	p	$\cdots$	p	p	$\cdots$	p	p	$\cdots$	p	p	$\cdots$	p

The exponent of the group is p.

Theorem 4.2. *Let $\mathcal{G} = H_{2n+1}(C_p)$ be the Heisenberg group and K be the finite field of characteristic q not equal to p. Then, for each subgroup of $T_{\mathcal{G},K}$ of order d_i,*

$$K\mathcal{G} \simeq K \oplus (K_{d_i})^{\frac{p^2-1}{d_i}} \oplus (M_{p^n}(K_{d_i}))^{\frac{p-1}{d_i}}$$

Proof. The group algebra $K\mathcal{G}$ is finite and so, Artinian. Therefore, by Wedderburn's theorem,

$$K\mathcal{G} \simeq M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_r}(D_r)$$

$$K\mathcal{G} \simeq M_{n_1}(K_{m_1}) \oplus M_{n_2}(K_{m_2}) \oplus \cdots \oplus M_{n_r}(K_{m_r})$$

In the above decomposition, each component is pairwise inequivalent simple components of the group algebra. Here, $r = p^{2n} + p - 1$ by proposition 3.2. Since the exponent of $\mathcal{G}$ is p, $T_{\mathcal{G},K} = \{1, 2, 3, \cdots, p-1\}$. Let $p - 1 = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_l^{\lambda_l}$ and $d_1, d_2, \cdots, d_\alpha$, where $\alpha = (\lambda_1 + 1)(\lambda_2 + 1) \cdots (\lambda_l + 1)$ are the divisors of $p - 1$. Then, for each divisor $d_i (1 \le i \le \alpha)$ there exist a unique subgroup of order d_i for $T_{\mathcal{G},K}$. For each subgroup of order d_i, $S_K(\gamma_e) = \{\gamma_e\}$ and $S_K(\gamma_g) = \left\{\gamma_g, \gamma_{g^2}, \cdots, \gamma_{g^{d_i}}\right\}$ for all $g \in \mathcal{G}$ except identity by lemma-2.3.

$$\Rightarrow |S_K(\gamma_g)| = d_i, \forall g (\neq e) \in \mathcal{G} \& |S_K(\gamma_e)| = 1$$

Use lemma 4.2, $\frac{\mathcal{G}}{\mathcal{G}'} \simeq (C_p)^{2n}$, where C_p is the cyclic group of order p.

Therefore, by lemma 3.2,

$$K\mathcal{G} \simeq K \oplus (K_{d_i})^{\frac{p^{2n}-1}{d_i}} \oplus (M_{n_1}(K_{d_i}))^{\frac{p-1}{d_i}}$$

Equate the dimensions both the sides.

$$p^{2n+1} = 1 + d_i\frac{p^{2n}-1}{d_i} + \frac{p-1}{d_i}d_i(n_1^2)$$

$$n_1^2 = \frac{p^{2n+1}-p^{2n}}{p-1}$$

$$n_1 = (p)^n$$

$\therefore K\mathcal{G} \simeq K \oplus (K_{d_i})^{\frac{p^{2n}-1}{d_i}} \oplus (M_{p^n}(K_{d_i}))^{\frac{p-1}{d_i}}$, for each subgroup of $T_{\mathcal{G},K}$ of order d_i, □

Corollary 4.3. *Notations as above. Let $\mathcal{U}(K\mathcal{G})$ denotes the unit group of the Heisenberg group algebra. Then, for each subgroup of $T_{\mathcal{G},K}$ of order d_i,*

$$\mathcal{U}(K\mathcal{G}) \simeq K^* \oplus (K_{d_i}^*)^{\frac{p^{2n}-1}{d_i}} \oplus (GL_{p^n}(K_{d_i}))^{\frac{p-1}{d_i}}$$

Corollary 4.4. *Notations as above. The order of $\mathcal{U}(K\mathcal{G})$ is given by,*

$$|\mathcal{U}(K\mathcal{G})| = \begin{cases} (\kappa-1)\times(\kappa^{d_i}-1)^{\frac{p^{2n}-1}{d_i}}\times \\ \left[\left((\kappa^{d_i})^{p^n}-1\right)\left((\kappa^{d_i})^{p^n}-\kappa^{d_i}\right)\cdots\left((\kappa^{d_i})^{p^n}-(\kappa^{d_i})^{p^n-1}\right)\right]^{\frac{p-1}{d_i}} \end{cases}$$

Example 1. *Consider $n=1, p=7$ and $\mathcal{G}=H_3(C_7)$. The exponent of the group $\mathcal{G}$ is 7. So, $T_{\mathcal{G},K}$ can be $\{1\},\{1,6\},\{1,2,4\},\{1,2,3,4,5,6\}$. Here, $d_1=1, d_2=2, d_3=3, d_4=6$. Therefore, the unit group of $K_{q^k}\mathcal{G}$ for $q\neq 7$ is given by,*

- *If $T_{\mathcal{G},K}=\{1\}$ or $q^k\equiv 1$ mod 7, then $\mathcal{U}(K\mathcal{G})=(K^*)^{49}\oplus(GL_7(K))^6$*
- *If $T_{\mathcal{G},K}=\{1,6\}$ or $q^k\equiv 6$ mod 7, then $\mathcal{U}(K\mathcal{G})=K^*\oplus(K_2^*)^{24}\oplus(GL_7(K_2))^3$*
- *If $T_{\mathcal{G},K}=\{1,2,4\}$ or $q^k\equiv\{2,4\}$ mod 7, then $\mathcal{U}(K\mathcal{G})=K^*\oplus(K_3^*)^{16}\oplus(GL_7(K_3))^2$*
- *If $T_{\mathcal{G},K}=\{1,2,3,4,5,6\}$ or $q^k\equiv\{3,5\}$ mod 7, then $\mathcal{U}(K\mathcal{G})=K^*\oplus(K_6^*)^8\oplus GL_7(K_6)$*

5. Conclusion

In this paper, the Heisenberg groups of higher dimensions are discussed completely and the unit groups of the corresponding group algebras are characterized in general. Overall, the generalization of the Heisenberg group to higher dimensions opens up new avenues for exploration, enhances our understanding of complex systems, and paves the way for advancements in multiple disciplines. The findings presented in this paper have the potential to inspire further research, leading to innovative solutions, improved models, and practical applications in a wide range of scientific and technological domains.

References

[1] M. Bonatto, D. Dikranjan, Generalize Heisenberg groups and self-duality, (2016). http://arxiv.org/abs/1611.02685.

[2] R.A. Ferraz, Simple components of center of $\mathbb{F}G/J(\mathbb{F}G)$, Commun. Algebra. 36 (2008), 3191–3199. https://doi.org/10.1080/00927870802103503.

[3] W. Gao, A. Geroldinger, F. Halter-Koch, Group algebras of finite Abelian groups and their applications to combinatorial problems, Rocky Mountain J. Math. 39 (2009), 805-823. https://www.jstor.org/stable/44239708.

[4] W. Heisenberg, Über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen, Z. Physik. 33 (1925), 879–893. https://doi.org/10.1007/BF01328377.

[5] T. Hurley, Convolutional codes from units in matrix and group rings, Int. J. Pure Appl. Math. 50 (2009), 431–463.

[6] M. Manfredini, G. Palatucci, M. Piccinini, S. Polidoro, Hölder continuity and boundedness estimates for non-linear fractional equations in the Heisenberg group, J. Geom. Anal. 33 (2023), 77. https://doi.org/10.1007/s12220-022-01124-6.

[7] C.P. Miles, S.K. Sehgal, An introduction to group rings, Kluwer Academic Publishers, Dordrcht, 2002.

[8] G. Mittal, S. Kumar, S. Narain, S. Kumar, Group ring based public key cryptosystems, J. Discr. Math. Sci. Cryptography. 25 (2022), 1683–1704. https://doi.org/10.1080/09720529.2020.1796868.

[9] T. Rossi, Integrability of the sub-Riemannian mean curvature at degenerate characteristic points in the Heisenberg group, Adv. Calc. Var. 16 (2023), 99–110. https://doi.org/10.1515/acv-2020-0098.

[10] S. Thangavelu, Gutzmer's formula and the Segal-Bargmann transform, in: Statistical Science and Interdisciplinary Research, World Scientific, 2009: pp. 209–221. https://doi.org/10.1142/9789814273657_0013.