Antiautomorphisms and Biantiautomorphisms of Some Finite Abelian Groups

Daniel López-Aguayo 1,*,† and Servando López Aguayo 1,2,†

1 Tecnologico de Monterrey, Escuela de Ingeniería y Ciencias, Ave. Eugenio Garza Sada 2501, Monterrey 64849, N.L., Mexico; servando@tec.mx
2 Photonics and Mathematical Optics Group, Tecnologico de Monterrey, Monterrey 64849, Mexico
* Correspondence: dlopez.aguayo@tec.mx
† These authors contributed equally to this work.

Received: 19 January 2020; Accepted: 3 February 2020; Published: 18 February 2020

Abstract: We extend the concepts of antimorphism and antiautomorphism of the additive group of integers modulo \( n \), given by Gaitanas Konstantinos, to abelian groups. We give a lower bound for the number of antiautomorphisms of cyclic groups of odd order and give an exact formula for the number of linear antiautomorphisms of cyclic groups of odd order. Finally, we give a partial classification of the finite abelian groups which admit antiautomorphisms and state some open questions.

Keywords: antimorphism; antiautomorphism; biantiautomorphism; fixed point free; Frobenius companion matrix

1. Introduction

In this paper we introduce the concept of biantiautomorphism which is a bijective antimorphism in the sense of [1]. The main result of this paper is Theorem 2 which gives a partial classification of the finite abelian groups which admit antiautomorphisms. The main tool for this classification is the use of generalized Wilson’s Theorem for finite abelian groups, the Frobenius companion matrix and the Chinese Remainder Theorem. We also give an exact formula for the number of linear antiautomorphisms of cyclic groups of odd order.

We begin by recalling the reader Problem 2014, proposed by Gaitanas Konstantinos in [1]:

Problem 2014. For every integer \( n \geq 2 \), let \( (\mathbb{Z}_n, +) \) be the additive group of integers modulo \( n \). Define an antimorphism of \( \mathbb{Z}_n \) to be any function \( f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n \) such that \( f(x) - f(y) \neq x - y \) whenever \( x, y \) are distinct elements of \( \mathbb{Z}_n \). We say that \( f \) is an antiautomorphism of \( \mathbb{Z}_n \) if \( f \) is a bijective antimorphism of \( \mathbb{Z}_n \). For what values of \( n \) does \( \mathbb{Z}_n \) admit an antiautomorphism?

For the reader’s convenience we first give a solution to Problem 2014.

Proposition 1. Let \( n \) be an odd number. Then \( \mathbb{Z}_n \) admits an antiautomorphism.

Proof. It suffices to consider \( \phi: \mathbb{Z}_n \rightarrow \mathbb{Z}_n \) defined by \( \phi([t]) = -[t] \).

Proposition 2. Let \( n \) be an even number. Then \( \mathbb{Z}_n \) does not admit an antiautomorphism.
Proof. Suppose that \( f \) is an antiautomorphism of \( \mathbb{Z}_{2n} \), where \( n \geq 1 \). We claim that the set \( \mathcal{A} = \{ f([x]) - [x] : [x] \in \mathbb{Z}_{2n} \} \) contains, at least, two repeated elements. If not, then \( \mathcal{A} = \mathbb{Z}_{2n} \) and since \( f \) is a bijection:

\[
0 = \sum_{x=0}^{2n-1} (f([x]) - [x]) = \left[ \sum_{x=0}^{2n-1} x \right] \equiv [-n] \pmod{2n}.
\]

The result follows. \( \square \)

Proposition 3. Let \( p \) be an odd prime. Then \( \mathbb{Z}_p \) admits at least \( p^2 - 2p \) antiautomorphisms.

Proof. Let \( \mathbb{Z}_p^* \) denote the group of units of \( \mathbb{Z}_p \). Fix \([a] \in \mathbb{Z}_p^* \setminus \{1\}\) and for each \([t] \in \mathbb{Z}_p^*\), define \( \varphi_a([t]) := [at] \). It is immediate to see that \( \varphi_a \) is an antiautomorphism. Thus we obtain at least \( p - 2 \) antiautomorphisms. To obtain \( p^2 - 2p \) antiautomorphisms, it suffices to consider all the translation maps of \( \varphi_a \); that is, \( \varphi_{a,b}(t) := \varphi_a(t) + b \) where \( b \in \mathbb{Z}_p \). \( \square \)

Remark 1. Note that the number of antiautomorphisms of \( \mathbb{Z}_p \) is bounded above by the number of injective maps \( \mathbb{Z}_p \to \mathbb{Z}_p \) which have a unique fixed point; this is given by \( !\left((p - 1) \cdot p\right) \) where \( !\left((p - 1) \cdot p\right) \) denotes the subfactorial of \( p - 1 \).

We now give a lower bound for the number of antiautomorphisms of cyclic groups of odd prime power order.

Proposition 4. Let \( a \geq 2 \) and let \( p \) be an odd prime. Then \( \mathbb{Z}_{pa} \) contains at least \( p^{2a} - 2p^{2a-1} \) antiautomorphisms.

Proof. Let \((m,n)\) denote the greatest common divisor of the integers \( m \) and \( n \). It suffices to compute the cardinality of the set \( W = \{ a \in [2, p^a - 1] : (a, p^a) = (a-1, p^a) = 1 \} \). Let \( X = \{ a \in [2, p^a - 1] : (a, p^a) = 1 \} \) and \( Y = \{ a \in [2, p^a - 1] : a \equiv 1 \pmod{p} \} \). Then \( |W| = |X \setminus Y| = \varphi(p^a) - 1 - \varphi(p^{a-1} - 1) = p^a - 2p^{a-1} \), where \( \varphi \) denotes Euler’s totient function. Therefore we obtain at least \( p^a - 2p^{a-1} \) antiautomorphisms, and by considering translations we get \( p^a(p^a - 2p^{a-1}) = p^{2a} - 2p^{2a-1} \). \( \square \)

Remark 2. In Section 3 we give an exact formula for the number of linear antiautomorphisms of cyclic groups of odd order.

2. Antiautomorphisms

Definition 1 (antiautomorphism). Let \( G \) be an abelian group and let \( f : G \to G \) be any function. We say that \( f \) is an antimorphism if the map \( \text{id}_G - f \) is injective. We say that an antimorphism \( f \) is an antiautomorphism of \( G \) if \( f \) is a bijection.

Remark 3. If \( G \) is finite, then \( \text{id}_G - f \) is bijective if and only if \( \text{id}_G - f \) is injective/surjective.

The following proposition generalizes Proposition 1; moreover, it implies that any torsion-free abelian group admits an antiautomorphism.

Proposition 5. Let \( G \) be an abelian group. Then the map \( f : G \to G \) given by \( f(x) = -x \) is an antiautomorphism if and only if \( G \) has no element of order 2.

Recall that every cyclic group of even order has a unique element of order 2; hence the following result is a natural generalization of Proposition 2.
Proposition 6. Let \( G \) be a finite abelian group that has exactly one element of order 2. Then \( G \) does not admit antiautomorphisms.

Proof. Using generalized Wilson’s Theorem for finite abelian groups ([2], Theorem 2.4), we have that if \( g \) is the unique element of order 2 then \( \sum_{h \in G} h = g \). Now suppose for the sake of contradiction that \( f \) is an antiautomorphism of \( G \). Since \( \text{id}_G - f \) is a bijection, then \( 0 = \sum_{h \in G} (h - f(h)) = \sum_{h \in G} h = g \), a contradiction. It follows that \( G \) does not admit antiautomorphisms. \( \square \)

We will make use of the following lemma, whose straightforward proof we omit.

Lemma 1. Let \( G_1, \ldots, G_n \) be abelian groups and let \( f_1, \ldots, f_n \) be antiautomorphisms of \( G_1, \ldots, G_n \), respectively. Then the direct sum map \( \varphi = f_1 \oplus \cdots \oplus f_n : \bigoplus_{i=1}^{n} G_i \to \bigoplus_{i=1}^{n} G_i \) given by \( (t_1, \ldots, t_n) \mapsto (f_1(t_1), \ldots, f_n(t_n)) \) is an antiautomorphism.

The following result gives an extension of Proposition 3.

Proposition 7. Let \( G \) be a cyclic group of order \( p_1^{a_1} \cdots p_k^{a_k} \) where \( p_1, \ldots, p_k \) are distinct odd primes, and \( a_i \geq 1 \) for all \( i \in \{1, \ldots, k\} \). Then \( G \) contains at least \( \prod_{i=1}^{k} (p_i^{2a_i} - 2p_i^{2a_i-1}) \) antiautomorphisms.

Proof. For a given group \( K \) and a positive integer \( r \), let \( K^r \) denote the direct sum of \( r \)-copies of \( K \). By the Chinese Remainder Theorem, \( G \) is isomorphic to \( \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{a_i}} \). By Proposition 4, for each \( i \in \{1, \ldots, k\} \), we get \( p_i^{2a_i} - 2p_i^{2a_i-1} \) antiautomorphisms. Now applying Lemma 1 yields the desired result. \( \square \)

Even though \( \mathbb{Z}_2 \) does not admit antiautomorphisms, we now show that for every \( r \geq 2 \), the group \( \mathbb{Z}_2^r \) always admits antiautomorphisms.

Proposition 8. For every \( r \geq 2 \), the group \( \mathbb{Z}_2^r \) admits antiautomorphisms.

Proof. We first deal with the case \( r = 2 \), the Klein four-group. In this case, the map \( f : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2 \) given by:

\[
\begin{align*}
(1,1) &\mapsto (0,0) \\
(0,1) &\mapsto (0,1) \\
(0,0) &\mapsto (1,0) \\
(1,0) &\mapsto (1,1)
\end{align*}
\]

is readily verified to be an antiautomorphism (in fact, there are 8 antiautomorphisms of \( \mathbb{Z}_2^2 \)). In the case \( r = 2k \) is an even number greater or equal than 4, then by Lemma 1, we get that the map \( f \oplus f \oplus \cdots \oplus f \) is an antiautomorphism of \( \mathbb{Z}_2^r \). Therefore, it suffices to prove the result when \( r \) is an odd number greater or equal than 3.

We now deal with the group \( \mathbb{Z}_3^2 \). We are required to find a bijection \( f \) of \( \mathbb{Z}_3^2 \) such that \( \text{id}_{\mathbb{Z}_3^2} - f \) is also a bijection. Note that \( \mathbb{Z}_3^2 \) has \( 8! = 40,320 \) bijections. With the aid of Matlab, one can find all
antiautomorphisms of $\mathbb{Z}_3^2$. In fact, there are 384 such antiautomorphisms; although for our purposes we only need to find one. An explicit antiautomorphism $\phi$ of $\mathbb{Z}_3^2$ is given by:

\[
\begin{align*}
(1,1,1) & \mapsto (0,0,0) \\
(1,0,1) & \mapsto (0,0,1) \\
(0,1,1) & \mapsto (0,1,0) \\
(0,0,1) & \mapsto (1,0,0) \\
(0,1,0) & \mapsto (1,0,1) \\
(1,1,0) & \mapsto (1,1,0) \\
(1,0,0) & \mapsto (1,1,1).
\end{align*}
\]

Note that every odd number, greater or equal than 5, can be written in the form $2t + 3$ where $t \geq 1$. Then if $r = 2t + 3$, by Lemma 1 we have that $f \oplus f \cdots \oplus f \oplus \phi$ is an antiautomorphism of $\mathbb{Z}_r^2$. This completes the proof. 

Remark 4. If one prefers to avoid coding, we now present a linear algebra approach to provide examples of (some) antiautomorphisms of certain finite elementary $p$-abelian groups. Let $\alpha \geq 2$ and suppose we would like to give an example of an antiautomorphism of $\mathbb{Z}_p^\alpha$. Recall that the set of all bijective $\mathbb{Z}_p$-linear maps $\mathbb{Z}_p^\alpha \rightarrow \mathbb{Z}_p^\alpha$ can be identified with the general linear group of matrices $\text{GL}_\alpha(\mathbb{Z}_p)$. Since the set of antiautomorphisms of $\mathbb{Z}_p^\alpha$ contains the elements of $\text{GL}_\alpha(\mathbb{Z}_p)$ that have no non-trivial fixed points, it suffices to find an invertible matrix $A \in \mathbb{Z}_p^{\alpha \times \alpha}$ such that $1$ is not an eigenvalue of $A$. For instance, if $p = 2$ and $\alpha = 3$ one can take the following matrix:

\[
A = \begin{bmatrix}
1 & 1 & 0 \\
0 & 1 & 1 \\
1 & 1 & 1
\end{bmatrix}.
\]

Note that the characteristic polynomial of $A$ is equal to $f(t) = 1 + t^2 + t^3$ and $f(1) \neq 0$ in $\mathbb{Z}_2$. It follows that the linear map $h : \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^3$ defined by $h([x],[y],[z]) = ([x+y],[y+z],[x+y+z])$ is an antiautomorphism of $\mathbb{Z}_2^3$. Observe that none of the maps given in Proposition 8 are linear (because they do not fix the identity); hence not every antiautomorphism is necessarily linear.

We also have the following result.

Proposition 9. For every $m, n \geq 2$, the group $\mathbb{Z}_2^m \oplus \mathbb{Z}_4^\alpha$ admits antiautomorphisms.

Proof. Recall that the reduction map $\mathbb{Z}_{2n} \rightarrow \mathbb{Z}_2$ induces a surjection $\text{GL}_n(\mathbb{Z}_{2n}) \rightarrow \text{GL}_n(\mathbb{Z}_2)$. For every $n \geq 2$, let $f(t) \in \mathbb{Z}_2[t]$ be an irreducible polynomial of degree $n$, and let $C(f)$ be its corresponding Frobenius companion matrix of order $n$. Since $C(f) \in \text{GL}_n(\mathbb{Z}_2)$, then $C(f) \in \text{GL}_n(\mathbb{Z}_{2n})$ as well. The result follows. 

3. Biantiautomorphisms

Definition 2 (biantiautomorphism). Let $G$ be a finite abelian group and let $f$ be an antiautomorphism of $G$. We say that $f$ is a biantiautomorphism of $G$ if $f$ is also a linear map.

The next Proposition gives an example of a group that admits an antiautomorphism but not a biantiautomorphism.

Proposition 10. The group $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ admits an antiautomorphism but no biantiautomorphism.
Proof. We first show that $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ admits an antiautomorphism. Indeed, consider the map:

$$
\begin{align*}
(1,3) &\mapsto (0,0) \\
(1,2) &\mapsto (0,1) \\
(0,3) &\mapsto (0,2) \\
(0,2) &\mapsto (0,3) \\
(1,0) &\mapsto (1,0) \\
(0,1) &\mapsto (1,1) \\
(0,0) &\mapsto (1,2) \\
(1,1) &\mapsto (1,3),
\end{align*}
$$

which is clearly not linear since it does not fixes $(0,0)$. Let us show that $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ does not admit a biantiautomorphism. By ([3], Lemma 11.1) we have that $\text{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_4) \cong D_4$, the dihedral group on four letters. Now realize $D_4$ as the unitriangular matrix group of degree three over $\mathbb{Z}_2$ (a.k.a the Heisenberg group modulo 2). It is easy to check that every matrix in this group has characteristic polynomial equal to $(t-1)^3$ and thus 1 is always an eigenvalue. Therefore $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ does not admit a biantiautomorphism, as claimed. 

Remark 5. The above Proposition shows that for 2-groups that contain more than one element of order 2, it is not always the case that biantiautomorphisms exist (even though in the above case an antiautomorphism exists).

Lemma 2. Let $p$ be a prime, $\alpha \geq 1$ and let $a \in \{2, p^\alpha - 1\}$ be such that $(a, p^\alpha) = 1$. Then a non-identity element $\varphi_a \in \text{Aut}(\mathbb{Z}_{p^\alpha})$ has no non-trivial fixed point if and only if $(a - 1, p^\alpha) = 1$.

Proof. First suppose that $\varphi_a : \mathbb{Z}_{p^\alpha} \to \mathbb{Z}_{p^\alpha}$ is a linear automorphism with 0 as its only fixed point. We claim that $(a - 1, p^\alpha) = 1$. Suppose not, then there exists $i \in [1, a - 1]$ such that $p^i$ divides $a - 1$; hence $a = tp^i + 1$ for some integer $t$. Then $\varphi_a(p^{\alpha-i}) = ap^{\alpha-i} = (tp^i + 1)p^{\alpha-i} = tp^\alpha + p^{\alpha-i} = p^{\alpha-i}$ in $\mathbb{Z}_{p^\alpha}$. It follows that $\varphi_a$ has a non-trivial fixed point, a contradiction. Therefore $(a - 1, p^\alpha) = 1$.

On the other hand, suppose that $(a - 1, p^\alpha) = 1$ and that there exists $[x]$ such that $\varphi_a([x]) = [x]$. It follows that $p^\alpha$ divides $x(a - 1)$. Since $(a - 1, p^\alpha) = 1$, then $p^\alpha$ divides $x$. It follows that $[x] = [0]$ and $\varphi_a$ has no non-trivial fixed point, as claimed.

Proposition 11. Let $\alpha \geq 2$ and let $p$ be an odd prime. Then $\mathbb{Z}_{p^\alpha}$ contains exactly $p^\alpha - 2p^{\alpha-1}$ biantiautomorphisms.

Proof. The non-identity elements of $\text{Aut}(\mathbb{Z}_{p^\alpha})$ are given by the multiplication maps $\varphi_a([t]) = [at]$ where $[a] \in (\mathbb{Z}_{p^\alpha})^* \setminus \{1\}$. Therefore, it suffices to count the number of maps $\varphi_a$ which have no non-trivial fixed point. By Lemma 2, this happens if and only if $(a - 1, p^\alpha) = 1$; and by the proof of Proposition 4, this number is exactly $p^\alpha - 2p^{\alpha-1}$. This completes the proof.

Theorem 1. Let $G$ be a cyclic group of odd order $n$. Then the number of biantiautomorphisms is given by

$$
\prod_{p \in \mathcal{P}_n} p^{\alpha-1}(p - 2),
$$

where $\mathcal{P}_n$ is the set of prime divisors of $n$ and $\alpha$ is the greatest integer such that $p^\alpha$ divides $n$.

Proof. Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where the $p_i$ are distinct odd primes and $\alpha_i \geq 1$. By the Chinese Remainder Theorem, there exists an isomorphism of abelian groups $G \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$. As the orders of the
Definition 3 (fixed point free automorphism). Let \( f \) be an automorphism of a finite abelian group \( G \). We say that \( f \) is a fixed point free automorphism of \( G \) if \( f \) which admit antiautomorphisms. We summarize this classification in the following Theorem 2.

Let \( G \) be a finite abelian group. Then:

1. If \( G \) has no elements of order 2, then \( G \) admits an antiautomorphism.
2. If \( G \) has exactly one element of order 2, then \( G \) does not admit antiautomorphisms.
3. If \( G = \mathbb{Z}_{2n} \), where \( n \geq 2 \) and \( m \geq 1 \), then \( G \) admits an antiautomorphism.

The following Lemma is well-known; in fact, it also holds in the more general context of \( R \)-modules.

Lemma 3. Let \( G \) be an abelian group and let \( H \leq G \) be a subgroup. Suppose that there exists a group homomorphism \( \varphi : G \to H \) such that \( \varphi(h) = h \) for each \( h \in H \). Then \( G \cong H \oplus \ker(\varphi) \).

It follows that if \( H \leq G \) and \( \varphi : G \to H \) is a retraction such that \( H \) and \( \ker(\varphi) \) admit antiautomorphisms, then by Lemma 1, \( G \) also admits antiautomorphisms.

Lemma 4. Let \( G \) be a finite abelian non-cyclic 2-group. Then there exists \( H \leq G \) and a retraction \( G \to H \).

Proof. Suppose that \( G \cong \mathbb{Z}_{2^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{2^{a_n}} \) where the elements \( a_i \) and \( n \) are both greater or equal than 2, and let \( H = \mathbb{Z}_2^n \). Then the reduction map \( f : G \to H \) given by \( f(x_1 + 2x_2, \ldots, x_n + 2x_2) = (x_1 + 2\mathbb{Z}_2, \ldots, x_n + 2\mathbb{Z}_2) \) is clearly a retraction. Note also that \( \ker(f) \) is isomorphic to \( \bigoplus_{i=1}^{n} \mathbb{Z}_{2^{a_i} - 1} \).

In order to prove that every finite abelian non-cyclic 2-group admits an antiautomorphism it suffices, by repeated applications of Lemmas 3, 4, together with Proposition 8; to show that both \( \mathbb{Z}_2 \oplus \mathbb{Z}_2^n \) and \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2^n \), where \( n \geq 2 \), admit an antiautomorphism.

Using Propositions 5, 6, 8 and 9, we obtain a partial classification of the finite abelian groups which admit antiautomorphisms. We summarize this classification in the following

Theorem 2. Let \( G \) be a finite abelian group. Then:

1. If \( G \) has no elements of order 2, then \( G \) admits an antiautomorphism.
2. If \( G \) has exactly one element of order 2, then \( G \) does not admit antiautomorphisms.
3. If \( G = \mathbb{Z}_{2n}^m \), where \( n \geq 2 \) and \( m \geq 1 \), then \( G \) admits an antiautomorphism.
Finally, we end the paper with the following questions:

Question 1. Is there an exact formula for the number of antiautomorphisms of $\mathbb{Z}_p^n$ for any prime number $p$ and $n \geq 2$?

In [5], C. Ryan gives a recursive relation for computing the exact number of bi-antiautomorphisms of $\mathbb{Z}_p^n$ for any prime number $p$ and $n \geq 2$. Note that this problem is equivalent to finding the number of elements of $\text{GL}_n(\mathbb{Z}_p)$ which have no non-trivial fixed points. However, the general case is not covered since an antiautomorphism is not necessarily linear.

Question 2. Which finite abelian 2-groups admit antiautomorphisms but not bi-antiautomorphisms?

Author Contributions: All authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Photonics and Mathematical Optics Group of the Tecnologico de Monterrey.

Acknowledgments: We thank Pete L. Clark, Florian Luca and Efrén Pérez Terrazas for very useful comments on a first draft of this paper; we also thank Peter Mayr for clarifying some results of his thesis and the referees for their suggestions and helpful remarks.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References
1. Problem 2014. *Math. Mag.* 2017, 90, 75–76.
2. Górowski, J.; Lomnicki, A. Simple proofs of some generalizations of the Wilson’s theorem. *Annales Universitatis Paedagogicae Cracoviensis* 2014, 13, 7–14. [CrossRef]
3. Izumi, M.; Kosaki, H. Kac Algebras Arising from Composition of Subfactors: General Theory and Classification. In *Memoirs of the American Mathematical Society*; American Mathematical Society: New York, NY, USA, 2002; Volume 158.
4. Mayr, P. Finite fixed point free automorphism groups. Master’s Thesis, University Linz, Linz, Austria, 1999.
5. Ryan, C. Linear sections of the general linear group: A geometric approach. *Discret. Appl. Math.* 1992, 35, 81–86. [CrossRef]