

# Automorphically Equivalent Elements in Finite Abelian Groups

Arjun Agarwal, Rachel Chen, and Rohan Garg

MIT PRIMES-USA

(Mentored by Dr. Jim Coykendall and Jared Kettinger)

Fall-Term PRIMES Conference

October 12-13, 2024

- 1 Group Theory Background
- 2 Condition for Automorphic Equivalence
- 3 Algorithms for Automorphic Equivalence
- 4 Computing Automorphic Orbits

## Definition

A set  $G$  along with a binary operation  $+$  is a **group** if the following axioms are satisfied:

- For all elements  $g_1, g_2, g_3 \in G$  we have  $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$ .
- There exists element  $0 \in G$  such that for all  $g \in G$ ,  $g + 0 = 0 + g = g$  (this is called the **identity** of  $G$ ).
- For all elements  $g \in G$ , there exists element  $-g \in G$  such that  $g + (-g) = (-g) + g = 0$ . The element  $-g$  is called the **inverse** of  $g$ .

Note that in general, groups do not have to be commutative.

## Definition

A group  $G$  (with  $+$ ) is **abelian** if  $g_1 + g_2 = g_2 + g_1$  for all  $g_1, g_2 \in G$ .

## Example

The integers  $\mathbb{Z}$  along with the operation addition is an abelian group.

- The identity of  $\mathbb{Z}$  is 0.
- The inverse of  $g$  is  $-g$ .
- Associativity and commutativity are well known in  $\mathbb{Z}$ .

## Example

The integers modulo  $n$  for some  $n \in \mathbb{N}$  (denoted  $\mathbb{Z}/n\mathbb{Z}$ ) is an abelian group along with addition modulo  $n$ .

- The identity of  $\mathbb{Z}/n\mathbb{Z}$  is  $0 + n\mathbb{Z}$ .
- The inverse of  $g + n\mathbb{Z}$  is  $-g + n\mathbb{Z}$ .
- Associativity and commutativity follow from the operation on  $\mathbb{Z}$ .

## Definition

We say that a group is a **finite abelian group** if it is abelian and it has a finite number of elements.

## Definition

A finite abelian group is a **p-group** if its number of elements is a power of prime  $p$ .

## Definition

The integers modulo  $n$  for some  $n \in \mathbb{N}$  with the operation being addition modulo  $n$  ( $\mathbb{Z}/n\mathbb{Z}$ ) is called the **cyclic group of order  $n$**  and throughout this presentation will be denoted by  $C_n$ .

## Example

The cyclic group of order 5 has elements  $\{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$ .

From now on, each equivalence class modulo  $n$  will be denoted by one of its representatives.

## Definition

Given groups  $G$  and  $H$ , we define the **direct sum** of  $G$  and  $H$ , denoted  $G \oplus H$ , to be the group

$$\{(g, h) \mid g \in G, h \in H\},$$

with

$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2).$$

The operations in each component are done in the group.

## Example

The direct sum  $C_2 \oplus C_3$  is the set  $\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$ .

## Definition

Let  $G, H$  be groups and consider  $\varphi : G \rightarrow H$ . The map  $\varphi$  is an **isomorphism** if the following conditions hold:

- For all  $g_1, g_2 \in G$ ,  $\varphi(g_1 + g_2) = \varphi(g_1) + \varphi(g_2)$
- $\varphi$  is injective and surjective.

If  $\varphi$  is an isomorphism, then we write  $G \cong H$  and say  $G$  is **isomorphic** to  $H$ .

## Definition

When the domain and codomain of an isomorphism are both the same group, then we say the isomorphism is an **automorphism**.

## Definition

Let  $G$  be a group and let  $x$  be an element of  $G$ . We define  $kx$  for a positive integer  $k$  to be

$$\underbrace{x + x + \cdots + x}_{k \text{ times}}.$$

## Definition

Let  $G$  be a finite group and let  $x$  be an element of  $G$ . The cyclic group generated by  $x$ , denoted  $\langle x \rangle$ , is the set of all values  $kx$  where  $k$  is a positive integer.

## Example

Let  $G = C_4 \oplus C_6$  and  $x = (2, 2)$ . Then

$$\langle x \rangle = \{(2, 2), (0, 4), (2, 0), (0, 2), (2, 4), (0, 0)\}.$$



## Definition

Let  $G$  be a group and let  $H$  be a subset of  $G$ . We say  $H$  is a **subgroup** of  $G$  if  $H$  forms a group under the same operation as  $G$ . We can denote this as  $H \leq G$ .

## Example

Let  $G = \mathbb{Z}$  and  $H = 2\mathbb{Z}$  (the set of even integers). Then  $H$  is a subgroup of  $G$  since the even integers form a group under addition and  $H$  is a subset of  $G$ .

## Definition

Let  $G$  be a group and let  $H \leq G$  be a subgroup of  $G$ . For all  $g \in G$ , the sets

$$g + H = \{g + h : h \in H\}$$

and

$$H + g = \{h + g : h \in H\}$$

are called the **left cosets** and **right cosets** of  $H$ . For finite abelian groups, the left and right cosets are the same. We define

$(g_1 + H) + (g_2 + H) = (g_1 + g_2) + H$  and the cosets form a group under this operation.

## Example

Consider the group  $C_4$  and its subgroup  $H = \langle 2 \rangle = \{0, 2\}$ . The two cosets of  $H$  are  $\{0, 2\}$  and  $\{1, 3\}$ .

## Definition

Let  $G$  be a finite abelian group and let  $H \leq G$  be a subgroup of  $G$ . The **quotient group  $G$  modulo  $H$**  denoted by  $G/H$  is the collection of all cosets of  $H$ .

$$G/H = \{g + H \mid g \in G\}.$$

## Example

Let  $G = \mathbb{Z}$  and  $H = 5\mathbb{Z}$ . Then the cosets of  $H$  are

$$0 + 5\mathbb{Z} = \{\dots, -10, -5, 0, 5, \dots\}$$

$$1 + 5\mathbb{Z} = \{\dots, -9, -4, 1, \dots\}$$

$$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, \dots\}$$

$$3 + 5\mathbb{Z} = \{\dots, -7, -2, 3, \dots\}$$

$$4 + 5\mathbb{Z} = \{\dots, -6, -1, 4, \dots\}.$$

Recall that this quotient group  $\mathbb{Z}/5\mathbb{Z}$  is also called  $C_5$ .

## Theorem (Fundamental Theorem of Finite Abelian Groups)

Let  $G$  be a finite abelian group. Then  $G$  can be expressed uniquely as

$$G \cong C_{a_1} \oplus C_{a_2} \oplus \cdots \oplus C_{a_n},$$

where  $a_1 \mid a_2 \mid \cdots \mid a_n$ .

- We say that  $n$  is the **rank** of the group.
- We say that  $a_n$  is the **exponent**.

## Example

Let  $G = C_6 \oplus C_{12} \oplus C_{16}$ . We can show

$$G \cong C_2 \oplus C_{12} \oplus C_{48},$$

where  $2 \mid 12 \mid 48$ . The rank of  $G$  is 3 and the exponent of  $G$  is 48.

This leads us to our main theorem.

## Theorem (A.-C.-G.-Kettinger, 2024)

In a finite abelian group  $G$  and  $x, y \in G$ , there exists an automorphism  $\varphi$  such that  $\varphi(x) = y$  if and only if  $G/\langle x \rangle \cong G/\langle y \rangle$ .

- It is significantly easier to compute quotient groups than check all possible automorphisms  $\varphi$ .
- We use this result to develop algorithms that can check whether two elements are automorphically equivalent.

## Example

Let  $G = C_2 \oplus C_2$ . Let  $x = (0, 1)$  and  $y = (1, 1)$ . Since  $G/\langle x \rangle \cong G/\langle y \rangle \cong C_2$ , there exists an automorphism  $\varphi$  with  $\varphi(x) = y$ .

This result can also be combined with other results to produce consequences that are not immediately obvious.

## Theorem (A.-C.-G.-Kettinger, 2024)

If  $x$  and  $y$  are both of maximal order in a finite abelian group  $G$ , they are automorphic images of each other.

## Corollary (A.-C.-G.-Kettinger, 2024)

Given two elements  $x, y \in G$  of maximal order,  $G/\langle x \rangle \cong G/\langle y \rangle$ .

- The quotient group  $G/\langle x \rangle$  can be computed by reducing a matrix to what is called Smith Normal Form; the time complexity of reducing a matrix to SNF (assuming multiplication of integers can be done in constant time) is the same as the time complexity of matrix multiplication of matrices with rank equal to the rank of  $G$ .
- The Strassen algorithm, the most practical matrix multiplication algorithm, can do this in  $O(n^{2.8074})$ , where  $n$  is the rank of  $G$ .

## Key Consequence

Therefore, to check whether there exists an automorphism  $\varphi$  that maps  $x$  to  $y$ , where  $x, y \in G$ , we can instead compute  $G/\langle x \rangle$  and  $G/\langle y \rangle$ , which can be done in  $O(n^{2.8074})$ .

We also present another algorithm that is typically significantly faster than the previous algorithm.

- By using fast prime factorization algorithms to factorize  $a_n$  (the exponent), we can represent a finite abelian group  $G$  as the direct product of several  $p$ -subgroups.
- A modified Smith Normal Form algorithm can compute  $G/\langle x \rangle$  if  $G$  is a  $p$ -group in  $O(n \log n)$ , where  $n$  is the rank of  $G$ .

## Key Consequence

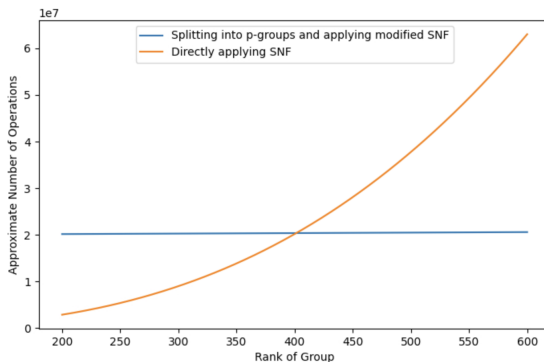
We can find our quotient group over each  $p$ -group component of  $G$  and  $x$  and combine them to get  $G/\langle x \rangle$ . There are at most  $\log_2(a_n)$  prime factors of  $a_n$  (the exponent), so there are at most  $\log_2(a_n)$   $p$ -group components. The overall complexity is  $O(n \log n \log a_n)$ .

- The algorithm is most practical when  $a_n \leq 10^{20}$ .



# Algorithms for Automorphic Equivalence

We can graph the number of operations (up to a small constant factor) it takes for the normal Smith Normal Form algorithm to run versus our modified one. For groups of larger rank, our algorithm shows a significant improvement.



## Definition

Consider a finite abelian group  $G$ . Define an **orbit**  $\mathcal{O}$  of  $G$  to be a nonempty subset of elements from  $G$  such that for each  $x \in \mathcal{O}$  and  $y \in G$ , there exists an automorphism mapping  $x$  to  $y$  if and only if  $y \in \mathcal{O}$ .

- The orbits of a group partition the group.
- The structure of these orbits has been studied, and there are algorithms counting the number of orbits, but computing the elements in each orbit and their sizes efficiently has not been done.



## Key Consequence

We have developed an algorithm that computes the orbits of  $G$  in  $O(\sqrt{|G|}n \log n)$  time, where  $n$  is the rank of  $G$ .

We would like to give our heartfelt gratitude to:

- Our amazing mentors Professor Coykendall and Jared Kettinger for their support and insights during the entire research process
- Dr. Felix Gotti and the PRIMES-USA research program for giving us this amazing opportunity to learn and conduct research
- Our friends and family for their support throughout this process.

-  Artin, M. (1955). *Algebra*. Prentice Hall. ISBN 978-0132413770.
-  Buzasi, K. (1981). Invariants of pairs of finite abelian groups. *Publ. Math. Debrecen*, 28(3-4), 317–326. (Russian).
-  Dutta, K., & Prasad, A. (2011). Degenerations and orbits in finite abelian groups. *Journal of Combinatorial Theory, Series A*, 118(6), 1685–1694.
-  Heyman, M., Khalid, A., Lippold, D., Ochieng, A., and Schroeder, B. (2021). Finding representatives for the orbits under the automorphism group of a bounded abelian group. *arXiv*.  
<https://doi.org/10.48550/arXiv.2103.10451>
-  Hillar, J., & Rhea, D. L. (2006). Automorphisms of finite abelian groups. *arXiv:math/0605185v1*.
-  Schwachhofer, M. & Stroppel, M. (1999). Finding Representatives for the Orbits under the Automorphism Group of a Bounded Abelian Group. *J. Algebra*, 221, 225–239.

-  Storjohann, A. (1996). Near optimal algorithms for computing Smith normal forms of integer matrices. *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*. ISSAC '96, 267–274.
-  Strassen, V. (1969). Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4), 354-356. <https://doi.org/10.1007/BF02165411>

**THANK YOU!**