On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials V: Over Commutative Rings

Joshua A. Grochow
University of Colorado Boulder
Boulder, USA
Joshua.Grochow@colorado.edu

Youming Qiao
University of Technology Sydney
Sydney, Australia
youming.qiao@uts.edu.au

Katherine E. Stange
University of Colorado Boulder
Boulder, USA
kstange@math.colorado.edu

Xiaorui Sun
University of Illinois at Chicago
Chicago, USA
sunsirius@gmail.com

Abstract

Tensors over commutative rings naturally appear in number theory, geometry, and group theory. For example, $2 \times 2 \times 2$ tensors over $\mathbb{Z}$ form the starting point of Bhargava's celebrated works generalising Gauss's composition law (Bhargava, *Ann. Math.*, 2004). Symmetric tensors over $\mathbb{Z}$ are central to the classification of Calabi–Yau threefolds (Yau, *Commun. Pure Appl. Math.*, 1978; Wall, *Invent. Math.*, 1966), geometric objects of significance in string theory. Additionally, tensors over finite commutative rings closely correspond to finite nilpotent groups of class 2 (Baer, *Trans. Am. Math. Soc.*, 1938).

In these settings, testing isomorphism of tensors is of great interest. For example, in mathematical physics, several recent works apply machine learning techniques to distinguish symmetric tensors from Calabi–Yau threefolds. For group isomorphism, a recent breakthrough of Sun (*STOC*, 2023) gives the first $N^{O(\log N)}$-time algorithm for testing isomorphism of p-groups of class 2 and exponent p of order N, using tensor-based techniques. Grunewald & Segal studied the computability of tensor isomorphism problems over $\mathbb{Z}$, showing that they are computable in finite time (*Ann. Math.*, 1980).

In this work, we study isomorphism testing of tensors over commutative rings from a complexity-theoretic viewpoint, and its applications. Some of our main results are as follows.

Let R be a commutative ring. We introduce two complexity classes: $3\mathsf{TI}_R$ consisting of problems that are polynomial-time reducible to isomorphism problems of tensor products of three modules over R, and $3\mathsf{FTI}_R$ consisting of problems that are polynomial-time reducible to isomorphism problems of tensor products of three free modules over R.

We show that some classical problems considered by Grunewald and Segal (ibid.), and the problem of classifying Calabi–Yau threefolds, are $3\mathsf{FTI}_{\mathbb{Z}}$-complete. We also show that many natural problems are complete for $3\mathsf{TI}_{\mathbb{Z}/p^e\mathbb{Z}}$.

We show that testing isomorphism of tensors in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ is polynomial-time equivalent to the principal ideal problem in algorithmic number theory. The key to this reduction is Bhargava's work (*Ann. Math.*, 2004). Using our equivalence, a result of Hallgren (*J. ACM*, 2007) then implies that $2 \times 2 \times 2$ tensor isomorphism over $\mathbb{Z}$ is in quantum polynomial time.

We present an $N^{O((\log N)^{8/9})}$-time algorithm for testing isomorphism of finite nilpotent groups of class 2 and odd order N. This is achieved by considering tensor isomorphism over $\mathbb{Z}/p^e\mathbb{Z}$. Following the strategy of (Sun, *STOC*, 2023), the algorithm is a reduction to testing the congruence of matrix tuples over $\mathbb{Z}/p^e\mathbb{Z}$, for which we present a polynomial-time solution following and generalizing (Ivanyos–Qiao, *SIAM J. Comput.*, 2019), who solved the analogous problem over finite fields of odd order.

CCS Concepts

• **Theory of computation → Complexity classes**; **Problems, reductions and completeness**; *Algebraic complexity theory*.

Keywords

tensor isomorphism, graph isomorphism, completeness, algebra isomorphism, polynomial isomorphism, commutative rings

ACM Reference Format:
Joshua A. Grochow, Youming Qiao, Katherine E. Stange, and Xiaorui Sun. 2025. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials V: Over Commutative Rings. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC '25), June 23–27, 2025, Prague, Czechia.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3717823.3718286

We study the problem of testing tensor isomorphism over commutative rings, significantly generalizing previous work that focused on tensors over fields. Tensors include vectors, matrices, and 3-dimensional and higher-dimensional arrays. Two 3-tensors T_{ijk}, T'_{ijk} over a field are isomorphic if they become equal after a change of basis in each of their three directions, that is, if there exist invertible matrices A, B, C such that

$$T_{ijk} = \sum_{i',j',k'} A_{ii'} B_{jj'} C_{kk'} T'_{i'j'k'} \quad (\forall i, j, k).$$

Over more general rings, we will need to refine our notion of what it means for tensors to be isomorphic, generalizing the above equation.

This work is licensed under a Creative Commons Attribution 4.0 International License.

STOC '25, Prague, Czechia

© 2025 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-1510-5/25/06
https://doi.org/10.1145/3717823.3718286

Tensors over commutative rings naturally appear in number theory, computability, geometry, mathematical physics, group theory, and cryptography. In particular, the algorithmic question of testing tensor isomorphism is of great interest in these contexts. To motivate our study, we first examine the connections to these various fields.

1 Motivations

Number theory: Bhargava's higher composition laws. Gauss's composition law for binary quadratic forms over $\mathbb{Z}$ is the first historical example of studying the class group in algebraic number theory. In the celebrated works [5–8], Bhargava discovered new composition laws for higher degree forms that go beyond class groups. Bhargava's starting point is the examination of $2 \times 2 \times 2$ tensors over $\mathbb{Z}$, which leads to a novel and visual description of Gauss's composition law. He proves a correspondence between $\mathrm{GL}(2,\mathbb{Z})$-orbits on $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ and isomorphism classes of certain ideal class triples in quadratic rings.

Geometry and mathematical physics: classifying Calabi–Yau threefolds. Calabi–Yau threefolds, that is Calabi–Yau manifolds of complex dimension 3, are of great interest in the study of geometry and mathematical physics [15, 38, 41, 60]. A key question in this context is to classify and bound the number of Calabi–Yau threefolds due to its implications to string theory [16, 26, 52], and Yau has long conjectured that the number should be finite (see e.g. [39]).

To connect the classification of Calabi–Yau threefolds with tensors over $\mathbb{Z}$, the classic theorem of Wall for Kähler manifolds is crucial [59]. Wall's theorem implies that the topological type of Calabi–Yau threefolds is determined by (1) Hodge numbers $h^{1,1}$, $h^{1,2} \in \mathbb{Z}^+$, (2) the triple intersection numbers $C_{i,j,k} \in \mathbb{N}$ for $i, j, k \in [h^{1,1}] = \{1, 2, \ldots, h^{1,1}\}$, which form a symmetric tensor, and (3) the second Chern class, which is a vector in $\mathbb{N}^{h^{1,1}}$. It is known [16, 26] that Calabi–Yau threefolds with the same Hodge numbers are diffeomorphic if and only if the triple intersection numbers and the second Chern class vectors are in the same orbit under $\mathrm{GL}(n,\mathbb{Z})$. Therefore, isomorphism of the integer 3-tensors with coordinates $C_{i,j,k}$ is a crucial step in classifying such manifolds.

Recently, machine learning methods have been applied to the classification of Calabi–Yau manifolds via Wall's theorem [39, 45]. In [45], it was noted that "there is no known algorithm to check this equivalence in finite time." However, as we now explain, such a finite-time algorithm does exist, although its complexity has not been analyzed and it may not be efficient in practice.

Computability: arithmetic group actions and the work of Grunewald & Segal. In a pair of articles [33, 34], Grunewald and Segal showed that several problems about arithmetic group actions are decidable in finite time. A main result in [33] is the decidability of the following problem. Let ρ be a rational action of $\mathrm{GL}(n,\mathbb{Z})$ on a vector space $\mathbb{C}^m$. Given $u, v \in \mathbb{C}^m$, the *orbit problem* asks whether there exists $T \in \mathrm{GL}(n,\mathbb{Z})$ such that $\rho(T) \circ u = v$.

Grunewald and Segal mentioned several applications of their solution to the orbit problem.

- (Matrix tuple conjugacy problem.) Suppose $(A_1, \ldots, A_m)$, $(B_1, \ldots, B_m) \in \mathrm{M}(n,\mathbb{Q})^m$. Decide if there exists $T \in \mathrm{GL}(n,\mathbb{Z})$ such that $\forall i \in [m]$, $TA_iT^{-1} = B_i$.
  Over fields, this is a classical problem in computer algebra known as the module isomorphism problem, for which polynomial-time algorithms exist [12, 18].
- (Form tuple equivalence problem.) Suppose $(f_1, \ldots, f_m)$ and $(g_1, \ldots, g_m)$ where f_i and $g_j \in \mathbb{Q}[x_1, \ldots, x_n]$ are homogeneous polynomials (a.k.a. forms). Decide if there exists $T \in \mathrm{GL}(n,\mathbb{Z})$ such that $\forall i \in [m]$, $f_i \circ T = g_i$.
  For single forms, this is a classical problem (generalizing equivalence of binary quadratic forms as in Gauss' work mentioned above), which has been studied by C. Jordan, H. Poincaré, and C. L. Siegel; see [35].
- (Algebra isomorphism problem.) Let $\phi, \psi : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z}^n$ be two $\mathbb{Z}$-bilinear maps. Decide if there exists $T \in \mathrm{GL}(n,\mathbb{Z})$, such that $\forall u, v \in \mathbb{Z}^n$, $\phi(T(u), T(v)) = T(\psi(u, v))$.
- (Multilinear form isomorphism problem.) Let $\phi, \psi : \mathbb{Z}^n \times \mathbb{Z}^n \times \cdots \times \mathbb{Z}^n \to \mathbb{Q}$ be two multilinear forms. Decide if there exists $T \in \mathrm{GL}(n,\mathbb{Z})$, such that $\phi \circ T = \psi$.

Group theory: finite nilpotent groups. The finite group isomorphism problem is to determine whether two finite groups are isomorphic. When the groups are given by their Cayley (multiplication) tables, this problem is one of the few natural problems in NP for which no polynomial-time algorithm is known, and which is not believed to be NP-complete (otherwise PH collapses to the second level).

Research on group isomorphism in theoretical computer science began in the 1970s. The first algorithm for group isomorphism had a running time of $N^{\log N + O(1)}$, where N denotes the order of the groups [24, 49][1]. Despite extensive study, the current best algorithm for group isomorphism has a running time of $N^{(1/4)\log N + O(1)}$ [53] (see [48, Sec. 2.2]). The recent celebrated work by Babai on quasipolynomial-time algorithms for graph isomorphism [1] has further highlighted the importance of the group isomorphism problem. That is, group isomorphism has become a bottleneck for the $n^{o(\log n)}$ time algorithm for graph isomorphism for graphs with n vertices, as group isomorphism reduces to graph isomorphism [47].

Class-2 nilpotent groups have long been recognized as the most challenging case for the group isomorphism problem. Despite significant efforts, the best-known algorithms for this class are not asymptotically better than for general groups.

Recently, progress has been made on special cases of class-2 nilpotent groups. In [57], an algorithm with a running time of $N^{O((\log N)^{5/6})}$ was proposed for p-groups of nilpotent class 2 and exponent p (meaning that every non-identity element has order p), for odd primes p. In [42], an algorithm with a running time of $N^{O(\sqrt{\log N})}$ was introduced for p-groups of Frattini class 2, whose group elements are of exponent at most p^2.[2] However, for the more

[1] Miller attributes the result to Tarjan.

[2] A p-group G is of *Frattini class* 2, if there exists $H \leq G$, such that H is central, and both H and G/H are elementary abelian. Note, however, that p-groups of Frattini class 2 do not even contain all p-groups of class 2 and exponent p^2.

general class of class-2 nilpotent groups—even those of odd order—no algorithm with a running time of $N^{o(\log N)}$ was known prior to our paper.

Cryptography: lattice isomorphism. While we will be mostly focusing on 3-tensors, 2-tensors (or matrices) over commutative rings already pose a nice challenge with possible applications in cryptography.

Let A and B be two $n \times n$ matrices over $\mathbb{Q}$. The Lattice Isomorphism Problem asks whether there exists an $n \times n$ unimodular matrix T—that is, a matrix with integer entries and determinant being ± 1—such that $T^t AT = B$. Haviv and Regev [37] showed that this problem is in the complexity class Statistical Zero Knowledge (SZK), and admits an algorithm in time $n^{O(n)} \cdot \mathrm{poly}(s)$, where s is the input size. This group action has recently received considerable attention in post-quantum cryptography [4, 21, 22]. In particular, a digital signature scheme called Hawk [11] based on lattice isomorphism has been implemented and has recently advanced to the second round of the call for post-quantum digital signature schemes by the U.S. National Institute of Standards and Technology (NIST) [58].

2 Tensors over Commutative Rings: Some Intriguing Phenomena

In this section, we walk through some intriguing phenomena for tensors over commutative rings, especially when compared with tensors of fields. While some basic ring theory will be needed to state and prove our results, in this introduction, we shall only assume some familiarity with two commutative rings: the ring of integers $\mathbb{Z}$, and the modulo ring $\mathbb{Z}/m\mathbb{Z}$ where $m \in \mathbb{N}$.

Rank notions. To start with, consider matrices, or 2-tensors. For matrices over fields, the rank notion has several equivalent interpretations, via its row span, column span, left kernel, right kernel, non-zero minors, and decompositions into sum of rank-1 matrices. We also have that an $n \times n$ matrix over a field $\mathbb{F}$ is full-rank (invertible), if its determinant is non-zero.

For matrices over rings, these notions do not coincide in general. Consider $\mathrm{R} = \mathbb{Z}/6\mathbb{Z}$ and the matrix $\begin{bmatrix} 4 & 0 \\ 0 & 3 \end{bmatrix}$ over R. Its image is spanned by $(4, 0)$ and $(0, 3)$. Its left-kernel is spanned by $(3, 0)$ and $(0, 2)$. Furthermore, it can be decomposed as $\begin{bmatrix} 2 \\ 3 \end{bmatrix} \begin{bmatrix} 2 & 3 \end{bmatrix}$. This suggests that several natural ways to formulate a rank notion for matrices over commutative rings are not equivalent.

As another example, over $\mathbb{Z}$, the matrix $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ might be considered to have full rank from several perspectives. However, as a linear map from $\mathbb{Z}^2$ to $\mathbb{Z}^2$, A is not surjective, and it does not admit an inverse. Indeed, over a commutative ring R, an $n \times n$ matrix is invertible if and only if its determinant is a *unit* in R, that is an element in R admitting a multiplicative inverse. Note that $\det(A) = 2$ which does not have an inverse in $\mathbb{Z}$.

In this work, we need to identify a suitable notion of ranks when dealing with matrices over certain R. It turns out that the notion of *inner ranks* [19], based on decomposition into a sum of rank-1, matrices works well for our purpose.

Modules: free or not. The ring-theoretic correspondence of vector spaces over $\mathbb{F}$ is modules over R. While vector spaces over $\mathbb{F}$ are determined up to isomorphism solely by their dimension, modules over R can be much more abundant and complicated.

First, the so-called free modules are in closer analogy with vector spaces, as they are isomorphic to R^n, the module of length-n vectors over R. However, there exist modules for which the notion of basis in a vector space does not behave well. Consider $\mathrm{R} = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. Then $2\mathbb{Z}/4\mathbb{Z} = \{0, 2\}$ is a module under the natural multiplication from $\mathbb{Z}/4\mathbb{Z}$, but it does not come with a basis because 2 in $2\mathbb{Z}/4\mathbb{Z}$ is not "independent", since a linear combination with non-zero coefficient results in zero, namely: $2 \times 2 = 0 \mod 4$.

As a result, in some settings we will need to formulate isomorphism problems for elements of tensor product of modules. The 3-dimensional array formulation is just for isomorphism problems of tensor products of *free* modules. Isomorphism of tensor products of (possibly) non-free modules will be crucial for our results on finite group isomorphism.

Equivalence of matrices. Let S and T be $m \times n$ matrices over R. We say that S and T are (left-right) equivalent, if there exists an $m \times m$ and $n \times n$ invertible matrices P and Q, such that $S = PTQ^t$. When $\mathrm{R} = \mathbb{F}$ is a field, S and T are equivalent if and only if they are of the same rank. When R is a general commutative ring, equivalence of S and T is generally more complicated. For example, for $\mathrm{R} = \mathbb{Z}$, the two matrices $S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ are not equivalent, despite that their row spans are both free modules of rank 2. Of course, over $\mathbb{Z}$ and more generally over principal ideal rings, equivalence classes of matrices are determined by their Smith Normal Forms. We shall make use of Smith Normal Form for some rings, but some of our results extend to rings over which Smith Normal Forms do not exist [56].

3 Our Main Results

In this paper we study isomorphism problems of tensors over commutative rings from a complexity-theoretic viewpoint. We first introduce a complexity class for tensor isomorphism over commutative rings. We then develop algorithms for $2 \times 2 \times 2$ free tensor isomorphism over $\mathbb{Z}$, and for testing isomorphism of class-2 finite nilpotent groups of odd order (with no restriction on their exponent).

Tensor Isomorphism complexity class. Over fields, the Tensor Isomorphism complexity class was developed in a series of recent works [17, 29–32]. Over commutative rings, as discussed in Section 2, to define a Tensor Isomorphism problem, we need to specify the (family of) modules under consideration.

We first define the Free-Module Tensor Isomorphism complexity class. For a commutative ring R, let R^n be the free module consisting of length-n row vectors over R. That is, $\mathrm{R}^n = \{(a_1, \ldots, a_n) \mid a_i \in \mathrm{R}\}$. Let $\mathrm{GL}(n, \mathrm{R})$ be the group of invertible matrices over R; recall that an $n \times n$ matrix T over R is *invertible* if $\det(T)$ is a unit (i.e. invertible) in R.

Let $U = \mathrm{R}^n$, $V = \mathrm{R}^m$, and $W = \mathrm{R}^\ell$. The tensor product space $U \otimes V \otimes W$ consists of $\ell \times m \times n$ cubes of elements from R. That is, $\mathtt{A} \in U \otimes V \otimes W$ is $\mathtt{A} = (a_{i,j,k})$ where $i \in [\ell]$, $j \in [m]$, $k \in [n]$ and

$a_{i,j,k} \in \mathrm{R}$. Given $L = (\alpha_{i,i'}), R = (\beta_{j,j'}), T = (\gamma_{k,k'})$, (L, R, T) sends A to $\mathsf{A}' = (a'_{i',j',k'})$ where

$$a'_{i',j',k'} = \sum_{i,j,k} \alpha_{i',i}\beta_{j',j}\gamma_{k',k}a_{i,j,k}. \tag{1}$$

The *Free Module 3-Tensor Isomorphism* problem asks, given A and $\mathsf{B} \in U \otimes V \otimes W$, whether there exists $(L, R, T) \in \mathrm{GL}(U) \times \mathrm{GL}(V) \times \mathrm{GL}(W)$ sending A to B.

Definition 3.1. Let R be a commutative ring. The Free Module 3-Tensor Isomorphism complexity class $3\mathsf{FTI}_{\mathrm{R}}$ consists of problems that are polynomial-time reducible to the Free 3-Tensor isomorphism problem over R.

More generally, for three modules A, B, C over a commutative ring R, the corresponding Tensor Isomorphism problem asks, given $s, t \in A \otimes B \otimes C$, whether there exist module isomorphisms $\alpha : A \to A$, $\beta : B \to B$, and $\gamma \in C \to C$, such that (α, β, γ) sends s to t.

Definition 3.2. Let $\bar{A}$, $\bar{B}$, and $\bar{C}$ be three families of modules over R. The $(\bar{A}, \bar{B}, \bar{C})$-$\mathsf{TI}_{\mathrm{R}}$ complexity class consists of these problems polynomial-time reducible to the (A, B, C)-TI_{R} problem for some $A \in \bar{A}$, $B \in \bar{B}$, and $C \in \bar{C}$.

If $\bar{A} = \bar{B} = \bar{C}$ is the set of all R-modules, then it is called the $3\mathsf{TI}_{\mathrm{R}}$ class for short.

Note that the $3\mathsf{FTI}_{\mathrm{R}}$ complexity class is $(\bar{A}, \bar{B}, \bar{C})$-$\mathsf{TI}_{\mathrm{R}}$ where $\bar{A} = \bar{B} = \bar{C}$ is the family of free modules.

Tensor Isomorphism complete problems: five actions. After introducing the $3\mathsf{TI}_{\mathrm{R}}$ and $3\mathsf{FTI}_{\mathrm{R}}$ complexity classes, we present complete problems for these classes. For convenience, we focus on $3\mathsf{FTI}_{\mathbb{Z}}$ and $3\mathsf{TI}_{\mathbb{Z}/p^e\mathbb{Z}}$ in the introduction.

To introduce these problems, we need the following definition. Let $\mathrm{T}(\ell \times m \times n, \mathrm{R})$ be the set of 3-way arrays of size $\ell \times m \times n$ over R. Note that unlike $U \otimes V \otimes W$, $\mathrm{T}(\ell \times m \times n, \mathrm{R})$ does not have a group action implicitly associated with it. Indeed, some natural actions on $\mathrm{T}(\ell \times m \times n, \mathrm{R})$ are as follows.

Definition 3.3. Let $U = \mathrm{R}^\ell$, $V = \mathrm{R}^m$, and $W = \mathrm{R}^n$.

(1) Given $\mathsf{A} \in \mathrm{T}(\ell \times m \times n, \mathrm{R})$, $(R, S, T) \in \mathrm{GL}(\ell, \mathrm{R}) \times \mathrm{GL}(m, \mathrm{R}) \times \mathrm{GL}(n, \mathrm{R})$ sends $\mathsf{A} = (a_{i,j,k})$ to $\mathsf{A}' = (a'_{i,j,k})$ as defined in Equation 1. This corresponds to the natural action of $\mathrm{GL}(U) \times \mathrm{GL}(V) \times \mathrm{GL}(W)$ on $U \otimes V \otimes W$.
(2) Given $\mathsf{A} \in \mathrm{T}(\ell \times \ell \times m, \mathrm{R})$, $(S, T) \in \mathrm{GL}(\ell, \mathrm{R}) \times \mathrm{GL}(m, \mathrm{R})$ sends A to A' by (S, S, T) on A as defined in Equation 1. This corresponds to the natural action of $\mathrm{GL}(U) \times \mathrm{GL}(W)$ on $U \otimes U \otimes W$.
(3) Given $\mathsf{A} \in \mathrm{T}(\ell \times \ell \times m, \mathrm{R})$, $(S, T) \in \mathrm{GL}(\ell, \mathrm{R}) \times \mathrm{GL}(m, \mathrm{R})$ sends A to A' by (S, S^{-t}, T) on A as defined in Equation 1. Here S^{-t} denotes the transpose inverse of S. This corresponds to the natural action of $\mathrm{GL}(U) \times \mathrm{GL}(W)$ on $U \otimes U^* \otimes W$, where $U^* := \mathrm{Hom}_R(U, R)$ denotes the dual module of U.
(4) Given $\mathsf{A} \in \mathrm{T}(\ell \times \ell \times \ell, \mathrm{R})$, $S \in \mathrm{GL}(\ell, \mathrm{R})$ sends A to A' by (S, S, S) on A as defined in Equation 1. This corresponds to the natural action of $\mathrm{GL}(U)$ on $U \otimes U \otimes U$.
(5) Given $\mathsf{A} \in \mathrm{T}(\ell \times \ell \times \ell, \mathrm{R})$, $S \in \mathrm{GL}(\ell, \mathrm{R})$ sends A to A' by (S, S, S^{-t}) on A as defined in Equation 1. This corresponds to the natural action of $\mathrm{GL}(U)$ on $U \otimes U \otimes U^*$. Note that in this case A can be viewed as recording the structure constants of some (possibly non-associative) algebra.

We also need the following notions for 3-way arrays. Let $\mathsf{A} \in \mathrm{T}(\ell \times m \times n, \mathbb{F})$. The *length* of A is defined as $\ell + m + n$. The *frontal slices* of A are $\{A_1, \ldots, A_n\} \subseteq \mathrm{M}(\ell \times m, \mathbb{F})$, where $A_k(i, j) = a_{i,j,k}$. Let $\mathsf{A} \in \mathrm{T}(n \times n \times n, \mathbb{F})$. Then A is *symmetric* if for any $\sigma \in \mathrm{S}_3$, $\mathsf{A}(i, j, k) = \mathsf{A}(\sigma(i), \sigma(j), \sigma(k))$, and A is *anti-symmetric* if for any $\sigma \in \mathrm{S}_3$, $\mathsf{A}(i, j, k) = \mathrm{sgn}(\sigma)\mathsf{A}(\sigma(i), \sigma(j), \sigma(k))$.

Our first result is about $3\mathsf{FTI}_{\mathrm{R}}$ where $\mathrm{R} = \mathbb{Z}$.

Theorem 3.4. *Let $\mathrm{R} = \mathbb{Z}$. For $i, j \in [5]$, $i \neq j$, let A and B two 3-way arrays of total length L whose sizes admit the ith action defined in Definition 3.3. Then there exists a polynomial-time computable function f that takes A and B and outputs 3-way arrays $f(\mathsf{A})$ and $f(\mathsf{B})$, such that A and B are in the same orbit under the ith action if and only if $f(\mathsf{A})$ and $f(\mathsf{B})$ are in the same orbit under the jth action.*

Furthermore, the above holds even with the following additional structural restrictions:

(1) For $j = 2$, i.e. the action of $\mathrm{GL}(U) \times \mathrm{GL}(W)$ on $U \otimes U \otimes W$, the frontal slices of $f(\mathsf{A})$ and $f(\mathsf{B})$ are symmetric (or skew-symmetric).
(2) For $j = 4$, i.e. the action of $\mathrm{GL}(U)$ on $U \otimes U \otimes U$, $f(\mathsf{A})$ and $f(\mathsf{B})$ are symmetric (or anti-symmetric) 3-way arrays.
(3) For $j = 5$, i.e. the action of $\mathrm{GL}(U)$ on $U \otimes U \otimes U^*$, $f(\mathsf{A})$ and $f(\mathsf{B})$ record the structure constants of associative or Lie algebras.

We then have the following result on the complexity of some natural algorithmic problems over $\mathbb{Z}$, some of which were considered in [35]. Note that in the following, we may consider tensors over $\mathbb{Q}$ but with actions from $\mathrm{GL}(n, \mathbb{Z})$. The complexity class $3\mathsf{FTI}_{\mathbb{Z}}$ can be generalised to take into this account naturally.

Corollary 3.5. *The following problems are $3\mathsf{FTI}_{\mathbb{Z}}$-complete.*

- *Matrix space conjugacy problem: suppose $(A_1, \ldots, A_m)$ and $(B_1, \ldots, B_m) \in \mathrm{M}(n, \mathbb{Q})^m$. Decide if there exists $T \in \mathrm{GL}(n, \mathbb{Z})$ and $S = (s_{i,j}) \in \mathrm{GL}(m, \mathbb{Z})$, such that $\forall i \in [m]$, $TA_iT^{-1} = \sum_{j \in [m]} s_{i,j}B_j$.*
- *Algebra isomorphism: given $\mathbb{Z}$-linear forms $\phi, \psi : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z}^n$, decide if there exists $T \in \mathrm{GL}(n, \mathbb{Z})$, such that $\forall u, v \in \mathbb{Z}^n$, $\phi(T(u), T(v)) = T(\psi(u, v))$.*
- *Trilinear form isomorphism: let $\phi, \psi : \mathbb{Z}^n \times \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Q}$ be two symmetric trilinear forms. Decide if there exists $T \in \mathrm{GL}(n, \mathbb{Z})$, such that $\phi \circ T = \psi$.*
- *Inhomogeneous trilinear form isomorphism: let $\phi, \psi : \mathbb{Z}^n \times \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{N}$ be two trilinear forms, and $f, g : \mathbb{Z}^n \to \mathbb{N}$ be two $\mathbb{Z}$-linear forms. Decide if there exists $T \in \mathrm{GL}(n, \mathbb{Z})$, such that $\phi \circ T = \psi$ and $f \circ T = g$.*

Note that inhomogeneous trilinear form isomorphism naturally arises from the Calabi–Yau threefold homeomorphism problem as discussed in Section 1.

Our second result is about $3\mathsf{TI}_{\mathrm{R}}$ where $\mathrm{R} = \mathbb{Z}/p^e\mathbb{Z}$ where p is prime. Let U be a $\mathbb{Z}/p^e\mathbb{Z}$ module. As $\mathbb{Z}/p^e\mathbb{Z}$ is a local ring (=unique maximal ideal), the rank of U is well-defined as the size of a minimal generating set of A. As $\mathbb{Z}/p^e\mathbb{Z}$ is a principal ideal ring (all ideals are generated by single elements), U is isomorphic to a direct sum of cyclic modules (=modules generated by a single element). This

means that in algorithms, U can be viewed as consisting of vectors where each coordinate is from $\mathbb{Z}/p^k\mathbb{Z}$ for some $k \in \{1, \ldots, e\}$. The automorphism group of U can be represented in a matrix format [40, 51].

These indicate that we can compute with $\mathbb{Z}/p^e\mathbb{Z}$-modules, their automorphism groups, and tensor products, in a manner not very different from the free module setting. In particular, for three $\mathbb{Z}/p^e\mathbb{Z}$-modules U, V, and W, let $\ell = \mathrm{rk}(U)$, $m = \mathrm{rk}(V)$, and $\ell = \mathrm{rk}(W)$. Then $U \otimes V \otimes W$ can be recorded as a 3-way array of size $\ell \times m \times n$, and three tuples of integers $(a_1, \ldots, a_\ell)$, $(b_1, \ldots, b_m)$, $(c_1, \ldots, c_n)$. Then we can define five actions on such 3-way arrays as in Definition 3.3.

For applications to group isomorphism, the following parameter is important. Let U, V, and W be three finite modules over $\mathbb{Z}/p^e\mathbb{Z}$. We define the "complex parameter" of $U \otimes V \otimes W$ as $\log_p(|U| \cdot |V| \cdot |W|)$.

Theorem 3.6. *Let* $\mathrm{R} = \mathbb{Z}/p^e\mathbb{Z}$. *Let* U, V, W *be finite* $\mathbb{Z}/p^e\mathbb{Z}$*-modules. For* $i, j \in [5]$, $i \neq j$, *let* A *and* B *two* 3*-way arrays in* $U \otimes V \otimes W$, *with complex parameters* L. *Then there exists a polynomial-time computable function* f *that takes* A *and* B *and outputs* 3*-way arrays* $f(\mathsf{A})$ *and* $f(\mathsf{B})$, *such that (1) the complex parameters of* $f(\mathsf{A})$ *and* $f(\mathsf{B})$ *are upper bounded by* $L^{O(1)}$, *and (2)* A *and* B *are in the same orbit under the* i*th action if and only if* $f(\mathsf{A})$ *and* $f(\mathsf{B})$ *are in the same orbit under the* j*th action.*

Furthermore, the above holds even with the following additional structural restrictions:

(1) For $j = 2$, *i.e. the action of* $\mathrm{GL}(U) \times \mathrm{GL}(W)$ *on* $U \otimes U \otimes W$, *the frontal slices of* $f(\mathsf{A})$ *and* $f(\mathsf{B})$ *are symmetric (or skew-symmetric).*

(2) For $j = 4$, *i.e. the action of* $\mathrm{GL}(U)$ *on* $U \otimes U \otimes U$, $f(\mathsf{A})$ *and* $f(\mathsf{B})$ *are symmetric (or anti-symmetric)* 3*-way arrays.*

(3) For $j = 5$, *i.e. the action of* $\mathrm{GL}(U)$ *on* $U \otimes U \otimes U^*$, $f(\mathsf{A})$ *and* $f(\mathsf{B})$ *record the structure constants of associative or Lie algebras.*

$2 \times 2 \times 2$ free tensor isomorphism over $\mathbb{Z}$. We study testing isomorphism of tensors of free modules over $\mathbb{Z}$. By the results of Grunewald and Segal on arithmetic group actions[33], this problem is decidable. The algorithms in [33] relies on Tarski's decidability of elementary theory over $\mathbb{R}$, so it is unlikely to be in NP [3, 27]. On the other hand, as mentioned in Section 1, $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ isomorphism was studied by Bhargava [5], so this gives hope that better complexity results can be obtained for testing isomorphism of tensors in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. This is indeed the case; the following result relies crucially on Bhargava's work [5].

Theorem 3.7. Tensor Isomorphism *for* $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ *is polynomial-time equivalent to the* Principality Decision Problem *for real quadratic fields. In particular, it is in* BQP.

Let us briefly review the Principality Decision Problem. In a number field order R, this problem is to determine, given an ideal I of R, whether I is principal. This is the decisional portion of the Principal Ideal Problem or the Principality Testing Problem; see [44, Chapter 16]. It is a subroutine of the most important algorithmic number theory problems for number fields, including class group and unit group computations. It is also important to the security of cryptography based on ideal lattices. In fact, there are reductions from γ-SVP (Shortest Vector Problem) to the Principal Ideal Problem for cyclotomic fields due to Cramer, Ducas, and Wesolowski [20].

Here we deal with the Principal Ideal Problem for real quadratic number field orders. This is the basis for the cryptographic scheme of Buchmann and Williams and others [13, 14, 54]. The best known unconditional classical methods in the maximal order are exponential [44, Chapter 16], with some conditional subexponential algorithms [44, Theorem 13.24]. For non-maximal orders, we additionally need to factor the discriminant and solve discrete logarithm problems in the prime fields for primes dividing the conductor; see [10] (which leaves us in the same position: unconditionally exponential, conditionally subexponential). However, it can be solved by a polynomial-time quantum algorithm [36], which was later generalized to arbitrary number fields [9].

Class-2 nilpotent group isomorphism. A group G is class-2 nilpotent if $G/Z(G)$ is Abelian, where $Z(G)$ denotes the center of G, the set of elements that commute with every element of G. As our main application of the Tensor Isomorphism complexity classes over $\mathbb{Z}/p^e\mathbb{Z}$, we give the first $N^{o(\log N)}$ time algorithm for testing isomorphism of two class-2 nilpotent groups of odd orders, where N is the order of the two groups.

Theorem 3.8. *There exists an algorithm that determines the isomorphism of two nilpotent class-2 groups of odd order in time* $N^{O((\log N)^{8/9})}$, *where* N *is the order of the two groups.*

4 Comments on Previous Works and Techniques

Equivalence between five actions on 3-way arrays. The equivalence of the actions in Definition 3.3 was shown over fields in [25, 29, 30, 32], with two types of gadgets having been designed to achieve this. The first type of gadget was first introduced in [25] and further developed in [29, 32]. For convenience, we call this gadget the Furtorny–Grochow–Sergeichuk gadget, or FGS gadget for short. The second type of gadget was introduced in [30], and we call such gadget the Grochow–Qiao gadget, or GQ gadget for short.

To use the FGS gadget in the commutative ring setting, one problem arises, namely it relies on the Krull–Schmidt theorem for quiver representations in the correctness proof [25]. Indeed, to use it in the orthogonal and unitary group setting, a version of Krull-Schmidt theorem for orthogonal and unitary representations of quivers was required [17], and such a result was shown by Sergeichuk [55]. However, over commutative rings, Krull–Schmidt type results are only known for certain families of commutative rings [23].

To use the GQ gadget in the commutative ring setting, there is an issue caused by the so-called non-degeneracy assumption, which is closely related to some distinctions between fields and commutative rings seen in Section 2. More specifically, consider the field setting. If $A \in \mathrm{M}(m \times n, \mathbb{F})$ with $m \leq n$ is full-rank (i.e., $\mathrm{rk}(A) = m$), then $TA = 0$ if and only if $T = 0$, for any $m \times m$ matrix T. Furthermore, if A is not full rank, we can efficiently compute $A' \in \mathrm{M}(r \times n)$ such that the rowspan of A and A' are the same, but A' is now full rank. Similarly, for equivalence of matrices under left-and-right column operations, the orbits over fields are completely determined by rank; if A, B are two matrices, and we build A', B' as

in the preceding, then A and B are equivalent if and only if A', B' are equivalent, but A', B' are now full rank. Being full rank is a kind of "non-degeneracy" assumption, and over fields, reduced row echelon form generally lets us reduce from the general case to the non-degenerate case.

In contrast, if $A, B \in \mathrm{M}(m \times n, \mathrm{R})$ where R is a commutative ring, the above procedure fails due to the lack of some basic notions such as ranks and the relation between kernels and bases. For example, the inner ranks of $A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix}$ over $\mathbb{Z}/6\mathbb{Z}$ are both 2, but they are not equivalent. We also note that $\ker(A)$ is non-zero, while the submodule spanned by the rows of A is not cyclic (i.e. not generated by 1 element). Several reductions in [29, 32] make use such non-degeneracy assumptions.

By a new combination of the FGS and GQ gadgets, we are able to avoid the need for such non-degeneracy assumptions, to generalize the reductions to a much wider class of commutative rings.

From isomorphism of $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ to principal decision. For a reduction from $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ isomorphism to the Principal Ideal Decision problem, we make use of a well-known invariant called discriminants. We first show that if the tensors are of square discriminants (which are considered a "degenerate" case in the setting of number theory), isomorphism can be decided in polynomial time. For the case of non-square discriminant, which is the more interesting and complicated setting from a number theoretic viewpoint, we use Bhargava's correspondence between isomorphism classes of $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ and the so-called balanced triples of oriented ideals in a quadratic number field order. This correspondence can be made constructive and paves the way to the Principal Ideal Decision problem.

Isomorphism testing for nilpotent class-2 groups. Our algorithm for testing isomorphism of nilpotent class-2 groups of odd order runs in time $N^{O((\log N)^{8/9})}$. It first applies Bear's correspondence [2, 46, 50] to reduce the group isomorphism problem to a Lie-ring isomorphism problem. We then generalize reductions from [30] to work over $\mathbb{Z}/p^e\mathbb{Z}$-Lie rings—even in the non-free-module case—and by a small trick we then reduce from Lie rings whose underlying Abelian group is arbitrary odd order, to Lie rings whose underlying Abelian group is a free $\mathbb{Z}/p^e\mathbb{Z}$-module, that is, of the form $(\mathbb{Z}/p^e\mathbb{Z})^n$ for some n.

Next, we generalize recent work on tensor isomorphism over a finite field $\mathbb{F}_p$ [42, 57] to tensor isomorphism over a finite ring $\mathbb{Z}/p^e\mathbb{Z}$. One challenge in this generalization is to ensure that the algorithm's efficiency depends not only on the tensor's dimension. For instance, let $G \cong (\oplus_{i=1}^{n-1}\mathbb{Z}/p\mathbb{Z}) \oplus \mathbb{Z}/p^e\mathbb{Z}$, $H \cong (\oplus_{i=1}^{m-1}\mathbb{Z}/p\mathbb{Z}) \oplus \mathbb{Z}/p^e\mathbb{Z}$, $G' \cong \oplus_{i=1}^{n}\mathbb{Z}/p\mathbb{Z}$, and $H' \cong \oplus_{i=1}^{m}\mathbb{Z}/p\mathbb{Z}$. Although two tensors encoding bilinear maps $G \times G \to H$ and $G' \times G' \to H'$ share the same dimension, the complexity of isomorphism testing differs. This is because the bilinear map $G' \times G' \to H'$ encodes more information than $G \times G \to H$. For the purpose of group isomorphism, it requires a running time that reflects the underlying complexity of the bilinear map encoded. This complication is the cause of the 8/9 in the exponent in Theorem 3.8, compared to the 5/6 [57] and 1/2 [42] of previous work.

In our solution, we handle matrix slices of the tensor based on their orders under matrix addition. We divide the tensor into multiple parts to decouple the correlation between matrices of high and low orders. For the high-order matrices, we enumerate a few matrices to establish the correspondence between high-order matrices in the two tensors. For the low-order matrices, we follow the strategy from the previous work over finite fields [42, 57]. To achieve the latter, we extend the individualization and refinement technique, as well as the low-rank matrix characterization method from over finite fields [42, 57], to finite rings. This generalization combines various measures of matrices over rings, rather than relying solely on inner rank. For example, in [57], the low-rank characterization critically depends on the fact that over a finite field, for a matrix X and a row vector x, if x is not in the row-span of X, then the rank of $\begin{bmatrix} X \\ x \end{bmatrix}$ is greater than the rank of X. However, over a ring, the rank of $\begin{bmatrix} X \\ x \end{bmatrix}$ may be the same as the rank of X. Therefore, in our approach, we sometimes use the number of distinct elements in the row-span of a matrix to track progress instead of inner rank.

As in [42, 57], we ultimately reduce to the Matrix Tuple Isometry problem, but now over $\mathbb{Z}/p^e\mathbb{Z}$ instead of over a finite field of odd order. Solving this problem in polynomial time over odd order fields was one of the main results of Ivanyos & Qiao [43]. We generalize their result to work over $\mathbb{Z}/p^e\mathbb{Z}$, and in fact over arbitrary finite local principal ideal rings of odd characteristic, which may have further applications to codes over such rings. The first part of the generalization requires using Smith Normal Form to reduce to the non-degenerate case (while this does not work over arbitrary commutative rings, it does work over $\mathbb{Z}/p^e\mathbb{Z}$ and finite PIRs). We then prove several algebraic lemmas about $\mathbb{Z}/p^e\mathbb{Z}$ that allow us to generalize their techniques to our setting. Finally, in the end the problem is reduced to a certain problem in semisimple $*$-algebras, and such algebras are algebras over a finite field, even if the algebras we started with were over $\mathbb{Z}/p^e\mathbb{Z}$ (or a finite local PIR). Thus, at that point, we can apply some of the results of [43] directly.

We note that for even-order nilpotent groups, not only is the group-theoretic situation itself more complicated, but it even remains open to just do the last step—solve Matrix Tuple Isometry—over *fields* of characteristic 2 (let alone rings) in polynomial time.

Acknowledgments

J. A. G. was partly supported by the National Science Foundation (NSF) CAREER award CCF-2047756..

Y. Q. was supported in part by Australian Research Council DP200100950 and LP220100332. Part of this work was done while Youming was a member of the Institute for Advanced Study in Princeton supported by the Ky Fan and Yu-Fen Fan Endowment Fund.

K. E. S. was partly supported the National Science Foundation (NSF) under Grant No. DMS-2401580.

X. S. was partly supported by the National Science Foundation (NSF) under Grant No. 2240024.

References

[1] László Babai. 2016. Graph isomorphism in quasipolynomial time. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. 684–697.

[2] Reinhold Baer. 1938. Groups with abelian central quotient group. *Trans. Amer. Math. Soc.* 44, 3 (1938), 357–386.

[3] Michael Ben-Or, Dexter Kozen, and John Reif. 1984. The complexity of elementary algebra and geometry. In *Proceedings of the sixteenth annual ACM symposium on Theory of computing*. 457–464.

[4] Benjamin Bencina, Alessandro Budroni, Jesús-Javier Chi-Domínguez, and Mukul Kulkarni. 2024. Properties of Lattice Isomorphism as a Cryptographic Group Action. In *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Oxford, UK, June 12-14, 2024, Proceedings, Part I (Lecture Notes in Computer Science, Vol. 14771)*, Markku-Juhani O. Saarinen and Daniel Smith-Tone (Eds.). Springer, 170–201. doi:10.1007/978-3-031-62743-9_6

[5] Manjul Bhargava. 2004. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)* 159, 1 (2004), 217–250. doi:10.4007/annals.2004.159.217

[6] Manjul Bhargava. 2004. Higher composition laws II: On cubic analogues of Gauss composition. *Annals of mathematics* 159, 2 (2004), 865–886.

[7] Manjul Bhargava. 2004. Higher composition laws III: The parametrization of quartic rings. *Annals of mathematics* 159, 3 (2004), 1329–1360.

[8] Manjul Bhargava. 2008. Higher composition laws IV: The parametrization of quintic rings. *Annals of Mathematics* (2008), 53–94.

[9] Jean-François Biasse and Fang Song. 2016. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the 27th annual ACM–SIAM symposium on discrete algorithms, SODA 2016, Arlington, VA, USA, January 10–12, 2016*. Philadelphia, PA: Society for Industrial and Applied Mathematics (SIAM); New York, NY: Association for Computing Machinery (ACM), 893–902. doi:10.1137/1.9781611974331.ch64

[10] Jean-Fran¸cois Biasse, Claus Fieker, and Michael J. Jacobson, Jr. 2016. Fast heuristic algorithms for computing relations in the class group of a quadratic order, with applications to isogeny evaluation. *LMS J. Comput. Math.* 19 (2016), 371–390. doi:10.1112/S1461157016000358

[11] Joppe W Bos, Olivier Bronchain, Léo Ducas, Serge Fehr, Yu-Hsuan Huang, Thomas Pornin, Eamonn W Postlethwaite, Thomas Prest, Ludo N Pulles, and Wessel van Woerden. 2023. Hawk: A Signature Scheme Inspired by the Lattice Isomorphism Problem. https://hawk-sign.info/.

[12] Peter A. Brooksbank and Eugene M. Luks. 2008. Testing isomorphism of modules. *Journal of Algebra* 320, 11 (2008), 4020 – 4029. doi:10.1016/j.jalgebra.2008.07.014

[13] Johannes Buchmann and H. C. Williams. 1988. A key-exchange system based on imaginary quadratic fields. *J. Cryptology* 1, 2 (1988), 107–118. doi:10.1007/BF02351719

[14] Johannes Buchmann and H. C. Williams. 1990. Quadratic fields and cryptography. In *Number theory and cryptography (Sydney, 1989)*. London Math. Soc. Lecture Note Ser., Vol. 154. Cambridge Univ. Press, Cambridge, 9–25.

[15] Philip Candelas, Gary T Horowitz, Andrew Strominger, and Edward Witten. 1985. Vacuum configurations for superstrings. *Nuclear Physics B* 258 (1985), 46–74.

[16] Aditi Chandra, Andrei Constantin, Cristofero S Fraser-Taliente, Thomas R Harvey, and Andre Lukas. 2024. Enumerating Calabi-Yau Manifolds: Placing Bounds on the Number of Diffeomorphism Classes in the Kreuzer-Skarke List. *Fortschritte der Physik* 72, 5 (2024), 2300264.

[17] Zhili Chen, Joshua A. Grochow, Youming Qiao, Gang Tang, and Chuanqi Zhang. 2024. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials III: Actions by Classical Groups. In *15th Innovations in Theoretical Computer Science Conference, ITCS 2024, January 30 to February 2, 2024, Berkeley, CA, USA (LIPIcs, Vol. 287)*, Venkatesan Guruswami (Ed.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 31:1–31:23. doi:10.4230/LIPICS.ITCS.2024.31

[18] Alexander Chistov, Gábor Ivanyos, and Marek Karpinski. 1997. Polynomial time algorithms for modules over finite dimensional algebras. In *Proceedings of the 1997 international symposium on Symbolic and algebraic computation*. ACM, 68–74.

[19] P. M. Cohn. 1985. *Free rings and their relations*. Number 19 in London Mathematical Society Monographs. Academic Press.

[20] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. 2017. Short Stickelberger class relations and application to ideal-SVP. In *Advances in cryptology—EUROCRYPT 2017. Part I*. Lecture Notes in Comput. Sci., Vol. 10210. Springer, Cham, 324–348. doi:10.1007/978-3-319-56620-7_12

[21] Léo Ducas and Shane Gibbons. 2023. Hull Attacks on the Lattice Isomorphism Problem. In *Public-Key Cryptography - PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7-10, 2023, Proceedings, Part I (Lecture Notes in Computer Science, Vol. 13940)*, Alexandra Boldyreva and Vladimir Kolesnikov (Eds.). Springer, 177–204. doi:10.1007/978-3-031-31368-4_7

[22] Léo Ducas and Wessel P. J. van Woerden. 2022. On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography. In *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III (Lecture Notes in Computer Science, Vol. 13277)*, Orr Dunkelman and Stefan Dziembowski (Eds.). Springer, 643–673. doi:10.1007/978-3-031-07082-2_23

[23] Alberto Facchini. 2003. The Krull-Schmidt theorem. In *Handbook of algebra*. Vol. 3. Elsevier, 357–397.

[24] V. Felsch and J. Neubüser. 1970. On a programme for the determination of the automorphism group of a finite group. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*. „ 59–60.

[25] Vyacheslav Futorny, Joshua A. Grochow, and Vladimir V. Sergeichuk. 2019. Wildness for tensors. *Lin. Algebra Appl.* 566 (2019), 212–244. doi:10.1016/j.laa.2018.12.022

[26] Naomi Gendler, Nate MacFadden, Liam McAllister, Jakob Moritz, Richard Nally, Andreas Schachner, and Mike Stillman. 2023. Counting Calabi-Yau Threefolds. *arXiv preprint arXiv:2310.06820* (2023).

[27] D Yu Grigor'ev. 1988. Complexity of deciding Tarski algebra. *Journal of symbolic Computation* 5, 1-2 (1988), 65–108.

[28] Joshua A. Grochow and Youming Qiao. 2019. Isomorphism problems for tensors, groups, and cubic forms: completeness and reductions. arXiv:1907.00309 [cs.CC].

[29] Joshua A. Grochow and Youming Qiao. 2023. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials I: Tensor Isomorphism-Completeness. *SIAM J. Comput.* 52 (2023), 568–617. Issue 2. doi:10.1137/21M1441110 Part of the preprint [28]. Preliminary version appeared at ITCS '21, DOI:10.4230/LIPIcs.ITCS.2021.31.

[30] Joshua A. Grochow and Youming Qiao. 2023. On the complexity of isomorphism problems for tensors, groups, and polynomials IV: linear-length reductions and their applications. *CoRR* abs/2306.16317 (2023). doi:10.48550/ARXIV.2306.16317 arXiv:2306.16317

[31] Joshua A. Grochow and Youming Qiao. 2024. On p-Group Isomorphism: Search-to-Decision, Counting-to-Decision, and Nilpotency Class Reductions via Tensors. *ACM Trans. Comput. Theory* 16, 1 (2024), 2:1–2:39. doi:10.1145/3625308

[32] Joshua A. Grochow, Youming Qiao, and Gang Tang. 2022. Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. *J. Groups Complex. Cryptol.* 14, 1 (2022), [Paper No. 9431], 21. doi:10.46298/jgcc.2022.14.1.9431 Extended abstract appeared in STACS '21.

[33] Fritz Grunewald and Daniel Segal. 1980. Some general algorithms. I: Arithmetic groups. *Annals of Mathematics* 112, 3 (1980), 531–583.

[34] Fritz Grunewald and Daniel Segal. 1980. Some general algorithms. II: Nilpotent groups. *Annals of Mathematics* 112, 3 (1980), 585–617.

[35] Fritz J. Grunewald and Daniel Segal. 1979. The solubility of certain decision problems in arithmetic and algebra. *Bulletin (New Series) of the American Mathematical Society* 1, 6 (1979), 915 – 918.

[36] Sean Hallgren. 2007. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *J. ACM* 54, 1 (2007), 19. doi:10.1145/1206035.1206039 Id/No 4.

[37] Ishay Haviv and Oded Regev. 2014. On the Lattice Isomorphism Problem. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, Chandra Chekuri (Ed.). SIAM, 391–404. doi:10.1137/1.9781611973402.29

[38] Yang-Hui He. 2021. *The Calabi–Yau Landscape: From Geometry, to Physics, to Machine Learning*. Vol. 2293. Springer Nature.

[39] Yang-Hui He, Zhi-Gang Yao, and Shing-Tung Yau. 2024. Distinguishing Calabi-Yau Topology using Machine Learning. *arXiv preprint arXiv:2408.05076* (2024).

[40] Christopher J. Hillar and Darren L. Rhea. 2007. Automorphisms of finite Abelian groups. *Am. Math. Mon.* 114, 10 (2007), 917–923. doi:10.1080/00029890.2007.11920485

[41] Tristan Hubsch. 1992. *Calabi-Yau manifolds: A Bestiary for physicists*. World scientific.

[42] Gábor Ivanyos, Euan Jacob Mendoza, Youming Qiao, Xiaorui Sun, and Chuanqi Zhang. 2024. Faster Isomorphism Testing of p-Groups of Frattini Class-2. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024*. IEEE, 1408–1424.

[43] Gábor Ivanyos and Youming Qiao. 2019. Algorithms Based on *-Algebras, and Their Applications to Isomorphism of Polynomials with One Secret, Group Isomorphism, and Polynomial Identity Testing. *SIAM J. Comput.* 48, 3 (2019), 926–963. doi:10.1137/18M1165682

[44] Michael J. Jacobson, Jr. and Hugh C. Williams. 2009. *Solving the Pell equation*. Springer, New York. xx+495 pages.

[45] Vishnu Jejjala, Washington Taylor, and Andrew Turner. 2022. *Identifying equivalent Calabi–Yau topologies: A discrete challenge from math and physics for machine learning*. Technical Report. MIT Center for Theoretical Physics. MIT-CTP-5406, arXiv:2202.0759.

[46] E. I. Khukhro. 1998. *p-automorphisms of finite p-groups*. London Mathematical Society Lecture Note Series, Vol. 246. Cambridge University Press, Cambridge. xviii+204 pages. doi:10.1017/CBO9780511526008

[47] Johannes Köbler, Uwe Schöning, and Jacobo Torán. 1993. *The graph isomorphism problem: its structural complexity*. Birkhauser Verlag, Basel, Switzerland, Switzerland.

[48] François Le Gall and David J. Rosenbaum. 2016. On the Group and Color Isomorphism Problems. arXiv:1609.08253.

[49] Gary L. Miller. 1978. On the $n^{\log n}$ isomorphism technique (A Preliminary Report). In *STOC* (San Diego, California, United States). ACM, New York, NY, USA, 51–58. doi:10.1145/800133.804331
[50] Vipul Naik. 2013. *Lazard correspondence up to isoclinism.* Ph. D. Dissertation. The University of Chicago. https://vipulnaik.com/thesis/
[51] A. Ranum. 1907. The group of classes of congruent matrices with application to the group of isomorphisms of any Abelian group. *Trans. Am. Math. Soc.* 8 (1907), 71–91. doi:10.2307/1986235
[52] Miles Reid. 1987. The moduli space of 3-folds with K= 0 may nevertheless be irreducible. *Math. Ann.* 278 (1987), 329–334.
[53] David J. Rosenbaum. 2013. Bidirectional collision detection and faster deterministic isomorphism testing. arXiv preprint arXiv:1304.3935 [cs.DS].
[54] Daniel Schielzeth and Michael E. Pohst. 2005. On real quadratic number fields suitable for cryptography. *Experiment. Math.* 14, 2 (2005), 189–197. http://projecteuclid.org/euclid.em/1128100131
[55] Vladimir V Sergeichuk. 1998. Unitary and Euclidean representations of a quiver. *Linear Algebra Appl.* 278, 1-3 (1998), 37–62. doi:10.1016/S0024-3795(98)00006-8
[56] Richard P Stanley. 2016. Smith normal form in combinatorics. *Journal of Combinatorial Theory, Series A* 144 (2016), 476–495.
[57] Xiaorui Sun. 2023. Faster Isomorphism for p-Groups of Class 2 and Exponent p. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, Barna Saha and Rocco A. Servedio (Eds.). ACM, 433–440. doi:10.1145/3564246.3585250
[58] NIST PQC Team. 2024. Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. (2024). https://doi.org/10.6028/NIST.IR.8528.
[59] Charles Terence Clegg Wall. 1966. Classification problems in differential topology. V: On certain 6-manifolds. *Inventiones mathematicae* 1, 4 (1966), 355–374.
[60] Shing-Tung Yau. 1978. On the Ricci curvature of a compact Kähler manifold and the complex Monge-Ampère equation, I. *Communications on pure and applied mathematics* 31, 3 (1978), 339–411.

Received 2024-11-04; accepted 2025-02-01