GENERALIZED IDEAL CLASSES IN APPLICATION TO TOROIDAL SOLENOIDS

MARIA SABITOVA

ABSTRACT. We study certain subgroups G_A of $\mathbb{Q}^n$ defined by non-singular $n\times n$-matrices A with integer coefficients. In the first non-trivial case when $n = 2$, we give necessary and sufficient conditions for two such groups to be isomorphic. Namely, in the generic case when the characteristic polynomial of A is irreducible, we attach a generalized ideal class to A and essentially, two groups are isomorphic if and only if the corresponding ideal classes are equivalent. The obtained results can be applied to studying associated toroidal solenoids.

1. INTRODUCTION

In this paper we study topological structures, such as solenoids, from an algebraic point of view. Solenoids appear in many areas of mathematics, *e.g.*, topology, homological algebra, dynamical systems and related C^*-algebras, to name a few. Toroidal solenoids were introduced by M. C. McCord in 1965 in [M65]. The problem of classifying toroidal solenoids (up to homeomorphisms) has been studied extensively based on their topological invariants and holonomy pseudogroup actions (see *e.g.*, [CHL13] and [BLP19]). However, the use of number theory in the approach described below appears to be novel.

1.1. **Subgroups of $\mathbb{Q}^n$ defined by a matrix.** For a non-singular $n \times n$-matrix A with integer coefficients, $A \in \mathrm{M}_n(\mathbb{Z})$, define

$$G_A = \left\{ A^{-k}\mathbf{x} \,\middle|\, \mathbf{x} \in \mathbb{Z}^n,\, k \in \mathbb{N} \cup \{0\} \right\}. \tag{1.1}$$

One can readily check that G_A is a subgroup of $\mathbb{Q}^n$. We are interested in the following

Problem 1. Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. Find necessary and sufficient conditions on A, B for groups G_A, G_B to be isomorphic (notationally, $G_A \cong G_B$).

1.2. **Connection with solenoids.** Problem 1 has applications to (*toroidal*) *solenoids*. Namely, let $\mathbb{T}^n$ denote a torus considered as a quotient of $\mathbb{R}^n$ by its subgroup $\mathbb{Z}^n$. A matrix $A \in \mathrm{M}_n(\mathbb{Z})$ induces a map $A : \mathbb{T}^n \longrightarrow \mathbb{T}^n$, $A([\mathbf{x}]) = [A\mathbf{x}]$, $[\mathbf{x}] \in \mathbb{T}^n$, $\mathbf{x} \in \mathbb{R}^n$. Consider the inverse system $(M_j, f_j)_{j\in\mathbb{N}}$, where $f_j : M_{j+1} \longrightarrow M_j$, $M_j = \mathbb{T}^n$ and $f_j = A$ for all $j \in \mathbb{N}$. The inverse limit $\mathcal{S}_A$ of the system is called a (*toroidal*) *solenoid*. As a set, $\mathcal{S}_A$ is a subset

Date: August 18, 2021.

of $\prod_{j=1}^{\infty} M_j$ consisting of points $(z_j) \in \prod_{j=1}^{\infty} M_j$ such that $z_j \in M_j$ and $f_j(z_{j+1}) = z_j$ for $\forall j \in \mathbb{N}$, *i.e.*,

$$\mathcal{S}_A = \left\{ (z_j) \in \prod_{j=1}^{\infty} \mathbb{T}^n \;\middle|\; z_j \in \mathbb{T}^n,\ A(z_{j+1}) = z_j,\ j \in \mathbb{N} \right\}.$$

Endowed with the natural group structure and the induced topology from the Tychonoff (product) topology on $\prod_{j=1}^{\infty} \mathbb{T}^n$, $\mathcal{S}_A$ is an n-dimensional topological abelian group. It is compact, metrizable, and connected, but not locally connected and not path connected. Toroidal solenoids are examples of topological inverse limits of dynamical systems. When $n = 1$ and $A = d$, $d \in \mathbb{Z}$, solenoids are called *d-adic solenoids* or *Vietoris solenoids*. The first examples were studied by L. Vietoris in 1927 for $d = 2$ [V27] and later in 1930 by van Dantzig for an arbitrary d [D30].

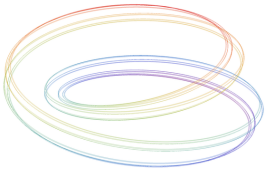

FIGURE 1. Toroidal solenoid for $n = 1$, $A = 2$.[1]

Problem 2. Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. Find necessary and sufficient conditions on A, B for $\mathcal{S}_A$, $\mathcal{S}_B$ to be isomorphic (as topological groups).

It is known that $\mathcal{S}_A \cong \mathcal{S}_B$ as topological groups if and only if $G_{A^t} \cong G_{B^t}$ as (abstract) groups, where A^t denotes the transpose of A (*cf.*, [M65]). Indeed, since $\mathcal{S}_A$ is a compact connected abelian group, the first Čech cohomology group $H^1(\mathcal{S}_A, \mathbb{Z})$ is isomorphic to the character group $\widehat{\mathcal{S}_A}$ of $\mathcal{S}_A$. On the other hand, one can check that $H^1(\mathcal{S}_A, \mathbb{Z}) \cong G_{A^t}$. Using Pontryagin duality theorem, we see that indeed $\mathcal{S}_A \cong \mathcal{S}_B$ if and only if $G_{A^t} \cong G_{B^t}$. Therefore, Problem 1 is equivalent to Problem 2.

If $n = 1$, we have $A, B \in \mathbb{Z}$ and $G_A \cong G_B$ if and only if A, B have the same prime divisors. Hence, for $n = 1$, Problem 1 and therefore Problem 2 have simple solutions.

In this paper we solve Problem 1 for $n = 2$. Note that if A, B are conjugate by a matrix in $\mathrm{GL}_n(\mathbb{Z})$, then clearly $G_A \cong G_B$. However, the converse is not true. Namely, there are many examples of non-conjugate matrices A, B with isomorphic groups G_A, G_B. For instance, see Example 2 below, where $G_A \cong G_B$, but A, B do not even share the same characteristic polynomial. In general, there is no direct connection between the conjugacy classes of A in $\mathrm{GL}_n(\mathbb{Q})$ and isomorphisms of groups G_A, *i.e.*, conjugate (resp., non-conjugate) A, B can equally produce isomorphic and non-isomorphic groups G_A, G_B (see Examples 3, 4, 5 below). To solve the problem, in the generic case, *i.e.*, when

[1]Picture source: https://en.wikipedia.org/wiki/Solenoid_(mathematics)

the characteristic polynomial of A is irreducible, we link G_A to a generalized ideal class generated by an eigenvector of A in the splitting field of the characteristic polynomial of A. We show that if $G_A \cong G_B$, then the characteristic polynomials of A, B share the same splitting field and, essentially, G_A and G_B are isomorphic if and only if the corresponding ideal classes are multiples of each other.

Acknowledgements. The author thanks Mario Bonk for suggesting the problem and useful discussions. The author also thanks an anonymous evaluator for suggesting valuable improvements to the paper.

2. Ideal classes

In this section we review the notion of ideal classes in number fields and their application to matrices with integer coefficients. We also introduce the notion of a generalized ideal class, which we use to analyze the structure of groups G_A defined by (1.1) when $n = 2$.

Let K be a number field of degree n, which is a field extension of degree n of the field $\mathbb{Q}$ of rational numbers. An order of K is a subring $\mathcal{O}$ of K that is also a finitely-generated $\mathbb{Z}$-module of rank n. A fractional $\mathcal{O}$-ideal of an order $\mathcal{O}$ is a non-zero finitely-generated $\mathcal{O}$-submodule I of K such that $xI \subseteq \mathcal{O}$ for some non-zero $x \in \mathcal{O}$. One defines an equivalence relation on fractional $\mathcal{O}$-ideals I, I' via $I \sim I'$ if and only if $I = xI'$ for some non-zero $x \in K$. The corresponding equivalence class of I is denoted by $[I]$ and called an $\mathcal{O}$-ideal class (see *e.g.*, [N99, p. 72, §12] or [C]).

Let A be an $n \times n$-matrix with integer coefficients (denoted by $A \in \mathrm{M}_n(\mathbb{Z})$). One can attach an ideal class to A. Namely, let $\overline{\mathbb{Q}}$ denote a fixed algebraic closure of $\mathbb{Q}$, let $\lambda \in \overline{\mathbb{Q}}$ be an eigenvalue of A, and let $K = \mathbb{Q}(\lambda)$. Then $\mathcal{O} = \mathbb{Z}[\lambda]$ is an order of K. Let $\mathbf{u} = \begin{pmatrix} u_1 & u_2 & \cdots & u_n \end{pmatrix}^t \in K^n$ be an eigenvector of A corresponding to λ. Denote

$$I_{\mathbb{Z}}(A, \lambda) = \{m_1 u_1 + m_2 u_2 + \cdots + m_n u_n \,|\, m_1, m_2, \ldots, m_n \in \mathbb{Z}\} \subset K. \tag{2.1}$$

Since A has integer coefficients, $I_{\mathbb{Z}}(A, \lambda)$ is a $\mathbb{Z}[\lambda]$-module, finitely-generated, and we have a $\mathbb{Z}[\lambda]$-ideal class $[I_{\mathbb{Z}}(A, \lambda)]$ attached to A. If the characteristic polynomial of A is irreducible over $\mathbb{Q}$, then each eigenspace of A is one-dimensional and the class $[I_{\mathbb{Z}}(A, \lambda)]$ does not depend on the choice of $\mathbf{u}$. These ideal classes are useful in determining when two matrices $A, B \in \mathrm{M}_n(\mathbb{Z})$ are conjugate by a non-singular matrix $S \in \mathrm{M}_n(\mathbb{Z})$ whose inverse S^{-1} also has integer coefficients (denoted by $S \in \mathrm{GL}_n(\mathbb{Z})$), equivalently, when A, B belong to the same $\mathrm{GL}_n(\mathbb{Z})$-conjugacy class. Note that a necessary condition for A, B to be conjugate by a matrix is that they share the same characteristic polynomial. The following is a well-known classical result from 1949.

Theorem 2.1 (Latimer–MacDuffee–Taussky Theorem, [T49])**.** *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ share the same characteristic polynomial $\chi \in \mathbb{Z}[t]$. Assume that χ is irreducible over $\mathbb{Q}$. Let $\lambda \in \overline{\mathbb{Q}}$ be a root of χ. Then there exists $S \in \mathrm{GL}_n(\mathbb{Z})$ such that*

$$A = SBS^{-1}$$

if and only if $[I_{\mathbb{Z}}(A,\lambda)] = [I_{\mathbb{Z}}(B,\lambda)]$.

Theorem 2.1 has come up in connection with tori as in [ATW97]. There, the authors study topological invariants of classes of topologically conjugate linear endomorphisms of a 2-dimensional torus $\mathbb{T}^2$. It is known that two linear endomorphisms f, g of $\mathbb{T}^2$ are topologically conjugate if and only if the corresponding matrices $M_f, M_g \in \mathrm{M}_2(\mathbb{Z})$ are conjugate by an element in $\mathrm{GL}_2(\mathbb{Z})$. Hence, one of the invariants considered by the authors is an ideal class attached to M_f.

We now consider the problem of classifying groups G_A defined in the introduction. Clearly, if non-singular A, B are conjugate by a matrix $S \in \mathrm{GL}_n(\mathbb{Z})$, then $G_A \cong G_B$ with the isomorphism defined by S. However, the converse is not true. In general, the class $\mathcal{C}(A)$ of non-singular matrices $B \in \mathrm{M}_n(\mathbb{Z})$ with $G_A \cong G_B$ is much larger than the $\mathrm{GL}_n(\mathbb{Z})$-conjugacy class of A. For instance, in Example 4 below we have

$$A = \begin{pmatrix} 0 & -6 \\ 1 & 1 \end{pmatrix},$$

and all the three $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of matrices in $\mathrm{M}_2(\mathbb{Z})$ with characteristic polynomial $h = x^2 - x + 6$ belong to $\mathcal{C}(A)$. Moreover, one can have $G_A \cong G_B$, even though A, B do not even share the same characteristic polynomial (see Example 2 below, where $G_A \cong G_B$, A has eigenvalues $4, 6$, and B has eigenvalues $2, 18$). In particular, this is different from [ATW97], if only because, on the matrix level, we are not restricted to $\mathrm{GL}_n(\mathbb{Z})$-conjugacy classes.

In light of the above, it is rather surprising that there are similarities between our solution to Problem 1 for $n = 2$ and Theorem 2.1. Namely, we introduce the notion of a generalized ideal class. More precisely, let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular with characteristic polynomial $h_A \in \mathbb{Z}[t]$. Let $\lambda \in \overline{\mathbb{Q}}$ be a root of h_A, $K = \mathbb{Q}(\lambda)$, $N = \det A$, and let

$$\mathcal{R} = \mathbb{Z}\left[\frac{1}{N}\right] = \left\{ \frac{x}{N^k} \;\middle|\; x, k \in \mathbb{Z} \right\} \subset \mathbb{Q}$$

denote the ring of N-adic integers. We define an equivalence relation on non-zero finitely-generated $\mathbb{Z}[\lambda]$-modules $I, I' \subset K$ via $I \sim_{\mathcal{R}} I'$ if and only if

$$I \otimes_{\mathbb{Z}} \mathcal{R} = x(I' \otimes_{\mathbb{Z}} \mathcal{R}), \quad x \in K,\ x \neq 0.$$

We call the corresponding equivalence classes $\mathcal{R}[\lambda]$-ideal classes. Note that $\mathcal{R}[\lambda]$ is not an order, since it is not a finitely generated $\mathbb{Z}$-module unless $N = \pm 1$. Therefore, we call classes $[I \otimes_{\mathbb{Z}} \mathcal{R}]$ generalized ideal classes. Denote

$$I_{\mathcal{R}}(A,\lambda) \;=\; I_{\mathbb{Z}}(A,\lambda) \otimes_{\mathbb{Z}} \mathcal{R},$$

where $I_{\mathbb{Z}}(A,\lambda)$ is defined by (2.1), and let $[I_{\mathcal{R}}(A,\lambda)]$ denote the corresponding $\mathcal{R}[\lambda]$-ideal class. Our main result is the following theorem:

Theorem 2.2. *Let $n = 2$. Suppose the characteristic polynomial of a non-singular $A \in \mathrm{M}_2(\mathbb{Z})$ is irreducible and there is a prime $p \in \mathbb{Z}$ that divides* $\det A$ *and does not divide*

$\operatorname{Tr} A$. *Then* $G_A \cong G_B$ *for a non-singular* $B \in \mathrm{M}_2(\mathbb{Z})$ *if and only if there exist eigenvalues* $\lambda, \mu \in \overline{\mathbb{Q}}$ *of* A, B, *respectively, such that*

(1) $\mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$ *and* λ, μ *have the same prime divisors in the ring of integers of* $K = \mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$;
(2) $[I_{\mathcal{R}}(A, \lambda)] = [I_{\mathcal{R}}(B, \mu)]$.

In the subsequent sections we develop techniques to prove Theorem 2.2. In particular, we employ the localization method (Section 3.2), which consists in studying $\mathbb{Z}_p$-modules $G_A \otimes_{\mathbb{Z}} \mathbb{Z}_p$, where $p \in \mathbb{Z}$ is a prime and $\mathbb{Z}_p$ denotes the ring of p-adic integers. We also consider special cases (Sections 3.1, 3.3, and 5), *e.g.*, when the characteristic polynomial of A is not irreducible. We prove Theorem 2.2 in Section 6 (Theorem 6.6).

To the best of our knowledge, the idea of generalized ideal classes and their application to studying groups G_A and the associated toroidal solenoids is new. We do not know whether Theorem 2.2 holds in higher dimensions $n > 2$. This is a direction for future investigation.

3. Arbitrary n: general results

Given a ring R we denote by $\mathrm{M}_n(R)$ the ring of $n \times n$-matrices with coefficients in R and we denote by $\mathrm{GL}_n(R) \subset \mathrm{M}_n(R)$ the subring of invertible matrices $A \in \mathrm{M}_n(R)$ such that $A^{-1} \in \mathrm{M}_n(R)$. For a non-singular $A \in \mathrm{M}_n(\mathbb{Z})$ we denote

$$G_A = \left\{ A^{-k}\mathbf{x} \,|\, \mathbf{x} \in \mathbb{Z}^n,\, k \in \mathbb{N} \cup \{0\} \right\}, \tag{3.1}$$

a subgroup of $\mathbb{Q}^n$ (with respect to addition) that contains $\mathbb{Z}^n$. In this section we prove results that hold for groups G_A for an arbitrary n. The following lemma shows that given a non-singular $B \in \mathrm{M}_n(\mathbb{Z})$, any homomorphism between groups G_A and G_B is the restriction of a linear map $T \in \mathrm{M}_n(\mathbb{Q})$.

Lemma 3.1. *For two non-singular* $A, B \in \mathrm{M}_n(\mathbb{Z})$ *we have* $G_A \cong G_B$ *if and only if there exists* $T \in \mathrm{GL}_n(\mathbb{Q})$ *that restricts to an isomorphism between* G_A *and* G_B. *Furthermore,* $T : G_A \longrightarrow G_B$ *is an isomorphism if and only if* $T \in \mathrm{GL}_n(\mathbb{Q})$, *for any* $m \in \mathbb{N} \cup \{0\}$ *there exists* $k_m \in \mathbb{N} \cup \{0\}$ *with*

$$B^{k_m} T A^{-m} \in \mathrm{M}_n(\mathbb{Z}), \tag{3.2}$$

and for any $l \in \mathbb{N} \cup \{0\}$ *there exists* $t_l \in \mathbb{N} \cup \{0\}$ *with*

$$A^{t_l} T^{-1} B^{-l} \in \mathrm{M}_n(\mathbb{Z}). \tag{3.3}$$

Proof. Let $\phi : G_A \longrightarrow G_B$ be a homomorphism and and let $\mathbf{e}_i \in \mathbb{Z}^n$ be the i-th standard basis vector, $i \in \{1, \ldots, n\}$. For any $k \in \mathbb{N} \cup \{0\}$ let

$$\phi(A^{-k}\mathbf{e}_i) \;=\; \mathbf{x}_i^{(k)}, \quad \mathbf{x}_i^{(k)} \in \mathbb{Q}^n,$$

so that for $T_k = \begin{pmatrix} \mathbf{x}_1^{(k)} & \cdots & \mathbf{x}_n^{(k)} \end{pmatrix} \in \mathrm{M}_n(\mathbb{Q})$ and any $\mathbf{x} \in \mathbb{Z}^n$ we have

$$\phi(A^{-k}\mathbf{x}) = T_k \mathbf{x}.$$

Since A has integer entries,

$$T_k\mathbf{x} = \phi(A^{-k}\mathbf{x}) = \phi(A^{-(k+1)}A\mathbf{x}) = T_{k+1}A\mathbf{x}$$

and hence

$$T_k = T_{k+1}A.$$

By induction,

$$T_k = T_0A^{-k},$$

so that for any $\mathbf{u} = A^{-k}\mathbf{x} \in G_A$ with $\mathbf{x} \in \mathbb{Z}^n$, we have

$$\phi(\mathbf{u}) = \phi(A^{-k}\mathbf{x}) = T_k\mathbf{x} = T_0A^{-k}\mathbf{x} = T_0\mathbf{u}.$$

Thus, ϕ is defined via matrix $T = T_0$. Equations (3.2), (3.3) now follow easily. □

In what follows we assume that $A, B \in \mathrm{M}_n(\mathbb{Z})$ are non-singular and if $T : G_A \longrightarrow G_B$ is a homomorphism, then $T \in \mathrm{M}_n(\mathbb{Q})$.

3.1. Note that $\det A \in \mathbb{Z}$. We first consider the case when $A \in \mathrm{GL}_n(\mathbb{Z})$, *i.e.*, $\det A = \pm 1$.

Lemma 3.2. (*i*) *Assume $A \in \mathrm{GL}_n(\mathbb{Z})$. Then $G_A \cong G_B$ if and only if $B \in \mathrm{GL}_n(\mathbb{Z})$ if and only if $G_A = G_B = \mathbb{Z}^n$.*

(*ii*) *Let $G_A \cong G_B$ and $A \notin \mathrm{GL}_n(\mathbb{Z})$, i.e., $\det A \neq \pm 1$. Then $\det B \neq \pm 1$ and $\det A$, $\det B$ have the same prime divisors (in $\mathbb{Z}$).*

Proof. Suppose $T : G_A \longrightarrow G_B$ is an isomorphism. It follows from (3.2) and (3.3) that

$$(\det B)^{k_m} \cdot \det T = \alpha_m \cdot (\det A)^m, \tag{3.4}$$

$$(\det A)^{t_l} = \beta_l \cdot \det T \cdot (\det B)^l \tag{3.5}$$

for any $m, l \in \mathbb{N}$ and some $\alpha_m, \beta_l \in \mathbb{Z}$. Since $\det T$ is a fixed non-zero rational number, and $|(\det A)^m|, |(\det B)^l|$ are arbitrarily big (unless $\det A = \pm 1$, $\det B = \pm 1$), statements (*i*) and (*ii*) follow from (3.4), (3.5). □

Since Lemma 3.2(*i*) covers the case $A \in \mathrm{GL}_n(\mathbb{Z})$ completely, in what follows we assume $A, B \notin \mathrm{GL}_n(\mathbb{Z})$.

Let $\mathcal{S} = \mathcal{S}(A) \subset \mathbb{Z}$ denote the set of all primes in $\mathbb{Z}$ dividing $\det A$. Since we assume $A \notin \mathrm{GL}_n(\mathbb{Z})$, we have $\mathcal{S} \neq \emptyset$. Let

$$\mathcal{A} = \{m \in \mathbb{Z} - \{0\} \mid m = \pm 1 \text{ or all prime divisors of } m \text{ belong to } \mathcal{S}\}.$$

Note that by Lemma 3.2, if $G_A \cong G_B$, then $\mathcal{S} = \mathcal{S}(A) = \mathcal{S}(B)$ is the same for A and B. Denote

$$\mathcal{R} = \left\{ \frac{x}{y} \;\middle|\; x, y \in \mathbb{Z},\, y \in \mathcal{A} \right\}, \tag{3.6}$$

which is a subring of $\mathbb{Q}$. Then $\mathcal{R}^\times = \{r \in \mathcal{R} - \{0\} \,|\, r^{-1} \in \mathcal{R}\}$ is the set of all $\mathcal{S}$-units. Note that $\mathcal{A}$ is a multiplicatively closed subset of $\mathbb{Z}$, so that $\mathcal{R} = \mathcal{A}^{-1}\mathbb{Z}$, the localization of $\mathbb{Z}$ with respect to $\mathcal{A}$. Equivalently, for $N = \det A$ we have

$$\mathcal{R} = \mathbb{Z}\left[\frac{1}{N}\right] = \left\{ \frac{x}{N^k} \;\middle|\; x, k \in \mathbb{Z} \right\}, \tag{3.7}$$

the ring of N-adic rationals.

Remark 3.3. Note that G_A is a (additive) subgroup of $\mathcal{R}^n$, since $A^{-k} = \frac{1}{(\det A)^k}\tilde{A}$ with $\tilde{A} \in \mathrm{M}_n(\mathbb{Z})$. However, $G_A \neq \mathcal{R}^n$ in general.

The next lemma shows that if $T \in \mathrm{GL}_n(\mathbb{Q})$ defines an isomorphism between G_A and G_B, then entries of T and T^{-1} are rational numbers with denominators divisible only by primes that divide $\det A$.

Lemma 3.4. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let $T : G_A \longrightarrow G_B$ be an isomorphism, $T \in \mathrm{GL}_n(\mathbb{Q})$. Then $T \in \mathrm{GL}_n(\mathcal{R})$.*

Proof. Let $T = \frac{1}{l}T'$, $l \in \mathbb{Z} - \{0\}$ and $T' \in \mathrm{M}_n(\mathbb{Z})$ such that $(T', l) = 1$, *i.e.*, the greatest common divisor of l and all the entries of T' is 1. If $l = \pm 1$, then $T \in \mathrm{M}_n(\mathbb{Z})$ and hence $T \in \mathrm{M}_n(\mathcal{R})$. Let $l \neq 1$ and let $p \in \mathbb{Z}$ be a prime dividing l and $p \notin \mathcal{S}$ (*i.e.*, p does not divide $\det A$, $\det B$). By Lemma 3.1, from (3.2) for any $m \in \mathbb{N}$ we have

$$B^{k_m}T' = lP_mA^m, \;\; P_m \in \mathrm{M}_n(\mathbb{Z}), \;\; k_m \in \mathbb{N} \cup \{0\}.$$

Since p does not divide $\det B$, we have $B \,(\mathrm{mod}\, p) \in \mathrm{GL}_n(\mathbb{F}_p)$ and hence $T' \equiv 0 \,(\mathrm{mod}\, p)$, which contradicts $(T', l) = 1$. Thus, $T \in \mathrm{M}_n(\mathcal{R})$. Similarly, using (3.3), $T^{-1} \in \mathrm{M}_n(\mathcal{R})$. □

For a prime $p \in \mathbb{Z}$ denote

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; m, n \in \mathbb{Z}, \;\; (p, n) = 1 \right\},$$

a subring of $\mathbb{Q}$. The following lemma shows that to check conditions (3.2) and (3.3) of Lemma 3.1 over $\mathbb{Z}$, it is enough to check them over $\mathbb{Z}_{(p)}$ for finitely many primes $p \in \mathcal{S}$, namely, for all primes p dividing $\det A$.

Lemma 3.5. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular, $A \notin \mathrm{GL}_n(\mathbb{Z})$, and $T \in \mathrm{GL}_n(\mathbb{Q})$. Then T defines an isomorphism $T : G_A \longrightarrow G_B$ if and only if $\det A$, $\det B$ have the same prime divisors in $\mathbb{Z}$, $T \in \mathrm{GL}_n(\mathcal{R})$ and for any $m \in \mathbb{N} \cup \{0\}$ and any $p \in \mathcal{S}$ there exists $k_m = k_m(p) \in \mathbb{N} \cup \{0\}$ with*

$$B^{k_m}TA^{-m} \in \mathrm{M}_n\left(\mathbb{Z}_{(p)}\right), \tag{3.8}$$

and for any $l \in \mathbb{N} \cup \{0\}$ and any $p \in \mathcal{S}$ there exists $t_l = t_l(p) \in \mathbb{N} \cup \{0\}$ with

$$A^{t_l}T^{-1}B^{-l} \in \mathrm{M}_n\left(\mathbb{Z}_{(p)}\right). \tag{3.9}$$

Proof. The necessary part follows from Lemma 3.1, Lemma 3.2, and Lemma 3.4. We now prove the sufficient part. Since $T \in \mathrm{GL}_n(\mathcal{R})$ and $\det A$, $\det B$ have the same prime divisors, all the entries of matrices $B^{k_m}TA^{-m}$, $A^{t_l}T^{-1}B^{-l}$ in (3.8), (3.9) have only primes in $\mathcal{S}$ in their denominators, *i.e.*, $B^{k_m}TA^{-m}, A^{t_l}T^{-1}B^{-l} \in \mathrm{M}_n(\mathcal{R})$. For any $m, l \in \mathbb{N} \cup \{0\}$ let

$$\tilde{k}_m = \max_{p\in\mathcal{S}}\{k_m(p)\}, \quad \tilde{t}_l = \max_{p\in\mathcal{S}}\{t_l(p)\}.$$

Using (3.8), $B^{\tilde{k}_m}TA^{-m} \in \mathrm{M}_n(\mathcal{R}) \cap \mathrm{M}_n\left(\mathbb{Z}_{(p)}\right)$ for any $p \in \mathcal{S}$. Hence, $B^{\tilde{k}_m}TA^{-m} \in \mathrm{M}_n(\mathbb{Z})$ and analogously, $A^{\tilde{t}_l}T^{-1}B^{-l} \in \mathrm{M}_n(\mathbb{Z})$. Thus, (3.2) and (3.3) hold, and T is an isomorphism by Lemma 3.1. □

3.2. **Localization.** In our study of groups G_A, it is helpful to consider tensor products $G_A \otimes_{\mathbb{Z}} \mathbb{Z}_p$, where $p \in \mathbb{Z}$ is a prime and $\mathbb{Z}_p$ denotes the ring of p-adic integers. The transition from G_A to $G_A \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is commonly referred to as localization.

Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let $\overline{G}_{A,p}$ be the (topological) closure of G_A in $\mathbb{Q}_p^n = \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p$ with the product topology of the standard p-adic topology on the field $\mathbb{Q}_p$ of p-adic numbers. Since $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, we have

$$\overline{G}_{A,p} = G_A \otimes_{\mathbb{Z}} \mathbb{Z}_p = \left\{A^k\mathbf{x} \,|\, \mathbf{x} \in \mathbb{Z}_p^n,\, k \in \mathbb{Z}\right\}, \tag{3.10}$$

a subgroup of $\mathbb{Q}_p^n$ that contains $\mathbb{Z}_p^n$ and has the natural structure of a $\mathbb{Z}_p$-module. The next lemma shows that we can check conditions (3.8), (3.9) in Lemma 3.5 over $\mathbb{Z}_p$ via the natural embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

Lemma 3.6. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular, $A \notin \mathrm{GL}_n(\mathbb{Z})$, and $T \in \mathrm{GL}_n(\mathbb{Q})$. Then T defines an isomorphism $T : G_A \longrightarrow G_B$ if and only if $\det A$, $\det B$ have the same prime divisors, $T \in \mathrm{GL}_n(\mathcal{R})$, and for any $p \in \mathcal{S}$, T considered as an element of $\mathrm{GL}_n(\mathbb{Q}_p)$ via the natural embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ induces a $\mathbb{Z}_p$-module isomorphism $T : \overline{G}_{A,p} \longrightarrow \overline{G}_{B,p}$.*

Proof. Let $p \in \mathbb{Z}$ be a prime. It follows from (3.10) that $T \in \mathrm{GL}_n(\mathbb{Q}_p)$ defines a $\mathbb{Z}_p$-module isomorphism from $\overline{G}_{A,p}$ to $\overline{G}_{B,p}$ if and only if conditions (3.2), (3.3) in Lemma 3.1 hold over $\mathbb{Z}_p$, *i.e.*, for any $m \in \mathbb{N} \cup \{0\}$ there exists $k_m \in \mathbb{N} \cup \{0\}$ with

$$B^{k_m}TA^{-m} \in \mathrm{M}_n(\mathbb{Z}_p),$$

and for any $l \in \mathbb{N} \cup \{0\}$ there exists $t_l \in \mathbb{N} \cup \{0\}$ with

$$A^{t_l}T^{-1}B^{-l} \in \mathrm{M}_n(\mathbb{Z}_p).$$

Therefore, the lemma follows from Lemma 3.5, since $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$ under the natural embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ and $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$. □

Remark 3.7. Note that for $T \in \mathrm{GL}_n(\mathbb{Q})$ we have $T \in \mathrm{GL}_n(\mathcal{R})$ if and only if $T \in \mathrm{GL}_n(\mathbb{Z}_p)$ for any $p \notin \mathcal{S}$.

It turns out that the structure of $\overline{G}_{A,p}$ as a $\mathbb{Z}_p$-module is relatively easy to determine.

Proposition 3.8. *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular, let $h_A \in \mathbb{Z}[t]$ be the characteristic polynomial of A, and let $p \in \mathbb{Z}$ be prime. Let l denote the multiplicity of zero in $\bar{h}_A \in \mathbb{F}_p[t]$, the reduction of h_A modulo p, $0 \leq l \leq n$. Then*

$$\overline{G}_{A,p} \cong \mathbb{Q}_p^l \oplus \mathbb{Z}_p^{n-l}.$$

In particular,

- *if p does not divide* $\det A$*, then $\overline{G}_{A,p} = \mathbb{Z}_p^n$,*
- *if $h_A \equiv t^n \,(mod\ p)$, then $\overline{G}_{A,p} = \mathbb{Q}_p^n$.*

Proof. In the proof, it is enough to assume that A has entries in $\mathbb{Z}_p$, *i.e.*, $A \in \mathrm{M}_n(\mathbb{Z}_p)$ is non-singular, $h_A \in \mathbb{Z}_p[t]$ is the characteristic polynomial of A, and

$$\overline{G}_{A,p} = G_A = \left\{ A^k \mathbf{x} \,|\, \mathbf{x} \in \mathbb{Z}_p^n,\, k \in \mathbb{Z} \right\} \subset \mathbb{Q}_p^n.$$

Clearly, if p does not divide $\det A$, then $\det A$ is a unit in $\mathbb{Z}_p$. Hence, $A^{-k} \in \mathrm{M}_n(\mathbb{Z}_p)$ for all k and $G_A \subseteq \mathbb{Z}_p^n$. Since $\mathbb{Z}_p^n \subseteq G_A$, we have $G_A = \mathbb{Z}_p^n$.

If $h_A \equiv t^n \,(\mathrm{mod}\ p)$, then it follows from Cayley–Hamilton theorem that $A^n = pC$, where $C \in \mathrm{M}_n(\mathbb{Z}_p)$ is non-singular. Then for the i-th standard basis vector $\mathbf{e}_i \in \mathbb{Q}_p^n$ and any $k \in \mathbb{N}$ we have $C^k \mathbf{e}_i \in \mathbb{Z}_p^n$ and hence $A^{-nk}(C^k \mathbf{e}_i) = p^{-k}\mathbf{e}_i \in G_A$, $i = \{1, 2, \ldots, n\}$. Since G_A is a $\mathbb{Z}_p$-module, we have $G_A = \mathbb{Q}_p^n$.

In particular, Proposition 3.8 holds for $n = 1$ and we will prove the general case by induction on n.

Let $\overline{\mathbb{Q}}_p$ denote an algebraic closure of $\mathbb{Q}_p$. Note that for an irreducible polynomial $\chi \in \mathbb{Z}_p[t]$, either p does not divide $\chi(0)$ or $\chi \equiv t^n \,(\mathrm{mod}\ p)$. Indeed, let n be the degree of χ, let $\lambda_1, \ldots, \lambda_n \in \overline{\mathbb{Q}}_p$ be roots of χ, and let $K = \mathbb{Q}_p(\lambda_1, \ldots, \lambda_n) \subset \overline{\mathbb{Q}}_p$ be the splitting field of χ. Let $\mathfrak{p}$ be the maximal ideal of the ring of integers $\mathcal{O}$ of K. If p divides $\chi(0)$, then $\mathfrak{p}$ divides some λ_i in $\mathcal{O}$. Since χ is irreducible, $\mathrm{Gal}(K/\mathbb{Q}_p)$ acts transitively on the set $\{\lambda_1, \ldots, \lambda_n\}$ and therefore $\mathfrak{p}$ divides all $\lambda_1, \ldots, \lambda_n$ and $\chi \equiv t^n \,(\mathrm{mod}\ p)$.

For the rest of the proof we assume that p divides $\det A$ and $h_A \not\equiv t^n \,(\mathrm{mod}\ p)$. Then by above, h_A is reducible, *i.e.*, $h_A = h_1 h_2$ for non-constant monic $h_i \in \mathbb{Z}_p[t]$ of degree n_i, $1 \leq n_i < n$, $i = 1, 2$. Without loss of generality we can assume that h_1 is irreducible and p divides $h_1(0)$. Then by above, $h_1 \equiv t^{n_1} \,(\mathrm{mod}\ p)$. There exists $M \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that

$$M^{-1} A M = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}, \quad A_i \in \mathrm{M}_{n_i}(\mathbb{Z}_p) \text{ non-singular},$$

and h_i is the characteristic polynomial of A_i, $i = 1, 2$ (see Appendix A, Theorem A.1 below). By induction, $G_{A_1} = \mathbb{Q}_p^{n_1}$ and $G_{A_2} \cong \mathbb{Q}_p^{l_2} \oplus \mathbb{Z}_p^{n_2 - l_2}$, where l_2 denotes the multiplicity of zero in the reduction of h_2 modulo p. Note that $l = l_2 + n_1$, $n_1 + n_2 = n$, and G_A is an

extension of G_{A_2} by G_{A_1} via

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Q}_p^{n_1} & \xrightarrow{\phi} & \mathbb{Q}_p^{n} & \longrightarrow & \mathbb{Q}_p^{n_2} & \longrightarrow & 0, \\ & & \| & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & G_{A_1} & \longrightarrow & G_A & \longrightarrow & G_{A_2} & \longrightarrow & 0 \end{array} \quad \phi(\mathbf{u}) = \begin{pmatrix} \mathbf{u} & 0 \end{pmatrix}^t, \ \mathbf{u} \in \mathbb{Q}_p^{n_1}.$$

Since $\mathbb{Q}_p^{n_1}$ is an injective $\mathbb{Z}_p$-module, the exact sequence with G_A splits, $G_A \cong G_{A_1} \oplus G_{A_2}$ as $\mathbb{Z}_p$-modules, and hence $G_A \cong \mathbb{Q}_p^l \oplus \mathbb{Z}_p^{n-l}$ as claimed. □

Corollary 3.9. *If $n = 2$ and $G_A \cong G_B$, then a prime $p \in \mathbb{Z}$ divides both $\det A$ and $\operatorname{Tr} A$ if and only if p divides both $\det B$ and $\operatorname{Tr} B$.*

Proof. If $G_A \cong G_B$, then $\overline{G}_{A,p} \cong \overline{G}_{B,p}$ as $\mathbb{Z}_p$-modules for each prime $p \in \mathbb{Z}$. If $n = 2$, by Proposition 3.8, we have

(1) $\overline{G}_{A,p} \cong \mathbb{Z}_p^2$, if p does not divide $\det A$,
(2) $\overline{G}_{A,p} \cong \mathbb{Q}_p^2$ if p divides both $\det A$, $\operatorname{Tr} A$,
(3) $\overline{G}_{A,p} \cong \mathbb{Z}_p \oplus \mathbb{Q}_p$, if p divides $\det A$, p does not divide $\operatorname{Tr} A$.

Since $\mathbb{Z}_p$-modules in cases (1), (2), and (3) are not isomorphic, the claim follows. □

Clearly, if $G_A \cong G_B$, then $\overline{G}_{A,p} \cong \overline{G}_{B,p}$ as $\mathbb{Z}_p$-modules for each prime $p \in \mathbb{Z}$. If $n = 1$, one can show that $G_A \cong G_B$ if and only if $\overline{G}_{A,p} \cong \overline{G}_{B,p}$ as $\mathbb{Z}_p$-modules for any prime $p \in \mathbb{Z}$ if and only if $A, B \in \mathbb{Z}$ have the same prime divisors. However, if $n > 1$, the condition $\overline{G}_{A,p} \cong \overline{G}_{B,p}$ as $\mathbb{Z}_p$-modules for any prime $p \in \mathbb{Z}$ is not sufficient for G_A, G_B to be isomorphic. The following is an example in the case $n = 2$.

Example 1. Let

$$A = \begin{pmatrix} -1 & 3 \\ 3 & 2 \end{pmatrix}, \ B = \begin{pmatrix} 0 & 1 \\ 11 & 1 \end{pmatrix}.$$

Since A and B share the same characteristic polynomial, $\overline{G}_{A,p} \cong \overline{G}_{B,p}$ as $\mathbb{Z}_p$-modules for any prime $p \in \mathbb{Z}$ by Proposition 3.8. However, G_A and G_B are not isomorphic. Indeed, $\det A = \det B = -11$, $\operatorname{Tr} A = \operatorname{Tr} B = 1$. For each prime $p \neq 11$, we have $A, B \in \mathrm{GL}_2(\mathbb{Z}_p)$ and therefore

$$\overline{G}_{A,p} = \overline{G}_{B,p} = \mathbb{Z}_p \oplus \mathbb{Z}_p, \quad p \neq 11.$$

For $p = 11$, as in the proof of Corollary 3.9, we have

$$\overline{G}_{A,11} \cong \overline{G}_{B,11} \cong \mathbb{Z}_{11} \oplus \mathbb{Q}_{11}. \tag{3.11}$$

Bases of the decompositions (3.11) consist of eigenvectors of A, B considered as elements of $(\mathbb{Q}_{11})^2$. Indeed,

$$\lambda_1 = \frac{1 + 3\sqrt{5}}{2}, \quad \lambda_2 = \frac{1 - 3\sqrt{5}}{2}$$

are common eigenvalues of A and B. By Hensel's lemma, the equation $x^2 = 5$ has a solution in $\mathbb{Z}_{11}$, since $4^2 \equiv 5 \pmod{11}$. Thus, we can choose $\sqrt{5} = 4 + 11\alpha$ for some

$\alpha \in \mathbb{Z}_{11}$, which can be calculated explicitly. Hence, $\lambda_1, \lambda_2 \in \mathbb{Z}_{11}$, $\lambda_1 \in \mathbb{Z}_{11}^\times$ is a unit, and λ_2 is divisible by 11 in $\mathbb{Z}_{11}$. In particular, $\frac{\lambda_2}{11} \in \mathbb{Z}_{11}$. If

$$M = \begin{pmatrix} 2-\lambda_1 & 2-\lambda_2 \\ -3 & -3 \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 \end{pmatrix}, \quad N = \begin{pmatrix} -\frac{\lambda_2}{11} & -\lambda_1 \\ 1 & 11 \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{pmatrix},$$

then

$$M^{-1}AM = NBN^{-1} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Note that $\det M = 9\sqrt{5} \in \mathbb{Z}_{11}^\times$, $\det N = 3\sqrt{5} \in \mathbb{Z}_{11}^\times$, and M, N have coefficients in $\mathbb{Z}_{11}$. Hence, $M, N \in \mathrm{GL}_2(\mathbb{Z}_{11})$ and

$$\begin{aligned} \overline{G}_{A,11} &= \mathbb{Z}_{11}\mathbf{u}_1 \oplus \mathbb{Q}_{11}\mathbf{u}_2, \\ \overline{G}_{B,11} &= \mathbb{Z}_{11}\mathbf{v}_1 \oplus \mathbb{Q}_{11}\mathbf{v}_2. \end{aligned}$$

Any $\mathbb{Z}_{11}$-module morphism T_{11} from $\overline{G}_{A,11}$ to $\overline{G}_{B,11}$ has the form $T_{11}(\mathbf{u}_2) = a_{22}\mathbf{v}_2$ and $T_{11}(\mathbf{u}_1) = a_{11}\mathbf{v}_1 + a_{12}\mathbf{v}_2$, where $a_{22}, a_{12} \in \mathbb{Q}_{11}$, $a_{11} \in \mathbb{Z}_{11}$. Hence, if $T_{11} \in \mathrm{GL}_2(\mathbb{Q}_{11})$ is a $\mathbb{Z}_{11}$-module isomorphism from $\overline{G}_{A,11}$ to $\overline{G}_{B,11}$, then

$$T_{11} = N \begin{pmatrix} a_{11} & 0 \\ a_{12} & a_{22} \end{pmatrix} M^{-1}, \quad a_{11} \in \mathbb{Z}_{11}^\times,\ a_{12}, a_{22} \in \mathbb{Q}_{11},\ a_{22} \neq 0.$$

By Lemma 3.6 and Remark 3.7, G_A and G_B are isomorphic if and only if there exists $T \in \mathrm{GL}_2(\mathbb{Q})$ such that under the natural embedding $\mathrm{GL}_2(\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_p)$ we have $T = T_{11}$ for some a_{ij}'s if $p = 11$ and $T \in \mathrm{GL}_2(\mathbb{Z}_p)$ for any prime $p \neq 11$. In other words, G_A and G_B are isomorphic if and only if there exist a_{ij}'s such that T_{11} is defined over $\mathbb{Q}$ (a priori, T_{11} is defined over $\mathbb{Q}_{11}$) and $T_{11} \in \mathrm{GL}_2(\mathbb{Z}_p)$ for any prime $p \neq 11$. One can show that such T_{11} does not exist. It requires tedious calculations to prove it directly in this setting. Instead, we prove the claim using a more efficient technique (via generalized ideal classes) in Example 5 below. In addition, here are two choices of T_{11} that illustrate the phenomenon. Namely, one can calculate

$$\tilde{T}_{11} = NM^{-1} = \begin{pmatrix} -\frac{\sqrt{5}}{33} - \frac{6}{11} & \frac{7\sqrt{5}}{33} - \frac{2}{11} \\ \frac{2\sqrt{5}}{3} & \frac{\sqrt{5}}{3} - 2 \end{pmatrix}.$$

Clearly, by above, $\tilde{T}_{11}$ defines an isomorphism from $\overline{G}_{A,11}$ to $\overline{G}_{B,11}$, but $\tilde{T}_{11}$ is not defined over $\mathbb{Q}$. On the other hand, if there exist $a_{11}, a_{12}, a_{22} \in \mathbb{Q}_{11}$ such that $a_{11} \in \mathbb{Z}_{11}^\times$, $a_{22} \neq 0$, and T_{11} is defined over $\mathbb{Q}$, then $T_{11} \notin \mathrm{GL}_2(\mathbb{Z}_p)$ for some prime $p \neq 11$. For instance,

$$\hat{T}_{11} = N \begin{pmatrix} -1 & 0 \\ 0 & -\frac{1}{11} \end{pmatrix} M^{-1} = \begin{pmatrix} \frac{1}{11} & \frac{1}{33} \\ 0 & \frac{1}{3} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}),$$

$\hat{T}_{11}$ defines an isomorphism from $\overline{G}_{A,11}$ to $\overline{G}_{B,11}$, but $\hat{T}_{11} \notin \mathrm{GL}_2(\mathbb{Z}_3)$. Essentially, the problem is that a priori each T_p is defined over $\mathbb{Q}_p$ and it might be impossible to find a common T defined over $\mathbb{Q}$ such that for any prime p it induces T_p when considered as an element of $\mathrm{M}_2(\mathbb{Q}_p)$ via the natural embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

3.3. **Special case.** We now consider the case when, in the notation of Proposition 3.8, $h_A \equiv t^n \pmod{p}$ for any prime $p \in \mathbb{Z}$ that divides $\det A$. In particular, if $n = 2$ this condition holds when every prime dividing the determinant of A also divides its trace.

Lemma 3.10. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let $h_A, h_B \in \mathbb{Z}[t]$ be their characteristic polynomials, respectively. Assume that for any prime $p \in \mathbb{Z}$ that divides $\det A$ we have*

$$h_A \equiv t^n \,(mod\ p).$$

Then $G_A \cong G_B$ (with $T = I_n$) if and only if $\det A$, $\det B$ have the same prime divisors and for any prime $p \in \mathbb{Z}$ that divides $\det B$ we have

$$h_B \equiv t^n \,(mod\ p).$$

Proof. Assume $\det A$, $\det B$ have the same prime divisors and for any prime $p \in \mathbb{Z}$ that divides $\det A$ we have $h_A \equiv h_B \equiv t^n \pmod{p}$. Then

$$\overline{G}_{A,p} = \overline{G}_{B,p} = \mathbb{Q}_p^n$$

by Proposition 3.8. Hence, $T = I_n$ is an isomorphism between G_A and G_B by Lemma 3.6.

Conversely, assume $G_A \cong G_B$. Then $\det A$, $\det B$ have the same prime divisors by Lemma 3.2. Let $p \in \mathbb{Z}$ be a prime that divides $\det A$. By assumption, $h_A \equiv t^n \pmod{p}$. This implies $\overline{G}_{A,p} = \mathbb{Q}_p^n$ by Proposition 3.8. Also, by Proposition 3.8, $\overline{G}_{B,p} \cong \mathbb{Q}_p^l \oplus \mathbb{Z}_p^{n-l}$ for some $0 \leq l \leq n$. Clearly, $\overline{G}_{A,p} \cong \overline{G}_{B,p}$, which is possible only when $l = n$, since $\mathbb{Q}_p^n$ is a divisible group and $\mathbb{Z}_p$ is not. Therefore, $h_B \equiv t^n \pmod{p}$. □

Remark 3.11. In particular, Lemma 3.10 applies when $n = 2$ and $A \in \mathrm{M}_2(\mathbb{Z})$ is not diagonalizable over an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Also, note that A is diagonalizable over $\overline{\mathbb{Q}}$ and $G_A \cong G_B$ does not imply that B is diagonalizable over $\overline{\mathbb{Q}}$. For example, let $\lambda \in \mathbb{Z}$ and let

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^2 \end{pmatrix},\ B = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Then $G_A \cong G_B$ by Lemma 3.10.

4. $n = 2$: general results

In this section we assume $n = 2$, $A \in \mathrm{M}_2(\mathbb{Z})$ is non-singular. Denote

$$\mathcal{S}'(A) \;=\; \{p \in \mathbb{Z} \text{ is prime} \mid p \text{ divides} \det A,\ p \text{ does not divide} \operatorname{Tr} A\}.$$

Note that if $G_A \cong G_B$, then $\mathcal{S}'(A) = \mathcal{S}'(B)$ by Lemma 3.2 and Corollary 3.9. The case $\mathcal{S}'(A) = \emptyset$ is covered by Lemma 3.2(i) and Lemma 3.10. Therefore, from now on we will assume that $\mathcal{S}'(A) \neq \emptyset$. Let $\overline{\mathbb{Q}}$ denote a fixed algebraic closure of $\mathbb{Q}$.

Proposition 4.1. *Suppose $A, B \in \mathrm{M}_2(\mathbb{Z})$ are non-singular, $\mathcal{S}'(A) \neq \emptyset$, and $G_A \cong G_B$. Then the following hold:*

1) *if $\lambda \in \overline{\mathbb{Q}}$ (resp., $\mu \in \overline{\mathbb{Q}}$) is an eigenvalue of A (resp., of B), then $\mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$;*

2) *let $K = \mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$, let $\mathcal{O}_K$ be the ring of integers of K, let $\mathbf{u} \neq \mathbf{0} \in K^2$ be an eigenvector of A corresponding to $\lambda \in \mathcal{O}_K$, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ dividing λ and lying above $p \in \mathcal{S}'(A)$ (i.e., p does not divide $\operatorname{Tr} A$). If $T : G_A \longrightarrow G_B$ is an isomorphism, then $T \in \mathrm{GL}_2(\mathcal{R})$ and $T\mathbf{u}$ is an eigenvector of B corresponding to an eigenvalue $\mu \in \mathcal{O}_K$ of B. Moreover, $\mathfrak{p}$ divides μ;*

3) *λ and μ have the same prime (ideal) divisors in $\mathcal{O}_K$.*

Proof. Let $p \in \mathcal{S}'(A)$, $K = \mathbb{Q}(\lambda)$, and let $\mathcal{O}$ be the ring of integers of K. We allow the case $K = \mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ lying above p that divides an eigenvalue $\lambda \in \mathcal{O}$ of A. Let $\mathbf{u} \neq \mathbf{0} \in K^2$ be an eigenvector of A corresponding to λ. Without loss of generality we can assume that $\mathbf{u} \in \mathcal{O}^2$. Since $G_A \cong G_B$, by Lemma 3.1 there exists $T \in \mathrm{GL}_2(\mathbb{Q})$ such that for any $m \in \mathbb{N} \cup \{0\}$ we have

$$B^{k_m} T = P_m A^m, \quad k_m \in \mathbb{N} \cup \{0\},\ P_m \in \mathrm{M}_2(\mathbb{Z}). \tag{4.1}$$

Let $T = \frac{1}{l} T'$ for some $l \in \mathbb{Z} - \{0\}$ and non-singular $T' \in \mathrm{M}_2(\mathbb{Z})$. Hence,

$$B^{k_m} T' \mathbf{u} = \lambda^m l P_m \mathbf{u}. \tag{4.2}$$

Denote $\mathbf{v} = T'\mathbf{u} \in \mathcal{O}^2$, $\mathbf{v} \neq \mathbf{0}$. Since $\mathfrak{p}$ divides λ, (4.2) implies

$$B^{k_m} \mathbf{v} \in \mathrm{M}_{2\times 1}(\mathfrak{p}^m). \tag{4.3}$$

We will show that (4.3) implies that $\mathbf{v}$ is an eigenvector of B. Indeed, let

$$C = \begin{pmatrix} \mathbf{v} & B\mathbf{v} \end{pmatrix} \in \mathrm{M}_2(\mathcal{O}).$$

It follows from (4.3) that $B^{k_m} C$ has coefficients in $\mathfrak{p}^m$. Suppose $\det C \neq 0$. Since C does not depend on m, it follows that $B^s \equiv 0 \,(\mathrm{mod}\ p)$ for some $s \in \mathbb{N}$, where 0 denotes the 2×2-zero matrix. This contradicts the assumption that $p \in \mathcal{S}'(A)$, since $\mathcal{S}'(A) = \mathcal{S}'(B)$ by by Lemma 3.2 and Corollary 3.9. Therefore, $\det C = 0$. In particular, $\mathbf{v}$ is an eigenvector of B. Hence, $T\mathbf{u}$ is also an eigenvector of B.

Let $\mathbf{w} = T\mathbf{u}$, $B\mathbf{w} = \mu\mathbf{w}$, $\mathbf{w} \neq \mathbf{0}$. Since B has integer entries, $\mathbf{w} \in K^2$, and $\mathbf{w} \neq \mathbf{0}$, we have $\mu \in K$ and since μ is integral over $\mathbb{Z}$, $\mu \in \mathcal{O}$. Thus, $\mathbb{Q}(\mu) \subseteq \mathbb{Q}(\lambda)$. Repeating the same argument as above with A replaced by B and using (3.3) instead of (3.2), we have $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}(\mu)$ and therefore, $\mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$, which proves 1). We now show that $\mathfrak{p}$ divides μ. Indeed, by above $T\mathbf{u}$ is an eigenvector of B corresponding to μ, *i.e.*,

$$B(T\mathbf{u}) = \mu(T\mathbf{u}).$$

Hence, multiplying (4.1) by $\mathbf{u}$, we get

$$\mu^{k_m} T\mathbf{u} = B^{k_m} T\mathbf{u} = P_m A^m \mathbf{u} = P_m \lambda^m \mathbf{u}, \quad \forall m \in \mathbb{N}. \tag{4.4}$$

Since $T\mathbf{u} \neq \mathbf{0}$, $T\mathbf{u}$ does not depend on m, and $\mathfrak{p}$ divides λ, this implies that $\mathfrak{p}$ divides μ (*e.g.*, this follows from the existence and uniqueness of decomposition of non-zero ideals into prime ideals in the Dedekind domain $\mathcal{O}$). Analogously, it follows from (4.4) that all prime (ideal) divisors of λ also divide μ (in $\mathcal{O}$). Repeating the same argument with A replaced by B and λ replaced by μ, we see that all prime divisors of μ also divide λ. Thus, λ and μ have the same prime divisors. This proves 2) and 3). □

Remark 4.2. It turns out that the converse of Proposition 4.1 also holds. The proof of the converse has two cases, and we consider them separately in the subsequent sections. More precisely, assume $\mathcal{S}'(A) \neq \emptyset$, $G_A \cong G_B$, and let $T : G_A \longrightarrow G_B$, $T \in \mathrm{GL}_2(\mathbb{Q})$, be an isomorphism. It follows from part 1) of Proposition 4.1 that either both characteristic polynomials of A and B are irreducible over $\mathbb{Q}$ or both characteristic polynomials of A and B are not irreducible over $\mathbb{Q}$.

If the characteristic polynomial of A is irreducible, equivalently, the eigenvalues of A do not belong to $\mathbb{Q}$, then by Proposition 4.1, $T\mathbf{u}$ is an eigenvector of B for any eigenvector $\mathbf{u}$ of A. Indeed, it follows from part 3) of Proposition 4.1 that there exists an eigenvector $\mathbf{u}$ of A such that $T\mathbf{u}$ is an eigenvector of B. Let $\lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$ be eigenvalues of A, $K = \mathbb{Q}(\lambda_1)$, and let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be the only non-trivial element of order 2. Then $\lambda_2 = \sigma(\lambda_1)$ and if $\mathbf{u}_1 \in K^2$ is an eigenvector of A corresponding to λ_1, then $\sigma(\mathbf{u}_1)$ is an eigenvector of A corresponding to λ_2. Thus, $T\sigma(\mathbf{u}) = \sigma(T\mathbf{u})$ is also an eigenvector of B.

Assume now that the characteristic polynomial of A is not irreducible, equivalently, the eigenvalues λ_1, λ_2 of A belong to $\mathbb{Q}$. Then $\lambda_1, \lambda_2 \in \mathbb{Z}$. There are two cases here: I) all prime divisors of one eigenvalue, *e.g.*, λ_2, are among prime divisors of the other eigenvalue, *e.g.*, λ_1 (denoted by $PD(\lambda_2) \subseteq PD(\lambda_1)$) and II) otherwise, *i.e.*, $PD(\lambda_1) \not\subseteq PD(\lambda_2)$, $PD(\lambda_2) \not\subseteq PD(\lambda_1)$. In case I), by part 3) of Proposition 4.1, $T\mathbf{u}$ is an eigenvector of B, if $\mathbf{u}$ is an eigenvector of A corresponding to λ_1. Indeed, note that λ_1, λ_2 do not share the same prime divisors, since $\mathcal{S}'(A) \neq \emptyset$. Therefore, there exists $p \in \mathcal{S}'(A)$ that divides λ_1 and hence, part 3) of Proposition 4.1 applies. However, part 3) of Proposition 4.1 does not guarantee that $T\mathbf{u}$ is an eigenvector of B, if $\mathbf{u}$ is an eigenvector of A corresponding to λ_2. In other words, in case I), $T\mathbf{u}$ is not necessarily an eigenvector of B for any eigenvector $\mathbf{u}$ of A. In case II), we still have that $T\mathbf{u}$ is an eigenvector of B for any eigenvector $\mathbf{u}$ of A, as in the case of non-rational eigenvalues. This observation makes case I) a special case, which we treat separately.

5. $n = 2$: special case $PD(\lambda_2) \subseteq PD(\lambda_1)$

In this section we consider the case when eigenvalues λ_1, λ_2 of $A \in \mathrm{M}_2(\mathbb{Z})$ belong to $\mathbb{Q}$ (equivalently, $\lambda_1, \lambda_2 \in \mathbb{Z}$) and prime divisors of one eigenvalue (*e.g.*, λ_2) are among prime divisors of the other eigenvalue (*e.g.*, λ_1), denoted by $PD(\lambda_2) \subseteq PD(\lambda_1)$. In this case, $G_A \cong G_B$ for a non-singular $B \in \mathrm{M}_2(\mathbb{Z})$ if and only if eigenvalues of A and B belong to $\mathbb{Z}$ and have the same prime divisors (Proposition 5.1 below), similar to the case $n = 1$.

Proposition 5.1. *Let $A \in \mathrm{M}_2(\mathbb{Z})$ be non-singular, let $\lambda_1, \lambda_2 \in \mathbb{Z}$ be eigenvalues of A, and let $\mathcal{S}'(A) \neq \emptyset$. Assume in addition that prime divisors of λ_2 are among prime divisors of λ_1. Then $G_A \cong G_B$ for a non-singular $B \in \mathrm{M}_2(\mathbb{Z})$ if and only if eigenvalues μ_1, μ_2 of B belong to $\mathbb{Z}$ and have the same prime divisors as λ_1, λ_2 (e.g., λ_1 and μ_1 (resp., λ_2 and μ_2) have the same prime divisors in $\mathbb{Z}$).*

Proof. The necessary part follows from Proposition 4.1. Indeed, assume $G_A \cong G_B$. Since $\lambda_1, \lambda_2 \in \mathbb{Q}$ and $\mathcal{S}'(A) \neq \emptyset$, we have $\mu_1, \mu_2 \in \mathbb{Q}$ by part 1) of Proposition 4.1. Let $p \in \mathcal{S}'(A)$. Since $PD(\lambda_2) \subseteq PD(\lambda_1)$, p divides λ_1 and does not divide λ_2. By parts 2), 3) of Proposition 4.1, without loss of generality we can assume that λ_1 and μ_1 have the same prime divisors (in $\mathbb{Z}$). We are left to show that λ_2 and μ_2 also have the same prime divisors (in $\mathbb{Z}$). If $p \in \mathbb{Z}$ is a prime that divides λ_2, then p divides λ_1, since $PD(\lambda_2) \subseteq PD(\lambda_1)$ by assumption. Hence, p divides both $\det A$ and $\operatorname{Tr} A$ and therefore, by Corollary 3.9, p divides $\operatorname{Tr} B$. Since by above, λ_1 and μ_1 have the same prime divisors, p divides μ_1. Thus, p divides $\operatorname{Tr} B$ and μ_1. Hence, p divides μ_2.

We now prove the sufficient part. We assume $\lambda_i, \mu_i \in \mathbb{Z}$ and λ_i, μ_i have the same prime divisors, $i \in \{1, 2\}$. Since $\mathcal{S}'(A) \neq \emptyset$, we have $\lambda_1 \neq \lambda_2$ and A is diagonalizable. By Corollary A.2, there exists $P \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$PAP^{-1} = M \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} M^{-1}, \quad M = \begin{pmatrix} 1 & u_1 \\ 0 & u_2 \end{pmatrix},$$

where

$$u_1, u_2 \in \mathbb{Z},\ u_2 \neq 0,\ (u_1, u_2) = 1,\ u_2 \,|\, (\lambda_1 - \lambda_2).$$

Analogously, $\mu_1 \neq \mu_2$ and B is diagonalizable, since by assumption λ_i, μ_i have the same prime divisors, $i \in \{1, 2\}$. Hence, by Corollary A.2, there exists $Q \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$QBQ^{-1} = N \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix} N^{-1}, \quad N = \begin{pmatrix} 1 & v_1 \\ 0 & v_2 \end{pmatrix},$$

where

$$v_1, v_2 \in \mathbb{Z},\ v_2 \neq 0,\ (v_1, v_2) = 1,\ v_2 \,|\, (\mu_1 - \mu_2).$$

Note that $A' = PAP^{-1}$, $B' = QBQ^{-1}$ ($A', B' \in \mathrm{M}_2(\mathbb{Z})$) share the same eigenvector $\mathbf{e}_1 = \begin{pmatrix} 1 & 0 \end{pmatrix}^t$, *i.e.*, $A'\mathbf{e}_1 = \lambda_1\mathbf{e}_1$, $B'\mathbf{e}_1 = \mu_1\mathbf{e}_1$, and $A'\mathbf{u} = \lambda_2\mathbf{u}$ for $\mathbf{u} = \begin{pmatrix} u_1 & u_2 \end{pmatrix}^t$.

In the rest of the proof we will show that $T = Q^{-1}P \in \mathrm{GL}_2(\mathbb{Z})$ induces a $\mathbb{Z}_p$-module isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$ for any $p \in \mathcal{S}(A)$. (In fact, one can show that T can be chosen to be in $\mathrm{SL}_2(\mathbb{Z})$, but $T \in \mathrm{GL}_2(\mathbb{Z})$ is enough for our purpose.)

For any $m, k_m \in \mathbb{N} \cup \{0\}$ we have

$$(B')^{k_m}(A')^{-m}\mathbf{e}_1 = \mu_1^{k_m}\lambda_1^{-m}\mathbf{e}_1.$$

By assumption, λ_1 and μ_1 have the same prime divisors, hence for any $m \in \mathbb{N} \cup \{0\}$ there exists $k_m \in \mathbb{N} \cup \{0\}$ big enough so that

$$(B')^{k_m}(A')^{-m}\mathbf{e}_1 \in \mathbb{Z}^2. \tag{5.1}$$

Let $p \in \mathcal{S}'(A)$. By assumption, prime divisors of λ_2 are among prime divisors of λ_1, hence p divides λ_1 and does not divide λ_2. In particular, p does not divide $\lambda_1 - \lambda_2$ and hence, $M \in \mathrm{GL}_2(\mathbb{Z}_p)$, since $\det M$ divides $\lambda_1 - \lambda_2$. Furthermore, for any $m, k_m \in \mathbb{N} \cup \{0\}$,

$$(B')^{k_m}(A')^{-m}\mathbf{u} = (B')^{k_m}\lambda_2^{-m}\mathbf{u} \in \mathbb{Z}_p^2, \tag{5.2}$$

since B', $\mathbf{u}$ have integer entries, and p does not divide λ_2. Since $M = \begin{pmatrix}\mathbf{e}_1 & \mathbf{u}\end{pmatrix}$, (5.1) and (5.2) imply

$$(B')^{k_m}(A')^{-m}M \in \mathrm{M}_2(\mathbb{Z}_p).$$

Since $M \in \mathrm{GL}_2(\mathbb{Z}_p)$, we have

$$(B')^{k_m}(A')^{-m} \in \mathrm{M}_2(\mathbb{Z}_p). \tag{5.3}$$

Recall that λ_i, μ_i have the same prime divisors, $i \in \{1, 2\}$. Thus, $\mathcal{S}'(A) = \mathcal{S}'(B)$ and the proof of (5.3) can be repeated with the roles of A and B switched. As a result, for any $n \in \mathbb{N} \cup \{0\}$ there exists $k_n \in \mathbb{N} \cup \{0\}$ such that

$$(A')^{l_n}(B')^{-n} \in \mathrm{M}_2(\mathbb{Z}_p). \tag{5.4}$$

Let $T = Q^{-1}P$. Since $A' = PAP^{-1}$, $B' = QBQ^{-1}$, $P, Q \in \mathrm{GL}_2(\mathbb{Z})$, equations (5.3), (5.4) imply

$$B^{k_m}TA^{-m} \in \mathrm{M}_2(\mathbb{Z}_p), \quad A^{l_n}T^{-1}B^{-n} \in \mathrm{M}_2(\mathbb{Z}_p)$$

for any $p \in \mathcal{S}'(A)$. Equivalently, T induces a $\mathbb{Z}_p$-module isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$ for any $p \in \mathcal{S}'(A)$.

We are left to consider primes in $\mathcal{S}(A)$ that do not belong to $\mathcal{S}'(A)$. Let $p \in \mathcal{S}(A)\backslash\mathcal{S}'(A)$ be such a prime. Then p divides both λ_1 and λ_2. Furthermore, p divides both μ_1 and μ_2, since λ_i, μ_i have the same prime divisors, $i \in \{1, 2\}$. Then $\overline{G}_{A,p} = \overline{G}_{B,p} = \mathbb{Q}_p^2$ by Proposition 3.8, and clearly, any element in $\mathrm{GL}_2(\mathbb{Q})$ induces a $\mathbb{Z}_p$-module isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$, in particular, T.

Note that $\det A$ and $\det B$ have the same prime divisors, since λ_i, μ_i have the same prime divisors, $i \in \{1, 2\}$. Also, $T \in \mathrm{GL}_2(\mathbb{Z})$. Thus, $G_A \cong G_B$ by Lemma 3.6. □

Remark 5.2. The proof of Proposition 5.1 also gives a way to construct an isomorphism between G_A and G_B provided that they are isomorphic. Namely, suppose a non-singular $A \in \mathrm{M}_2(\mathbb{Z})$ satisfies the assumptions of Proposition 5.1, *i.e.*, A has eigenvalues $\lambda_1, \lambda_2 \in \mathbb{Z}$, $PD(\lambda_2) \subseteq PD(\lambda_1)$, and $\mathcal{S}'(A) \neq \emptyset$. Let $G_A \cong G_B$ for a non-singular $B \in \mathrm{M}_2(\mathbb{Z})$. Then by Proposition 5.1, B has eigenvalues $\mu_1, \mu_2 \in \mathbb{Z}$ and λ_i, μ_i have the same prime divisors, $i \in \{1, 2\}$. It follows from the proof of Proposition 5.1 that there exist $P, Q \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$PAP^{-1} = \begin{pmatrix}\lambda_1 & * \\ 0 & \lambda_2\end{pmatrix}, \; QBQ^{-1} = \begin{pmatrix}\mu_1 & * \\ 0 & \mu_2\end{pmatrix}$$

(or by Theorem A.1 in Appendix A below). Then $T = Q^{-1}P$ is an isomorphism from G_A to G_B.

Example 2. Let

$$A = \begin{pmatrix} 2 & -2 \\ 4 & 8 \end{pmatrix},\ B = \begin{pmatrix} 13 & 5 \\ 11 & 7 \end{pmatrix}.$$

Here A has eigenvalues $4, 6$ and B has eigenvalues $2, 18$. In the notation of Proposition 5.1, $\lambda_1 = 6$, $\lambda_2 = 4$, $\mu_1 = 18$, $\mu_2 = 2$. Also, $G_A \cong G_B$ by Proposition 5.1. We now find an isomorphism $T \in \mathrm{GL}_2(\mathbb{Q})$ between G_A and G_B, using Remark 5.2. Let

$$P = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix},\ Q = \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix}.$$

We have $P, Q \in \mathrm{GL}_2(\mathbb{Z})$ and

$$PAP^{-1} = \begin{pmatrix} 6 & 0 \\ 0 & 4 \end{pmatrix},\ QBQ^{-1} = \begin{pmatrix} 18 & -27 \\ 0 & 2 \end{pmatrix}.$$

One can check directly that $G_{PAP^{-1}} \cong G_{QBQ^{-1}}$, *i.e.*, $T = Q^{-1}P$ is an isomorphism from G_A to G_B. Indeed, let $A' = PAP^{-1}$, $B' = QBQ^{-1}$. One can check by induction that for $k \in \mathbb{N}$ we have

$$(B')^k = \begin{pmatrix} 18^k & \alpha_k \\ 0 & 2^k \end{pmatrix},\ (B')^{-k} = \begin{pmatrix} 18^{-k} & \frac{\beta_k}{36^k} \\ 0 & 2^{-k} \end{pmatrix},$$

where $\alpha_k, \beta_k \in \mathbb{Z}$ and 2^{k-1} divides α_k. Therefore, for $n \in \mathbb{N}$ we have

$$(B')^k(A')^{-n} = \begin{pmatrix} 6^{-n}18^k & 4^{-n}\alpha_k \\ 0 & 4^{-n}2^k \end{pmatrix},\ (A')^n(B')^{-k} = \begin{pmatrix} 18^{-k}6^n & \frac{\beta_k}{36^k}6^n \\ 0 & 2^{-k}4^n \end{pmatrix}.$$

Clearly, these imply that for any $n \in \mathbb{N}$ there exists $k \in \mathbb{N}$ such that $(B')^k(A')^{-n} \in \mathrm{M}_2(\mathbb{Z})$, since 2^{k-1} divides α_k, and for any $k \in \mathbb{N}$ there exists $n \in \mathbb{N}$ such that $(A')^n(B')^{-k} \in \mathrm{M}_2(\mathbb{Z})$. This implies $G_{A'} = G_{B'}$ and hence $T = Q^{-1}P$ is an isomorphism from G_A to G_B.

6. $n = 2$: REMAINING CASES

6.1. **Eigenvectors.** In this section we consider two remaining cases: A) generic case when the characteristic polynomial of $A \in \mathrm{M}_2(\mathbb{Z})$ is irreducible over $\mathbb{Q}$ (equivalently, eigenvalues λ_1, λ_2 of A are not in $\mathbb{Q}$) and B) the characteristic polynomial of A is not irreducible over $\mathbb{Q}$ (equivalently, $\lambda_1, \lambda_2 \in \mathbb{Q}$) and the condition of section 5 does not hold, *i.e.*, there is a prime $p \in \mathbb{Z}$ (resp., a prime $q \in \mathbb{Z}$) that divides λ_1 (resp., λ_2) and does not divide λ_2 (resp., λ_1). Both cases are treated together in Theorem 6.1 below. Roughly, the main idea is that $G_A \cong G_B$ for non-singular $A, B \in \mathrm{M}_2(\mathbb{Z})$ if and only if eigenvectors of A correspond to eigenvectors of B under an isomorphism between G_A and G_B.

Let $\lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$ denote eigenvalues of $A \in \mathrm{M}_2(\mathbb{Z})$, let $K = \mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_2)$ be the splitting field of the characteristic polynomial of A. If $\lambda_1, \lambda_2 \in \mathbb{Z}$ (equivalently, $K = \mathbb{Q}$) and any prime $p \in \mathbb{Z}$ dividing λ_1 also divides λ_2, we write $PD(\lambda_1) \subseteq PD(\lambda_2)$. Recall that $\mathcal{S}'(A)$ denotes the set of all primes $p \in \mathbb{Z}$ that divide $\det A$ and do not divide $\mathrm{Tr}\, A$. In what follows we will need the following conditions:

(a) $\mathcal{S}'(A) \neq \emptyset$,

(b) either $K \neq \mathbb{Q}$ or $K = \mathbb{Q}$, $PD(\lambda_2) \not\subseteq PD(\lambda_1)$, $PD(\lambda_1) \not\subseteq PD(\lambda_2)$ (hence, $\lambda_1 \neq \lambda_2$ and A is diagonalizable).

Let $B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular and let $\mu_1, \mu_2 \in \overline{\mathbb{Q}}$ denote eigenvalues of B.

Theorem 6.1. *Assume conditions (a), (b) hold. Then $G_A \cong G_B$ if and only if*

(1) $\mathbb{Q}(\lambda_1) = \mathbb{Q}(\mu_1)$ *and* λ_1, μ_1 *(resp.,* λ_2, μ_2*) have the same prime divisors in the ring of integers of* $K = \mathbb{Q}(\lambda_1) = \mathbb{Q}(\mu_1)$;

(2) *there exists* $T \in \mathrm{GL}_2(\mathcal{R})$*, where* $\mathcal{R}$ *is defined by* (3.7)*, such that for any eigenvector* $\mathbf{u}_i \in K^2$ *of* A *corresponding to* λ_i*,* $T\mathbf{u}_i$ *is an eigenvector of* B *corresponding to* μ_i*,* $i = 1, 2$.

Proof. The necessary part of the theorem follows from Lemma 3.4, Proposition 4.1, and Remark 4.2.

We now show that conditions (1), (2) in Theorem 6.1 imply $G_A \cong G_B$. Note that (1) implies that $\det A$, $\det B$ have the same prime divisors and a prime $p \in \mathbb{Z}$ divides both $\det A$ and $\mathrm{Tr}\, A$ if and only if p divides both $\det B$ and $\mathrm{Tr}\, B$, *i.e.*, $\mathcal{S} = \mathcal{S}(A) = \mathcal{S}(B)$ and $\mathcal{S}' = \mathcal{S}'(A) = \mathcal{S}'(B)$. Let $T \in \mathrm{GL}_2(\mathcal{R})$ be such that $T\mathbf{u}_i$ is an eigenvector of B corresponding to μ_i for any eigenvector $\mathbf{u}_i$ of A corresponding to λ_i, $i = 1, 2$. In what follows, we will explore when T, considered as an element of $\mathrm{GL}_2(\mathbb{Q}_p)$ via the natural embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, induces a $\mathbb{Z}_p$-module isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$ for any $p \in \mathcal{S}$.

Let $p \in \mathcal{S}'$. Note that there is a natural embedding $\pi : K \hookrightarrow \mathbb{Q}_p$. Indeed, it is clear if $K = \mathbb{Q}$. Let $K \neq \mathbb{Q}$ and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal of ring of integers $\mathcal{O}_K$ of K lying above p such that $\mathfrak{p}$ divides λ_2 in $\mathcal{O}_K$. Then $\mathfrak{p}$ does not divide λ_1, hence p splits in K, and $K_{\mathfrak{p}} = \mathbb{Q}_p$. Thus, we have a natural embedding $K \hookrightarrow K_{\mathfrak{p}} = \mathbb{Q}_p$ in this case as well. By abuse of notation, for any $x \in K$ we will denote $\pi(x) \in \mathbb{Q}_p$ by $x \in \mathbb{Q}_p$. In particular, $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{Z}_p$ and $\lambda_1, \mu_1 \in \mathbb{Z}_p^\times$, $\lambda_2, \mu_2 \in p\mathbb{Z}_p$. Also, if $\mathbf{w}_i \in \mathbb{Q}_p^2$ is an eigenvector of A corresponding to λ_i, then $T\mathbf{w}_i \in \mathbb{Q}_p^2$ is an eigenvector of B corresponding to μ_i, by condition (2) of the theorem.

By Corollary A.2, there exists $S \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that

$$SAS^{-1} = M \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} M^{-1}, \quad M = \begin{pmatrix} 1 & u_1 \\ 0 & u_2 \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_p),$$

where $u_2 \neq 0$, u_1, u_2 are coprime in $\mathbb{Z}_p$, and u_2 divides $\lambda_1 - \lambda_2$. Since $\lambda_1 \in \mathbb{Z}_p^\times$ and $\lambda_2 \in p\mathbb{Z}_p$, we have $\lambda_1 - \lambda_2 \in \mathbb{Z}_p^\times$, hence $u_2 \in \mathbb{Z}_p^\times$ and $M \in \mathrm{GL}_2(\mathbb{Z}_p)$. Thus, there exists $L \in \mathrm{GL}_2(\mathbb{Z}_p)$, namely, $L = M^{-1}S$, such that LAL^{-1} is diagonal, *i.e.*,

$$LAL^{-1} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Analogously, there exists $P \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that

$$PBP^{-1} = \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix}.$$

In other words, there is a basis $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}_p^2$ (resp., a basis $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}_p^2$) of $\mathbb{Z}_p^2$ consisting of eigenvectors of A (resp., of B) corresponding to eigenvalues λ_1, λ_2 (resp., μ_1, μ_2). Thus,

$$\overline{G}_{A,p} = \{n_1\mathbf{u}_1 + n_2\mathbf{u}_2 \,|\, n_1 \in \mathbb{Z}_p,\, n_2 \in \mathbb{Q}_p\} \cong \mathbb{Z}_p \times \mathbb{Q}_p, \tag{6.1}$$

$$\overline{G}_{B,p} = \{n_1\mathbf{v}_1 + n_2\mathbf{v}_2 \,|\, n_1 \in \mathbb{Z}_p,\, n_2 \in \mathbb{Q}_p\} \cong \mathbb{Z}_p \times \mathbb{Q}_p. \tag{6.2}$$

Let $T\mathbf{u}_1 = x\mathbf{v}_1$, $T\mathbf{u}_2 = y\mathbf{v}_2$, for some $x, y \in \mathbb{Q}_p$. From (6.1) and (6.2), it is easy to see that T induces an isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$ if and only if $x \in \mathbb{Z}_p^\times$. We now see that T can be modified by multiplying by an appropriate power of p. Namely, let $T' = p^\gamma T$ with $\gamma = -\operatorname{val}_p x$. Then $T' \in \mathrm{GL}_2(\mathcal{R})$. Since $\mathcal{S}'$ is finite, applying the procedure to each p will result in $\tilde{T} \in \mathrm{GL}_2(\mathcal{R})$, which induces an isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$ for any $p \in \mathcal{S}'$.

Let $p \in \mathcal{S}\backslash\mathcal{S}'$. By Proposition 3.8, $\overline{G}_{A,p} = \overline{G}_{B,p} = \mathbb{Q}_p^2$ and hence, clearly, $\tilde{T}$ induces a $\mathbb{Z}_p$-module isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$.

Thus, we have showed that $\det A$, $\det B$ have the same prime divisors and $\tilde{T} \in \mathrm{GL}_2(\mathcal{R})$ induces an isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$ for any $p \in \mathcal{S}$. Therefore, $G_A \cong G_B$ by Lemma 3.6. □

Remark 6.2. Note that condition (2) of Theorem 6.1 is equivalent to the condition that A, B are diagonalizable and there exist $M, N \in \mathrm{GL}_2(K)$ diagonalizing A, B, respectively, such that $T = NM^{-1} \in \mathrm{GL}_2(\mathcal{R})$. Also, it follows from the proof of Theorem 6.1, that T is *not* an isomorphism between G_A and G_B in general, but rather there is $a \in \mathcal{R}^\times$ such that aT is an isomorphism between G_A and G_B.

Corollary 6.3. *Assume conditions (a), (b) hold. Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular. Assume, in addition, that A, B share the same characteristic polynomial, equivalently, A, B are conjugate in $\mathrm{GL}_2(\mathbb{Q})$. Then $G_A \cong G_B$ if and only if A, B are conjugate in $\mathrm{GL}_2(\mathcal{R})$.*

6.2. **Other criterions.** In this section, we give additional criterions for $T \in \mathrm{GL}_2(\mathbb{Q})$ to define an isomorphism between G_A and G_B under the assumptions of Theorem 6.1. In particular, in Lemma 6.4 below we give *rational* conditions, even when the characteristic polynomial of A is irreducible, and Lemma 6.5 provides an explicit criterion for T to be an isomorphism when A, B are conjugate over $\mathbb{Q}$ (unlike Corollary 6.3, which only addresses whether G_A and G_B are isomorphic or not).

More precisely, let $n = 1$ and $A \in \mathbb{Z}$, so that

$$G_A = \{A^k c \mid k, c \in \mathbb{Z}\}.$$

It is easy to check that for $B \in \mathbb{Z}$, we have $G_A \cong G_B$ if and only if A and B have the same prime divisors in $\mathbb{Z}$ if and only if there exist $k, l \in \mathbb{N}$, $P, Q \in \mathbb{Z}$, such that $A^k = PB$, $B^l = QA$. Thus, in the 1-dimensional case, $T : G_A \longrightarrow G_B$ is an isomorphism ($T \in \mathrm{GL}_1(\mathbb{Q})$) if and only if $T = 1$, $A^k = PB$, $B^l = QA$ for some $k, l \in \mathbb{N}$, $P, Q \in \mathbb{Z}$. We have the following result that generalizes this observation from the 1-dimensional case to the 2-dimensional one.

Lemma 6.4. *Assume that conditions (a), (b) in Theorem* 6.1 *hold. Then $T \in \mathrm{GL}_2(\mathbb{Q})$ defines an isomorphism $T : G_A \longrightarrow G_B$ if and only if there exist $k, l \in \mathbb{N} \cup \{0\}$ and $P, Q \in \mathrm{M}_2(\mathbb{Z})$ such that P (resp., Q) commutes with B (resp., with A), $T^{-1}P, TQ \in \mathrm{M}_2(\mathbb{Z})$ and*

$$TA^kT^{-1} = PB, \tag{6.3}$$

$$T^{-1}B^lT = QA. \tag{6.4}$$

Proof. First, we show that the conditions are sufficient for any non-singular $A, B \in \mathrm{M}_2(\mathbb{Z})$ regardless whether A, B satisfy conditions (a), (b). Indeed, (6.3) implies

$$T^{-1}B^{-n} = A^{-kn}T^{-1}P^n, \quad n \in \mathbb{N},$$

since P commutes with B. Therefore, for $\mathbf{x} \in \mathbb{Z}^2$ we have $\mathbf{u} = B^{-n}\mathbf{x} \in G_B$ and

$$T^{-1}\mathbf{u} \in G_A,$$

since $T^{-1}P^n \in \mathrm{M}_2(\mathbb{Z})$. Hence, $T^{-1}(G_B) \subseteq G_A$. Analogously, using (6.4), $T(G_A) \subseteq G_B$. Thus, $T : G_A \longrightarrow G_B$ is an isomorphism.

Conversely, assume $T \in \mathrm{GL}_2(\mathbb{Q})$ and $T : G_A \longrightarrow G_B$ is an isomorphism. We will show that (6.4) holds for $Q \in \mathrm{M}_2(\mathbb{Z})$ such that Q commutes with A and $TQ \in \mathrm{M}_2(\mathbb{Z})$. Equation (6.3) and corresponding conditions are proved similarly.

By Lemma 3.1, equation (3.2), there exist $l \in \mathbb{N}$ and $U \in \mathrm{M}_2(\mathbb{Z})$ such that $B^lTA^{-1} = U$. Hence, for $Q = T^{-1}U \in \mathrm{GL}_2(\mathbb{Q})$ we have

$$T^{-1}B^lT = QA,$$

which gives (6.4). By definition, $TQ = U \in \mathrm{M}_2(\mathbb{Z})$. Now we are left to show that Q commutes with A and $Q \in \mathrm{M}_2(\mathbb{Z})$. Let $K \subset \overline{\mathbb{Q}}$ be the splitting field of the characteristic polynomial of A. It follows from Remark 4.2 that K^2 has a basis $\{\mathbf{u}_1, \mathbf{u}_2\}$ consisting of eigenvectors of A such that $T\mathbf{u}_1$, $T\mathbf{u}_2$ are eigenvectors of B. Therefore, to check that Q commutes with A, it is enough to check that $QA\mathbf{u} = AQ\mathbf{u}$ for any eigenvector $\mathbf{u}$ of A. The latter follows easily from the definition of Q and the fact that $\mathbf{u}$ (resp., $T\mathbf{u}$) is an eigenvector of A (resp., B).

Finally, we show that Q has integer entries. First, note that $Q = T^{-1}U \in \mathrm{GL}_2(\mathcal{R})$, *i.e.*, entries of Q are rational numbers with only powers of primes dividing $\det A$ (equivalently, $\det B$ by Lemma 3.2 (*ii*)) in denominators. (This follows from Lemma 3.4.) Therefore, $Q \in \mathrm{M}_2(\mathbb{Z})$ if and only if $Q \in \mathrm{M}_2(\mathbb{Z}_p)$ (under the natural embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$) for any prime $p \in \mathbb{Z}$ dividing $\det B$ (*i.e.*, $p \in \mathcal{S}$). Furthermore, let p be a prime dividing both

$\det B$ and $\operatorname{Tr} B$. By Cayley–Hamilton theorem, $B^2 = pC$, where $C \in \mathrm{M}_2(\mathbb{Z})$. Therefore, replacing l by a bigger number if necessary, we get that entries of $Q = T^{-1}B^lTA^{-1}$ do not have powers of p in their denominators, *i.e.*, $Q \in \mathrm{M}_2(\mathbb{Z}_p)$.

We now assume that $p \in \mathbb{Z}$ is a prime in $\mathcal{S}'$, *i.e.*, p divides $\det B$ and p does not divide $\operatorname{Tr} B$. Since $T : G_A \longrightarrow G_B$ is an isomorphism, conditions (1), (2) of Theorem 6.1 hold. Therefore, as in the proof of the sufficient part of the theorem, A (resp., B) considered as an element of $\mathrm{M}_2(\mathbb{Z}_p)$ has two eigenvalues $\lambda_1, \lambda_2 \in \mathbb{Q}_p$ (resp., $\mu_1, \mu_2 \in \mathbb{Q}_p$) such that $\lambda_1 \in \mathbb{Z}_p^\times$ and $\lambda_2 \in p\mathbb{Z}_p$ (resp., $\mu_1 \in \mathbb{Z}_p^\times$ and $\mu_2 \in p\mathbb{Z}_p$). Moreover, there exist $M, N \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that

$$A = M\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}M^{-1}, \quad B = N\begin{pmatrix}\mu_1 & 0\\ 0 & \mu_2\end{pmatrix}N^{-1}, \quad T = N\begin{pmatrix}x & 0\\ 0 & y\end{pmatrix}M^{-1}$$

for some $x, y \in \mathbb{Q}_p^\times$. Then

$$Q = T^{-1}B^lTA^{-1} = M\begin{pmatrix}\frac{\mu_1^l}{\lambda_1} & 0\\ 0 & \frac{\mu_2^l}{\lambda_2}\end{pmatrix}M^{-1}.$$

Since $M \in \mathrm{GL}_2(\mathbb{Z}_p)$, $\lambda_1, \mu_1 \in \mathbb{Z}_p^\times$, $\lambda_2, \mu_2 \in p\mathbb{Z}_p$, for l big enough (we can always increase the power l without violating the other conditions related to (6.4)) we have $\frac{\mu_1^l}{\lambda_1}$, $\frac{\mu_2^l}{\lambda_2} \in \mathbb{Z}_p$, *i.e.*, $Q \in \mathrm{M}_2(\mathbb{Z}_p)$.

Therefore, $Q \in \mathrm{M}_2(\mathbb{Z}_p)$ for any $p \in \mathcal{S}$ and consequently, $Q \in \mathrm{M}_2(\mathbb{Z})$. □

We now apply Lemma 6.4 in the case when matrices A, B are conjugate over $\mathbb{Q}$. The result is a useful criterion of whether a given $T \in \mathrm{GL}_2(\mathbb{Q})$ defines an isomorphism between G_A and G_B.

Lemma 6.5. *Assume non-singular $A, B \in \mathrm{M}_2(\mathbb{Z})$ have the same characteristic polynomial irreducible over $\mathbb{Q}$ (in particular, A and B are conjugate in $\mathrm{GL}_2(\mathbb{Q})$) and let $\mathcal{S}'(A) \neq \emptyset$. Then, $T : G_A \longrightarrow G_B$, $T \in \mathrm{GL}_2(\mathbb{Q})$, is an isomorphism if and only if $TAT^{-1} = B$ and*

$$T^{-1}B^k, \quad TA^l \in \mathrm{M}_2(\mathbb{Z}) \text{ for some } k, l \in \mathbb{N} \cup \{0\}. \tag{6.5}$$

Proof. Assume that $T : G_A \longrightarrow G_B$ is an isomorphism. Then $TAT^{-1} = B$ by Remark 4.2. Also, by Lemma 3.1, equations (3.2) for $m = 1$ and (3.3) for $l = 1$, there exist $k_1, t_1 \in \mathbb{N}$ such that

$$B^{k_1}TA^{-1} = TA^{k_1-1} \in \mathrm{M}_2(\mathbb{Z}),$$

$$A^{t_1}T^{-1}B^{-1} = T^{-1}B^{t_1-1} \in \mathrm{M}_2(\mathbb{Z}),$$

and (6.5) holds with $k = t_1 - 1$, $l = k_1 - 1 \in \mathbb{N} \cup \{0\}$.

Conversely, assume $TAT^{-1} = B$ and (6.5) holds for some $T \in \mathrm{GL}_2(\mathbb{Q})$. Then T is an isomorphism by Lemma 6.4 with $P = B^k$, $Q = A^l$. □

6.3. **Case** A**.** Assume the characteristic polynomial of $A \in \mathrm{M}_2(\mathbb{Z})$ is irreducible over $\mathbb{Q}$. Let $\lambda \in \overline{\mathbb{Q}}$ be an eigenvalue of A and let $K = \mathbb{Q}(\lambda)$, $K \neq \mathbb{Q}$. Let $\mathbf{u} = \begin{pmatrix} u_1 & u_2 \end{pmatrix}^t \in K^2$ be an eigenvector of A corresponding to λ. Denote

$$\begin{aligned} I_{\mathbb{Z}}(A,\lambda) &= \{m_1u_1 + m_2u_2 \,|\, m_1, m_2 \in \mathbb{Z}\} \subset K, \\ I_{\mathcal{R}}(A,\lambda) &= I_{\mathbb{Z}}(A,\lambda) \otimes_{\mathbb{Z}} \mathcal{R} \subset K, \end{aligned}$$

where $\mathcal{R}$ is defined by (3.7), *i.e.*,

$$\mathcal{R} = \mathbb{Z}\left[\frac{1}{N}\right] = \left\{ \frac{x}{N^k} \;\middle|\; x, k \in \mathbb{Z} \right\}, \quad N = \det A.$$

Since $\lambda\mathbf{u} = A\mathbf{u}$ and A has integer entries, $I_{\mathbb{Z}}(A,\lambda)$ is a $\mathbb{Z}[\lambda]$-module and $I_{\mathcal{R}}(A,\lambda)$ is an $\mathcal{R}[\lambda]$-module.

Theorem 6.6. *Suppose the characteristic polynomial of a non-singular* $A \in \mathrm{M}_2(\mathbb{Z})$ *is irreducible and there is a prime* $p \in \mathbb{Z}$ *that divides* $\det A$ *and does not divide* $\operatorname{Tr} A$*. Then* $G_A \cong G_B$ *for a non-singular* $B \in \mathrm{M}_2(\mathbb{Z})$ *if and only if there exist eigenvalues* $\lambda, \mu \in \overline{\mathbb{Q}}$ *of* A, B*, respectively, such that*

1. $\mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$ *and* λ*,* μ *have the same prime divisors in the ring of integers of* $K = \mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$*;*
2. *there exists* $x \in K$ *with* $I_{\mathcal{R}}(A,\lambda) = xI_{\mathcal{R}}(B,\mu)$*.*

Proof. Note that conditions (a), (b) in Theorem 6.1 hold. Assume $G_A \cong G_B$. By Theorem 6.1, there are eigenvalues $\lambda, \mu \in \overline{\mathbb{Q}}$ of A, B, respectively, such that condition (1) in Theorem 6.6 holds and there is $T \in \mathrm{GL}_2(\mathcal{R})$ such that for an eigenvector $\mathbf{u}$ of A corresponding to λ, $T\mathbf{u}$ is an eigenvector of B corresponding to μ. This implies $I_{\mathcal{R}}(A,\lambda) = xI_{\mathcal{R}}(B,\mu)$ for some $x \in K$ and therefore, condition (2) in Theorem 6.6 holds as well.

Assume now that conditions (1), (2) in Theorem 6.6 hold. Since $I_{\mathcal{R}}(A,\lambda) = xI_{\mathcal{R}}(B,\mu)$, there exists $T \in \mathrm{GL}_2(\mathcal{R})$ such that for an eigenvector $\mathbf{u}$ of A corresponding to λ, $T\mathbf{u}$ is an eigenvector of B corresponding to μ. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be non-trivial. In the notation of Theorem 6.1, $\lambda_1 = \lambda$, $\lambda_2 = \sigma(\lambda)$, $\mu_1 = \mu$, $\mu_2 = \sigma(\mu)$, $\mathbf{u}_1 = \mathbf{u}$, $\mathbf{u}_2 = \sigma(\mathbf{u})$, and $T\sigma(\mathbf{u}) = T\mathbf{u}_2$ is an eigenvector of B corresponding to $\sigma(\mu) = \mu_2$. Clearly, λ_2, μ_2 have the same prime divisors, since λ_1, μ_1 have the same prime divisors. Thus, Theorem 6.6 follows from Theorem 6.1. □

Remark 6.7. One can show that conjugate (resp., non-conjugate) in $\mathrm{GL}_n(\mathbb{Q})$ non-singular $A, B \in \mathrm{M}_n(\mathbb{Z})$ can equally produce isomorphic and non-isomorphic groups G_A, G_B (see Examples 3, 4, 5 below). For a moment consider the special case when $A, B \in \mathrm{M}_n(\mathbb{Z})$ do share the same irreducible characteristic polynomial with root λ. Latimer–MacDuffee–Taussky theorem (Theorem 2.1 above) states that A, B are conjugate in $\mathrm{GL}_n(\mathbb{Z})$ if and only if $I_{\mathbb{Z}}(A,\lambda) = xI_{\mathbb{Z}}(B,\lambda)$ for $x \in \mathbb{Q}(\lambda)$. In our case, if $A, B \in \mathrm{M}_2(\mathbb{Z})$ share the same irreducible characteristic polynomial with root λ and $\mathcal{S}'(A) \neq \emptyset$, then $G_A \cong G_B$ if and only if $I_{\mathcal{R}}(A,\lambda) = xI_{\mathcal{R}}(B,\lambda)$ for $x \in \mathbb{Q}(\lambda)$ if and only if A, B are conjugate in $\mathrm{GL}_2(\mathcal{R})$ (*c.f.*, Corollary 6.3).

Remark 6.8. If $G_A \cong G_B$ and $n = 2$, then $\mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$, but $\mathbb{Z}[\lambda] \neq \mathbb{Z}[\mu]$ and $\mathcal{R}[\lambda] \neq \mathcal{R}[\mu]$ in general (see Example 6 below).

6.4. **Case** B**.** We now apply Theorem 6.1 in the case when $A \in \mathrm{M}_2(\mathbb{Z})$ has rational (hence, integer) eigenvalues and assumption (b) of Theorem 6.1 holds, *i.e.*, $PD(\lambda_2) \not\subseteq PD(\lambda_1)$, $PD(\lambda_1) \not\subseteq PD(\lambda_2)$. In particular, A has distinct eigenvalues and hence A is diagonalizable over $\mathbb{Q}$.

Proposition 6.9. *Assume $A \in \mathrm{M}_2(\mathbb{Z})$ is non-singular with eigenvalues $\lambda_1, \lambda_2 \in \mathbb{Z}$ satisfying $PD(\lambda_2) \not\subseteq PD(\lambda_1)$, $PD(\lambda_1) \not\subseteq PD(\lambda_2)$. Let $B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular. We have $G_A \cong G_B$ if and only if there exist $P, Q \in \mathrm{GL}_2(\mathbb{Z})$ such that*

$$PAP^{-1} = \begin{pmatrix} \lambda_1 & u \\ 0 & \lambda_2 \end{pmatrix}, \quad QBQ^{-1} = \begin{pmatrix} \mu_1 & v \\ 0 & \mu_2 \end{pmatrix}, \tag{6.6}$$

where $\lambda_i, \mu_i \in \mathbb{Z}^\times$, $u, v \in \mathbb{Z}$, λ_i, μ_i have the same prime divisors, $i = 1, 2$, and

$$\frac{u}{\lambda_2 - \lambda_1}\nu + \frac{v}{\mu_2 - \mu_1} \in \mathcal{R} \quad \text{for } \nu \in \mathcal{R}^\times, \tag{6.7}$$

where

$$\mathcal{R} = \mathbb{Z}\left[\frac{1}{N}\right] = \left\{ \frac{x}{N^k} \;\middle|\; x, k \in \mathbb{Z} \right\}, \quad N = \det A.$$

Proof. Since λ_1, λ_2 do not share the same prime divisors, we have $\lambda_1 \neq \lambda_2$ and hence A is diagonalizable over $\mathbb{Q}$. Let $\mu_1, \mu_2 \in \overline{\mathbb{Q}}$ be eigenvalues of B.

Assume $G_A \cong G_B$. The conditions $PD(\lambda_2) \not\subseteq PD(\lambda_1)$, $PD(\lambda_1) \not\subseteq PD(\lambda_2)$ imply that there are $p, q \in \mathcal{S}'(A)$ such that p divides λ_1 and q divides λ_2. Then, by Proposition 4.1 part 1), $\mu_1, \mu_2 \in \mathbb{Q}$ and hence $\mu_1, \mu_2 \in \mathbb{Z}$. By Proposition 4.1 part 3), we can assume that λ_i and μ_i have the same prime divisors, $i = 1, 2$. In particular, $\mu_1 \neq \mu_2$ and hence, B is also diagonalizable over $\mathbb{Q}$. By Theorem A.1, we have (6.6). Since both A, B are diagonalizable over $\mathbb{Q}$, we have

$$\begin{pmatrix} \lambda_1 & u \\ 0 & \lambda_2 \end{pmatrix} = M \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} M^{-1}, \quad \begin{pmatrix} \mu_1 & v \\ 0 & \mu_2 \end{pmatrix} = N \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix} N^{-1},$$

where

$$M = \begin{pmatrix} 1 & \frac{u}{\lambda_2 - \lambda_1} \\ 0 & 1 \end{pmatrix}, \quad N = \begin{pmatrix} 1 & \frac{v}{\mu_2 - \mu_1} \\ 0 & 1 \end{pmatrix}. \tag{6.8}$$

By Theorem 6.1, there exist $\nu_1, \nu_2 \in \mathbb{Q}^\times$ such that

$$T = N \begin{pmatrix} \nu_1 & 0 \\ 0 & \nu_2 \end{pmatrix} M^{-1} \in \mathrm{GL}_2(\mathcal{R}). \tag{6.9}$$

By direct calculation, $T \in \mathrm{GL}_2(\mathcal{R})$ implies (6.7) with $\nu = -\nu_1/\nu_2 \in \mathcal{R}^\times$.

Conversely, assume (6.6), (6.7) hold for $\nu = -\nu_1/\nu_2$, where $\nu_1, \nu_2 \in \mathbb{Z}$ and $(\nu_1, \nu_2) = 1$. Let T be defined by (6.9), where M, N are given by (6.8). Then, condition (6.7) implies $T \in \mathrm{GL}_2(\mathcal{R})$. By assumption, λ_i and μ_i have the same prime divisors, $i = 1, 2$. Therefore, $G_A \cong G_B$ by Theorem 6.1. □

7. Examples

Example 3. [C, p. 2, Example 2] Let

$$A = \begin{pmatrix} 0 & 4 \\ 2 & 0 \end{pmatrix}, \ B = \begin{pmatrix} 0 & 8 \\ 1 & 0 \end{pmatrix}.$$

Both A and B have the same characteristic polynomial $x^2 - 8$, irreducible over $\mathbb{Q}$, so that A and B are conjugate over $\mathbb{Q}$ and have the same eigenvalues. Here $\operatorname{Tr} A = \operatorname{Tr} B = 0$, $\det A = \det B$, and therefore, $G_A \cong G_B$ (more precisely, $G_A = G_B$) by Lemma 3.10. Also, for a non-singular $C \in \mathrm{M}_2(\mathbb{Z})$ we have $G_A \cong G_C$ (equivalently, $G_A = G_C$) if and only if $\operatorname{Tr} C = 2k$ and $\det C = 2^l$ for some $k \in \mathbb{N} \cup \{0\}$, $l \in \mathbb{N}$ (by Lemma 3.10).

Example 4. [C, p. 7, Example 12] Let

$$A = \begin{pmatrix} 0 & -6 \\ 1 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 0 & -3 \\ 2 & 1 \end{pmatrix}, \ C = \begin{pmatrix} -6 & -12 \\ 4 & 7 \end{pmatrix}.$$

All three A, B, and C have the same characteristic polynomial $h = x^2 - x + 6$ with root $\lambda = \frac{1+\sqrt{-23}}{2}$ and therefore they are all conjugate to each other in $\mathrm{GL}_2(\mathbb{Q})$. Moreover, A is a companion matrix of B and C. The three matrices above give (all) three equivalence classes of integer matrices with characteristic polynomial h up to conjugation by elements in $\mathrm{GL}_2(\mathbb{Z})$, *i.e.*, any matrix in $\mathrm{M}_2(\mathbb{Z})$ with characteristic polynomial h is $\mathrm{GL}_2(\mathbb{Z})$-conjugate to A, B, or C, and any two matrices out of A, B, and C are not $\mathrm{GL}_2(\mathbb{Z})$-conjugate to each other. We will explore which groups among G_A, G_B, and G_C are isomorphic.

Clearly, we only need to check condition (2) of Theorem 6.6. It is known that there are three $\mathbb{Z}[\lambda]$-ideal classes generated by $\{1, \lambda\}$, $\{2, \lambda\}$, and $\{4, 6 + \lambda\}$ corresponding to A, B, and C, respectively ([C, p. 7]). Since $\det A = 6$, we have $2, 3 \in \mathcal{R}^\times$ and

$$\operatorname{Span}_{\mathcal{R}}(1, \lambda) = \operatorname{Span}_{\mathcal{R}}(2, \lambda) = \operatorname{Span}_{\mathcal{R}}(4, 6 + \lambda),$$

i.e., $I_{\mathcal{R}}(A, \lambda) = I_{\mathcal{R}}(B, \lambda) = I_{\mathcal{R}}(C, \lambda)$. Thus, $G_A \cong G_B \cong G_C$ by Theorem 6.6. We now find corresponding isomorphisms. Let

$$\Lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \sigma(\lambda) \end{pmatrix}, \ M = \begin{pmatrix} -\sigma(\lambda) & -\lambda \\ 1 & 1 \end{pmatrix},$$
$$N = \begin{pmatrix} -\sigma(\lambda) & -\lambda \\ 2 & 2 \end{pmatrix}, \ L = \begin{pmatrix} -6 - \sigma(\lambda) & -6 - \lambda \\ 4 & 4 \end{pmatrix},$$

where $\sigma(\lambda) = \frac{1-\sqrt{-23}}{2}$ and

$$A = M\Lambda M^{-1}, \ B = N\Lambda N^{-1}, \ C = L\Lambda L^{-1}.$$

Let $K = \mathbb{Q}(\lambda)$, let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be non-trivial, and let $T \in \mathrm{GL}_2(\mathbb{Q})$ be an isomorphism from G_A to G_B. By Remark 6.2, $T \in \mathrm{GL}_2(\mathcal{R})$ and

$$T = T(x) = N \begin{pmatrix} x & 0 \\ 0 & \sigma(x) \end{pmatrix} M^{-1}, \quad x \in K. \tag{7.1}$$

In particular, when $x = 1/2$, we have $T_1 = T(1/2) \in \mathrm{GL}_2(\mathcal{R})$:

$$T_1 = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}. \tag{7.2}$$

One can verify that T_1 gives an isomorphism from G_A to G_B (*e.g.*, by Lemma 6.5 with $k = 0$, $l = 1$). Note that A, B, and C have the following principal slopes:

$$\omega_A = -\sigma(\lambda), \quad \omega_B = \frac{-\sigma(\lambda)}{2}, \quad \omega_C = \frac{-6 - \sigma(\lambda)}{4}$$

(see [ATW97] for the definition of a principal slope). Here ω_A, ω_B, $\omega_C \in K$ and $\mathrm{M}_2(K)$ acts on K via fractional linear transformations:

$$\Gamma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{M}_2(K), \quad \Gamma(\omega_A) = \frac{\alpha\omega_A + \beta}{\gamma\omega_A + \delta},$$

so that T_1 given by (8.9) is a matrix that transforms ω_A to ω_B, *i.e.*, $T_1(\omega_A) = \omega_B$ (which is equivalent to $T_1 A T_1^{-1} = B$). Let

$$T_2 = \begin{pmatrix} 1/4 & -3/2 \\ 0 & 1 \end{pmatrix},$$

so that $T_2(\omega_A) = \omega_C$ and hence $T_2 A T_2^{-1} = C$. It can be verified that $T_2 : G_A \longrightarrow G_C$ is an isomorphism by Lemma 6.5 with $k = 0$, $l = 2$. Also,

$$T_2 = \frac{1}{4} L M^{-1}.$$

Example 5. [ATW97, p. 1635] Let

$$A = \begin{pmatrix} -1 & 3 \\ 3 & 2 \end{pmatrix}, \; B = \begin{pmatrix} 0 & 1 \\ 11 & 1 \end{pmatrix}.$$

Here B is a companion matrix of A, so that A and B are conjugate in $\mathrm{GL}_2(\mathbb{Q})$. It is known (see [ATW97]) that A and B are not conjugate in $\mathrm{GL}_2(\mathbb{Z})$. We will show that G_A and G_B are not isomorphic. We have $\operatorname{Tr} A = 1$ and $\det A = -11$, so that in the above notation $\mathcal{R} = \{m11^n \,|\, m, n \in \mathbb{Z}\}$. Here $\lambda = \frac{1+3\sqrt{5}}{2}$, $K = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega = \frac{1+\sqrt{5}}{2}$, $3\omega = \lambda + 1$, and $\mathbb{Z}[\lambda] \neq \mathcal{O}_K$. It is known that $\mathcal{O}_K$ is a PID, and $\mathbb{Z}[\sqrt{5}]$ is not a PID. Also, $\mathcal{O}_K \not\subseteq \mathcal{R}[\lambda]$, since $1/3 \notin \mathcal{R}$. Note that

$$\mathbf{u} = \begin{pmatrix} -\omega + 1 \\ -1 \end{pmatrix}, \quad \mathbf{v} = \begin{pmatrix} 3\omega - 2 \\ 11 \end{pmatrix}$$

are eigenvectors of A, B, respectively, corresponding to λ. Then $I_{\mathcal{R}}(A, \lambda) = \mathcal{R}[\omega]$ and $I_{\mathcal{R}}(B, \lambda) = \mathcal{R}[3\omega]$. It is easy to see that $[I_{\mathcal{R}}(A, \lambda)] \neq [I_{\mathcal{R}}(B, \lambda)]$, *i.e.*, there is no $x \in K$

such that $I_{\mathcal{R}}(A,\lambda) = xI_{\mathcal{R}}(B,\lambda)$. Indeed, if there exists $x \in K$ such that $\mathcal{R}[\omega] = x\mathcal{R}[3\omega]$, then x is a unit in $\mathcal{R}[\omega]$, since $\mathcal{R}[3\omega] \subset \mathcal{R}[\omega]$. Therefore, $\mathcal{R}[\omega] = \mathcal{R}[3\omega]$, which implies $3 \in \mathcal{R}^\times$, contradiction. Hence, G_A and G_B are not isomorphic by Theorem 6.6.

Example 6. In this example, we have $G_A \cong G_C$, where A and C are not conjugate in $\mathrm{GL}_2(\mathbb{Q})$. Let

$$A = \begin{pmatrix} 0 & 3 \\ -1 & 1 \end{pmatrix},\ B = \begin{pmatrix} 0 & -9 \\ 3 & -8 \end{pmatrix},\ C = \begin{pmatrix} -3 & -6 \\ 2 & -5 \end{pmatrix},$$

so that the corresponding characteristic polynomials are

$$h_A = x^2 - x + 3, \quad h_B = h_C = x^2 + 8x + 27,$$

respectively. Here $\det A$, $\det B$, and $\det C$ have the same prime divisors in $\mathbb{Z}$, namely, $\mathcal{S} = \mathcal{S}_A = \mathcal{S}_B = \mathcal{S}_C = \{3\}$ and $\mathcal{R} = \mathcal{R}_A = \mathcal{R}_B = \mathcal{R}_C = \{m3^n \,|\, m, n \in \mathbb{Z}\}$. Also, $\lambda = (1 + \sqrt{-11})/2$ is an eigenvalue of A, $\mu = -3 - 2\lambda$ is an eigenvalue of B and C, so that h_A, h_B, and h_C share the same splitting field $K = \mathbb{Q}(\sqrt{-11})$. Moreover, $\mathcal{O}_K = \mathbb{Z}[\lambda]$, $\mathbb{Z}[\lambda] \neq \mathbb{Z}[\mu]$, and $\mathcal{R}[\lambda] \neq \mathcal{R}[\mu]$. One could also check that λ, μ have the same prime divisors in $\mathcal{O}_K$. Denote by $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w}$ eigenvectors of A, B, C corresponding to λ, μ, μ, respectively. Then

$$\mathbf{u} = \begin{pmatrix} \lambda - 1 \\ -1 \end{pmatrix}, \quad \mathbf{v} = \begin{pmatrix} 9 \\ 3 + 2\lambda \end{pmatrix}, \quad \mathbf{w} = \begin{pmatrix} 3 \\ \lambda \end{pmatrix},$$

and

$$I_{\mathcal{R}}(A,\lambda) = \mathcal{R}[\lambda],\ I_{\mathcal{R}}(B,\mu) = \mathcal{R}[2\lambda],\ \text{and } I_{\mathcal{R}}(C,\mu) = I_{\mathcal{R}}(A,\lambda) = \mathcal{R}[\lambda].$$

Since $2 \notin \mathcal{R}^\times$, it is easy to check that $[I_{\mathcal{R}}(A,\lambda)] \neq [I_{\mathcal{R}}(B,\mu)]$. Therefore, G_A is not isomorphic to G_B and $G_A \cong G_C$ by Theorem 6.6.

We now give examples, when condition (b) of Theorem 6.1 holds for rational eigenvalues λ_1, λ_2 of A, *i.e.*, $PD(\lambda_2) \not\subseteq PD(\lambda_1)$, $PD(\lambda_1) \not\subseteq PD(\lambda_2)$. In other words, there exists a prime $p \in \mathbb{Z}$ that divides λ_2 and does not divide λ_1 and there exists a prime $q \in \mathbb{Z}$ that divides λ_1 and does not divide λ_2. Since $\lambda_1, \lambda_2 \in \mathbb{Q}$, by Theorem A.1 (see Appendix A below), there exists $S \in \mathrm{GL}_2(\mathbb{Z})$ such that SAS^{-1} is upper-triangular.

Example 7. Let

$$A = \begin{pmatrix} 88 & -68 \\ 34 & -14 \end{pmatrix},\ B = \begin{pmatrix} -192 & 304 \\ -144 & 248 \end{pmatrix}.$$

Then A has eigenvalues $20, 54$ and B has eigenvalues $-40, 96$. Let

$$\begin{aligned}\lambda_1 &= 20 = 2^2 \cdot 5,\\ \lambda_2 &= 54 = 2 \cdot 3^3,\\ \mu_1 &= -40 = -2^3 \cdot 5,\\ \mu_2 &= 96 = 2^5 \cdot 3,\\ \lambda_2 - \lambda_1 &= 34 = 2 \cdot 17,\\ \mu_2 - \mu_1 &= 136 = 2^3 \cdot 17.\end{aligned}$$

Thus,

$$\mathcal{R} = \left\{x 2^u 3^v 5^w \mid x, u, v, w \in \mathbb{Z}\right\}.$$

We first conjugate A, B into upper-triangular matrices. Namely, one can show that

$$A = S \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} S^{-1}, \quad S = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}),$$

$$B = P \begin{pmatrix} \mu_1 & 8 \\ 0 & \mu_2 \end{pmatrix} P^{-1}, \quad P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

Thus, in the notation of Proposition 6.9,

$$u = 0, \quad v = 8,$$

and (6.7) becomes

$$\frac{u}{\lambda_2 - \lambda_1}\nu + \frac{v}{\mu_2 - \mu_1} = \frac{8}{2^3 \cdot 17} = \frac{1}{17}.$$

Since $1/17 \notin \mathcal{R}$, we have G_A, G_B are not isomorphic by Proposition 6.9.

Example 8. We keep the notation of the previous example, Example 7. Let

$$C = \begin{pmatrix} 87 & -67 \\ 33 & -13 \end{pmatrix}, \; B = \begin{pmatrix} -192 & 304 \\ -144 & 248 \end{pmatrix},$$

where C has eigenvalues $\lambda_1 = 20, \lambda_2 = 54$, and B is the same as in Example 7. In this case, we still have

$$\mathcal{R} = \left\{x 2^u 3^v 5^w \mid x, u, v, w \in \mathbb{Z}\right\}.$$

We claim that $G_C \cong G_B$. Indeed,

$$C = S \begin{pmatrix} \lambda_1 & -1 \\ 0 & \lambda_2 \end{pmatrix} S^{-1}, \quad S = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}),$$

$$B = P \begin{pmatrix} \mu_1 & 8 \\ 0 & \mu_2 \end{pmatrix} P^{-1}, \quad P = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

Thus, in the notation of Proposition 6.9,

$$u = -1, \quad v = 8.$$

Then (6.7) holds for $\nu = 2$, since $\nu \in \mathcal{R}^\times$, $\lambda_2 - \lambda_1 = 2 \cdot 17$, $\mu_2 - \mu_1 = 2^3 \cdot 17$, and

$$\frac{u}{\lambda_2 - \lambda_1}\nu + \frac{v}{\mu_2 - \mu_1} = 0 \in \mathcal{R}.$$

Therefore, $G_C \cong G_B$ by Proposition 6.9.

We now find an isomorphism T between G_C and G_B. Let

$$M = \begin{pmatrix} 1 & -1 \\ 0 & 34 \end{pmatrix}, \; N = \begin{pmatrix} 1 & 1 \\ 0 & 17 \end{pmatrix},$$

so that

$$C' = \begin{pmatrix} \lambda_1 & -1 \\ 0 & \lambda_2 \end{pmatrix} = M \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} M^{-1}, \quad B' = \begin{pmatrix} \mu_1 & 8 \\ 0 & \mu_2 \end{pmatrix} = N \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix} N^{-1}.$$

Define

$$T = PN \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M^{-1} S^{-1} = \begin{pmatrix} -5/2 & 9/2 \\ -3/2 & 5/2 \end{pmatrix}.$$

One can check that T defines an isomorphism $T : G_C \longrightarrow G_B$. Indeed, let

$$T' = N \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1/2 \end{pmatrix}.$$

First, we will use Lemma 3.6 to show that T' is an isomorphism from $G_{C'}$ to $G_{B'}$. Indeed, $\det C'$, $\det B'$ have the same prime divisors, $\mathcal{S} = \{2, 3, 5\}$, and $\mathcal{S}' = \{3, 5\}$. Clearly, $T' \in \mathrm{GL}_2(\mathcal{R})$ and we are left to show that T' induces a $\mathbb{Z}_p$-module isomorphism from $\overline{G}_{C',p}$ to $\overline{G}_{B',p}$ for any $p \in \mathcal{S}$ (as in the proof of Theorem 6.1). By Proposition 3.8, for $p = 2$, $\overline{G}_{C',2} = \overline{G}_{B',2} = (\mathbb{Q}_2)^2$ and clearly, T' induces an isomorphism between $\overline{G}_{C',2}$ and $\overline{G}_{B',2}$. For $p = 3, 5$, we have $M, N \in \mathrm{GL}_2(\mathbb{Z}_p)$. Let $M = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 \end{pmatrix}$, $N = \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{pmatrix}$. Hence, $T'\mathbf{u}_1 = \mathbf{v}_1$, $T'\mathbf{u}_2 = -\mathbf{v}_2$,

$$\overline{G}_{C',3} = \{n_1\mathbf{u}_1 + n_2\mathbf{u}_2 \,|\, n_1 \in \mathbb{Z}_3,\, n_2 \in \mathbb{Q}_3\},$$

$$\overline{G}_{B',3} = \{n_1\mathbf{v}_1 + n_2\mathbf{v}_2 \,|\, n_1 \in \mathbb{Z}_3,\, n_2 \in \mathbb{Q}_3\},$$

$$\overline{G}_{C',5} = \{n_1\mathbf{u}_1 + n_2\mathbf{u}_2 \,|\, n_1 \in \mathbb{Q}_5,\, n_2 \in \mathbb{Z}_5\},$$

$$\overline{G}_{B',5} = \{n_1\mathbf{v}_1 + n_2\mathbf{v}_2 \,|\, n_1 \in \mathbb{Q}_5,\, n_2 \in \mathbb{Z}_5\},$$

and $T'(\overline{G}_{C',p}) = \overline{G}_{B',p}$. Therefore, T' is an isomorphism from $G_{C'}$ to $G_{B'}$ by Lemma 3.6. Recall that $C = SC'S^{-1}$, $B = PB'P^{-1}$, $T = PT'S^{-1}$, where $P, S \in \mathrm{GL}_2(\mathbb{Z})$. Thus, T induces an isomorphism from G_C to G_B.

8. Applications

8.1. **Toroidal solenoids.** Recall that $G_A \cong G_B$ for non-singular $A, B \in \mathrm{M}_n(\mathbb{Z})$ if and only if the corresponding toroidal solenoids $\mathcal{S}_A$, $\mathcal{S}_B$ are homeomorphic (see Introduction for more detail). Using Theorem 6.6, one can now obtain certain results about the number of isomorphism classes of groups G_A or, equivalently, homeomorphism classes of 2-dimensional toroidal solenoids. Namely, let $\lambda \in \overline{\mathbb{Q}}$ be an algebraic integer, $K = \mathbb{Q}(\lambda)$. Let $d = \mathrm{N}_{K/\mathbb{Q}}(\lambda)$ be the norm of λ and let

$$\mathcal{R} = \mathbb{Z}\left[\frac{1}{d}\right] = \left\{ \frac{x}{d^k} \;\middle|\; x, k \in \mathbb{Z} \right\} \subset \mathbb{Q}.$$

Define an equivalence relation on non-zero finitely-generated $\mathbb{Z}[\lambda]$-modules $I, I' \subset K$ via $I \sim_{\mathbb{Z}} I'$ if and only if $I = xI'$ for $x \in K^\times$. It is well-known that the number $h(\lambda)$ of the corresponding equivalence classes (also called $\mathbb{Z}[\lambda]$-ideal classes) is finite. Also, if λ is an eigenvalue of $A \in \mathrm{M}_n(\mathbb{Z})$, then $I_{\mathbb{Z}}(A, \lambda)$ is a non-zero finitely-generated $\mathbb{Z}[\lambda]$-module (see the paragraph before Theorem 6.6 for more detail). Moreover, if $\chi \in \mathbb{Z}[t]$ is the minimal polynomial of λ of degree n, then by Latimer–MacDuffee–Taussky Theorem (Theorem 2.1 above), $\mathbb{Z}[\lambda]$-ideal classes correspond to $\mathrm{GL}_n(\mathbb{Z})$-conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$ with characteristic polynomial χ. More precisely, if $A, B \in \mathrm{M}_n(\mathbb{Z})$ have characteristic polynomial χ, then there exists $S \in \mathrm{GL}_n(\mathbb{Z})$ such that $SAS^{-1} = B$ if and only if $I_{\mathbb{Z}}(A, \lambda) = xI_{\mathbb{Z}}(B, \lambda)$ for $x \in K^\times$.

We define another equivalence relation on non-zero finitely-generated $\mathbb{Z}[\lambda]$-modules $I, I' \subset K$ via $I \sim_{\mathcal{R}} I'$ if and only if $I \otimes_{\mathbb{Z}} \mathcal{R} = x(I' \otimes_{\mathbb{Z}} \mathcal{R})$ for $x \in K^\times$. We call the corresponding equivalence classes $\mathcal{R}[\lambda]$-ideal classes. Since $h(\lambda)$ is finite and $I \sim_{\mathbb{Z}} I'$ implies $I \sim_{\mathcal{R}} I'$, the number $N(\lambda)$ of $\mathcal{R}[\lambda]$-ideal classes is also finite and $N(\lambda) \leq h(\lambda)$. Together with Theorem 6.6, that proves the following

Corollary 8.1. *Let $\lambda \in \overline{\mathbb{Q}}$ be an algebraic integer of degree 2. The number $N(\lambda)$ of isomorphism classes $[G_A]$ (equivalently, $N(\lambda)$ is the number of homeomorphism classes $[\mathcal{S}_A]$) with $A \in \mathrm{M}_2(\mathbb{Z})$ having λ as its eigenvalue is equal to the number of $\mathcal{R}[\lambda]$-ideal classes.*

Using Theorem 6.6 and Corollary 8.1, one can also effectively answer questions of the form:

Question 1. Given monic quadratic polynomials $\chi_1, \chi_2 \in \mathbb{Z}[t]$, describe all non-singular $A, B \in \mathrm{M}_2(\mathbb{Z})$ such that χ_1 is the characteristic polynomial of A, χ_2 is the characteristic polynomial of B, and $G_A \cong G_B$ (equivalently, $\mathcal{S}_A \cong \mathcal{S}_B$).

Question 2. Given a non-singular $A \in \mathrm{M}_2(\mathbb{Z})$, describe all non-singular $B \in \mathrm{M}_2(\mathbb{Z})$ such that $G_A \cong G_B$ (equivalently, $\mathcal{S}_A \cong \mathcal{S}_B$).

Let $\chi_1 = x^2 + a_1 x + a_2$, $a_1, a_2 \in \mathbb{Z}$. For simplicity, assume the generic case, *i.e.*, χ_1 is irreducible and there is a prime $p \in \mathbb{Z}$ that divides a_2 and does not divide a_1. Then if χ_1 is the characteristic polynomial of $A \in \mathrm{M}_2(\mathbb{Z})$, the assumptions of Theorem 6.6 hold. To

answer Question 1, one first checks that there are roots $\lambda_i \in \overline{\mathbb{Q}}$ of χ_i, $i = 1, 2$, such that condition (1) of Theorem 6.6 holds, namely, $\mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_2)$ and prime decompositions of ideals (λ_1), (λ_2) have the same prime ideals in the ring of integers of $\mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_2)$. If this is the case, one looks at finitely many $\mathbb{Z}[\lambda_1]$- and $\mathbb{Z}[\lambda_2]$-ideal classes and decides which ones satisfy condition (2) of Theorem 6.6. More precisely, if $[I_i]$ is a $\mathbb{Z}[\lambda_i]$-ideal class, $i = 1, 2$, whether $I_1 \otimes_{\mathbb{Z}} \mathcal{R} = x(I_2 \otimes_{\mathbb{Z}} \mathcal{R})$ for some $x \in \mathbb{Q}(\lambda_1)$. Corresponding matrices A, B can then be recovered from I_1, I_2. Question 2 can be handled similarly. Finally, Questions 1 and 2 can be formulated in terms of solenoids $\mathcal{S}_A$, $\mathcal{S}_B$.

Many explicit results, examples and numerical algorithms have been accumulated regarding quadratic fields, their class numbers, and class numbers of subrings of their rings of integers (see *e.g.*, Wolfram, [W04], [K13]). Thanks to Theorem 6.6, these data can now be useful in studying groups G_A and associated solenoids.

8.2. **$\mathbb{Z}^n$-odometers.** In this section we will show how our results concerning groups G_A can be useful in studying $\mathbb{Z}^n$-odometers.

$\mathbb{Z}^n$-odometer is a dynamical system consisting of a topological space X and an action of the group $\mathbb{Z}^n$ on X (by homeomorphisms). There is a way to construct a $\mathbb{Z}^n$-odometer out of a subgroup H of $\mathbb{Q}^n$ that contains $\mathbb{Z}^n$ [GPS19, p. 914]. Namely, the associated odometer Y_H is the Pontryagin dual of the quotient $H/\mathbb{Z}^n$, *i.e.,* $Y_H = \widehat{H/\mathbb{Z}^n}$. The action of $\mathbb{Z}^n$ on Y_H is given as follows. Let ρ denote the embedding

$$\rho : H/\mathbb{Z}^n \hookrightarrow \mathbb{Q}^n/\mathbb{Z}^n \hookrightarrow \mathbb{T}^n, \quad \mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n.$$

Identifying Pontryagin dual $\widehat{\mathbb{T}^n}$ of $\mathbb{T}^n$ with $\mathbb{Z}^n$, we have the induced map

$$\widehat{\rho} : \mathbb{Z}^n \longrightarrow Y_H = \widehat{H/\mathbb{Z}^n}.$$

The action of $\mathbb{Z}^n$ on Y_H is given by $\widehat{\rho}$. Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. Applying the process to the group $H = G_A$, we get the associated $\mathbb{Z}^n$-odometer Y_{G_A}. For simplicity, we denote Y_{G_A} by Y_A.

Another way to obtain a $\mathbb{Z}^n$-odometer is to consider a decreasing sequence of finite-index subgroups of $\mathbb{Z}^n$

$$G = \mathbb{Z}^n \supseteq G_1 \supseteq G_2 \supseteq \cdots$$

and the natural maps $\pi_i : G/G_{i+1} \longrightarrow G/G_i$, $i \in \mathbb{N}$. The associated $\mathbb{Z}^n$-odometer is the inverse limit

$$X = \varprojlim (G/G_i) \tag{8.1}$$

together with the natural action of $\mathbb{Z}^n$. For the sequence

$$G_i = \left\{ A^i \mathbf{x} \,\middle|\, \mathbf{x} \in \mathbb{Z}^n \right\}, \quad i \in \mathbb{N},$$

denote by X_A the corresponding odometer. Using duality, one can prove that X_A and Y_{A^t} are conjugate $\mathbb{Z}^n$-odometers [GPS19, Theorem 2.6].

The following theorem classifies $\mathbb{Z}^n$-actions on odometers Y_H up to various equivalences in terms of groups H [GPS19, Theorem 1.5].

Theorem 8.2 (*c.f.*, Theorem 1.5, [GPS19])**.** *Let H, K be dense subgroups of $\mathbb{Q}^2$ such that $\mathbb{Z}^2 \subseteq H$, $\mathbb{Z}^2 \subseteq K$. Then*

(1) *$\mathbb{Z}^2$-actions Y_H, Y_K are conjugate if and only if $H = K$.*
(2) *$\mathbb{Z}^2$-actions Y_H, Y_K are isomorphic if and only if there exists $T \in \mathrm{GL}_2(\mathbb{Z})$ such that $T(H) = K$.*
(3) *$\mathbb{Z}^2$-actions Y_H, Y_K are continuously orbit equivalent if and only if there exists $T \in \mathrm{GL}_2(\mathbb{Q})$ such that $\det T = \pm 1$ and $T(H) = K$.*
(4) *$\mathbb{Z}^2$-actions Y_H, Y_K are orbit equivalent if and only if $[[H : \mathbb{Z}^2]] = [[K : \mathbb{Z}^2]]$.*

Remark 8.3. If H is a union of an increasing sequence of finite-index extensions H_k of $\mathbb{Z}^n$, $k \geq 1$, then $[[H : \mathbb{Z}^n]]$ can be defined as

$$[[H : \mathbb{Z}^n]] = \bigcup_{k=1}^{\infty} \{l \in \mathbb{N} \,|\, l \text{ divides } [H_k : \mathbb{Z}^n]\}$$

[GPS19, p. 917, Prop. 2.9].

In what follows we combine Theorem 8.2 and our results on groups G_A to classify odometers of the form Y_A, where $A \in \mathrm{M}_2(\mathbb{Z})$ is non-singular. Since Theorem 8.2 applies to dense subgroups of $\mathbb{Q}^2$, we start by analyzing when G_A is dense in $\mathbb{Q}^2$ (Lemma 8.4). Next, we calculate $[[G_A : \mathbb{Z}^n]]$ (Lemma 8.5).

Lemma 8.4. *Let $A \in \mathrm{M}_2(\mathbb{Z})$ be non-singular. If G_A is dense in $\mathbb{Q}^2$, then $\det A \neq \pm 1$ and ± 1 are not eigenvalues of A. Conversely,*

(1) *if there is a prime $p \in \mathbb{Z}$ that divides both $\det A$ and $\operatorname{Tr} A$, then G_A is dense in $\mathbb{Q}^2$;*
(2) *if there is a prime $p \in \mathbb{Z}$ that divides $\det A$ and does not divide $\operatorname{Tr} A$, and ± 1 are not eigenvalues of A, then G_A is dense in $\mathbb{Q}^2$.*

Proof. Let $H \subseteq \mathbb{Q}^n$ be a subgroup and let $\mathbb{Z}^n \subseteq H$. It is known that H is dense in $\mathbb{Q}^n$ if and only if the $\mathbb{Z}^n$-action on Y_H is free. Also, the $\mathbb{Z}^n$-action on an odometer X defined by (8.1) is free if and only if

$$\bigcap_{i=1}^{\infty} G_i = \{0\} \tag{8.2}$$

[GPS19]. By above, X_{A^t} and Y_A are conjugate $\mathbb{Z}^n$-odometers, hence G_A is dense in $\mathbb{Q}^n$ if and only if (8.2) holds for

$$G_i = \left\{ (A^t)^i \mathbf{x} \,\middle|\, \mathbf{x} \in \mathbb{Z}^n \right\}, \quad i \in \mathbb{N}.$$

Also, since the conditions in Lemma 8.4 hold for A^t if and only if they hold for A, without loss of generality, we can assume that G_i's are defined by A, *i.e.*,

$$G_i = \left\{ A^i \mathbf{x} \,\middle|\, \mathbf{x} \in \mathbb{Z}^n \right\}, \quad i \in \mathbb{N}.$$

Note that $\mathbf{y} \in \bigcap_{i=1}^{\infty} G_i$ if and only if

$$A^{-i}\mathbf{y} \in \mathbb{Z}^n \text{ for any } i \in \mathbb{N}. \tag{8.3}$$

Thus, G_A is dense in $\mathbb{Q}^n$ if and only if (8.3) for $\mathbf{y} \in \mathbb{Z}^n$ implies $\mathbf{y} = \mathbf{0}$.

Clearly, if $\det A = \pm 1$, then $G_i = \mathbb{Z}^n$ for any $i \in \mathbb{N}$ and (8.2) does not hold. Also, if $\lambda = \pm 1$ is an eigenvalue of A, then there exists an eigenvector $\mathbf{y} \in \mathbb{Z}^n$ of A corresponding to λ. Clearly, $\mathbf{y} \neq \mathbf{0}$ and $\mathbf{y}$ satisfies (8.3). This proves the necessary part of the lemma.

For the rest of the proof we assume $\det A \neq \pm 1$ and $n = 2$. Suppose there is a prime $p \in \mathbb{Z}$ that divides both $\det A$ and $\operatorname{Tr} A$. It follows from Cayley–Hamilton theorem that $A^2 = p \cdot C$ for a non-singular $C \in \mathrm{M}_2(\mathbb{Z})$. Let $\mathbf{y} \in \mathbb{Z}^2$ satisfy (8.3). Then $A^{-2i}\mathbf{y} \in \mathbb{Z}^2$ implies $p^{-i}\mathbf{y} \in \mathbb{Z}^2$ for any i. Hence, $\mathbf{y} = \mathbf{0}$ and G_A is dense in $\mathbb{Q}^2$. This proves statement (1) of the lemma.

Assume there exists a prime $p \in \mathbb{Z}$ that divides $\det A$ and does not divide $\operatorname{Tr} A$. Let $\lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$ be eigenvalues of A. Then $\lambda_1 \neq \lambda_2$ and A is diagonalizable. Let $K = \mathbb{Q}(\lambda_1)$ with ring of integers $\mathcal{O}_K$ and let $\mathbf{u}_j \in K^2$ be eigenvectors of A corresponding to λ_j $(j = 1, 2)$. Without loss of generality, we can assume $\mathbf{u}_1, \mathbf{u}_2 \in (\mathcal{O}_K)^2$. Let $\mathbf{y} \in \mathbb{Z}^2$ satisfy (8.3) and let

$$\mathbf{y} = \alpha_1\mathbf{u}_1 + \alpha_2\mathbf{u}_2, \quad \alpha_1, \alpha_2 \in K,$$

so that

$$A^{-i}\mathbf{y} = \alpha_1\lambda_1^{-i}\mathbf{u}_1 + \alpha_2\lambda_2^{-i}\mathbf{u}_2 \in \mathbb{Z}^2 \text{ for any } i \in \mathbb{N}.$$

By multiplying $\mathbf{y}$ by an appropriate integer, without loss of generality, we can assume $\alpha_1, \alpha_2 \in \mathcal{O}_K$. As in the proof of Theorem 6.1 above, K can be embedded into $\mathbb{Q}_p$ such that $\lambda_1 \in \mathbb{Z}_p^{\times}$ and $\lambda_2 \in p\mathbb{Z}_p$. Under the embedding $K \hookrightarrow \mathbb{Q}_p$, we have $\mathbf{u}_j \in \mathbb{Z}_p^2$, $\alpha_j \in \mathbb{Z}_p$ $(j = 1, 2)$ and

$$A^{-i}\mathbf{y} = \alpha_1\lambda_1^{-i}\mathbf{u}_1 + \alpha_2\lambda_2^{-i}\mathbf{u}_2 \in \mathbb{Z}_p^2 \text{ for any } i \in \mathbb{N}.$$

Since $\lambda_1 \in \mathbb{Z}_p^{\times}$, $\lambda_2 \in p\mathbb{Z}_p$, this implies $\alpha_2 = 0$ and, therefore, $\mathbf{y}$ is an eigenvector of A corresponding to λ_1. Thus,

$$A^{-i}\mathbf{y} = \lambda_1^{-i}\mathbf{y} \in \mathbb{Z}^2 \text{ for any } i \in \mathbb{N},$$

and $\mathbf{y} \neq \mathbf{0}$ if and only if $\lambda_1 = \pm 1$. This proves statement (2) of the lemma. □

Lemma 8.5. *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular, $\det A \neq \pm 1$. If*

$$\det A = \alpha p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t},$$

where $\alpha = \pm 1$, $a_1, a_2, \ldots, a_t \in \mathbb{N}$, and $p_1, p_2, \ldots, p_t \in \mathbb{N}$ are distinct primes, then

$$[[G_A : \mathbb{Z}^n]] = \left\{ p_1^{b_1} p_2^{b_2} \cdots p_t^{b_t} \,|\, b_1, b_2, \ldots, b_t \in \mathbb{N} \cup \{0\} \right\}.$$

Proof. We will use Remark 8.3 with $H = G_A$ and

$$H_k = \{A^{-k}\mathbf{x} \,|\, \mathbf{x} \in \mathbb{Z}^n\}.$$

For a prime $p \in \mathbb{Z}$ let $x = x_0 + x_1 \in \mathbb{Q}_p$, where $x_1 \in \mathbb{Z}_p$ and $x_0 \in \mathbb{Q}$ is a "fractional" part of x. It is well-known that the correspondence $\phi_p(x) = x_0$ induces a well-defined injective homomorphism $\phi_p : \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z}$ and that $\phi = \bigoplus_p \phi_p$ is a group isomorphism

$$\phi = \bigoplus_p \phi_p : \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z},$$

where p runs through all primes of $\mathbb{Z}$. By composing ϕ^n with certain natural isomorphisms as follows

$$\bigoplus_p \mathbb{Q}_p^n/\mathbb{Z}_p^n \xrightarrow{\sim} \bigoplus_p (\mathbb{Q}_p/\mathbb{Z}_p)^n \xrightarrow{\sim} \left(\bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p\right)^n \xrightarrow{\phi^n} (\mathbb{Q}/\mathbb{Z})^n \xrightarrow{\sim} \mathbb{Q}^n/\mathbb{Z}^n,$$

we get a group isomorphism

$$\psi : \bigoplus_p \mathbb{Q}_p^n/\mathbb{Z}_p^n \xrightarrow{\sim} \mathbb{Q}^n/\mathbb{Z}^n.$$

Denote $H_{k,p} = H_k \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $H_{k,p} \subseteq \mathbb{Q}_p^n$. Then, ψ restricts to a group isomorphism

$$\psi_k : \bigoplus_p H_{k,p}/\mathbb{Z}_p^n \xrightarrow{\sim} H_k/\mathbb{Z}^n.$$

Indeed, recall that A has integer entries and, therefore, for any $i \in \mathbb{N}$ the multiplication by A^i extends to operators on $\mathbb{Q}_p^n/\mathbb{Z}_p^n$ and $\mathbb{Q}^n/\mathbb{Z}^n$ and commutes with ψ. Furthermore, $\mathbf{u} \in H_{k,p}$ (resp., $\mathbf{v} \in H_k$) if and only if $A^k\mathbf{u} \in \mathbb{Z}_p^n$ (resp., $A^k\mathbf{v} \in \mathbb{Z}^n$).

Finally, for any p that does not divide $\det A$ we have $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ and, hence, $H_{k,p}/\mathbb{Z}_p^n$ is trivial. Therefore, ψ_k is an isomorphism between the following groups

$$\psi_k : \bigoplus_{i=1}^{t} H_{k,p_i}/\mathbb{Z}_{p_i}^n \xrightarrow{\sim} H_k/\mathbb{Z}^n.$$

Hence,

$$[H_k : \mathbb{Z}^n] = \prod_{i=1}^{t} [H_{k,p_i} : \mathbb{Z}_{p_i}^n]. \tag{8.4}$$

Note that $H_{j,p} = H_{j+1,p}$ for some j and a prime $p \in \mathbb{Z}$ if and only if p does not divide $\det A$. Also,

$$\mathbb{Z}_{p_i}^n \subset H_{k,p_i} \subseteq \frac{1}{p_i^{a_i k}} \mathbb{Z}_{p_i}^n,$$

and each index $[H_{k,p_i} : \mathbb{Z}_{p_i}^n]$ is a power of p_i. Therefore, as k grows, the indices $[H_{k,p_i} : \mathbb{Z}_{p_i}^n]$ become unbounded powers of p_i. Together with (8.4) and Remark 8.3 this proves the lemma. □

We are now ready to classify odometers of the form Y_A up to the equivalences appearing in Theorem 8.2. The statements are direct consequences of the results of the current paper and Theorem 8.2.

8.3. **Orbit equivalence.**

Lemma 8.6. *Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular such that G_A (resp., G_B) is dense in $\mathbb{Q}^2$ (see Lemma 8.4). Then $\mathbb{Z}^2$-actions Y_A, Y_B are orbit equivalent if and only if $\det A, \det B$ have the same prime divisors.*

Proof. Follows from Theorem 8.2 and Lemma 8.5. □

Recall that our solution to the classification problem for groups G_A is split into cases. Therefore, in what follows, we classify odometers Y_A based on those cases.

8.4. $\boldsymbol{p \,|\, \det A \Rightarrow p \,|\, \mathrm{Tr}\, A}$

Lemma 8.7. *Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular such that G_A (resp., G_B) is dense in $\mathbb{Q}^2$ (see Lemma 8.4). Suppose any prime $p \in \mathbb{Z}$ that divides $\det A$ also divides $\mathrm{Tr}\, A$. Then the following are equivalent:*

(1) *$\mathbb{Z}^2$-actions Y_A, Y_B are conjugate;*
(2) *$\mathbb{Z}^2$-actions Y_A, Y_B are isomorphic;*
(3) *$\mathbb{Z}^2$-actions Y_A, Y_B are continuously orbit equivalent;*
(4) *$\det A$, $\det B$ have the same prime divisors and any prime $p \in \mathbb{Z}$ that divides $\det B$ also divides $\mathrm{Tr}\, B$.*

Proof. Follows from Lemma 3.10 and Theorem 8.2. □

8.5. $\boldsymbol{PD(\lambda_2) \subseteq PD(\lambda_1)}$. This is the case when A has rational (equivalently, integer) eigenvalues λ_1, λ_2 and all prime divisors of one eigenvalue (*e.g.*, λ_2) are among prime divisors of the other (*e.g.*, λ_1).

Lemma 8.8. *Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular such that G_A (resp., G_B) is dense in $\mathbb{Q}^2$ (see Lemma 8.4). Let $\lambda_1, \lambda_2 \in \mathbb{Z}$ be eigenvalues of A. Suppose there is a prime p that divides $\det A$ and does not divide $\mathrm{Tr}\, A$ and all prime divisors of λ_2 are among prime divisors of λ_1. Then*

(1) *$\mathbb{Z}^2$-actions Y_A, Y_B are conjugate if and only if there exists $P \in \mathrm{GL}_2(\mathbb{Z})$ such that*

$$PAP^{-1} = \begin{pmatrix} \lambda_1 & * \\ 0 & \lambda_2 \end{pmatrix}, \; PBP^{-1} = \begin{pmatrix} \mu_1 & * \\ 0 & \mu_2 \end{pmatrix}, \quad \mu_1, \mu_2 \in \mathbb{Z}, \tag{8.5}$$

λ_1 and μ_1 (resp., λ_2 and μ_2) have the same prime divisors in $\mathbb{Z}$.

(2) *$\mathbb{Z}^2$-actions Y_A, Y_B are isomorphic if and only if continuously orbit equivalent if and only if eigenvalues μ_1, μ_2 of B belong to $\mathbb{Z}$ and have the same prime divisors as λ_1, λ_2 (e.g., λ_1 and μ_1 (resp., λ_2 and μ_2) have the same prime divisors in $\mathbb{Z}$).*

Proof. We only need to prove that (8.5) is a necessary condition in statement (1) of the lemma. The rest follows easily from Proposition 5.1, Remark 5.2, and Theorem 8.2.

Assume $\mathbb{Z}^2$-actions Y_A, Y_B are conjugate. Hence, $G_A = G_B$ by Theorem 8.2 and eigenvalues μ_1, μ_2 of B belong to $\mathbb{Z}$ by Proposition 5.1. Assume λ_1 and μ_1 (resp., λ_2 and μ_2) have the same prime divisors in $\mathbb{Z}$ (by Proposition 5.1). By assumption, there is a prime $p \in \mathbb{Z}$ that divides λ_1 and does not divide λ_2. In particular, $\lambda_1 \neq \lambda_2$, $\mu_1 \neq \mu_2$, and both A, B are diagonalizable over $\mathbb{Q}$. As in Remark 5.2, there exist $P, Q \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$PAP^{-1} = \begin{pmatrix} \lambda_1 & * \\ 0 & \lambda_2 \end{pmatrix},\ QBQ^{-1} = \begin{pmatrix} \mu_1 & * \\ 0 & \mu_2 \end{pmatrix}.$$

Denote $PAP^{-1} = \Lambda$, $QBQ^{-1} = M$, $PQ^{-1} = S$. Then

$$G_\Lambda = P(G_A) = P(G_B) = G_{SMS^{-1}},$$

since $P \in \mathrm{GL}_2(\mathbb{Z})$ and $G_A = G_B$ by assumption. Thus, the identity $T = I_2$ is an isomorphism between G_Λ and $G_{SMS^{-1}}$ and by Proposition 4.1, the image under T of an eigenvector $\mathbf{u}$ of Λ corresponding to λ_1 is an eigenvector of SMS^{-1} corresponding to μ_1. Since we can take $\mathbf{u} = \mathbf{e}_1$ and $T = I_2$, this implies that the 1st column of S is a multiple of $\mathbf{e}_1$ and, hence, S is an upper triangular (non-singular) matrix. Therefore,

$$PBP^{-1} = SQBQ^{-1}S^{-1} = SMS^{-1} = \begin{pmatrix} \mu_1 & * \\ 0 & \mu_2 \end{pmatrix},$$

which proves (8.5). □

8.6. **Remaining cases.** We are left with the case when there is a prime $p \in \mathbb{Z}$ that divides $\det A$ and does not divide $\operatorname{Tr} A$ and either A has rational (equivalently, integer) eigenvalues λ_1, λ_2 such that

$$PD(\lambda_2) \not\subseteq PD(\lambda_1), \quad PD(\lambda_1) \not\subseteq PD(\lambda_2),$$

or the characteristic polynomial of A is irreducible (these are the assumptions of Theorem 6.1 above). Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular, let $\lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$ (resp., $\mu_1, \mu_2 \in \overline{\mathbb{Q}}$) denote eigenvalues of A (resp., B), and let $T \in \mathrm{GL}_2(\mathbb{Q})$ satisfy $T(G_A) = G_B$. Recall that by Theorem 6.1, we have

(8.6) $\mathbb{Q}(\lambda_1) = \mathbb{Q}(\mu_1)$ and λ_1, μ_1(resp., λ_2, μ_2) have the same prime divisors in the ring of integers of $K = \mathbb{Q}(\lambda_1) = \mathbb{Q}(\mu_1)$.

Moreover, both A and B are diagonalizable over $\overline{\mathbb{Q}}$ and there exist $M, N \in \mathrm{GL}_2(K)$ such that

$$A = M \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} M^{-1},\ B = N \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix} N^{-1}, \tag{8.7}$$

and $T = NM^{-1}$ by Proposition 4.1 and Remark 4.2. Assume G_A (resp., G_B) is dense in $\mathbb{Q}^2$. If $\mathbb{Z}^2$-actions Y_A, Y_B are conjugate (or isomorphic, or continuously orbit equivalent), then by Theorem 8.2, we have $T = I_2$ (or $T \in \mathrm{GL}_2(\mathbb{Z})$, or $\det T = \pm 1$) and, hence, $M = N$ (or $NM^{-1} \in \mathrm{GL}_2(\mathbb{Z})$, or $\det NM^{-1} = \pm 1$). This proves the following lemma:

Lemma 8.9. *Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular such that G_A (resp., G_B) is dense in $\mathbb{Q}^2$ (see Lemma 8.4). Assume A satisfies the assumptions of Theorem 6.1. If $\mathbb{Z}^2$-actions Y_A, Y_B are conjugate (or isomorphic, or continuously orbit equivalent), then (8.6) holds, there exist $M, N \in \mathrm{GL}_2(K)$ such that (8.7) holds, and $M = N$ (or $NM^{-1} \in \mathrm{GL}_2(\mathbb{Z})$, or $\det NM^{-1} = \pm 1$).*

It turns out that the conditions in Lemma 8.9 are also sufficient in the cases of conjugacy and isomorphism.

Lemma 8.10. *Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular such that G_A (resp., G_B) is dense in $\mathbb{Q}^2$ (see Lemma 8.4). Assume A satisfies the assumptions of Theorem 6.1.*

(i) If (8.6) holds and there exists $M \in \mathrm{GL}_2(K)$ such that (8.7) holds for $N = M$, then $\mathbb{Z}^2$-actions Y_A, Y_B are conjugate.

(ii) If (8.6) holds, there exist $M, N \in \mathrm{GL}_2(K)$ such that (8.7) holds, and $NM^{-1} \in \mathrm{GL}_2(\mathbb{Z})$, then $\mathbb{Z}^2$-actions Y_A, Y_B are isomorphic.

Proof. One can prove the lemma following the same steps as in the proof of Theorem 6.1. In addition, we also give a slightly different proof. First, (ii) follows easily from (i). Indeed, assume (8.6) and (8.7) hold and let $X = NM^{-1} \in \mathrm{GL}_2(\mathbb{Z})$. Then $XM = N$ and

$$G_{XAX^{-1}} = X(G_A) = G_{N\Lambda N^{-1}} = G_B, \quad \Lambda = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Here, $G_{XAX^{-1}} = X(G_A)$, since $X \in \mathrm{GL}_2(\mathbb{Z})$, and $G_{N\Lambda N^{-1}} = G_B$ by (i) and Theorem 8.2 (clearly, $G_{N\Lambda N^{-1}}$ is dense, since G_A is dense by assumption). Since $X(G_A) = G_B$ and $X \in \mathrm{GL}_2(\mathbb{Z})$, $\mathbb{Z}^2$-actions Y_A, Y_B are isomorphic by Theorem 8.2.

We now prove (i). Assume (8.6), (8.7) hold and $N = M$. Then A, B commute and by Lemma 6.4 applied to $T = I_2$, $P = A^k B^{-1}$, and $Q = B^l A^{-1}$, it is enough to show that there exist $k, l \in \mathbb{N}$ such that $A^k B^{-1}, B^l A^{-1} \in \mathrm{M}_2(\mathbb{Z})$. We show that $A^k B^{-1} \in \mathrm{M}_2(\mathbb{Z})$ for some $k \in \mathbb{N}$ and $B^l A^{-1} \in \mathrm{M}_2(\mathbb{Z})$ for some $l \in \mathbb{N}$ can be proved analogously. Note that $A^k B^{-1} \in \mathrm{M}_2(\mathbb{Z})$ if and only if $A^k B^{-1} \in \mathrm{M}_2(\mathbb{Z}_p)$ for any prime p that divides $\det B$.

Assume $p \in \mathbb{Z}$ is a prime that divides both $\det B$ and $\operatorname{Tr} B$. Note that (8.6) implies that p divides both $\det A$ and $\operatorname{Tr} A$. It follows from Cayley–Hamilton theorem that $A^2 = p \cdot C$ for a non-singular $C \in \mathrm{M}_2(\mathbb{Z})$. Then, clearly, there exists $k = k(p) \in \mathbb{N}$ such that

$$A^{2k} B^{-1} = p^k C^k B^{-1} \in \mathrm{M}_2(\mathbb{Z}_p).$$

Assume $p \in \mathbb{Z}$ is a prime that divides $\det B$ and does not divide $\operatorname{Tr} B$. Note that (8.6) implies that p divides $\det A$ and does not divide $\operatorname{Tr} A$. As in the proof of Theorem 6.1, K can be embedded into $\mathbb{Q}_p$ such that $\lambda_1, \mu_1 \in \mathbb{Z}_p^\times$ and $\lambda_2, \mu_2 \in p\mathbb{Z}_p$. Moreover, there exists $L \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that

$$A = L\Lambda L^{-1}.$$

Then $N = M$ implies

$$B = L \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix} L^{-1},$$

and hence

$$A^k B^{-1} = L \begin{pmatrix} \frac{\lambda_1^k}{\mu_1} & 0 \\ 0 & \frac{\lambda_2^k}{\mu_2} \end{pmatrix} L^{-1}.$$

Since $\lambda_1, \mu_1 \in \mathbb{Z}_p^\times$, $\lambda_2, \mu_2 \in p\mathbb{Z}_p$, and $L \in \mathrm{GL}_2(\mathbb{Z}_p)$, clearly, there is $k = k(p) \in \mathbb{N}$ such that $A^k B^{-1} \in \mathrm{M}_2(\mathbb{Z}_p)$.

Let k' be the maximum of all $k(p)$, where p runs through all the prime divisors of $\det B$. Then, by above, $A^{k'} B^{-1} \in \mathrm{M}_2(\mathbb{Z})$. Analogously, there exists l such that $B^l A^{-1} \in \mathrm{M}_2(\mathbb{Z})$. Hence, $T = I_2$ is an isomorphism between G_A and G_B by Lemma 6.4, and $\mathbb{Z}^2$-actions Y_A, Y_B are conjugate by Theorem 8.2. □

Remark 8.11. Assume the characteristic polynomial of A is irreducible. Then the condition $NM^{-1} \in \mathrm{GL}_2(\mathbb{Z})$ is equivalent to

$$I_{\mathbb{Z}}(A, \lambda_1) = x I_{\mathbb{Z}}(B, \mu_1) \text{ for } x \in K$$

(see Section 6.3 for the definition of $I_{\mathbb{Z}}(A, \lambda_1)$).

Remark 8.12. Note that $M = N$ implies A, B commute. However, $AB = BA$ does not imply conjugacy, since the ordering of eigenvalues matters. For example,

$$A = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, \; B = \begin{pmatrix} 5 & 0 \\ 0 & 3 \end{pmatrix},$$

and $G_A \neq G_B$.

Remark 8.13. It turns out that in the case of odometers Y_A defined by matrices $A \in \mathrm{M}_2(\mathbb{Z})$, continuous orbit equivalence is more subtle than conjugacy and isomorphism. The reason is that, in general, not every $T = NM^{-1}$ with $T \in \mathrm{GL}_2(\mathcal{R})$ and M, N satisfying (8.7) defines an isomorphism between G_A and G_B (see Remark 6.2). General sufficient conditions for $\mathbb{Z}^2$-actions Y_A, Y_B to be continuously orbit equivalent under the conditions of Theorem 6.1 become rather technical. However, it is possible to resolve the question in each particular case based on the techniques discussed above (see *e.g.*, Example 11 below).

We finish the section with examples of equivalent odometers of the form Y_A, $A \in \mathrm{M}_2(\mathbb{Z})$.

Example 9. Let

$$A = \begin{pmatrix} 0 & 4 \\ 2 & 0 \end{pmatrix}, \; B = \begin{pmatrix} 0 & 8 \\ 1 & 0 \end{pmatrix}.$$

In Example 3 above we showed that $G_A = G_B$. Hence, $\mathbb{Z}^2$-actions Y_A, Y_B are conjugate by Theorem 8.2. Moreover, for a non-singular $C \in \mathrm{M}_2(\mathbb{Z})$ such that G_C is dense in $\mathbb{Q}^2$ we have $\mathbb{Z}^2$-actions Y_A, Y_C are conjugate if and only if $G_A = G_C$ if and only if $\operatorname{Tr} C = 2k$ and $\det C = 2^l$ for some $k \in \mathbb{N} \cup \{0\}$, $l \in \mathbb{N}$ (by Lemma 8.7).

Example 10. Let

$$A = \begin{pmatrix} 2 & -2 \\ 4 & 8 \end{pmatrix},\ B = \begin{pmatrix} 13 & 5 \\ 11 & 7 \end{pmatrix}.$$

In Example 2 above we showed that there exists an isomorphism $T \in \mathrm{GL}_2(\mathbb{Z})$ from G_A to G_B. Thus, $\mathbb{Z}^2$-actions Y_A, Y_B are isomorphic by Theorem 8.2 and Lemma 8.4.

Example 11. Let

$$A = \begin{pmatrix} 0 & -6 \\ 1 & 1 \end{pmatrix},\ B = \begin{pmatrix} 0 & -3 \\ 2 & 1 \end{pmatrix},$$

$\operatorname{Tr} A = \operatorname{Tr} B = 1$, $\det A = \det B = 6$. We showed in Example 4 above that $G_A \cong G_B$. We now find an isomorphism $T \in \mathrm{GL}_2(\mathbb{Q})$ such that $T(G_A) = G_B$ and $\det T = 1$, so that $\mathbb{Z}^2$-actions Y_A, Y_B are continuously orbit equivalent by Theorem 8.2. Note that G_A (resp., G_B) is dense in $\mathbb{Q}^2$ by Lemma 8.4. Let

$$\Lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \sigma(\lambda) \end{pmatrix},\ M = \begin{pmatrix} -\sigma(\lambda) & -\lambda \\ 1 & 1 \end{pmatrix},$$
$$N = \begin{pmatrix} -\sigma(\lambda) & -\lambda \\ 2 & 2 \end{pmatrix},$$

where $\lambda = \frac{1+\sqrt{-23}}{2}$, $\sigma(\lambda) = \frac{1-\sqrt{-23}}{2}$ are common eigenvalues of A, B, and

$$A = M\Lambda M^{-1},\ B = N\Lambda N^{-1}.$$

Let $K = \mathbb{Q}(\lambda)$, let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be non-trivial, and let $T \in \mathrm{GL}_2(\mathbb{Q})$ be an isomorphism from G_A to G_B. By Remark 6.2, $T \in \mathrm{GL}_2(\mathcal{R})$ and

$$T = T(x) = N \begin{pmatrix} x & 0 \\ 0 & \sigma(x) \end{pmatrix} M^{-1}, \quad x \in K^\times. \tag{8.8}$$

In particular, when $x = \frac{3+\sqrt{-23}}{4}$, $\sigma(x) = \frac{3-\sqrt{-23}}{4}$, we have

$$T = \begin{pmatrix} 1/2 & -3 \\ 1 & 2 \end{pmatrix}. \tag{8.9}$$

One can verify that $T \in \mathrm{GL}_2(\mathcal{R})$, but $T(G_A) \neq G_B$. Let

$$T' = \frac{1}{2}T.$$

Then $T'(G_A) = G_B$ and $\det T' = 1$. Hence, $\mathbb{Z}^2$-actions Y_A, Y_B are continuously orbit equivalent by Theorem 8.2.

Example 12. Let

$$A = \begin{pmatrix} -1 & 3 \\ 3 & 2 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 11 & 1 \end{pmatrix},$$

$\det A = \det B = -11$, $\operatorname{Tr} A = \operatorname{Tr} B = 1$. By Lemma 8.4, G_A (resp., G_B) is dense in $\mathbb{Q}^2$. In Example 1 above we showed that G_A and G_B are not isomorphic. Hence, $\mathbb{Z}^2$-actions

Y_A, Y_B are not continuously orbit equivalent by Theorem 8.2. However, $\mathbb{Z}^2$-actions Y_A, Y_B are orbit equivalent by Lemma 8.6.

Appendix A. Similarity to a block-triangular matrix over PID

In this section we give a proof of the fact that a matrix A over a principal ideal domain R with field of fractions of characteristic zero is similar over R to a block-triangular matrix. This is proved in [N72, p. 50, Thm. III.12] for $R = \mathbb{Z}$ and the same proof works for a general principal ideal domain (PID) with field of fractions of characteristic zero. In particular, when $R = \mathbb{Z}_p$, the case of our interest. We repeat the proof here for completeness.

Theorem A.1. *Let R be a PID with field of fractions of characteristic zero and let $A \in \mathrm{M}_n(R)$. Then there exists $S \in \mathrm{GL}_n(R)$ such that*

$$SAS^{-1} = \begin{pmatrix} A_{11} & * & \cdots & * \\ 0 & A_{22} & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_{tt} \end{pmatrix},$$

where each A_{ii} is a square matrix with irreducible characteristic polynomial, $i \in \{1, 2, \ldots, t\}$, $1 \le t \le n$.

Proof. Let F denote the field of fractions of R and let $h_A \in R[t]$ denote the characteristic polynomial of A. If h_A is irreducible, there is nothing to prove. Assume h_A is not irreducible, *i.e.*, $h_A = h_1 h_2$, where $h_1, h_2 \in R[t]$ are monic, and h_1 is irreducible of degree k, $1 \le k < n$. Let $\overline{F}$ denote a fixed algebraic closure of F, let $\alpha \in \overline{F}$ be a root of h_1, and let $L = F(\alpha)$. Then L is a finite separable extension of F of degree k and let $\mathcal{O}$ denote the integral closure of R in L. It is known that $\mathcal{O}$ is a free R-module of rank k and hence there exists a basis $\omega_1, \ldots, \omega_k \in \mathcal{O}$ of $\mathcal{O}$ over R. Let $\mathbf{u} \in (\overline{F})^n$ be an eigenvector of A corresponding to α. Without loss of generality, we can assume that $\mathbf{u} \in \mathcal{O}^n$. Then

$$\mathbf{u} = C\omega, \quad \omega = \begin{pmatrix} \omega_1 & \ldots & \omega_k \end{pmatrix}^t$$

for some $C \in \mathrm{M}_{n\times k}(R)$. Also, there exists $B \in \mathrm{M}_k(R)$ such that $\alpha\omega = B\omega$. Then

$$A\mathbf{u} = AC\omega = \alpha C\omega = CB\omega$$

and hence $AC = CB$, since entries of $AC - CB$ belong to R and $\omega_1, \ldots, \omega_k$ are R-linearly independent. Since R is a PID, matrix C has a Smith normal form, *i.e.*, there exist $\lambda_1, \ldots, \lambda_r \in R - \{0\}$, $U \in \mathrm{GL}_n(R)$, and $V \in \mathrm{GL}_k(R)$ such that

$$C = UTV, \quad T = \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix},$$

where $T \in \mathrm{M}_{n\times k}(R)$, $\Lambda = \mathrm{diag}(\lambda_1, \ldots, \lambda_r) \in \mathrm{GL}_r(R)$ is a non-singular diagonal matrix, and $1 \leq r \leq k$. We write

$$U^{-1}AU = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix},$$

where $A_1 \in \mathrm{M}_r(R)$, and A_2, A_3, A_4 are matrices over R of appropriate sizes. It follows from $AC = CB$ that

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} V = \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} VB. \tag{A.1}$$

Thus, $A_3\Lambda = 0$, the zero $(n-r)\times r$-matrix, and since Λ is non-singular, we have $A_3 = 0$. We now show that α is an eigenvalue of A_1 and hence $k = r$. Indeed, multiplying (A.1) by ω on the right, we get

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} V\omega = \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} VB\omega = \alpha \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} V\omega, \tag{A.2}$$

since $B\omega = \alpha\omega$. Let $\mathbf{v} \in \mathrm{M}_{r\times 1}(L)$ denote the first r entries of $V\omega \in \mathrm{M}_{k\times 1}(L)$ and let $\mathbf{w} = \Lambda\mathbf{v}$. Note that $\mathbf{v}$ is non-zero, since ω is a basis and V is non-singular. Also, $\mathbf{w}$ is non-zero, since $\Lambda = \mathrm{diag}(\lambda_1, \ldots, \lambda_r)$ is non-singular. Then (A.2) implies

$$A_1\mathbf{w} = \alpha\mathbf{w}.$$

Since $\mathbf{w}$ is non-zero, α is an eigenvalue of A_1. Hence, $k = r$, h_1 is the characteristic polynomial of A_1, and h_2 is the characteristic polynomial of A_4. Applying the induction process on n, the statement of the theorem holds for $A_4 \in \mathrm{M}_{n-k}(R)$ and therefore holds for A. □

Corollary A.2. *Let R be a PID with field of fractions F of characteristic zero. Assume a non-singular $A \in \mathrm{M}_2(R)$ has eigenvalues $\lambda_1, \lambda_2 \in R$, $\lambda_1 \neq \lambda_2$. Then, there exists $S \in \mathrm{GL}_2(R)$ such that*

$$SAS^{-1} = M \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} M^{-1}, \quad M = \begin{pmatrix} 1 & u \\ 0 & v \end{pmatrix},\ u, v \in R,\ (u, v) = 1,\ v \,|\, (\lambda_1 - \lambda_2).$$

Proof. Since $\lambda_1, \lambda_2 \in R$, the characteristic polynomial h_A of A has the form

$$h_A(t) = (t - \lambda_1)(t - \lambda_2) \in R[t].$$

By Theorem A.1, there exists $S \in \mathrm{GL}_2(R)$ such that

$$SAS^{-1} = \begin{pmatrix} \lambda_1 & * \\ 0 & \lambda_2 \end{pmatrix}.$$

We now diagonalize matrix SAS^{-1}, namely, there exist $u, v \in R$ such that $v \neq 0$, and

$$SAS^{-1} = M \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} M^{-1}, \quad M = \begin{pmatrix} 1 & u \\ 0 & v \end{pmatrix} \in \mathrm{M}_2(R).$$

Clearly, without loss of generality, we can assume that u, v are coprime in R. Also, it is easy to check that $SAS^{-1} \in \mathrm{M}_2(R)$ implies that v divides $\lambda_1 - \lambda_2$. □

References

[ATW97] R. Adler, C. Tresser, P. A. Worfolk, *Topological conjugacy of linear endomorphisms of the 2-torus*, Trans. Amer. Math. Soc. 349 (1997), no. 4, 1633–1652.

[BLP19] J. Bergfalk, M. Lupini, A. Panagiotopoulos, *Definable (co)homology, pro-torus rigidity, and (co)homological classification*, September 2019.

[C] K. Conrad, *Ideal classes and matrix conjugation over* $\mathbb{Z}$, http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/matrixconj.pdf

[CHL13] A. Clark, S. Hurder, and O. Lukina, *Classifying matchbox manifolds*, Geom. Topol. 23 (2019), no. 1, 1–27.

[D30] D. van Dantzig, *Ueber topologisch homogene Kontinua*, Fundam. Math. 15 (1930), 102–125.

[GPS19] T. Giordano, I. Putnam, C. Skau, *$\mathbb{Z}^d$-odometers and cohomology*, Groups Geom. Dyn. 13 (2019), no. 3, 909–938.

[K13] J. Klaise, *Orders in quadratic imaginary fields of small class number*, 2013.

[M65] M. C. McCord, *Inverse limit sequences with covering maps*, Trans. Amer. Math. Soc. 114, 1965, 197–209.

[N99] J. Neukirch, Algebraic number theory. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999.

[N72] M. Newman, *Integral matrices*, Pure and Applied Mathematics, Vol. 45. Academic Press, New York-London, 1972.

[T49] O. Taussky, *On a theorem of Latimer and MacDuffee*, Canad. J. Math. 1 (1949), 300–302.

[V27] L. Vietoris, *Über den höheren Zusammenhang kompakter Räume und eine Klasse von zusammenhangstreuen Abbildungen*, Math. Ann. 97 (1927), no. 1, 454–472.

[W04] M. Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. 73 (2004), no. 246, 907–938.

Department of Mathematics, CUNY Queens College, 65-30 Kissena Blvd., Flushing, NY 11367, USA

Email address: Maria.Sabitova@qc.cuny.edu