A NUMBER THEORETIC CLASSIFICATION OF TOROIDAL SOLENOIDS

MARIA SABITOVA

Abstract. We classify toroidal solenoids defined by non-singular $n \times n$-matrices A with integer coefficients by studying associated first Čech cohomology groups. In a previous work, we classified the groups in the case $n = 2$ using generalized ideal classes in the splitting field of the characteristic polynomial of A. In this paper we explore the classification problem for an arbitrary n.

1. Introduction

The goal of this paper is to classify toroidal solenoids defined by non-singular matrices with integer coefficients as introduced by M. C. McCord in 1965 [M65]. More precisely, 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 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 inverse limit 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 [D37]. 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]). In [S22] and the present work, we employ a number-theoretic approach to solving the problem.

It is known that the first Čech cohomology group $H^1(\mathcal{S}_A, \mathbb{Z})$ of $\mathcal{S}_A$ is isomorphic to a subgroup G_{A^t} of $\mathbb{Q}^n$ defined by the transpose A^t of A as follows:

$$G_{A^t} = \left\{ (A^t)^{-k}\mathbf{x} \;\middle|\; \mathbf{x} \in \mathbb{Z}^n,\ k \in \mathbb{Z} \right\}.$$

Date: August 12, 2022.

On the other hand, since $\mathcal{S}_A$ is a compact connected abelian group, $H^1(\mathcal{S}_A, \mathbb{Z})$ is isomorphic to the character group $\widehat{\mathcal{S}_A}$ of $\mathcal{S}_A$. Thus, for a non-singular $B \in \mathrm{M}_n(\mathbb{Z})$, using Pontryagin duality theorem, we see that $\mathcal{S}_A$, $\mathcal{S}_B$ are isomorphic as topological groups if and only if G_{A^t}, G_{B^t} are isomorphic as abstract groups. Therefore, we study isomorphism classes of groups of the form G_A, where $A \in \mathrm{M}_n(\mathbb{Z})$ is non-singular.

If $n = 1$, we have $A, B \in \mathbb{Z}$ and G_A, G_B are isomorphic if and only if A, B have the same prime divisors. Note that if A, B are conjugate by a matrix in $\mathrm{GL}_n(\mathbb{Z})$, then clearly G_A, G_B are isomorphic (notationally, $G_A \cong G_B$). However, the converse is not true. In general, the class of matrices $A, B \in \mathrm{M}_n(\mathbb{Z})$ with isomorphic groups G_A, G_B is much larger than the class of $\mathrm{GL}_n(\mathbb{Z})$-conjugate matrices. We have an example, where given an irreducible polynomial $h \in \mathbb{Z}[x]$, there are three $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of matrices with integer coefficients and characteristic polynomial h, but all three classes constitute just one class of isomorphic groups of the form G_A [S22, Example 4]. It might also happen that $G_A \cong G_B$, but A, B do not even share the same characteristic polynomial, so that A, B are not conjugate by a matrix in $\mathrm{GL}_n(\mathbb{Q})$ (see *e.g.*, [S22, Example 2]). In [S22] we classified groups G_A in the case $n = 2$. In the generic case, *i.e.*, when the characteristic polynomial of A is irreducible, we linked G_A to a generalized ideal class generated by an eigenvector of A in the splitting field of the characteristic polynomial of A. We showed 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. It turns out that this is no longer true when $n > 2$. In this paper, we finish the classification of groups G_A (and hence, the associated toroidal solenoids $\mathcal{S}_A$) for an arbitrary n. We provide necessary and sufficient conditions for $G_A \cong G_B$ for any $A, B \in \mathrm{M}_n(\mathbb{Z})$ and consider special cases as well. In particular, we formulate sufficient conditions under which $G_A \cong G_B$ if and only if the corresponding ideal classes are multiples of each other. We give examples illustrating how our theorems can be used to check whether $G_A \cong G_B$ for given $A, B \in \mathrm{M}_n(\mathbb{Z})$ in practice. We also consider applications of the obtained results to the class of $\mathbb{Z}^n$-odometers defined by matrices $A \in \mathrm{M}_n(\mathbb{Z})$.

Acknowledgements. The author thanks Mario Bonk for suggesting the problem and useful discussions. Support for this project was provided by PSC-CUNY Awards TRADA-51-133, TRADB-53-92 jointly funded by The Professional Staff Congress and The City University of New York.

2. Localization

For a non-singular $n \times n$-matrix A with integer coefficients, $A \in \mathrm{M}_n(\mathbb{Z})$, define

$$G_A = \left\{ A^{-k}\mathbf{x} \,\middle|\, \mathbf{x} \in \mathbb{Z}^n,\, k \in \mathbb{Z} \right\}, \quad \mathbb{Z}^n \subseteq G_A \subseteq \mathbb{Q}^n. \tag{2.1}$$

One can readily check that G_A is a subgroup of $\mathbb{Q}^n$.

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

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; m, n \in \mathbb{Z},\ n \neq 0,\ (p, n) = 1 \right\},$$

a subring of $\mathbb{Q}$. (Here (p, n) denotes the greatest common divisor of p and n.) Let $\mathbb{Q}_p$ denote the field of p-adic numbers with the subgring of p-adic integers $\mathbb{Z}_p$. For $N = \det A$, $N \in \mathbb{Z}$, $N \neq 0$, let

$$\mathcal{R} = \mathbb{Z}\left[\frac{1}{N}\right] = \left\{ \frac{m}{N^k} \;\middle|\; m, k \in \mathbb{Z} \right\} \tag{2.2}$$

be the ring of N-adic rationals.

Remark 2.1. Note that G_A is a (additive) subgroup of $\mathcal{R}^n$, since $A^{-k} = \frac{1}{(\det A)^k}\tilde{A}$, $k \in \mathbb{N}$, with $\tilde{A} \in \mathrm{M}_n(\mathbb{Z})$. However, $G_A \neq \mathcal{R}^n$ in general.

Lemma 2.2. *For a prime $p \in \mathbb{N}$ denote $G_{A,p} = G_A \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. Then*

$$G_A = \bigcap_p G_{A,p} = \mathcal{R}^n \bigcap_{p \,|\, \det A} G_{A,p}.$$

Here $G_{A,p}$ is considered as a subset of $\mathbb{Q}^n$.

Proof. See [F73, p. 183, Lemma 93.1] for the first equality, which holds for any abelian subgroup of $\mathbb{Q}^n$ and, more generally, for an abelian torsion free group of at most countable rank. Hence, taking into account Remark 2.1, we have $G_A \subseteq \mathcal{R}^n \bigcap_{p \,|\, \det A} G_{A,p}$. The opposite inclusion is proved as in *loc.cit.* Namely, let $x \in \mathcal{R}^n \bigcap_{p \,|\, \det A} G_{A,p}$. Then

$$x = \sum x_i a_i, \quad x_i \in \mathbb{Z}_{(p)},\ a_i \in G_A,$$

and there exists $s \in \mathbb{Z}$ coprime with p such that $sx \in G_A$. Since $x \in \mathcal{R}^n$, there exists a power of N such that $N^k x \in \mathbb{Z}^n$, $k \in \mathbb{N}$, $N = \det A$. Let $p_1, p_2, \ldots, p_l \in \mathbb{N}$ be all the prime divisors of N. Since $x \in \bigcap_{p \,|\, \det A} G_{A,p}$, by above, for each p_i there exists $s_i \in \mathbb{Z}$ coprime with p_i such that $s_i x \in G_A$. Since $N^k, s_1, s_2, \ldots, s_l$ are coprime and $\mathbb{Z}^n \subset G_A$, we have $x \in G_A$. □

For a prime $p \in \mathbb{N}$ denote $\overline{G}_{A,p} = G_A \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Naturally, $\mathbb{Z}_p^n \subseteq \overline{G}_{A,p} \subseteq \mathbb{Q}_p^n$.

Lemma 2.3. *Let $\overline{G}_{A,p} = G_A \otimes_{\mathbb{Z}} \mathbb{Z}_p$, $G_{A,p} = G_A \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. Then*

$$\mathbb{Q}^n \cap \overline{G}_{A,p} = G_{A,p},$$

where $\mathbb{Q}^n \hookrightarrow \mathbb{Q}_p^n$, and the intersection is in $\mathbb{Q}_p^n$.

Proof. See [F73, p. 183, Lemma 93.2], [D37]. It is proved there that if G is an abelian torsion free group of at most countable rank, then

$$(G \otimes_{\mathbb{Z}} \mathbb{Q}) \cap (G \otimes_{\mathbb{Z}} \mathbb{Z}_p) = G \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}.$$

Apply the result to $G = G_A$ and note that $G_A \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}^n$. □

Corollary 2.4.

$$G_A = \bigcap_p (\mathbb{Q}^n \cap \overline{G}_{A,p}) = \bigcap_{p \,|\, \det A} (\mathcal{R}^n \cap \overline{G}_{A,p}).$$

Proof. Follows from Lemma 2.2 and Lemma 2.3. □

Proposition 2.5. [S22, Prop. 3.8] *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular, let $h_A \in \mathbb{Z}[x]$ be the characteristic polynomial of A, and let $p \in \mathbb{Z}$ be prime. Let $t_p = t_p(A)$ denote the multiplicity of zero in the reduction of h_A modulo p, $0 \le t_p \le n$. Then, as $\mathbb{Z}_p$-modules,*

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

In particular,

(1) *p does not divide* $\det A$ *if and only if* $\overline{G}_{A,p} = \mathbb{Z}_p^n$;

(2) $h_A \equiv x^n \,(mod\ p)$ *if and only if* $\overline{G}_{A,p} = \mathbb{Q}_p^n$.

Thus,

$$\overline{G}_{A,p} = D_p(A) \oplus R_p(A), \tag{2.3}$$

where $D_p(A) \cong \mathbb{Q}_p^{t_p}$ denotes a divisible part of $\overline{G}_{A,p}$ and $R_p(A) \cong \mathbb{Z}_p^{n-t_p}$ denotes a reduced $\mathbb{Z}_p$-submodule of $\overline{G}_{A,p}$. Let

$$\det A = a p_1^{s_1} p_2^{s_2} \cdots p_l^{s_l}$$

be the prime-power factorization of $\det A$, where $p_1, p_2, \ldots, p_l \in \mathbb{N}$ are distinct primes, $a = \pm 1$, and $s_1, s_2, \ldots, s_l \in \mathbb{N}$. Let

$$\mathcal{P} = \mathcal{P}(A) = \{p_1, p_2, \ldots, p_l\}.$$

The case $\mathcal{P} = \emptyset$, equivalently, $A \in \mathrm{GL}_n(\mathbb{Z})$, has been settled as follows:

Lemma 2.6. [S22, Lemma 3.2] *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular.*

(*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* $\mathbb{Z}$).

Therefore, for the rest of the paper we assume $\mathcal{P} \neq \emptyset$. Denote

$$\mathcal{P}' = \mathcal{P}'(A) \;\; = \;\; \{p \in \mathcal{P},\ h_A \not\equiv x^n \,(\mathrm{mod}\ p)\},$$

where $h_A \in \mathbb{Z}[x]$ denotes the characteristic polynomial of A. The case $\mathcal{P}' = \emptyset$ has been settled as well.

Lemma 2.7. [S22, Lemma 3.10] *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let $h_A, h_B \in \mathbb{Z}[x]$ be their respective characteristic polynomials. Assume that for any prime $p \in \mathbb{N}$ that divides* $\det A$ *we have*

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

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

Therefore, for the rest of the paper we assume $\mathcal{P}' \neq \emptyset$.

Remark 2.8. By Proposition 2.5, for non-singular $A, B \in \mathrm{M}_n(\mathbb{Z})$, if $G_A \cong G_B$, then $\mathcal{P}(A) = \mathcal{P}(B)$, $\mathcal{P}'(A) = \mathcal{P}'(B)$, and $t_p(A) = t_p(B)$ for any prime $p \in \mathbb{N}$. The converse is not true (see *e.g.*, [S22, Example 1], where non-singular $A, B \in \mathrm{M}_2(\mathbb{Z})$ share the same characteristic polynomial, but G_A is not isomorphic to G_B).

Corollary 2.9.

$$G_A = \bigcap_{p \in \mathcal{P}'} (\mathcal{R}^n \cap \overline{G}_{A,p}).$$

Proof. Follows from Corollary 2.4, since

$$\overline{G}_{A,p} = \mathbb{Q}_p^n \quad \text{for any } p \in \mathcal{P} \backslash \mathcal{P}'$$

by Proposition 2.5. ∎

The following lemma provides an explicit basis for the decomposition of $\overline{G}_{A,p}$ as in (2.3). Let $t_p = t_p(A)$ denote the multiplicity of zero in the reduction of the characteristic polynomial of A modulo p, $0 \leq t_p \leq n$. Let

$$\mathbb{Z}(p^\infty) = \mathbb{Q}_p / \mathbb{Z}_p$$

denote the Prüfer p-group.

Lemma 2.10. *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. For any $p \in \mathcal{P}$ there exists $W_p \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that*

$$W_p^{-1} A W_p = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}, \tag{2.4}$$

where $A_1 \in \mathrm{M}_{t_p}(\mathbb{Z}_p)$, $A_2 \in \mathrm{GL}_{n-t_p}(\mathbb{Z}_p)$, and A_1 has characteristic polynomial $h_1 \in \mathbb{Z}_p[x]$ with

$$h_1 \equiv x^{t_p} \, (mod \; p). \tag{2.5}$$

Let $W_p = \begin{pmatrix} \mathbf{w}_{p1} & \dots & \mathbf{w}_{pn} \end{pmatrix}$, where $\mathbf{w}_{p1}, \dots, \mathbf{w}_{pn} \in \mathbb{Z}_p^n$. Then

$$D_p(A) = \mathrm{Span}_{\mathbb{Q}_p}(\mathbf{w}_{p1}, \dots, \mathbf{w}_{pt_p}) \cong \mathbb{Q}_p^{t_p}, \tag{2.6}$$

$$R_p(A) = \mathrm{Span}_{\mathbb{Z}_p}(\mathbf{w}_{pt_p+1}, \dots, \mathbf{w}_{pn}) \cong \mathbb{Z}_p^{n-t_p}. \tag{2.7}$$

In particular,

$$\overline{G}_{A,p} / \mathbb{Z}_p^n \cong \mathbb{Z}(p^\infty)^{t_p}. \tag{2.8}$$

Proof. One can show that for an irreducible polynomial $\chi \in \mathbb{Z}_p[x]$ of degree n, either p does not divide $\chi(0)$ or $\chi \equiv x^n \, (\mathrm{mod}\; p)$ (see, *e.g.*, the proof of [S22, Prop. 3.8]). Therefore, the existence of $W_p \in \mathrm{GL}_n(\mathbb{Z}_p)$ satisfying (2.4) and (2.5) follows from Theorem 9.1 below. Moreover, the proof of Theorem 9.1 gives an algorithm to construct W_p. Let $\tilde{A} = W_p^{-1} A W_p$, $\tilde{A} \in \mathrm{M}_n(\mathbb{Z}_p)$, and

$$G_{\tilde{A}} = \left\{ \tilde{A}^{-k} \mathbf{x} \;\middle|\; \mathbf{x} \in \mathbb{Z}_p^n, \, k \in \mathbb{Z} \right\} = \mathbb{Q}_p \mathbf{e}_1 \oplus \dots \oplus \mathbb{Q}_p \mathbf{e}_{t_p} \oplus \mathbb{Z}_p \mathbf{e}_{t_p+1} \oplus \dots \oplus \mathbb{Z}_p \mathbf{e}_n,$$

i.e., with respect to the standard basis $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ of $\mathbb{Q}_p^n$,

$$G_{\tilde{A}} = \mathbb{Q}_p^{t_p} \oplus \mathbb{Z}_p^{n-t_p}$$

(this follows, *e.g.*, from Proposition 2.5 applied to A_1 and A_2). Since $W_p \in \mathrm{GL}_n(\mathbb{Z}_p)$, we have $\overline{G}_{A,p} = W_p(G_{\tilde{A}})$ and $\{W_p\mathbf{e}_1, \dots, W_p\mathbf{e}_n\}$ is a free $\mathbb{Z}_p$-basis of $\mathbb{Z}_p^n$, $\mathbf{w}_{pi} = W_p\mathbf{e}_i$, $1 \le i \le n$. Hence, (2.6) – (2.8) follow. □

3. Minimax groups

Definition 3.1. [GM81] A torsion-free abelian group G of rank n is called a *minimax* group if there exists a free subgroup H of G of rank n such that

$$G/H \cong \bigoplus_{i=1}^{l} \mathbb{Z}(p_i^\infty)^{t_i},$$

where $p_1, p_2, \dots, p_l \in \mathbb{N}$ are distinct primes and $t_1, t_2, \dots, t_l \in \mathbb{N}$.

Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. We show that G_A defined by (2.1) is a minimax group in the lemma below. Let $h_A \in \mathbb{Z}[x]$ denote the characteristic polynomial of A.

Lemma 3.2. *G_A is a minimax group. Namely,*

$$G_A/\mathbb{Z}^n \cong \bigoplus_{i=1}^{l} \mathbb{Z}(p_i^\infty)^{t_i},$$

where $p_1, p_2, \dots, p_l \in \mathbb{N}$ are all distinct prime divisors of $\det A$*, and t_i is the multiplicity of zero in the reduction of h_A modulo p_i, $0 < t_i \le n$, $1 \le i \le l$.*

Proof. Let $p \in \mathbb{N}$ be prime, and 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

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

Let

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

be the natural isomorphism induced by ϕ. It restricts to an isomorphism

$$\psi_A : \bigoplus_p \overline{G}_{A,p}/\mathbb{Z}_p^n \xrightarrow{\sim} G_A/\mathbb{Z}^n.$$

Indeed, recall that A has integer entries and therefore, multiplication by A^i commutes with ψ for any non-negative integer i. Furthermore, $\mathbf{u} \in \overline{G}_{A,p}$ (resp., $\mathbf{v} \in G_A$) if and only if $A^k\mathbf{u} \in \mathbb{Z}_p^n$ (resp., $A^k\mathbf{v} \in \mathbb{Z}^n$) for some $k \in \mathbb{N} \cup \{0\}$. Finally, $\overline{G}_{A,p}/\mathbb{Z}_p^n$ is trivial for any p

that does not divide $\det A$ by Proposition 2.5. Therefore, ψ_A is an isomorphism between the following groups

$$\psi_A : \bigoplus_{i=1}^{l} \overline{G}_{A,p_i}/\mathbb{Z}_{p_i}^n \xrightarrow{\sim} G_A/\mathbb{Z}^n. \tag{3.1}$$

Combined with (2.8), this proves the lemma. □

Using Lemma 2.10 and isomorphism ψ_A in (3.1), one can now write down (infinitely many) group generators of G_A (*c.f.*, [GM81]).

Lemma 3.3. *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. For each $p \in \mathcal{P}'$, let*

$$W_p = \begin{pmatrix} \mathbf{w}_{p1} & \dots & \mathbf{w}_{pn} \end{pmatrix}$$

be as in Lemma 2.10, $\mathbf{w}_{pj} \in \mathbb{Z}_p^n$, $1 \le j \le n$. Then

$$G_A = < \mathbf{e}_1, \dots, \mathbf{e}_n, q^{-\infty}\mathbf{e}_1, \dots, q^{-\infty}\mathbf{e}_n, p^{-\infty}\mathbf{w}_{p1}, \dots, p^{-\infty}\mathbf{w}_{pt_p} >, \tag{3.2}$$

i.e., G_A is generated over $\mathbb{Z}$ by $\mathbf{e}_1, \dots, \mathbf{e}_n$, $q^{-s}\mathbf{e}_1, \dots, q^{-s}\mathbf{e}_n$, and $p^{-k}\mathbf{w}_{pi}^{(k)}$, where $\mathbf{w}_{pi}^{(k)}$ is the $(k-1)$-st partial sum of the standard p-adic expansion of $\mathbf{w}_{pi}$, $k, s \in \mathbb{N}$, $1 \le i \le t_p$, $q \in \mathcal{P} \backslash \mathcal{P}'$, $p \in \mathcal{P}'$.

Proof. Let $h_A \in \mathbb{Z}[x]$ denote the characteristic polynomial of A. Let $q \in \mathcal{P} \backslash \mathcal{P}'$, *i.e.*, $q \in \mathbb{N}$ is a prime such that

$$h_A \equiv x^n \pmod{q}, \quad t_q = n.$$

By Proposition 2.5, we have $\overline{G}_{A,q} = \mathbb{Q}_q^n$. Then $\overline{G}_{A,q}$ is generated over $\mathbb{Z}_q$ by $\mathbf{e}_1, \dots, \mathbf{e}_n$, $q^{-s}\mathbf{e}_1, \dots, q^{-s}\mathbf{e}_n$, where $s \in \mathbb{N}$, *i.e.*, in our notation,

$$\overline{G}_{A,q} = \mathrm{Span}_{\mathbb{Z}_q}(\mathbf{e}_1, \dots, \mathbf{e}_n, q^{-\infty}\mathbf{e}_1, \dots, q^{-\infty}\mathbf{e}_n). \tag{3.3}$$

For $p \in \mathcal{P}'$, by (2.6), (2.7), $\overline{G}_{A,p}$ is generated over $\mathbb{Z}_p$ by $\mathbf{e}_1, \dots, \mathbf{e}_n$, $p^{-k}\mathbf{w}_{pi}$, where $k \in \mathbb{N}$, *i.e.*,

$$\overline{G}_{A,p} = \mathrm{Span}_{\mathbb{Z}_p}(\mathbf{e}_1, \dots, \mathbf{e}_n, p^{-\infty}\mathbf{w}_{p1}, \dots, p^{-\infty}\mathbf{w}_{pt_p}). \tag{3.4}$$

Applying isomorphism ψ_A in (3.1) to the generators of $\overline{G}_{A,p}$ in (3.3) and (3.4), we get (3.2). □

Generators of G_A in (3.2) are written in terms of the standard basis $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ and vectors $\{\mathbf{w}_{p1}, \dots, \mathbf{w}_{pn}\}$, $p \in \mathcal{P}'$. In what follows, we show the existence of a free basis $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ of $\mathbb{Z}^n$ (that does not depend on p) and p-adic integers $\alpha_{pij} \in \mathbb{Z}_p$ with $1 \le i \le t_p$, $t_p + 1 \le j \le n$, $p \in \mathcal{P}'$, that determine generators of G_A. It is often useful to extend constants from $\mathbb{Q}$ to a number field K, a finite extension of $\mathbb{Q}$, *i.e.*, to consider $G_A \otimes_{\mathbb{Z}} \mathcal{O}_K$, where $\mathcal{O}_K$ denotes the ring of integers of K (see Remark 4.4 below). Therefore, we start with a preliminary result, which holds over K.

Lemma 3.4. *Let $\mathcal{S}$ be a finite set of primes in $\mathbb{N}$, let K be a number field, and $n \in \mathbb{N}$. For each $p \in \mathcal{S}$ let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above p and let $V_\mathfrak{p}$ denote a non-zero proper subspace of $K_\mathfrak{p}^n$, where $K_\mathfrak{p}$ is the completion of K with respect to $\mathfrak{p}$, $\dim V_\mathfrak{p} = t_p$, $0 < t_p < n$. There exists a basis $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ of $\mathbb{Z}^n$ such that for any $p \in \mathcal{S}$ there are $\alpha_{pij} \in \mathcal{O}_\mathfrak{p}$, $1 \leq i \leq t_p < j \leq n$, such that*

$$\mathbf{x}_{pi} = \mathbf{f}_i + \sum_{j=t_p+1}^{n} \alpha_{pij}\mathbf{f}_j, \quad 1 \leq i \leq t_p, \tag{3.5}$$

is a $K_\mathfrak{p}$-basis of $V_\mathfrak{p}$. (Here, $\mathcal{O}_\mathfrak{p}$ denotes the ring of integers of $K_\mathfrak{p}$.)

Proof. It is a straightforward generalization of [GM81, p. 194, Lemma 1] from $\mathbb{Q}$ to a number field. We repeat their argument in order to use later in specific examples. The argument does not depend on the choice of prime ideals $\mathfrak{p}$. Therefore, for simplicity, we denote $\mathcal{O}_p = \mathcal{O}_\mathfrak{p}$, $K_p = K_\mathfrak{p}$, $V_p = V_\mathfrak{p}$, and so on.

For a fixed $p \in \mathcal{S}$ let $\mathbf{y}_{p1}, \ldots, \mathbf{y}_{pt_p}$ be a K_p-basis of V_p. Let (π) be the maximal ideal of $\mathcal{O}_p$. Let

$$\mathbf{y}_{pi} = \sum_{k=1}^{n} \gamma_{pi}^k \mathbf{e}_k,$$

where $\forall \gamma_{pi}^k \in K_p$. By multiplying or dividing by positive powers of π if necessary, without loss of generality, we can assume that $\forall \gamma_{pi}^k \in \mathcal{O}_p$ and for $\forall i$ there is a unit among $\gamma_{pi}^1, \ldots, \gamma_{pi}^n$. Let $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ be an ordered basis of $\mathbb{Z}^n$ obtained by permuting elements in the standard basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, so that

$$\mathbf{y}_{p1} = \sum_{k=1}^{n} \delta_{p1}^k \mathbf{f}_k, \quad \delta_{p1}^1 \in \mathcal{O}_p^\times. \tag{3.6}$$

Here $\mathcal{O}_p^\times$ denotes the set of all units in $\mathcal{O}_p$. Now we show that, without loss of generality, we can assume $\delta_{q1}^1 \in \mathcal{O}_q^\times$ for any $q \in \mathcal{S}$ other than p. Indeed, denote by Γ the set of all primes $q \in \mathcal{S}$ such that $\delta_{q1}^1 \in \mathcal{O}_q^\times$. By (3.6), $\Gamma \neq \emptyset$ and let

$$t = \prod_{p \in \Gamma} p. \tag{3.7}$$

Let $s \in \mathcal{S} \backslash \Gamma$, *i.e.*, $\delta_{s1}^1 \in \mathcal{O}_s$ is not a unit. By assumption, there is $j \in \{2, \ldots, n\}$ such that $\delta_{s1}^j \in \mathcal{O}_s^\times$. Consider $\mathbf{f}_j' = \mathbf{f}_j - t\mathbf{f}_1$ and $\mathbf{f}_i' = \mathbf{f}_i$ for any $i \neq j$, $1 \leq i \leq n$. Then, with respect to the new basis $\{\mathbf{f}_1', \ldots, \mathbf{f}_n'\}$ of $\mathbb{Z}^n$, we have

$$\mathbf{y}_{p1} = \sum_{k=1}^{n} \tilde{\delta}_{p1}^k \mathbf{f}_k', \quad \tilde{\delta}_{p1}^1 \in \mathcal{O}_p^\times$$

for any $p \in \Gamma$ and $p = s$. We now add s to Γ and change t in (3.7) to ts. Repeating the process for the remaining elements in $\mathcal{S} \backslash \Gamma$, we obtain a basis $\{\mathbf{f}_1'', \ldots, \mathbf{f}_n''\}$ of $\mathbb{Z}^n$ such that for any $p \in \mathcal{S}$ we have

$$\mathbf{y}_{pi} = \sum_{k=1}^{n} \epsilon_{pi}^{k} \mathbf{f}_k'', \quad \epsilon_{p1}^1 \in \mathcal{O}_p^\times, \quad \epsilon_{pi}^2, \dots, \epsilon_{pi}^n \in \mathcal{O}_p, \quad 1 \le i \le t_p.$$

By dividing $\mathbf{y}_{p1}$ by ϵ_{p1}^1, without loss of generality, $\epsilon_{p1}^1 = 1$. Let $\mathcal{S}' = \{p \in \mathcal{S},\ t_p \ge 2\}$. For any $p \in \mathcal{S}'$ and $2 \le i \le t_p$, let $\tilde{\mathbf{y}}_{pi} = \mathbf{y}_{pi} - \epsilon_{pi}^1 \mathbf{y}_{p1}$. Then

$$\tilde{\mathbf{y}}_{pi} \in \operatorname{Span}_{\mathcal{O}_p}(\mathbf{f}_2'', \dots, \mathbf{f}_n''), \quad 2 \le i \le t_p,\ p \in \mathcal{S}'.$$

Applying induction to vectors $\tilde{\mathbf{y}}_{pi}$, $2 \le i \le t_p$, $p \in \mathcal{S}'$, we get a free $\mathbb{Z}$-basis $\{\mathbf{g}_2, \dots, \mathbf{g}_n\}$ of $\operatorname{Span}_{\mathbb{Z}}(\mathbf{f}_2'', \dots, \mathbf{f}_n'')$ such that

$$\hat{\mathbf{y}}_{pi} = \mathbf{g}_i + \sum_{j=t_p+1}^{n} \mu_{pi}^{j} \mathbf{g}_j, \quad \mu_{pi}^{t_p+1}, \dots, \mu_{pi}^{n} \in \mathcal{O}_p,\ 2 \le i \le t_p,$$
$$\operatorname{Span}_{\mathcal{O}_p}(\tilde{\mathbf{y}}_{p2}, \dots, \tilde{\mathbf{y}}_{pt_p}) = \operatorname{Span}_{\mathcal{O}_p}(\hat{\mathbf{y}}_{p2}, \dots, \hat{\mathbf{y}}_{pt_p}),\ p \in \mathcal{S}'.$$

Finally, for any $p \in \mathcal{S}$ let

$$\tilde{\mathbf{y}}_{p1} = \mathbf{f}_1'' + \sum_{k=2}^{n} \mu_{p1}^{k} \mathbf{g}_k, \quad \mu_{p1}^2, \dots, \mu_{p1}^n \in \mathcal{O}_p,$$
$$\hat{\mathbf{y}}_{p1} = \tilde{\mathbf{y}}_{p1} - \sum_{k=2}^{t_p} \mu_{p1}^{k} \hat{\mathbf{y}}_{pk} = \mathbf{f}_1'' + \sum_{j=t_p+1}^{n} \tilde{\mu}_{p1}^{j} \mathbf{g}_j.$$

Hence, with respect to the $\mathbb{Z}$-basis $\{\mathbf{f}_1'', \mathbf{g}_2, \dots, \mathbf{g}_n\}$, $\mathbf{x}_{pi} = \hat{\mathbf{y}}_{pi}$, $1 \le i \le t_p$, $p \in \mathcal{S}$, have the form (3.5). □

In the next lemma we apply Lemma 3.4 to divisible parts of $\overline{G}_{A,p}$ and more generally, to the divisible parts of $\overline{G}_{A,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}}$. The result is a free basis $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ of $\mathbb{Z}^n$ and numbers $\alpha_{pij} \in \mathbb{Z}_p$, $p \in \mathcal{P}'(A)$, that produce generators of G_A over $\mathbb{Z}$.

Lemma 3.5. *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let K be a number field. There exists a basis $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ of $\mathbb{Z}^n$ such that for any $p \in \mathcal{P}'(A)$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p there are $\alpha_{pij} \in \mathcal{O}_{\mathfrak{p}}$, $i \in \{1, \dots, t_p\}$, $j \in \{t_p+1, \dots, n\}$, such that*

$$\overline{G}_{A,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}} = \operatorname{Span}_{K_{\mathfrak{p}}}(\mathbf{x}_{p1}, \dots, \mathbf{x}_{pt_p}) \oplus \operatorname{Span}_{\mathcal{O}_{\mathfrak{p}}}(\mathbf{f}_{t_p+1}, \dots, \mathbf{f}_n), \tag{3.8}$$

$$\mathbf{x}_{pi} = \mathbf{f}_i + \sum_{j=t_p+1}^{n} \alpha_{pij} \mathbf{f}_j, \quad 1 \le i \le t_p. \tag{3.9}$$

Moreover, all α_{pij} belong to $\mathbb{Z}_p$, they do not depend on K, $\mathfrak{p}$ above p, and are uniquely defined for a fixed ordered basis $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$. Furthermore,

$$G_A = < \mathbf{f}_1, \dots, \mathbf{f}_n, q^{-\infty}\mathbf{f}_1, \dots, q^{-\infty}\mathbf{f}_n, p^{-\infty}\mathbf{x}_{pi} >, \quad q \in \mathcal{P} \backslash \mathcal{P}', \quad 1 \le i \le t_p. \tag{3.10}$$

Proof. By Lemma 2.3, $\overline{G}_{A,p} = D_p(A) \oplus R_p(A)$, where as $\mathbb{Z}_p$-modules, $D_p(A) \cong \mathbb{Q}_p^{t_p}$, $R_p(A) \cong \mathbb{Z}_p^{n-t_p}$. Denote

$$\begin{aligned} \overline{G}_{\mathfrak{p}} &= \overline{G}_{A,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}}, \\ D_{\mathfrak{p}} &= D_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}}, \\ R_{\mathfrak{p}} &= R_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}}. \end{aligned}$$

Then $\overline{G}_{\mathfrak{p}} = D_{\mathfrak{p}} \oplus R_{\mathfrak{p}}$, where as $\mathcal{O}_{\mathfrak{p}}$-modules, $D_{\mathfrak{p}} \cong K_{\mathfrak{p}}^{t_p}$, $R_{\mathfrak{p}} \cong \mathcal{O}_{\mathfrak{p}}^{n-t_p}$. We apply Lemma 3.4 to $\mathcal{S} = \mathcal{P}'(A)$, K, and $V_{\mathfrak{p}} = D_{\mathfrak{p}}$. Then there exists a basis $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$ of $\mathbb{Z}^n$ such that for any $p \in \mathcal{P}'(A)$, $D_{\mathfrak{p}} = \mathrm{Span}_{K_{\mathfrak{p}}}(\mathbf{x}_{p1}, \dots, \mathbf{x}_{pt_p})$, and $\mathbf{x}_{pi}$'s are given by (3.5). We only need to show $\overline{G}_{\mathfrak{p}} \subseteq D_{\mathfrak{p}} \oplus \mathrm{Span}_{\mathcal{O}_{\mathfrak{p}}}(\mathbf{f}_{t_p+1}, \dots, \mathbf{f}_n)$. Indeed, by (2.7), for any $\mathbf{u} \in R_{\mathfrak{p}}$,

$$\mathbf{u} = \sum_{i=t_p+1}^{n} \alpha_i \mathbf{w}_{pi} = \sum_{i=1}^{n} \beta_i \mathbf{f}_i = \sum_{i=1}^{t_p} \gamma_i \mathbf{x}_{pi} + \sum_{i=t_p+1}^{n} \gamma_i \mathbf{f}_i,$$

where all $\alpha_i \in \mathcal{O}_{\mathfrak{p}}$ by definition of $R_{\mathfrak{p}}$, and all $\beta_i \in \mathcal{O}_{\mathfrak{p}}$, since all $\mathbf{w}_{pi} \in \mathbb{Z}_p^n$. Finally, all $\gamma_i \in \mathcal{O}_{\mathfrak{p}}$ by definition of $\mathbf{x}_{pi}$. This proves (3.8).

We now show that for any K, all $\alpha_{pij} \in \mathbb{Z}_p$. By enlarging K if necessary, without loss of generality, we assume K is Galois over $\mathbb{Q}$. Let $p \in \mathcal{P}'(A)$ be arbitrary. By above, (3.8), (3.9) hold. For any $\sigma \in \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$, we have $\sigma(\overline{G}_{\mathfrak{p}}) = \overline{G}_{\mathfrak{p}}$, $\sigma(R_{\mathfrak{p}}) = R_{\mathfrak{p}}$, and $\sigma(D_{\mathfrak{p}}) = \mathrm{Span}_{K_{\mathfrak{p}}}(\sigma(\mathbf{x}_{pi}))$, where

$$\sigma(\mathbf{x}_{pi}) = \mathbf{f}_i + \sum_{j=t_p+1}^{n} \sigma(\alpha_{pij}) \mathbf{f}_j, \quad 1 \le i \le t_p,$$

since A, $\mathbf{f}_1, \dots, \mathbf{f}_n$ are defined over $\mathbb{Z}$. By the uniqueness of the divisible part, we have $\mathrm{Span}_{K_{\mathfrak{p}}}(\sigma(\mathbf{x}_{pi})) = \mathrm{Span}_{K_{\mathfrak{p}}}(\mathbf{x}_{pi})$ and hence $\sigma(\alpha_{pij}) = \alpha_{pij}$ for any i, j. Since $\alpha_{pij} \in \mathcal{O}_{\mathfrak{p}}$, this implies $\alpha_{pij} \in \mathbb{Z}_p$ and hence $\mathbf{x}_{pij} \in \mathbb{Z}_p^n$ for all p, i, j. Furthermore, $\overline{G}_{A,p}$ consists of elements in $G_{\mathfrak{p}}$ invariant under the action of $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$. Hence,

$$\overline{G}_{A,p} = \mathrm{Span}_{\mathbb{Q}_{\mathfrak{p}}}(\mathbf{x}_{p1}, \dots, \mathbf{x}_{pt_p}) \oplus \mathrm{Span}_{\mathbb{Z}_p}(\mathbf{f}_{t_p+1}, \dots, \mathbf{f}_n).$$

On the other hand, if (3.8), (3.9) hold for $K = \mathbb{Q}_p$ and the same basis $\mathbf{f}_1, \dots, \mathbf{f}_n$, then

$$\begin{aligned} \overline{G}_{A,p} &= \mathrm{Span}_{\mathbb{Q}_{\mathfrak{p}}}(\mathbf{x}'_{p1}, \dots, \mathbf{x}'_{pt_p}) \oplus \mathrm{Span}_{\mathbb{Z}_p}(\mathbf{f}_{t_p+1}, \dots, \mathbf{f}_n), \\ \mathbf{x}'_{pi} &= \mathbf{f}_i + \sum_{j=t_p+1}^{n} \alpha'_{pij} \mathbf{f}_j, \quad 1 \le i \le t_p, \end{aligned}$$

for some $\alpha'_{pij} \in \mathbb{Z}_p$, a priori, different from $\alpha_{pij} \in \mathbb{Z}_p$. As above, by the uniqueness of the divisible part, we have $\alpha_{pij} = \alpha'_{pij}$ for all p, i, j. This shows that α_{pij}'s do not depend on K and $\mathfrak{p}$'s.

For each $p \in \mathcal{P}'(A)$ let $\mathbf{w}_{p1}, \ldots, \mathbf{w}_{pt_p}$ be as in Lemma 2.10. By (2.6), $\{\mathbf{w}_{p1}, \ldots, \mathbf{w}_{pt_p}\}$ is a $\mathbb{Q}_p$-basis of $D_p(A)$. By Lemma 3.4 applied to $\mathcal{S} = \mathcal{P}'(A)$, $K = \mathbb{Q}$, and $V_p = D_p(A)$, we get $\mathrm{Span}_{\mathbb{Q}_p}(\mathbf{w}_{p1}, \ldots, \mathbf{w}_{pt_p}) = \mathrm{Span}_{\mathbb{Q}_p}(\mathbf{x}_{p1}, \ldots, \mathbf{x}_{pt_p})$. Thus, (3.10) follows from (3.2). □

Definition 3.6. [GM81] Let $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ and $\alpha_{pij} \in \mathbb{Z}_p$ be as in Lemma 3.5. The set

$$M(A; \mathbf{f}_1, \ldots, \mathbf{f}_n) = \{\alpha_{pij} \in \mathbb{Z}_p \,|\, p \in \mathcal{P}',\, 1 \le i \le t_p < j \le n\}$$

is called the *characteristic* of G_A relative to the ordered basis $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$.

Remark 3.7. To calculate a characteristic of G_A in practice, one can start with a basis $\mathcal{W}_p = \{\mathbf{w}_{p1}, \ldots, \mathbf{w}_{pt_p}\}$ of the divisible part $D_p(A)$, and then apply the procedure in the proof of Lemma 3.4 for $\mathcal{S} = \mathcal{P}'(A)$, $K = \mathbb{Q}$, $V_{\mathfrak{p}} = D_p(A)$ (see Lemma 2.10 for the definition of $\mathcal{W}_p$). In turn, to find $\mathcal{W}_p$, one can use the procedure described in the proof of Theorem 9.1 below.

Our ultimate goal is to characterize when $G_A \cong G_B$ for non-singular $A, B \in \mathrm{M}_n(\mathbb{Z})$. In the next lemma we show that by conjugating A by a matrix in $\mathrm{GL}_n(\mathbb{Z})$ corresponding to $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$, without loss of generality, we can assume that the characteristics of both G_A, G_B are given with respect to the standard basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$.

Lemma 3.8. *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let $M(A; \mathbf{f}_1, \ldots, \mathbf{f}_n)$ be the characteristic of G_A relative to a free $\mathbb{Z}$-basis $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ of $\mathbb{Z}^n$. Let $\{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$ be another free $\mathbb{Z}$-basis of $\mathbb{Z}^n$ and let $S \in \mathrm{GL}_n(\mathbb{Z})$ be a change-of-basis matrix: $S\mathbf{f}_i = \mathbf{g}_i$, $1 \le i \le n$. Then $S(G_A) = G_{SAS^{-1}}$, $\mathcal{P}'(A) = \mathcal{P}'(SAS^{-1})$, $t_p(A) = t_p(SAS^{-1})$, and*

$$M(SAS^{-1}; \mathbf{g}_1, \ldots, \mathbf{g}_n) = M(A; \mathbf{f}_1, \ldots, \mathbf{f}_n).$$

Proof. Follows easily from the definition (2.1) of G_A and Lemma 3.5. □

Lemma 3.9. *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let*

$$M(A; \mathbf{f}_1, \ldots, \mathbf{f}_n) = \{\alpha_{pij} \,|\, p \in \mathcal{P}',\, 1 \le i \le t_p < j \le n\}$$

be the characteristic of G_A relative to a free basis $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ of $\mathbb{Z}^n$. For $\mathbf{b} \in \mathbb{Q}^n$ let $\mathbf{b} = \sum_{k=1}^n b_k \mathbf{f}_k$, $b_1, \ldots, b_n \in \mathbb{Q}$. Then $\mathbf{b} \in \overline{G}_{A,p}$ for $p \in \mathcal{P}'$ if and only if

$$b_j - \sum_{i=1}^{t_p} b_i \alpha_{pij} \in \mathbb{Z}_p,\ t_p + 1 \le j \le n. \tag{3.11}$$

Moreover, $\mathbf{b} \in G_A$ if and only if $b_1, \ldots, b_n \in \mathcal{R}$ and (3.11) holds for any $p \in \mathcal{P}'$.

Proof. It follows easily from [GM81, p. 195, Lemma 2]. We repeat the argument adapted to our case. Since $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ is a free $\mathbb{Z}$-basis of $\mathbb{Z}^n$, it follows from Corollary 2.9 that $\mathbf{b} \in G_A$ if and only if $b_1, \ldots, b_n \in \mathcal{R}$ and $\mathbf{b} \in \overline{G}_{A,p}$ for any $p \in \mathcal{P}'$. Since $\mathbb{Z}_p^n \subseteq \overline{G}_{A,p}$, by Lemma 3.5, $\{\mathbf{x}_{p1}, \ldots, \mathbf{x}_{pt_p}, \mathbf{f}_{t_p+1}, \ldots, \mathbf{f}_n\}$ is a basis of $\mathbb{Q}_p^n$ as a $\mathbb{Q}_p$-vector space. Thus,

$$\mathbf{b} = \sum_{k=1}^n b_k \mathbf{f}_k = \sum_{i=1}^{t_p} y_i \mathbf{x}_{pi} + \sum_{j=t_p+1}^n y_j \mathbf{f}_j, \quad y_1, \ldots, y_n \in \mathbb{Q}_p. \tag{3.12}$$

Hence, by Lemma 3.5 applied to $K = \mathbb{Q}$, $\mathbf{b} \in \overline{G}_{A,p}$ if and only if $y_{t_p+1}, \dots, y_n \in \mathbb{Z}_p$. Comparing coefficients in (3.12) and using (3.5), each $y_i = b_i$ and each $y_j = b_j - \sum_{i=1}^{t_p} b_i \alpha_{pij}$, hence (3.11). □

We are interested in studying isomorphism classes of groups G_A, *i.e.,* when $G_A \cong G_B$ for non-singular $A, B \in \mathrm{M}_n(\mathbb{Z})$. 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 in $\mathbb{Z}$. Therefore, for the rest of the paper we assume $n \geq 2$.

The next result is a criterion for G_A, G_B to be isomorphic. It is based on the facts that any isomorphism ϕ between G_A and G_B is induced by a matrix $T \in \mathrm{GL}_n(\mathbb{Q})$ ([S22, Lemma 3.1]), ϕ induces a $\mathbb{Z}_p$-module isomorphism between $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$ for any prime $p \in \mathbb{N}$, and, therefore, ϕ restricts to an isomorphism between the divisible parts $D_p(A)$, $D_p(B)$ (see (2.6) for the definition).

Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. Define

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

By Lemma 3.8, without loss of generality, we can assume that we have the characteristics of G_A, G_B with respect to the same standard basis $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$, *i.e.,*

$$M(A; \mathbf{e}_1, \dots, \mathbf{e}_n) = \{\alpha_{pij}(A) \,|\, p \in \mathcal{P}'(A),\ 1 \leq i \leq t_p(A) < j \leq n\}, \tag{3.13}$$

$$M(B; \mathbf{e}_1, \dots, \mathbf{e}_n) = \{\alpha_{pij}(B) \,|\, p \in \mathcal{P}'(B),\ 1 \leq i \leq t_p(B) < j \leq n\}. \tag{3.14}$$

We say that $T \in \mathrm{GL}_n(\mathbb{Q})$ satisfies the condition (A, B, p), $p \in \mathcal{P}'(B)$, if

$$j - \text{th column } \begin{pmatrix} \gamma_{1j} & \cdots & \gamma_{nj} \end{pmatrix} \text{ of } T \text{ satisfies}$$

$$\gamma_{kj} - \sum_{i=1}^{t_p} \gamma_{ij} \alpha_{pik}(B) \in \mathbb{Z}_p \text{ for any } k, j \in \{t_p + 1, n\}.$$

Theorem 3.10. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let G_A, G_B have characteristics* (3.13), (3.14)*, respectively. For $T \in \mathrm{GL}_n(\mathbb{Q})$ we have $T(G_A) = G_B$ if and only if*

$$\begin{aligned} \mathcal{P} = \mathcal{P}(A) &= \mathcal{P}(B), \\ \mathcal{P}' = \mathcal{P}'(A) &= \mathcal{P}'(B), \\ \mathcal{R} = \mathcal{R}(A) &= \mathcal{R}(B), \\ t_p(A) &= t_p(B), \quad \forall p \in \mathcal{P}, \end{aligned}$$

$T \in \mathrm{GL}_n(\mathcal{R})$, $T(D_p(A)) = D_p(B)$, and T (resp., T^{-1}) satisfies the condition (A, B, p) (resp., (B, A, p)) for any $p \in \mathcal{P}'$.

Proof. By Corollary 2.4, $T(G_A) = G_B$ if and only if for any prime $p \in \mathbb{N}$

$$T(\overline{G}_{A,p}) = \overline{G}_{B,p}.$$

In particular, using Proposition 2.5, if $T(G_A) = G_B$, then $\mathcal{P}(A) = \mathcal{P}(B)$, $\mathcal{P}'(A) = \mathcal{P}'(B)$, $t_p(A) = t_p(B)$, and hence $\mathcal{R}(A) = \mathcal{R}(B)$. Also, $T \in \mathrm{GL}_n(\mathcal{R})$ by [S22, Lemma 3.4].

By Lemma 3.5 applied to $K = \mathbb{Q}$,

$$\overline{G}_{A,p} = D_p(A) \oplus \mathrm{Span}_{\mathbb{Z}_p}(\mathbf{e}_{t_1+1}, \dots, \mathbf{e}_n), \tag{3.15}$$

$$\overline{G}_{B,p} = D_p(B) \oplus \mathrm{Span}_{\mathbb{Z}_p}(\mathbf{e}_{t_2+1}, \dots, \mathbf{e}_n), \tag{3.16}$$

where $t_1 = t_p(A)$, $t_2 = t_p(B)$, and $D_p(A) \cong \mathbb{Q}_p^{t_1}$, $D_p(B) \cong \mathbb{Q}_p^{t_2}$ as $\mathbb{Z}_p$-modules. Therefore, T defines a $\mathbb{Z}_p$-module isomorphism from $\overline{G}_{A,p}$ to $\overline{G}_{B,p}$ if and only if $t = t_1 = t_2$, $T(D_p(A)) = D_p(B)$, and with respect to the decompositions (3.15) and (3.16), T has the form

$$\tilde{T} = \begin{pmatrix} T_1 & * \\ 0 & T_2 \end{pmatrix}, \quad T_1 \in \mathrm{GL}_t(\mathbb{Q}_p),\ T_2 \in \mathrm{GL}_{n-t}(\mathbb{Z}_p).$$

Note that $T_2 \in \mathrm{GL}_{n-t}(\mathbb{Z}_p)$ if and only if $T\mathbf{e}_j \in \overline{G}_{B,p}$ and $T^{-1}\mathbf{e}_j \in \overline{G}_{A,p}$ for any $j \in \{t+1, \dots, n\}$, which is equivalent to the conditions (A, B, p), (B, A, p) for columns of T, T^{-1}, respectively, by Lemma 3.9. □

4. Generalized eigenvectors

Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. Using Theorem 3.10, one can already check whether $G_A \cong G_B$ and also find such isomorphisms if they exist. In this section, we make Theorem 3.10 even more practical by describing the $\mathbb{Z}_p$-divisible part $D_p(A)$ of $G_A \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in terms of generalized eigenvectors of A.

Throughout the text, $\overline{\mathbb{Q}}$ denotes a fixed algebraic closure of $\mathbb{Q}$. Let $K \subset \overline{\mathbb{Q}}$ be a finite extension of $\mathbb{Q}$ that contains all the eigenvalues of A. Let $\mathcal{O}_K$ denote the ring of integers of K. Throughout the paper, $\lambda_1, \dots, \lambda_n \in \mathcal{O}_K$ denote (not necessarily distinct) eigenvalues of A and $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ denotes a Jordan canonical basis of A. Without loss of generality, we can assume that each $\mathbf{u}_i \in (\mathcal{O}_K)^n$, $i = 1, \dots, n$. For a prime $p \in \mathbb{N}$ let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above p and let $X_{A,\mathfrak{p}}$ denote the span over K of vectors in $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$ corresponding to eigenvalues divisible by $\mathfrak{p}$. Note that

$$\dim_K X_{A,\mathfrak{p}} = t_p(A),$$

where $t_p = t_p(A)$ denotes the multiplicity of zero in the reduction $\bar{h}_A$ modulo p of the characteristic polynomial h_A of A, $0 \le t_p \le n$. Indeed, $\dim_K X_{A,\mathfrak{p}}$ is the number of eigenvalues (with multiplicities) of A divisible by $\mathfrak{p}$. One can write $h_A = (x-\lambda_1)\cdots(x-\lambda_n)$ over $\mathcal{O}_K$. Considering the reduction $\bar{h}_A$ of h_A modulo $\mathfrak{p}$, we see that the number of eigenvalues of A divisible by $\mathfrak{p}$ is equal to the multiplicity t_p of zero in $\bar{h}_A$. Equivalently, $X_{A,\mathfrak{p}}$ is generated over K by generalized λ-eigenvectors of A for any eigenvalue λ of A divisible by $\mathfrak{p}$.

Lemma 4.1. *Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. Let $p \in \mathbb{N}$ be prime and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above p. Let $\mathcal{O}_\mathfrak{p}$ denote the ring of integers of $K_\mathfrak{p}$, the completion of K with respect to $\mathfrak{p}$. Then, considered as subsets of $K_\mathfrak{p}^n$,*

$$D_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} = X_{A,\mathfrak{p}} \otimes_K K_\mathfrak{p},$$

i.e., upon the extension of constants from $\mathbb{Z}_p$ to $\mathcal{O}_\mathfrak{p}$, the divisible part of $\overline{G}_{A,p}$ is generated over $K_\mathfrak{p}$ by generalized eigenvectors of A (considered as elements of $K_\mathfrak{p}^n$ via the embedding $K \hookrightarrow K_\mathfrak{p}$) corresponding to eigenvalues divisible by $\mathfrak{p}$.

Proof. Let $(\pi) \subset \mathcal{O}_\mathfrak{p}$ denote the prime ideal of $\mathcal{O}_\mathfrak{p}$. Via $K \hookrightarrow K_\mathfrak{p}$, we have $\lambda_1, \ldots, \lambda_n \in \mathcal{O}_\mathfrak{p}$ and without loss of generality, we can assume $\lambda_1, \ldots, \lambda_{t_p} \in (\pi)$, $\lambda_{t_p+1}, \ldots, \lambda_n \in (\mathcal{O}_\mathfrak{p})^\times$. Thus, $Y = X_{A,\mathfrak{p}} \otimes_K K_\mathfrak{p}$ is generated over $K_\mathfrak{p}$ by generalized eigenvectors of A corresponding to λ_i, $i = 1, \ldots, t_p$. Let

$$Z = \overline{G}_{A,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} = \left\{ A^{-k}\mathbf{x} \,\middle|\, \mathbf{x} \in \mathcal{O}_\mathfrak{p}^n,\, k \in \mathbb{Z} \right\}, \quad \mathcal{O}_\mathfrak{p}^n \subseteq Z \subseteq K_\mathfrak{p}^n.$$

Using Lemma 2.10, we have

$$Z = \overline{G}_{A,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} = \left(D_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} \right) \oplus \left(R_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} \right),$$

where, as $\mathcal{O}_\mathfrak{p}$-modules,

$$D_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} \cong K_\mathfrak{p}^{t_p}, \quad R_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} \cong \mathcal{O}_\mathfrak{p}^{n-t_p}.$$

We first prove $Y \subseteq Z$, by showing $\operatorname{Span}_{K_\mathfrak{p}}(\mathbf{u}) \subseteq Z$ for any generalized eigenvector $\mathbf{u}$ corresponding to λ_i, $i = 1, \ldots, t_p$. The proof is by induction on the rank of $\mathbf{u}$. Without loss of generality, we can assume $\mathbf{u} \in \mathcal{O}_\mathfrak{p}^n$. If $\operatorname{rank} \mathbf{u} = 1$, then $\mathbf{u}$ is an eigenvector of A corresponding to λ_i and hence $\lambda_i^{-k}\mathbf{u} = A^{-k}\mathbf{u} \in Z$ for any $k \in \mathbb{Z}$. Since $\lambda_i = \pi^\alpha \beta$ for $\alpha \in \mathbb{N}$, $\beta \in (\mathcal{O}_\mathfrak{p})^\times$, and Z is an $\mathcal{O}_\mathfrak{p}$-module, we have $\operatorname{Span}_{K_\mathfrak{p}}(\mathbf{u}) \subseteq Z$. Assume now $\operatorname{rank} \mathbf{u} = m$, $m > 1$. Then, $(A - \lambda_i \operatorname{Id})^m \mathbf{u} = \mathbf{0}$, where Id denotes the $n \times n$-identity matrix, and $\mathbf{v} = (A - \lambda_i \operatorname{Id})\mathbf{u}$ is of rank $m - 1$. By induction on m, $\operatorname{Span}_{K_\mathfrak{p}}(\mathbf{v}) \subseteq Z$. We have $\mathbf{v} = A\mathbf{u} - \lambda_i \mathbf{u}$ and hence

$$\lambda_i^{-k} A^{-1}\mathbf{v} = \lambda_i^{-k}\mathbf{u} - \lambda_i^{-k+1} A^{-1}\mathbf{u}, \qquad k \in \mathbb{Z}. \tag{4.1}$$

From (4.1), we can show $\lambda_i^{-k}\mathbf{u} \in Z$ by induction on $k \geq 0$. Indeed, for $k = 0$, we have $\mathbf{u} \in Z$, since $\mathbf{u} \in \mathcal{O}_\mathfrak{p}^n$. Assume $\lambda_i^{-(k-1)}\mathbf{u} \in Z$. Then $A^{-1}(\lambda_i^{-(k-1)}\mathbf{u}) = \lambda_i^{-k+1} A^{-1}\mathbf{u} \in Z$, since Z is A^{-1}-invariant. Analogously, $\lambda_i^{-k} A^{-1}\mathbf{v} \in Z$, since $\lambda_i^{-k}\mathbf{v} \in Z$ by induction on the rank. Thus, $\lambda_i^{-k}\mathbf{u} \in Z$ by (4.1). As before, it shows $\operatorname{Span}_{K_\mathfrak{p}}(\mathbf{u}) \subseteq Z$. Here $\mathbf{u}$ is a generalized eigenvector of an arbitrary rank corresponding to an eigenvalue of A divisible by $\mathfrak{p}$ and hence $Y \subseteq Z$. Finally, since Y is a divisible $\mathcal{O}_\mathfrak{p}$-module, it is contained inside the divisible part of Z, *i.e.*, $Y \subseteq D_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p}$. Since both have the same dimension t_p over $K_\mathfrak{p}$, they coincide and the claim follows. ☐

Remark 4.2. Note that we cannot claim that the reduced part $R_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p}$ of $\overline{G}_{A,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p}$ is generated by generalized eigenvectors of A over $\mathcal{O}_\mathfrak{p}$, since in general, $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ is not a free basis of $\mathcal{O}_\mathfrak{p}^n$. Equivalently, the matrix $\begin{pmatrix} \mathbf{u}_1 & \ldots & \mathbf{u}_n \end{pmatrix}$ might not be in $\mathrm{GL}_n(\mathcal{O}_\mathfrak{p})$.

Combining Lemma 4.1 with Theorem 3.10, we get a criterion for $G_A \cong G_B$ in terms of generalized eigenvectors of A and B.

Theorem 4.3. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular, let $K \subset \overline{\mathbb{Q}}$ be any finite extension of $\mathbb{Q}$ that contains the eigenvalues of both A and B, and let G_A, G_B have characteristics* (3.13), (3.14)*, respectively. For $T \in \mathrm{GL}_n(\mathbb{Q})$ we have $T(G_A) = G_B$ if and only if*

$$\begin{aligned} \mathcal{P} = \mathcal{P}(A) &= \mathcal{P}(B), \\ \mathcal{P}' = \mathcal{P}'(A) &= \mathcal{P}'(B), \\ \mathcal{R} = \mathcal{R}(A) &= \mathcal{R}(B), \\ t_p(A) &= t_p(B), \quad \forall p \in \mathcal{P}, \end{aligned}$$

$T \in \mathrm{GL}_n(\mathcal{R})$, for any $p \in \mathcal{P}'$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p we have

$$T(X_{A,\mathfrak{p}}) = X_{B,\mathfrak{p}},$$

and T (resp., T^{-1}) satisfies the condition (A, B, p) (resp., (B, A, p)) for any $p \in \mathcal{P}'$.

Proof. We have $T(D_p(A)) = D_p(B)$ if and only if $T(D_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p}) = D_p(B) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p}$, since T is defined over $\mathbb{Q}$. By Lemma 4.1, $D_p(A) \otimes_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} = X_{A,\mathfrak{p}} \otimes_K K_\mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p. Finally, $T(X_{A,\mathfrak{p}} \otimes_K K_\mathfrak{p}) = X_{B,\mathfrak{p}} \otimes_K K_\mathfrak{p}$ if and only if $T(X_{A,\mathfrak{p}}) = X_{B,\mathfrak{p}}$, since T is defined over $\mathbb{Q}$. Thus, the theorem follows from Theorem 3.10. □

Remark 4.4. We find Theorem 4.3 more practical than Theorem 3.10. The difference between the two is that to find a characteristic of G_A using Theorem 3.10, for each p one finds a possibly different matrix W_p and then modifies the rows according to the procedure described in Lemma 3.4 to get a basis $\{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ (see Remark 3.7). Whereas, in Theorem 4.3, we can start with a Jordan canonical basis of A (which does not depend on p) and then modify it using the same procedure (see Example 8 below). By Lemma 3.5 (and, possibly, Lemma 3.8), up to an isomorphism of G_A, both ways produce the same characteristic.

5. Reducible characteristic polynomials

Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular with G_A, G_B defined by (2.1). In this section we explore necessary conditions for $G_A \cong G_B$, when at least one of the characteristic polynomials of A, B is reducible in $\mathbb{Z}[t]$.

5.1. **Irreducible isomorphisms.** We start by introducing the notion of *an irreducible isomorphism* between G_A and G_B. Let $K \subset \overline{\mathbb{Q}}$ denote a finite Galois extension of $\mathbb{Q}$ that contains all the eigenvalues of A and B and let $G = \mathrm{Gal}(K/\mathbb{Q})$. For an eigenvalue $\lambda \in K$ of A let $K(A, \lambda)$ denote the generalized λ-eigenspace of A. By definition, $K(A, \lambda)$ is generated over K by all generalized eigenvectors of A corresponding to λ or, equivalently, by vectors in a Jordan canonical basis of A corresponding to λ. Let $h_A \in \mathbb{Z}[t]$ denote the characteristic polynomial of A. Assume $h_A = fg$ for non-constant $f, g \in \mathbb{Z}[t]$. By Theorem 9.1 below, there exists $S \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$SAS^{-1} = \begin{pmatrix} A' & * \\ 0 & A'' \end{pmatrix},$$

where A', A'' are matrices with integer coefficients of appropriate sizes such that the characteristic polynomial of A' (resp., A'') is f (resp., g). We have a natural embedding $G_{A'} \hookrightarrow G_{SAS^{-1}}$ induced by $\mathbf{x} \mapsto \begin{pmatrix} \mathbf{x} & \mathbf{0} \end{pmatrix}$, where $\mathbf{x} \in \mathbb{Q}^{n_1}$, $n_1 = \deg f$, and $\mathbf{0}$ is the zero vector in $\mathbb{Q}^{n-n_1}$. There is an exact sequence

$$0 \longrightarrow G_{A'} \longrightarrow G_A \longrightarrow G_{A''} \longrightarrow 0, \tag{5.1}$$

since $S(G_A) = G_{SAS^{-1}}$. We denote $G_{A'} = G_f$, $G_{A''} = G_g$.

Definition 5.1. We say that an isomorphism $T : G_A \longrightarrow G_B$ is *reducible* if there exist $S, L \in \mathrm{GL}_n(\mathbb{Z})$ and non-constant $f, g, f', g' \in \mathbb{Z}[t]$ such that $h_A = fg$, $h_B = f'g'$,

$$SAS^{-1} = \begin{pmatrix} A' & * \\ 0 & A'' \end{pmatrix}, \quad LBL^{-1} = \begin{pmatrix} B' & * \\ 0 & B'' \end{pmatrix},$$

$h_{A'} = f$, $h_{B'} = f'$, $\deg f = \deg f'$, and $LTS^{-1}(G_f) = G_{f'}$. Otherwise, we say that T is *irreducible.*

Clearly, if the characteristic polynomial of A or B is irreducible, then an isomorphism $T : G_A \longrightarrow G_B$ is irreducible. The converse is not true in general. For instance,

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

where both characteristic polynomials h_A, h_B are reducible, but $T : G_A \longrightarrow G_B$ is an irreducible isomorphism. Indeed, any $S, L, T \in \mathrm{GL}_2(\mathbb{Q})$ satisfying the conditions in Definition 5.1 have to be upper-triangular. However, for $\mathcal{R} = \mathbb{Z}\left[\frac{1}{2}\right]$ any $T \in \mathrm{GL}_2(\mathcal{R})$ is an isomorphism between G_A and G_B by Corollary 2.4 and Proposition 2.5.

Note that $LTS^{-1}(G_f) = G_{f'}$ if and only if

$$T\left(\sum_{\lambda} K(A, \lambda)\right) = \sum_{\mu} K(B, \mu), \tag{5.2}$$

where $\lambda \in \overline{\mathbb{Q}}$ (resp., $\mu \in \overline{\mathbb{Q}}$) runs through all the roots of f (resp., f'). Also, $LTS^{-1}(G_f) = G_{f'}$ implies $LTS^{-1}(G_g) = G_{g'}$. Thus, if T is reducible, then $G_f \cong G_{f'}$, $G_g \cong G_{g'}$. In other words, if $h_A = fg$ and there is a reducible isomorphism $G_A \cong G_B$, then $G_f \cong G_{f'}$, $G_g \cong G_{g'}$ for some $f', g' \in \mathbb{Z}[t]$ such that $h_B = f'g'$. The converse is not true in general.

Example 1. Let

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 4 \\ 0 & 5 \end{pmatrix}.$$

Here, in the notation of Definition 5.1, $f(t) = f'(t) = t - 2$, $g(t) = g'(t) = t - 5$, $G_A \cong G_f \oplus G_g$, where $G_f = \{\frac{k}{2^n} \mid k, n \in \mathbb{Z}\}$, $G_g = \{\frac{k}{5^n} \mid k, n \in \mathbb{Z}\}$. Using Theorem 3.10 together with Lemma 4.1, one can show $G_A \not\cong G_B$, hence the sequence

$$0 \longrightarrow G_{f'} \longrightarrow G_B \longrightarrow G_{g'} \longrightarrow 0$$

does not split. This is also an example when $G_f \cong G_{f'}$, $G_g \cong G_{g'}$, but $G_A \not\cong G_B$.

5.2. **Splitting sequences.** There is a case, however, when sequence (5.1) splits, namely, when $\det A'' = \pm 1$. Then, $G_{A''} = \mathbb{Z}^k$ is a free $\mathbb{Z}$-module, $A'' \in \mathrm{M}_k(\mathbb{Z})$. More precisely, let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular with characteristic polynomial $h_A \in \mathbb{Z}[t]$. Let $h_A = fg$, where $f, g \in \mathbb{Z}[t]$ are non-constant, $f = f_1 f_2 \cdots f_s$, $f_i(0) \neq \pm 1$ for each irreducible component $f_i \in \mathbb{Z}[t]$ of f, $1 \leq i \leq s$, $g(0) = \pm 1$. Then $G_g = \mathbb{Z}^k$, $k = k(A) = \deg g$, and hence the sequence

$$0 \longrightarrow G_f \longrightarrow G_A \longrightarrow G_g \longrightarrow 0$$

splits, *i.e.*,

$$G_A \cong G_f \oplus \mathbb{Z}^{k(A)}. \tag{5.3}$$

Lemma 5.2. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular with corresponding characteristic polynomials $h_A, h_B \in \mathbb{Z}[t]$. Then*

$$G_A \cong G_B \iff k(A) = k(B), \quad G_f \cong G_{f'},$$

where $h_B = f'g'$, $r(0) \neq \pm 1$ for each irreducible component $r \in \mathbb{Z}[t]$ of f', and $g'(0) = \pm 1$.

Proof. Clearly, the conditions are sufficient by (5.3). We now show that they are necessary. Assume $G_A \cong G_B$. By (5.3), without loss of generality, we can assume that

$$G_A = G_f \oplus \mathbb{Z}^{k(A)}, \quad G_B = G_{f'} \oplus \mathbb{Z}^{k(B)}.$$

By Lemma 8.1 below, G_f is dense in $\mathbb{Q}^{n-k(A)}$. Therefore, the closure $\overline{G}_A$ of G_A in $\mathbb{Q}^n$ with its usual topology is

$$\overline{G}_A = \mathbb{Q}^{n-k(A)} \oplus \mathbb{Z}^{k(A)}$$

and, analogously, for B

$$\overline{G}_B = \mathbb{Q}^{n-k(B)} \oplus \mathbb{Z}^{k(B)}.$$

An isomorphism between G_A and G_B is induced by a linear isomorphism $T \in \mathrm{GL}_n(\mathbb{Q})$ of $\mathbb{Q}^n$ [S22, Lemma 3.1] such that $T(G_A) = G_B$. Thus, $T(\overline{G}_A) = \overline{G}_B$, hence $k(A) = k(B)$, $T(\mathbb{Q}^{n-k(A)}) = \mathbb{Q}^{n-k(B)}$, and therefore $T(G_f) = G_{f'}$. □

Remark 5.3. By Lemma 5.2, without loss of generality, for the rest of the section we can assume that $r(0) \neq \pm 1$ for any irreducible component $r \in \mathbb{Z}[t]$ of h_A, and the same holds for h_B.

5.3. **Properties of irreducible isomorphisms.** We now explore necessary conditions for an isomorphism between G_A and G_B to be irreducible. For any $p \in \mathcal{P}'(A)$ let $\tilde{h}, h_{A,p} \in \mathbb{Z}[t]$ be such that $h_A = \tilde{h} h_{A,p}$, p does not divide $\tilde{h}(0)$, and p divides $r(0)$ for any irreducible component $r \in \mathbb{Z}[t]$ of $h_{A,p}$. Also, let $S_{A,p}$ denote the set of distinct roots of $h_{A,p}$ (not counting multiplicities). For a prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K above p, let

$$X_{A,p} = \sum_{\sigma \in G} \sigma(X_{A,\mathfrak{p}}) = \sum_{\sigma \in G} X_{A,\sigma(\mathfrak{p})},$$

where the second equality holds, since A is defined over $\mathbb{Q}$, $G = \mathrm{Gal}(K/\mathbb{Q})$, and $X_{A,\mathfrak{p}}$ is defined in Section 4. Equivalently,

$$X_{A,p} = \sum_{\lambda \in S_{A,p}} K(A,\lambda), \quad S_{A,p} = \{\lambda \in \mathcal{O}_K \mid h_{A,p}(\lambda) = 0\},$$

since G acts transitively on the roots of an irreducible component $r \in \mathbb{Z}[t]$ of h_A. Note that

$$\dim X_{A,p} = \deg h_{A,p}, \quad \sigma(X_{A,p}) = X_{A,p} \text{ for any } \sigma \in G.$$

Moreover, for $p_1, \ldots, p_k \in \mathcal{P}'(A)$ denote recursively

$$X_{A,p_1\cdots p_k} = X_{A,p_1\cdots p_{k-1}} \cap X_{A,p_k} = \sum_{\lambda \in S_{A,p_1} \cap \cdots \cap S_{A,p_k}} K(A,\lambda),$$

where the second equality holds, since generalized eigenvectors corresponding to distinct eigenvalues are linearly independent. We write $h_A = h_1 \cdots h_s$, where each $h_i = r_i^{u_i}$, $u_i \in \mathbb{N}$, $r_i \in \mathbb{Z}[t]$ is irreducible, and h_i, h_j have no common roots in $\overline{\mathbb{Q}}$ for $i \neq j$. In this notation,

$$h_{A,p} = \prod_{p \mid h_i(0)} h_i, \quad h_{A,p_1\cdots p_k} = \prod_{p_1\cdots p_k \mid h_i(0)} h_i,$$

where $p_1, \ldots, p_k$ are assumed to be distinct. Then, $\dim X_{A,p_1\cdots p_k} = \deg h_{A,p_1\cdots p_k}$. We now assume $B \in \mathrm{M}_n(\mathbb{Z})$ is non-singular and $T(G_A) = G_B$ for some $T \in \mathrm{GL}_n(\mathbb{Q})$. Then, by Theorem 4.3, we have $\mathcal{P}' = \mathcal{P}'(A) = \mathcal{P}'(B)$ and $T(X_{A,\mathfrak{p}}) = X_{B,\mathfrak{p}}$. Since T, A, B are all defined over $\mathbb{Q}$, for any $\sigma \in G$ we have

$$T(X_{A,\sigma(\mathfrak{p})}) = T\sigma(X_{A,\mathfrak{p}}) = \sigma(T(X_{A,\mathfrak{p}})) = \sigma(X_{B,\mathfrak{p}}) = X_{B,\sigma(\mathfrak{p})},$$

and hence $T(X_{A,p}) = X_{B,p}$. This implies the following lemma.

Lemma 5.4. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let $T(G_A) = G_B$, $T \in \mathrm{GL}_n(\mathbb{Q})$. Then $\mathcal{P}' = \mathcal{P}'(A) = \mathcal{P}'(B)$ and for any $k \in \mathbb{N}$ with distinct $p_1, \ldots, p_k \in \mathcal{P}'$,*

$$T(X_{A,p_1\cdots p_k}) = X_{B,p_1\cdots p_k}.$$

In particular,

$$\deg h_{A,p_1\cdots p_k} = \deg h_{B,p_1\cdots p_k}.$$

Example 2. Let $A, B \in \mathrm{M}_5(\mathbb{Z})$ be non-singular with characteristic polynomials

$$h_A = (t^2 + t + 2)(t^3 + t + 6), \quad h_B = (t^2 + 4)(t^3 + t + 3).$$

Then $\mathcal{P}' = \mathcal{P}'(A) = \mathcal{P}'(B) = \{2, 3\}$, $t_2(A) = t_2(B) = 2$, $t_3(A) = t_3(B) = 1$. However,

$$h_{A,2} = h_A, \quad h_{B,2} = t^2 + 4,$$

so that $\deg h_{A,2} \neq \deg h_{B,2}$ and hence $G_A \ncong G_B$ by Lemma 5.4.

Corollary 5.5. *If an isomorphism $T : G_A \longrightarrow G_B$ is irreducible, then for all the irreducible components $f_1, \ldots, f_k \in \mathbb{Z}[t]$ (resp., $g_1, \ldots, g_s \in \mathbb{Z}[t]$) of the characteristic polynomial of A (resp., of B), all $f_1(0), \ldots, f_k(0)$ (resp., $g_1(0), \ldots, g_s(0)$) have the same prime divisors (in $\mathbb{Z}$).*

Proof. Assume $T(G_A) = G_B$, $T \in \mathrm{GL}_n(\mathbb{Q})$. By Theorem 4.3, $\mathcal{P}' = \mathcal{P}'(A) = \mathcal{P}'(B)$. In the above notation, for $p \in \mathcal{P}'$ and the characteristic polynomial h_A (resp., h_B) of A (resp., B) let $\tilde{h}, \hat{h}, h_{A,p}, h_{B,p} \in \mathbb{Z}[t]$ be such that $h_A = \tilde{h}h_{A,p}$, $h_B = \hat{h}h_{B,p}$, p does not divide $\tilde{h}(0)\hat{h}(0)$, and p divides $r(0)$ for any irreducible component $r \in \mathbb{Z}[t]$ of $h_{A,p}h_{B,p}$. It follows from Lemma 5.4, (5.2), and the paragraph preceding Definition 5.1 that $LTS^{-1}(G_{h_{A,p}}) = G_{h_{B,p}}$ for some $L, S \in \mathrm{GL}_n(\mathbb{Z})$. Since T is irreducible, $\tilde{h}$ is constant. Since $p \in \mathcal{P}'$ is arbitrary, we conclude that for all the irreducible components $f_1, \ldots, f_k \in \mathbb{Z}[t]$ of h_A, $f_1(0), \ldots, f_k(0)$ have the same prime divisors (in $\mathbb{Z}$). By symmetry, the same holds for B. □

5.4. **Galois action.** We explore the action of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ on eigenvalues of non-singular $A, B \in \mathrm{M}_n(\mathbb{Z})$ when $G_A \cong G_B$. Let A, B have characteristic polynomials $h_A = h_1^{\alpha_1} \cdots h_k^{\alpha_k}$, $h_B = r_1^{\beta_1} \cdots r_s^{\beta_s}$, respectively, where $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_s \in \mathbb{N}$, and $h_1, \ldots, h_k \in \mathbb{Z}[t]$ (resp., $r_1, \ldots, r_s \in \mathbb{Z}[t]$) are distinct and irreducible. Let $K \subset \overline{\mathbb{Q}}$ be a finite Galois extension of $\mathbb{Q}$ that contains all the eigenvalues of A and B. Let $\Sigma \subset K$ (resp., $\Sigma' \subset K$) denote the set of all distinct eigenvalues of A (resp., B) with cardinality denoted by $|\Sigma|$, and let $\Sigma = \Sigma_1 \sqcup \cdots \sqcup \Sigma_k$ (resp., $\Sigma' = \Sigma'_1 \sqcup \cdots \sqcup \Sigma'_s$), where each Σ_i (resp., Σ'_j) is the set of all (distinct) roots of h_i (resp., r_j), $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, s\}$. Thus,

$$n = \sum_{i=1}^{k} \alpha_i |\Sigma_i| = \sum_{j=1}^{s} \beta_j |\Sigma'_j|, \quad n_i(A) = |\Sigma_i|, \quad n_j(B) = |\Sigma'_j|,$$

where $n_i(A)$ (resp., $n_j(B)$) is the number of distinct roots of h_i (resp., r_j).

Let $T : G_A \longrightarrow G_B$ be an isomorphism. By Theorem 4.3, $\mathcal{R} = \mathcal{R}(A) = \mathcal{R}(B)$, $\mathcal{P} = \mathcal{P}(A) = \mathcal{P}(B)$, $\mathcal{P}' = \mathcal{P}'(A) = \mathcal{P}'(B)$, and $t_p = t_p(A) = t_p(B)$ for any prime $p \in \mathcal{P}$. By assumption, $\mathcal{P}' \neq \emptyset$ and for any $p \in \mathcal{P}'$ we have $1 \leq t_p \leq n - 1$. For a subset M of Σ (resp., M' of Σ') we denote

$$\begin{aligned} U_M &= \bigoplus_{\lambda \in M} K(A, \lambda), \quad M = M_1 \sqcup \cdots \sqcup M_k, \\ V_{M'} &= \bigoplus_{\mu \in M'} K(B, \mu), \quad M' = M'_1 \sqcup \cdots \sqcup M'_s, \end{aligned}$$

where each M_i (resp., M'_j) is a subset of Σ_i (resp., Σ'_j), and $K(A, \lambda)$ (resp., $K(B, \mu)$) denotes the generalized λ-eigenspace of A (resp., generalized μ-eigenspace of B). Denote

$$||M|| = \sum_{i=1}^{k} \alpha_i |M_i|, \quad ||M'|| = \sum_{j=1}^{s} \beta_j |M'_j|.$$

By Theorem 4.3, we have $T(X_{A,\mathfrak{p}}) = X_{B,\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p, *i.e.*, in the above notation there exist $M \subset \Sigma$, $M' \subset \Sigma'$ such that

$$T(U_M) = V_{M'}, \quad t_p = ||M|| = ||M'||, \quad t_{p,i}(A) = |M_i|, \quad t_{p,j}(B) = |M'_j|. \tag{5.4}$$

Here, $t_{p,i}(A)$ (resp., $t_{p,j}(B)$) is the number of distinct roots of h_i (resp., r_j) divisible by $\mathfrak{p}$. Equivalently, $t_{p,i}(A)$ (resp., $t_{p,j}(B)$) is the multiplicity of zero in the reduction of h_i (resp., r_j) modulo p.

Lemma 5.6. *Assume $T : G_A \longrightarrow G_B$ is an irreducible isomorphism. Let $S \subset \Sigma$ be a non-empty subset of Σ of the smallest cardinality with the property that there exists $S' \subset \Sigma'$ with*

$$T(U_S) = V_{S'}, \quad S = S_1 \sqcup \cdots \sqcup S_k, \quad S' = S'_1 \sqcup \cdots \sqcup S'_s,$$

where each S_i (resp., S'_j) is a subset of Σ_i (resp., Σ'_j). Then, $S_i \neq \emptyset$, $S'_j \neq \emptyset$ for any $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, s\}$. Moreover, $||S|| = ||S'||$, for any i, $p \in \mathcal{P}'$,
(a) $||S||$ divides n, t_p,
(b) $|S_i|$ divides $n_i(A)$, $t_{p,i}(A)$,
(c) $\frac{n_i(A)}{|S_i|} = \frac{n}{||S||}$,
(d) $\frac{t_{p,i}(A)}{|S_i|} = \frac{t_p}{||S||}$,
and, similarly, for B.

Proof. By (5.4), S exists and $1 \leq ||S|| < n$. Assume T is irreducible and there exists $S_i = \emptyset$, *e.g.*, $S_1 = \cdots = S_l = \emptyset$, $S_{l+1}, \ldots, S_k$ are non-empty, $l \in \mathbb{N}$, $1 \leq l \leq k-1$, $f = h_{l+1}^{\alpha_{l+1}} \cdots h_k^{\alpha_k}$, $J = \{j \mid S'_j \neq \emptyset\}$, $J \neq \emptyset$, and $f' = \prod_{j \in J} r_j^{\beta_j}$. From the definition of S, S', we have

$$T\left(\bigoplus_{\lambda \in S} K(A, \lambda)\right) = \bigoplus_{\mu \in S'} K(B, \mu). \tag{5.5}$$

By applying any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ to (5.5) and using the transitivity of the Galois action on roots of irreducible polynomials with rational coefficients, we see that

$$T\left(\bigoplus_{\lambda \in \{\text{roots of } f\}} K(A, \lambda)\right) = \bigoplus_{\mu \in \{\text{roots of } f'\}} K(B, \mu).$$

By the dimension count, this implies $\deg f' = \deg f < n$ and (5.2) holds. This contradicts the assumption that T is irreducible. Thus, all $S_i \neq \emptyset$ and, analogously, all $S'_j \neq \emptyset$.

The Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ acts on Σ by acting on each Σ_i, *i.e.*, $\sigma(\Sigma_i) = \Sigma_i$ for any $i \in \{1, \ldots, k\}$, $\sigma \in G$. Note that for any $P, R \subseteq \Sigma$, $P', R' \subseteq \Sigma'$ and $\sigma \in G$ we have

$$U_P \cap U_R = U_{P \cap R}, \quad V_{P'} \cap V_{R'} = V_{P' \cap R'}, \tag{5.6}$$

$$\sigma(U_P) = U_{\sigma(P)}, \qquad \sigma(V_{P'}) = V_{\sigma(P')}. \tag{5.7}$$

Let $N \subseteq \Sigma$, $N' \subseteq \Sigma'$ satisfy

$$T(U_N) = V_{N'}. \tag{5.8}$$

Let $\sigma \in G$ be arbitrary. Applying σ to (5.8) and using properties (5.6), (5.7), we have $T(U_{\sigma(N)}) = V_{\sigma(N')}$, since $T \in \mathrm{GL}_n(\mathbb{Q})$. Hence, $T(U_{S \cap \sigma(N)}) = V_{S' \cap \sigma(N')}$. Since S is the smallest with this property, either $S \cap \sigma(N) = S$ or $S \cap \sigma(N) = \emptyset$. Equivalently, $\sigma(S) \cap N = \sigma(S)$ or $\sigma(S) \cap N = \emptyset$. In particular, taking $N = \tau(S)$ for an arbitrary $\tau \in G$, either $\sigma(S) = \tau(S)$ or $\sigma(S) \cap \tau(S) = \emptyset$. Let

$$S = S_1 \sqcup \cdots \sqcup S_k, \quad N = N_1 \sqcup \cdots \sqcup N_k, \quad \forall S_i, N_i \subseteq \Sigma_i,$$

$i \in \{1, \ldots, k\}$. Then for any $\sigma \in G$, we have either $\sigma(S_i) \cap N_i = \sigma(S_i)$ for all i or $\sigma(S_i) \cap N_i = \emptyset$ for all i. Analogously, for any $\sigma, \tau \in G$, we have either $\sigma(S_i) = \tau(S_i)$ for all i or $\sigma(S_i) \cap \tau(S_i) = \emptyset$ for all i. Moreover, since each h_i is irreducible, G acts transitively on Σ_i. This implies that each N_i is a disjoint union of orbits $\sigma(S_i)$ of S_i, $\sigma \in G$ and, furthermore, there exists a subset $H \subseteq G$ depending on N such that

$$N_i = \bigsqcup_{\sigma \in H} \sigma(S_i), \quad |N_i| = |H| \cdot |S_i| \text{ for all } i. \tag{5.9}$$

Clearly, (5.8) holds for $N = \Sigma$ and also for $N = M$ by (5.4). Thus, by (5.9), there exists $H_1, H_2 \subseteq G$ such that

$$\begin{aligned} n_i(A) = |H_1||S_i|, \quad n &= \sum_{i=1}^{k} \alpha_i |\Sigma_i| = |H_1| \sum_{i=1}^{k} \alpha_i |S_i| = |H_1| \cdot ||S||, \\ t_{p,i}(A) = |H_2||S_i|, \quad t_p &= \sum_{i=1}^{k} \alpha_i |M_i| = |H_2| \sum_{i=1}^{k} \alpha_i |S_i| = |H_2| \cdot ||S||. \end{aligned}$$

Hence, (a), (b), (c), and (d) hold. By symmetry, we have analogous formulas for B. □

We now use Lemma 5.6 in a special case when the greatest common divisor (n, t_p) of n and t_p is one, *e.g.*, when $t_p = 1$, or $t_p = n - 1$, or n is prime. The conclusion is that an irreducible isomorphism T between G_A, G_B implies that both characteristic polynomials h_A, h_B are irreducible and T takes any eigenvector of A to an eigenvector of B.

Proposition 5.7. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. Assume there exists a prime $p \in \mathcal{P}'(A)$ with $(n, t_p(A)) = 1$. If $T \in \mathrm{GL}_n(\mathbb{Q})$ is an irreducible isomorphism from G_A to G_B, then both h_A, h_B are irreducible in $\mathbb{Z}[t]$, and there exist eigenvalues $\lambda, \mu \in \overline{\mathbb{Q}}$ of A, B, respectively, such that $K = \mathbb{Q}(\lambda) = \mathbb{Q}(\mu)$. Moreover, λ and μ have the same prime ideal divisors in $\mathcal{O}_K$, and for an eigenvector $\mathbf{u} \in (\overline{\mathbb{Q}})^n$ of A, $T(\mathbf{u})$ is an eigenvector of B.*

Proof. By Lemma 5.6, $||S|| = 1$ and each S_i is non-empty. Hence $k = \alpha_1 = 1$, $|S_1| = 1$ and h_A is irreducible. By symmetry, h_B is irreducible and T takes an eigenvector of A to an eigenvector of B. Assume $A\mathbf{u} = \lambda\mathbf{u}$, $B\mathbf{v} = \mu\mathbf{v}$ for some $\lambda, \mu \in \overline{\mathbb{Q}}$. Without loss of generality, we can assume $\mathbf{u} \in \mathbb{Q}(\lambda)^n$. From $T\mathbf{u} = \mathbf{v}$ we have $BT\mathbf{u} = B\mathbf{v} = \mu T\mathbf{u}$. Since B, T are defined over $\mathbb{Q}$, this implies $\mu \in \mathbb{Q}(\lambda)$ and hence $\mathbb{Q}(\mu) = \mathbb{Q}(\lambda)$.

We now show the existence of eigenvalues of A, B sharing the same prime ideal divisors in the ring of integers $\mathcal{O}_K$ of K. The argument is the same as in the proof of [S22, Proposition 4.1]. We repeat it for the sake of completeness. By the previous paragraph, there exist $\mu \in \mathcal{O}_K$ and an eigenvector $\mathbf{u} \in \mathcal{O}_K^n$ corresponding to an eigenvalue $\lambda \in \mathcal{O}_K$ of A such that $T(\mathbf{u})$ is an eigenvector of B corresponding to μ. Since $T(G_A) = G_B$, by definition (2.1) of groups G_A, G_B, for any $m \in \mathbb{N}$ we have

$$B^{k_m}T = P_m A^m, \quad k_m \in \mathbb{N} \cup \{0\},\ P_m \in \mathrm{M}_n(\mathbb{Z}). \tag{5.10}$$

Let $T = \frac{1}{l}T'$ for some $l \in \mathbb{Z} - \{0\}$ and non-singular $T' \in \mathrm{M}_n(\mathbb{Z})$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ that divides λ. By above, $B(T\mathbf{u}) = \mu(T\mathbf{u})$. Hence, multiplying (5.10) by $\mathbf{u}$, we get

$$\mu^{k_m}T\mathbf{u} = B^{k_m}T\mathbf{u} = P_m A^m\mathbf{u} = P_m\lambda^m\mathbf{u}, \quad \forall m \in \mathbb{N}. \tag{5.11}$$

Here $T\mathbf{u} \neq \mathbf{0}$, $T\mathbf{u}$ 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 $\mathcal{O}_K$). Analogously, it follows from (5.11) that all prime (ideal) divisors of λ also divide μ (in $\mathcal{O}_K$). 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. □

Example 3. We demonstrate how Lemma 5.6 can be used to describe irreducible isomorphisms when $2 \leq n \leq 4$. If $n = 2, 3$, then any irreducible isomorphism between G_A, G_B implies h_A, h_B are irreducible by Proposition 5.7. Let $n = 4$ and assume there is an irreducible isomorphism between G_A, G_B. Using properties (a)–(d) in Lemma 5.6 and Proposition 5.7, one can show that either h_A is irreducible or $h_A = h_1h_2$, where $h_1, h_2 \in \mathbb{Z}[t]$ are irreducible of degree 2 and, analogously, for h_B. In particular, *e.g.*, one cannot have $h_A = f_1f_2$, where $f_1, f_2 \in \mathbb{Z}[t]$, f_1 is linear, and f_2 is irreducible of degree 3.

6. Irreducible characteristic polynomials, ideal classes

We first show that in the case of irreducible characteristic polynomials h_A, h_B, it is enough to assume that T takes an eigenvector of A to an eigenvector of B for $T(G_A) = G_B$.

Lemma 6.1. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let G_A, G_B have characteristics* (3.13), (3.14)*, respectively. Assume the characteristic polynomials of A, B are irreducible. Assume there exist eigenvalues $\lambda, \mu \in \mathcal{O}_K$ corresponding to eigenvectors $\mathbf{u}, \mathbf{v} \in K^n$ of A, B, respectively, such that λ, μ have the same prime ideal divisors in the ring of integers of K. Then $\mathcal{P} = \mathcal{P}(A) = \mathcal{P}(B)$, $\mathcal{P}' = \mathcal{P}'(A) = \mathcal{P}'(B)$, and $\mathcal{R} = \mathcal{R}(A) = \mathcal{R}(B)$. If $T \in \mathrm{GL}_n(\mathcal{R})$, $T(\mathbf{u}) = \mathbf{v}$, and T (resp., T^{-1}) satisfies the condition (A, B, p) (resp., (B, A, p)) for any $p \in \mathcal{P}'$, then $T(G_A) = G_B$.*

Proof. By enlarging K if necessary, without loss of generality, we can assume that K is Galois over $\mathbb{Q}$. For any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\lambda)$ and $\sigma(\mu)$ have the same prime ideal divisors. Thus, since $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on roots of irreducible polynomials $h_A, h_B \in \mathbb{Z}[t]$, we have $t_p(A) = t_p(B)$, $\mathcal{P}(A) = \mathcal{P}(B)$, $\mathcal{P}' = \mathcal{P}'(A) = \mathcal{P}'(B)$, and hence $\mathcal{R}(A) = \mathcal{R}(B)$.

Furthermore, for $p \in \mathcal{P}'$, a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p, and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\mathbf{u})$ (resp., $\sigma(\mathbf{v})$) is an eigenvector of A (resp., B) corresponding to $\sigma(\lambda)$ (resp., $\sigma(\mu)$) and $T(\sigma(\mathbf{u})) = \sigma(\mathbf{v})$, since A, B, T are defined over $\mathbb{Q}$. Thus, $T(X_{A,\mathfrak{p}}) = X_{B,\mathfrak{p}}$ and the lemma follows from Theorem 4.3. □

Remark 6.2. We know that when $G_A \cong G_B$ and $n \geq 4$, not every isomorphism between G_A and G_B takes an eigenvector of A to an eigenvector of B (see Example 10 below). Also, in general, if $n > 2$, $G_A \cong G_B$, and the characteristic polynomial of A is irreducible, then not necessarily the characteristic polynomial of B is also irreducible (see Example 11 below).

We now recall generalized ideal classes introduced in [S22]. Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let $\lambda \in \overline{\mathbb{Q}}$ be an eigenvalue of A corresponding to an eigenvector $\mathbf{u} = \begin{pmatrix} u_1 & u_2 & \dots & u_n \end{pmatrix}^t \in \mathbb{Q}(\lambda)^n$ of A. For the rest of this section we assume that the characteristic polynomials of A, B are irreducible. Denote

$$\begin{aligned} I_{\mathbb{Z}}(A,\lambda) &= \{m_1u_1 + \cdots + m_nu_n \,|\, m_1, \dots, m_n \in \mathbb{Z}\} \subset \mathbb{Q}(\lambda), \\ I_{\mathcal{R}}(A,\lambda) &= I_{\mathbb{Z}}(A,\lambda) \otimes_{\mathbb{Z}} \mathcal{R} \subset \mathbb{Q}(\lambda),\ \mathcal{R} = \mathcal{R}(A), \end{aligned}$$

where $\mathcal{R}$ is given by (2.2). 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. Let $\mu \in \overline{\mathbb{Q}}$ be an eigenvalue of B, and let K be a number field with ring of integers $\mathcal{O}_K$ such that $\lambda, \mu \in \mathcal{O}_K$. Assume $\mathcal{R} = \mathcal{R}(A) = \mathcal{R}(B)$ (which is a necessary condition for $G_A \cong G_B$). There exists $T \in \mathrm{GL}_n(\mathcal{R})$ such that $T(\mathbf{u})$ is an eigenvector of B corresponding to μ if and only if

$$I_{\mathcal{R}}(A,\lambda) = yI_{\mathcal{R}}(B,\mu), \quad y \in K^\times,$$

denoted by $[I_{\mathcal{R}}(A,\lambda)] = [I_{\mathcal{R}}(B,\mu)]$. We know that $[I_{\mathcal{R}}(A,\lambda)] = [I_{\mathcal{R}}(B,\mu)]$ is among sufficient conditions for $G_A \cong G_B$ for any $n \geq 2$ (Lemma 6.1 above). In [S22, Theorem 6.6] we prove that this is also a necessary condition when $n = 2$. Proposition 6.3 below extends the result to an arbitrary n under an additional assumption that there exists t_p coprime with n (denoted by $(n, t_p) = 1$). In fact, the proposition shows more, namely, than *any* isomorphism takes an eigenvector of A to an eigenvector of B. It turns out that $[I_{\mathcal{R}}(A,\lambda)] = [I_{\mathcal{R}}(B,\mu)]$ is not a necessary condition for $G_A \cong G_B$ for an arbitrary n (see Example 10 below, where the condition $(n, t_p) = 1$ does not hold). The next proposition is a direct consequence of Proposition 5.7, since if the characteristic polynomial of A is irreducible, then clearly, any isomorphism between G_A, G_B is irreducible.

Proposition 6.3. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular. Assume the characteristic polynomial of A is irreducible and there exists a prime $p \in \mathcal{P}'(A)$ with $(n, t_p(A)) = 1$. Let $K \subset \overline{\mathbb{Q}}$ be a finite extension of $\mathbb{Q}$ that contains the eigenvalues of both A and B. If $T \in \mathrm{GL}_n(\mathbb{Q})$ is an isomorphism from G_A to G_B (equivalently, $T(G_A) = G_B$), then there exist eigenvectors $\mathbf{u}, \mathbf{v} \in K^n$ corresponding to eigenvalues $\lambda, \mu \in \mathcal{O}_K$ of A, B, respectively, such that $T(\mathbf{u}) = \mathbf{v}$, and λ, μ have the same prime ideal divisors in $\mathcal{O}_K$.*

Combining Proposition 6.3 with Lemma 6.1 and Theorem 4.3, we get the following necessary and sufficient criterion for $G_A \cong G_B$ under the additional condition in Proposition 6.3.

Proposition 6.4. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular with irreducible characteristic polynomials and let G_A, G_B have characteristics* (3.13), (3.14)*, respectively. Assume there exists a prime p with $(t_p(A), n) = 1$. Let $K \subset \overline{\mathbb{Q}}$ be a finite extension of $\mathbb{Q}$ that contains the eigenvalues of both A and B. Then $T \in \mathrm{GL}_n(\mathbb{Q})$ is an isomorphism from G_A to G_B if and only if there exist eigenvalues $\lambda, \mu \in \mathcal{O}_K$ corresponding to eigenvectors $\mathbf{u}, \mathbf{v} \in K^n$ of A, B, respectively, such that λ, μ have the same prime ideal divisors in $\mathcal{O}_K$, $T \in \mathrm{GL}_n(\mathcal{R})$, $T(\mathbf{u}) = \mathbf{v}$, and T (resp., T^{-1}) satisfies the condition (A, B, p) (resp., (B, A, p)) for any $p \in \mathcal{P}'$.*

In the case $n = 2$, to decide whether G_A and G_B are isomorphic, we can omit conditions (A, B, p), (B, A, p).

Proposition 6.5. [S22, Theorem 6.6] *Let $A, B \in \mathrm{M}_2(\mathbb{Z})$ be non-singular. Assume the characteristic polynomial of A is irreducible and $\mathcal{P}'(A) \neq \emptyset$. Then $G_A \cong G_B$ if and only if there exist eigenvalues $\lambda, \mu \in \mathcal{O}_K$ of A, B, respectively, such that λ, μ have the same prime ideal divisors in $\mathcal{O}_K$ and*

$$[I_{\mathcal{R}}(A, \lambda)] = [I_{\mathcal{R}}(B, \mu)], \quad \mathcal{R} = \mathcal{R}(A).$$

Proposition 6.5 can be generalized to an arbitrary n under an additional condition, which automatically holds when $n = 2$. Namely, $t_p = n - 1$ for any $p \in \mathcal{P}'$.

Lemma 6.6. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular with irreducible characteristic polynomials, $\mathcal{P}'(A) \neq \emptyset$, and $t_p(A) = n - 1$ for any $p \in \mathcal{P}'(A)$. Then $G_A \cong G_B$ if and only if there exist eigenvalues $\lambda, \mu \in \mathcal{O}_K$ of A, B, respectively, such that λ, μ have the same prime ideal divisors in $\mathcal{O}_K$ and*

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

Proof. By Proposition 6.4, it is enough to show the sufficient part. As in the proof of Lemma 6.1, we have

$$\mathcal{P} = \mathcal{P}(A) = \mathcal{P}(B), \ \mathcal{P}' = \mathcal{P}'(A) = \mathcal{P}'(B), \ \mathcal{R} = \mathcal{R}(A) = \mathcal{R}(B),$$

and $t_p = t_p(A) = t_p(B)$ for any prime $p \in \mathbb{N}$. Note that $[I_{\mathcal{R}}(A, \lambda)] = [I_{\mathcal{R}}(B, \mu)]$ is equivalent to the existence of $T \in \mathrm{GL}_n(\mathcal{R})$ such that $T(\mathbf{u})$ is an eigenvector of B corresponding to μ for an eigenvector $\mathbf{u}$ of A corresponding to λ. As in the proofs of Theorem 4.3 and Lemma 6.1, such T induces an isomorphism between the divisible parts $D_p(A)$ and $D_p(B)$ of $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$, respectively, for any p. Under the assumption $t_p = n - 1$, $p \in \mathcal{P}'$, the reduced parts $R_p(A)$ and $R_p(B)$ of $\overline{G}_{A,p}$ and $\overline{G}_{B,p}$, respectively, are free $\mathbb{Z}_p$-modules of rank 1. Hence, there exists $k \in \mathbb{Z}$ such that for $T' = p^k T$ we have

$$T'(R_p(A)) \subseteq D_p(B) \oplus R_p(B) \quad \text{and} \quad (T')^{-1}(R_p(B)) \subseteq D_p(A) \oplus R_p(A). \tag{6.1}$$

Indeed, as follows from (3.15) and (3.16), $T(\mathbf{e}_n) = a + y\mathbf{e}_n$ for some $a \in D_p(B)$ and $y \in \mathbb{Q}_p$. Let $y = p^{-k}u$ for some $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Then $T'(\mathbf{e}_n) = p^k a + u\mathbf{e}_n$, where $p^k a \in D_p(B)$ and hence $T'(\mathbf{e}_n) \in \overline{G}_{B,p}$, since $\overline{G}_{B,p} = D_p(B) \oplus \mathbb{Z}_p\mathbf{e}_n$. Clearly, T' still induces an isomorphism between $D_p(A)$, $D_p(B)$, and $T' \in \mathrm{GL}_n(\mathcal{R})$, since $p \in \mathcal{P}'$. Moreover, for a prime q distinct from p, qT' also satisfies (6.1), since $q \in \mathbb{Z}_p^\times$. Since $\mathcal{P}'$ is finite, it shows that there exists $a \in \mathcal{R}^\times$ such that $aT \in \mathrm{GL}_n(\mathcal{R})$ is an isomorphism from $\overline{G}_{A,p}$ to $\overline{G}_{B,p}$ for any $p \in \mathcal{P}'$ and hence aT is an isomorphism from G_A to G_B by Corollary 2.9. □

7. Examples

Example 4. One of the easiest examples is when $\mathcal{P}' = \emptyset$. 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. There is only one prime $p = 2$ that divides $\det A$ and it also divides $\operatorname{Tr} A = 0$. Hence, by Lemma 3.3,

$$G_A = G_B = < \mathbf{e}_1, \mathbf{e}_2, 2^{-\infty}\mathbf{e}_1, 2^{-\infty}\mathbf{e}_2 > .$$

In general, if $h_A \equiv x^n \pmod{p}$ for any prime p that divides $\det A$, then

$$G_A = < p^{-k}\mathbf{e}_i \mid i \in \{1, 2, \dots, n\},\ p \mid \det A,\ k \in \mathbb{N} \cup \{0\} > .$$

Example 5. In this and the next examples we show how Theorem 3.10 can be effectively used in the case when the characteristic polynomials are not irreducible. Let

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

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

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

Thus,

$$\begin{aligned} \mathcal{P} &= \mathcal{P}(A) = \mathcal{P}(B) = \{2, 3, 5\}, \\ \mathcal{P}' &= \mathcal{P}'(A) = \mathcal{P}'(B) = \{3, 5\}, \\ t_3 &= t_3(A) = t_3(B) = 1, \\ t_5 &= t_5(A) = t_5(B) = 1, \\ \mathcal{R} &= \mathcal{R}(A) = \mathcal{R}(B) = \left\{ n2^k3^l5^m \mid k, l, m, n \in \mathbb{Z} \right\}. \end{aligned}$$

We have

$$A = S\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}S^{-1}, \quad S = \begin{pmatrix}1 & 2\\ 1 & 1\end{pmatrix} = \begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

Thus, in the notation of Lemma 3.3, $W_5 = W_5(A) = S$, $W_3 = W_3(A) = \begin{pmatrix}\mathbf{u}_2 & \mathbf{u}_1\end{pmatrix}$, and

$$G_A =< \mathbf{u}_1, \mathbf{u}_2, 2^{-\infty}\mathbf{u}_1, 2^{-\infty}\mathbf{u}_2, 5^{-\infty}\mathbf{u}_1, 3^{-\infty}\mathbf{u}_2 > .$$

Also,

$$G_A =< \mathbf{e}_1, \mathbf{e}_2, 2^{-\infty}\mathbf{e}_1, 2^{-\infty}\mathbf{e}_2, 5^{-\infty}(\mathbf{e}_1+\mathbf{e}_2), 3^{-\infty}(\mathbf{e}_1 + 2^{-1}\mathbf{e}_2) >,$$

since $2 \in \mathbb{Z}_3^\times$. Thus,

$$M(A; \mathbf{e}_1, \mathbf{e}_2) = \{\alpha_{512}(A) = 1, \alpha_{312}(A) = 2^{-1}\}$$

is the characteristic of G_A with respect to $\{\mathbf{e}_1, \mathbf{e}_2\}$. Similarly, we find a characteristic of G_B. One can show that

$$B = P\begin{pmatrix}\mu_1 & 0\\ 0 & \mu_2\end{pmatrix}P^{-1}, \quad P = \begin{pmatrix}2 & 19\\ 1 & 18\end{pmatrix} = \begin{pmatrix}\mathbf{v}_1 & \mathbf{v}_2\end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

Note that $\det P = 17 \in \mathbb{Z}_p^\times$ for any $p \in \mathcal{P}' = \{3, 5\}$. Thus, in the notation of Lemma 3.3, $W_5 = W_5(B) = P$, $W_3 = W_3(B) = \begin{pmatrix}\mathbf{v}_2 & \mathbf{v}_1\end{pmatrix}$, and

$$\begin{aligned} G_B &= < \mathbf{e}_1, \mathbf{e}_2, 2^{-\infty}\mathbf{e}_1, 2^{-\infty}\mathbf{e}_2, 5^{-\infty}\mathbf{v}_1, 3^{-\infty}\mathbf{v}_2 >= \\ &= < \mathbf{e}_1, \mathbf{e}_2, 2^{-\infty}\mathbf{e}_1, 2^{-\infty}\mathbf{e}_2, 5^{-\infty}(\mathbf{e}_1 + 2^{-1}\mathbf{e}_2), 3^{-\infty}(\mathbf{e}_1 + \frac{18}{19}\mathbf{e}_2) >, \end{aligned}$$

since $2 \in \mathbb{Z}_5^\times$, $19 \in \mathbb{Z}_3^\times$. Thus,

$$M(B; \mathbf{e}_1, \mathbf{e}_2) = \left\{\alpha_{512}(B) = 2^{-1}, \alpha_{312}(B) = \frac{18}{19}\right\}$$

is the characteristic of G_B with respect to $\{\mathbf{e}_1, \mathbf{e}_2\}$. Using Theorem 3.10, one can show that G_A is not isomorphic to G_B. Namely, one can show that if $T \in \mathrm{GL}_2(\mathbb{Q})$ and $T(\mathbf{u}_i) = m_i\mathbf{v}_i$, $i = 1, 2$, for some $m_1, m_2 \in \mathbb{Q}$, then $T \notin \mathrm{GL}_2(\mathcal{R})$.

Example 6. 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 5. We claim that $G_C \cong G_B$. Indeed,

$$C = S\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}S^{-1}, \quad S = \begin{pmatrix}1 & -67\\ 1 & -33\end{pmatrix} = \begin{pmatrix}\mathbf{w}_1 & \mathbf{w}_2\end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

We have $\mathcal{P} = \{2, 3, 5\}$, $\mathcal{P}' = \{3, 5\}$, $t_3 = 1$, $t_5 = 1$. Since $\det S = 34 \in \mathbb{Z}_p^\times$ for any $p \in \mathcal{P}'$, by Lemma 3.3, $W_5 = W_5(C) = S$, $W_3 = W_3(C) = \begin{pmatrix}\mathbf{w}_2 & \mathbf{w}_1\end{pmatrix}$, and

$$\begin{aligned} G_C &= < \mathbf{e}_1, \mathbf{e}_2, 2^{-\infty}\mathbf{e}_1, 2^{-\infty}\mathbf{e}_2, 5^{-\infty}\mathbf{w}_1, 3^{-\infty}\mathbf{w}_2 >= \\ &= < \mathbf{e}_1, \mathbf{e}_2, 2^{-\infty}\mathbf{e}_1, 2^{-\infty}\mathbf{e}_2, 5^{-\infty}(\mathbf{e}_1 + \mathbf{e}_2), 3^{-\infty}(\mathbf{e}_1 + \frac{33}{67}\mathbf{e}_2) >, \end{aligned}$$

since $67 \in \mathbb{Z}_3^\times$. Thus,

$$M(C; \mathbf{e}_1, \mathbf{e}_2) = \left\{ \alpha_{512}(C) = 1, \alpha_{312}(C) = \frac{33}{67} \right\}$$

is the characteristic of G_C with respect to $\{\mathbf{e}_1, \mathbf{e}_2\}$. Using Theorem 3.10, one can find $T \in \mathrm{GL}_2(\mathcal{R})$ such that $T(\mathbf{v}_i) = m_i \mathbf{w}_i$, $m_i \in \mathbb{Q}$, $i = 1, 2$. For example,

$$T = \begin{pmatrix} 5 & -9 \\ 3 & -5 \end{pmatrix}, \quad \det T = 2 \in \mathcal{R}^\times,$$

the conditions in Theorem 3.10 are satisfied and, hence, $T : G_B \longrightarrow G_C$ is an isomorphism.

There are several examples in [S22] when $n = 2$ and characteristic polynomials are irreducible. We now look at higher-dimensional examples.

Example 7. In this and the next examples we show two ways to compute characteristics. Let $n = 3$, $h = t^3 + t^2 + 2t + 6$, and

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

a rational canonical form of h. Note that $h \in \mathbb{Z}[t]$ is irreducible in $\mathbb{Q}[t]$. We will compute the characteristic of G_A with respect to the standard basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$. The calculation is justified by the proof of Theorem 9.1.

We have $\det A = -6$, $\mathcal{P} = \mathcal{P}' = \{2, 3\}$. Let $p = 2$. Then

$$h \equiv t^2 \cdot (t+1) \pmod 2, \quad \overline{G}_{A,p} \cong \mathbb{Q}_p^2 \oplus \mathbb{Z}_p, \quad t_p = 2,$$

by Proposition 2.5 above. As follows from the proof of Lemma 3.5, to determine a characteristic of G_A, we need to find generators of the divisible part $D_p(A)$ of $\overline{G}_{A,p}$, *i.e.*, a $\mathbb{Z}_p$-submodule of $\overline{G}_{A,p}$ isomorphic to $\mathbb{Q}_p^2$. By Hensel's lemma, $h = (t - \lambda)g(t)$, where $\lambda \in \mathbb{Z}_p^\times$ and $g \in \mathbb{Z}_p[t]$ is of degree 2. One can show that g is irreducible over $\mathbb{Q}_p$. Let $\alpha \in \overline{\mathbb{Q}}_p$ be a root of g. Let $\mathbf{u}(\alpha) \in \mathbb{Z}_p[\alpha]^3$ denote an eigenvector of A corresponding to α. We can take

$$\mathbf{u}(\alpha) = \begin{pmatrix} -6 \\ \alpha(\alpha+1) \\ \alpha \end{pmatrix} = C \begin{pmatrix} 1 \\ \alpha \end{pmatrix}, \quad C = \begin{pmatrix} -6 & 0 \\ 6\lambda^{-1} & -\lambda \\ 0 & 1 \end{pmatrix} \in \mathrm{M}_{3\times 2}(\mathbb{Z}_p).$$

We then look for a Smith normal form of C:

$$C = U \begin{pmatrix} -6 & 0 \\ 0 & -\lambda \\ 0 & 0 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 0 & 0 \\ -\lambda^{-1} & 1 & 0 \\ 0 & -\lambda^{-1} & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z}_p).$$

The first two columns $\mathbf{u}_{21}$, $\mathbf{u}_{22}$ of U give us generators of $D_p(A)$:

$$\mathbf{u}_{21} = \begin{pmatrix} 1 \\ -\lambda^{-1} \\ 0 \end{pmatrix}, \quad \mathbf{u}_{22} = \begin{pmatrix} 0 \\ 1 \\ -\lambda^{-1} \end{pmatrix}.$$

Analogously, for $p = 3$ we have

$$h \equiv t \cdot (t^2 + t + 2) \,(\mathrm{mod}\ 3), \quad \overline{G}_{A,p} \cong \mathbb{Q}_p \oplus \mathbb{Z}_p^2, \quad t_p = 1,$$

by Proposition 2.5 above. By Hensel's lemma, h has a root $\gamma \in p\mathbb{Z}_p$. As a generator of $D_p(A)$, we can take an eigenvector $\mathbf{u}_{31} = \mathbf{u}(\gamma)$ of A corresponding to γ. By Lemma 3.3,

$$G_A = < \mathbf{e}_1, \mathbf{e}_2, 2^{-\infty}\mathbf{u}_{21}, 2^{-\infty}\mathbf{u}_{22}, 3^{-\infty}\mathbf{u}_{31} > .$$

We now change the system $\{\mathbf{u}_{ij}\}$ so that it has the form (3.5) with respect to $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$. For $\mathbf{x}_{21} = \mathbf{u}_{21} + \lambda^{-1}\mathbf{u}_{22}$, $\mathbf{x}_{22} = \mathbf{u}_{22}$, $\mathbf{x}_{31} = (-1/6)\mathbf{u}_{31}$, we have

$$\begin{aligned} \mathbf{x}_{21} &= \mathbf{e}_1 - \lambda^{-2}\mathbf{e}_3, \quad p = 2, \\ \mathbf{x}_{22} &= \mathbf{e}_2 - \lambda^{-1}\mathbf{e}_3, \quad p = 2, \\ \mathbf{x}_{31} &= \mathbf{e}_1 - (1/2)(\gamma/3)(\gamma+1)\mathbf{e}_2 - (1/2)(\gamma/3)\mathbf{e}_3, \quad p = 3. \end{aligned}$$

Note that in $\mathbf{x}_{31}$, 2 is a unit in $\mathbb{Z}_3$ and 3 divides γ in $\mathbb{Z}_3$, so that $1/2, \gamma/3 \in \mathbb{Z}_3$. Therefore,

$$M(A; \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3) = \{\alpha_{213}, \alpha_{223}, \alpha_{312}, \alpha_{313}\},$$

where

$$\begin{aligned} &\alpha_{213} = -\lambda^{-2}, \quad \alpha_{312} = -(1/2)(\gamma/3)(\gamma+1), \\ &\alpha_{223} = -\lambda^{-1}, \quad \alpha_{313} = -(1/2)(\gamma/3) \end{aligned}$$

is the characteristic of G_A with respect to $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$.

Example 8. In this example we show another way to calculate a characteristic. We use Remark 4.4 above that a characteristic can be calculated over an extension of $\mathbb{Q}_p$ for each prime p. We find a characteristic of G_{A^t}, where A is from Example 7 and A^t is the transpose of A. Note that if δ is an eigenvalue of A, then $\mathbf{v}(\delta) = \begin{pmatrix} 1 & \delta & \delta^2 \end{pmatrix}^t$ is an eigenvector of A^t corresponding to δ. We use the notation of Example 7. For $p = 2$, let $\alpha_1, \alpha_2 \in \overline{\mathbb{Q}}_p$ be (distinct) roots of g. By Lemma 4.1, $\mathbf{v}(\alpha_1), \mathbf{v}(\alpha_2)$ are generators of the divisible part of $\overline{G}_{A,p}$ over the ring of integers of a finite extension of $\mathbb{Q}_p$ that contains α_1, α_2. We now change $\{\mathbf{v}(\alpha_1), \mathbf{v}(\alpha_2)\}$ so that it has the form (3.5). Namely, let

$$\begin{aligned} \mathbf{v}_{22} &= \frac{1}{\alpha_2 - \alpha_1}(\mathbf{v}(\alpha_2) - \mathbf{v}(\alpha_1)) = \begin{pmatrix} 0 & 1 & \alpha_1 + \alpha_2 \end{pmatrix}^t, \\ \mathbf{v}_{21} &= \mathbf{v}(\alpha_1) - \alpha_1\mathbf{v}_{22} = \begin{pmatrix} 1 & 0 & -\alpha_1\alpha_2 \end{pmatrix}^t. \end{aligned}$$

Since $\alpha_1, \alpha_2, \lambda$ are roots of h and $h = t^3 + t^2 + 2t + 6$, we have $\alpha_1 + \alpha_2 + \lambda = -1$ and $\alpha_1\alpha_2\lambda = -6$. Recall $\lambda \in \mathbb{Z}_p^\times$. Hence,

$$\begin{aligned}\mathbf{v}_{21} &= \mathbf{e}_1 + 6\lambda^{-1}\mathbf{e}_3,\\ \mathbf{v}_{22} &= \mathbf{e}_2 - (\lambda+1)\mathbf{e}_3,\\ \mathbf{v}_{31} &= \mathbf{v}(\gamma) = \mathbf{e}_1 + \gamma\mathbf{e}_2 + \gamma^2\mathbf{e}_3.\end{aligned}$$

Therefore, $M(A^t; \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3) = \{\alpha'_{213}, \alpha'_{223}, \alpha'_{312}, \alpha'_{313}\}$, where

$$\begin{aligned}\alpha'_{213} &= 6\lambda^{-1}, & \alpha'_{312} &= \gamma,\\ \alpha'_{223} &= -(\lambda+1), & \alpha'_{313} &= \gamma^2\end{aligned}$$

is the characteristic of G_{A^t} with respect to the basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$.

Example 9. Using Examples 7 and 8, we show $G_A \cong G_{A^t}$. Let

$$A = \begin{pmatrix} 0 & 0 & -6\\ 1 & 0 & -2\\ 0 & 1 & -1\end{pmatrix}, \quad \mathbf{u} = \begin{pmatrix} -6\\ \delta(\delta+1)\\ \delta\end{pmatrix}, \quad \mathbf{v} = \begin{pmatrix} 1\\ \delta\\ \delta^2\end{pmatrix},$$

where $\mathbf{u}$, $\mathbf{v}$ are eigenvectors of A, A^t, respectively, corresponding to an eigenvalue δ. Thus,

$$\begin{aligned}\mathcal{R} &= \mathcal{R}(A) = \mathcal{R}(A^t) = \left\{n2^k3^l \mid n, k, l \in \mathbb{Z}\right\},\\ I_{\mathcal{R}}(A, \delta) &= \mathrm{Span}_{\mathcal{R}}(-6, \delta, \delta(\delta+1)) = \mathrm{Span}_{\mathcal{R}}(1, \delta, \delta^2),\end{aligned}$$

since $6 \in \mathcal{R}^\times$, and

$$I_{\mathcal{R}}(A^t, \delta) = \mathrm{Span}_{\mathcal{R}}(1, \delta, \delta^2) = I_{\mathcal{R}}(A, \delta).$$

We obtain $T \in \mathrm{GL}_3(\mathcal{R})$ by expressing coordinates of $\mathbf{u}$ in terms of coordinates of $\mathbf{v}$:

$$T = \begin{pmatrix} -6 & 0 & 0\\ 0 & 1 & 1\\ 0 & 1 & 0\end{pmatrix}, \quad T^{-1} = \begin{pmatrix} -1/6 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & -1\end{pmatrix}.$$

Note that we were able to compute the characteristics of both G_A, G_{A^t} with respect to the standard basis, without having to change the basis (or, equivalently, conjugate A, A^t by matrices in $\mathrm{GL}_3(\mathbb{Z})$). Therefore, T (resp., T^{-1}) satisfies the condition (A, B, p) (resp., (B, A, p)) for any $p \in \mathcal{P}'$, since 2nd and 3rd columns of both T, T^{-1} consist of integers. Since $T \in \mathrm{GL}_3(\mathcal{R})$, characteristics of both A, A^t are with respect to the standard basis, and A, A^t share the same eigenvalues, by Proposition 6.4, $T : G_{A^t} \longrightarrow G_A$ is an isomorphism.

Example 10. Assume $A, B \in \mathrm{M}_n(\mathbb{Z})$ have irreducible characteristic polynomials. By Proposition 6.4, if $G_A \cong G_B$, then $[I_{\mathcal{R}}(A, \lambda)] = [I_{\mathcal{R}}(B, \mu)]$ under some additional conditions on A. In this example we show that this is not true in general. More precisely, $A, B \in \mathrm{M}_4(\mathbb{Z})$ share the same irreducible characteristic polynomial, $G_A \cong G_B$, but $[I_{\mathcal{R}}(A, \lambda)] \neq [I_{\mathcal{R}}(B, \mu)]$. In particular, it shows that even when the characteristic polynomials of A, B are irreducible and $G_A \cong G_B$, not every isomorphism between G_A

and G_B takes an eigenvector of A to an eigenvector of B (unlike *e.g.*, the case of a prime dimension n). Here $n = 4$ and $t_p = 2$, so that the condition $(t_p, n) = 1$ in Proposition 6.4 does not hold.

Let $h(t) = t^4 - 2t^3 + 21t^2 - 20t + 5$, irreducible over $\mathbb{Q}$, and let $\lambda \in \overline{\mathbb{Q}}$ be a root of h. By [LMFDB], $\mathcal{O}_K = \mathbb{Z}[\lambda]$, K is Galois over $\mathbb{Q}$, $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, and the ideal class group of K is non-trivial. Thus, there exists an ideal J_1 of $\mathbb{Z}[\lambda]$ such that its ideal class $[J_1]$ is not trivial, *i.e.*, there is no $x \in K$ such that $J_1 = x\mathbb{Z}[\lambda]$. By [SAGE], we can take J_1 to be the ideal of $\mathbb{Z}[\lambda]$ generated by 7 and $\lambda^3 - \lambda^2 + 20\lambda - 4$ over $\mathbb{Z}[\lambda]$, denoted by $J_1 = (7, \lambda^3 - \lambda^2 + 20\lambda - 4)$. One can also find a $\mathbb{Z}$-basis of J_1, *e.g.*, $J_1 = \mathbb{Z}[\omega_1, \omega_2, \omega_3, \omega_4]$, where

$$\begin{aligned} \omega_1 &= 7, \\ \omega_2 &= 2\lambda^3 - 3\lambda^2 + 41\lambda - 16, \\ \omega_3 &= \lambda^3 - \lambda^2 + 20\lambda - 4, \\ \omega_4 &= -2\lambda^3 + 3\lambda^2 - 40\lambda + 25. \end{aligned}$$

Since $[J_1]$ is non-trivial, by Latimer–MacDuffee–Taussky Theorem [T49], matrices A, B corresponding to $(1) = \mathbb{Z}[\lambda]$ and J_1, respectively, are not conjugated by a matrix from $\mathrm{GL}_4(\mathbb{Z})$. We find A, B from the condition that

$$\mathbf{u} = \begin{pmatrix} 1 & \lambda & \lambda^2 & \lambda^3 \end{pmatrix}^t, \quad \mathbf{v} = \begin{pmatrix} \omega_1 & \omega_2 & \omega_3 & \omega_4 \end{pmatrix}^t$$

are eigenvectors of A, B, respectively, corresponding to λ. Thus,

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -5 & 20 & -21 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} -9 & 7 & 0 & 7 \\ -6 & 4 & 1 & 4 \\ 5 & -4 & 1 & -4 \\ -8 & 5 & 1 & 6 \end{pmatrix}.$$

Both A, B have characteristic polynomial $h(t) = t^4 - 2t^3 + 21t^2 - 20t + 5$, $\det A = \det B = 5$, $\mathcal{P} = \mathcal{P}' = \{5\}$, $t_5 = 2$, and $[I_{\mathbb{Z}}(A, \lambda)] \neq [I_{\mathbb{Z}}(B, \lambda)]$. We show $[I_{\mathcal{R}}(A, \lambda)] \neq [I_{\mathcal{R}}(B, \lambda)]$, where $\mathcal{R} = \{\frac{m}{5^k} \mid m, k \in \mathbb{Z}\}$. Equivalently, we show that there is no $x \in K$ such that

$$x(I_{\mathbb{Z}}(A, \lambda) \otimes_{\mathbb{Z}} \mathcal{R}) = I_{\mathbb{Z}}(B, \lambda) \otimes_{\mathbb{Z}} \mathcal{R}, \tag{7.1}$$

where

$$\begin{aligned} I_{\mathbb{Z}}(A, \lambda) &= \mathbb{Z}[1, \lambda, \lambda^2, \lambda^3] = (1), \\ I_{\mathbb{Z}}(B, \lambda) &= \mathbb{Z}[\omega_1, \omega_2, \omega_2, \omega_3] = J_1. \end{aligned}$$

We also demonstrate how the standard methods of working with fractional ideals of $\mathcal{O}_K$ (such as the prime ideal factorization and divisibility properties) can be used in the case of the ring $\mathcal{R}$. This suggests the practicality of using generalized ideal classes. Assume there exists $x \in K$ satisfying (7.1). Then $5^k x \in J_1$ for some $k \in \mathbb{N} \cup \{0\}$. In particular, $y = 5^k x \in \mathbb{Z}[\lambda]$. Then $y \in J_1$ implies that J_1 divides the ideal $(y) = y\mathbb{Z}[\lambda]$ of $\mathbb{Z}[\lambda]$ generated by y, *i.e.*, $(y) = J_1\mathfrak{A}$ for an (integral) ideal $\mathfrak{A} \subseteq \mathbb{Z}[\lambda]$ of $\mathbb{Z}[\lambda]$. Note that $\mathfrak{A}$ is not principal (*i.e.*, $\mathfrak{A} \neq x\mathbb{Z}[\lambda]$ for any $x \in K$), since the class of J_1 is non-trivial. Analogously, (7.1) implies $5^t J_1 \subseteq (y)$ and hence $5^t J_1 = (y)\mathfrak{A}'$ for an (integral) ideal $\mathfrak{A}' \subseteq \mathbb{Z}[\lambda]$ of $\mathbb{Z}[\lambda]$. Combining the two equalities, we get

$$5^t J_1 = (y)\mathfrak{A}' = J_1 \mathfrak{A}\mathfrak{A}'.$$

Cancelling J_1, this implies $(5^t) = \mathfrak{A}\mathfrak{A}'$. Using [SAGE], we can check that all the prime ideal divisors of the ideal (5) are principal, hence $\mathfrak{A}$ is principal and so is J_1, which is a contradiction. This shows $[I_{\mathcal{R}}(A,\lambda)] \neq [I_{\mathcal{R}}(B,\lambda)]$. Nonetheless, we show next that $G_A \cong G_B$.

By [SAGE], $(5) = \mathfrak{p}_1^2\mathfrak{p}_2^2$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are prime ideals of $\mathbb{Z}[\lambda]$, $\mathfrak{p}_1 = (\lambda)$, and there exists $g \in \mathrm{Gal}(K/\mathbb{Q})$ of order 2 such that $g(\mathfrak{p}_i) = \mathfrak{p}_i$, $i = 1, 2$. In the notation of Theorem 4.3, $X_{A,\mathfrak{p}_1} = \mathrm{Span}_K(\mathbf{u}, g(\mathbf{u}))$, $X_{B,\mathfrak{p}_1} = \mathrm{Span}_K(\mathbf{v}, g(\mathbf{v}))$. We look for $f_1, f_2 \in K$ such that $f_1\mathbf{v} + f_2 g(\mathbf{v}) \in \mathcal{R}[\lambda]$. Using the action of g, the condition is equivalent to the existence of $T \in \mathrm{GL}_4(\mathcal{R})$ with $T(X_{A,\mathfrak{p}_1}) = X_{B,\mathfrak{p}_1}$, namely, $f_1\mathbf{v} + f_2 g(\mathbf{v}) = T(\mathbf{u})$. Note that any element in K can be written as $\mathbb{Q}$-linear combination of $1, \lambda, \lambda^2, \lambda^3$, since $K = \mathbb{Q}(\lambda)$ of degree 4 over $\mathbb{Q}$. In other words, for any $f_1, f_2 \in K$ there is $L \in \mathrm{GL}_4(\mathbb{Q})$ such that $f_1\mathbf{v} + f_2 g(\mathbf{v}) = L(\mathbf{u})$. The goal is to find $f_1, f_2 \in K$ so that both L, L^{-1} have coefficients in $\mathcal{R}$, *i.e.*, the denominators of coefficients of both L, L^{-1} are powers of 5. It turns out that such f_1, f_2 exist, namely,

$$\begin{aligned} f_1 &= \frac{39}{350}\lambda^3 - \frac{29}{175}\lambda^2 + \frac{739}{350}\lambda - \frac{5}{14}, \\ f_2 &= \frac{61}{350}\lambda^3 - \frac{46}{175}\lambda^2 + \frac{1261}{350}\lambda - \frac{27}{14}, \end{aligned}$$

and $f_1\mathbf{v} + f_2 g(\mathbf{v}) = T(\mathbf{u})$ with

$$T = \begin{pmatrix} -21 & 40 & -3 & 2 \\ -\frac{72}{5} & \frac{141}{5} & -\frac{11}{5} & \frac{7}{5} \\ 0 & 1 & 0 & 0 \\ -20 & 40 & -3 & 2 \end{pmatrix}, \quad \det T = -\frac{1}{5}, \quad T \in \mathrm{GL}_4(\mathcal{R}).$$

We use Theorem 4.3 to show that T is an isomorphism from G_A to G_B, *i.e.*, $T(G_A) = G_B$. First, we find characteristics of G_A, G_B. We apply the process described in the proof of Lemma 3.4 to vectors $\mathbf{u}, g(\mathbf{u})$. We have

$$\mathbf{u} = \begin{pmatrix} 1 & \lambda & \lambda^2 & \lambda^3 \end{pmatrix}^t, \quad g(\mathbf{u}) = \begin{pmatrix} 1 & g(\lambda) & g(\lambda^2) & g(\lambda^3) \end{pmatrix}^t,$$

where

$$\begin{aligned} g(\lambda) &= -4\lambda^3 + 6\lambda^2 - 81\lambda + 40, \\ g(\lambda^2) &= -4\lambda^3 + 5\lambda^2 - 80\lambda + 20, \\ g(\lambda^3) &= 75\lambda^3 - 114\lambda^2 + 1520\lambda - 770. \end{aligned}$$

Applying column operations on $\begin{pmatrix}\mathbf{u} & g(\mathbf{u})\end{pmatrix}$ corresponding to multiplications by matrices from $\mathrm{GL}_4(\mathbb{Z}_5)$, we arrive at

$$\begin{pmatrix}1 & 0 & -\delta & -2\delta+10 \\ 0 & 1 & 2\delta+40 & 3\delta+40\end{pmatrix}^t, \quad \delta = -2\lambda^3+3\lambda^2-40\lambda+20.$$

Therefore,

$$M(A;\mathbf{e}_1,\dots,\mathbf{e}_4) = \{\alpha_{513}(A), \alpha_{514}(A), \alpha_{523}(A), \alpha_{524}(A)\},$$

where

$$\alpha_{513}(A) = -\delta, \qquad \alpha_{514}(A) = -2\delta+10,$$
$$\alpha_{523}(A) = 2\delta+40, \quad \alpha_{524}(A) = 3\delta+40.$$

Note that $K_{\mathfrak{p}_1}$ is an extension of $\mathbb{Q}_5$ of degree 2 and $\mathrm{Gal}(K_{\mathfrak{p}_1}/\mathbb{Q}_5)$ is generated by g. Since $\delta \in \mathbb{Z}[\lambda]$, under an embedding $K \hookrightarrow K_{\mathfrak{p}_1}$, δ becomes an element of the ring of integers of $K_{\mathfrak{p}_1}$. Since $\delta = \lambda \cdot g(\lambda)$, δ is an integral element of $\mathbb{Q}_5$ and therefore, $\delta \in \mathbb{Z}_5$. Therefore, all the elements $\alpha_{5ij}(A)$ in $M(A;\mathbf{e}_1,\dots,\mathbf{e}_4)$ belong to $\mathbb{Z}_5$. To find a characteristic of G_B, we repeat the above process for vectors $\mathbf{v}, g(\mathbf{v})$. We arrive at

$$\begin{pmatrix}1 & 0 & \frac{1}{7}(1-4\delta) & \frac{1}{7}(\delta+5) \\ 0 & 1 & \delta & 0\end{pmatrix}^t, \quad \delta = -2\lambda^3+3\lambda^2-40\lambda+20,$$

and

$$M(B;\mathbf{e}_1,\dots,\mathbf{e}_4) = \{\alpha_{513}(B), \alpha_{514}(B), \alpha_{523}(B), \alpha_{524}(B)\},$$

where

$$\alpha_{513}(B) = \frac{1}{7}(1-4\delta), \quad \alpha_{514}(B) = \frac{1}{7}(\delta+5),$$
$$\alpha_{523}(B) = \delta, \qquad \alpha_{524}(B) = 0.$$

Note that all $\alpha_{5ij}(B) \in \mathbb{Z}_5$. We can now check the condition $(A,B,5)$ for T in Theorem 4.3. It holds, because $\alpha(B)_{523} = \delta$, $\alpha(B)_{524} = 0$ are both divisible by 5 in $\mathbb{Z}_5$ (by the choice of $\mathfrak{p}_1$, λ is divisible by $\mathfrak{p}_1$ in $\mathcal{O}_{\mathfrak{p}_1}$). Since T^{-1} has integer coefficients, the condition $(B,A,5)$ holds automatically. In Theorem 4.3, the conditions

$$\mathcal{P}(A) = \mathcal{P}(B) = \{5\}, \quad \mathcal{R} = \mathcal{R}(A) = \mathcal{R}(B),$$
$$\mathcal{P}'(A) = \mathcal{P}'(B) = \{5\}, \quad t_5(A) = t_5(B) = 2$$

hold automatically, since A, B share the same eigenvalues. Also, $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ above 5, so there exists $g' \in \mathrm{Gal}(K/\mathbb{Q})$ such that $g'(\mathfrak{p}_1) = \mathfrak{p}_2$. By above, $T(X_{A,\mathfrak{p}_1}) = X_{B,\mathfrak{p}_1}$, $T \in \mathrm{GL}_4(\mathcal{R})$, and applying g', we get $T(X_{A,\mathfrak{p}_2}) = X_{B,\mathfrak{p}_2}$. By Theorem 4.3, $G_A \cong G_B$, but $[I_{\mathcal{R}}(A,\lambda)] \neq [I_{\mathcal{R}}(B,\lambda)]$, even though the characteristic polynomials of A, B are irreducible over $\mathbb{Q}$.

Example 11. The motivation behind this example is the following question. Assume the characteristic polynomial of A is irreducible and $G_A \cong G_B$. Is necessarily the characteristic polynomial of B also irreducible? This is true for $n = 2$ (see [S22, Remark 4.2]) and it turns out that this is not true for an arbitrary n. In our example, $n = 4$, $A, C \in \mathrm{M}_4(\mathbb{Z})$ have the same irreducible characteristic polynomial $h(t) = t^4 + t^2 + 9$, and $G_A = G_C$. Let $B = C^2$. Then the minimal polynomial of B is $t^2 + t + 9$, so that the characteristic polynomial of B is $(t^2+t+9)^2$, not irreducible. However, $G_B = G_C = G_A$. More precisely,

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -9 & 0 & -1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & -1 & 0 \\ 9 & 0 & 2 & 1 \\ 9 & 0 & 1 & 1 \\ -18 & -9 & 7 & -1 \end{pmatrix},$$

where $\det A = \det C = 9$, $\mathcal{P} = \mathcal{P}' = \{3\}$, and $t_3 = 2$. By Hensel's lemma, there exists a root $\lambda \in \overline{\mathbb{Q}}$ of h such that $\lambda \in \mathbb{Z}_3^\times$ under $\mathbb{Q}(\lambda) \hookrightarrow \mathbb{Q}(\lambda)_\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of the ring of integers of $\mathbb{Q}(\lambda)$ above 3. One can show that

$$G_A = G_C = < \mathbf{e}_1, \ldots, \mathbf{e}_4, 3^{-\infty}(\mathbf{e}_1 + \lambda^2\mathbf{e}_3), 3^{-\infty}(\mathbf{e}_2 + \lambda^2\mathbf{e}_4) > .$$

(For example, we can apply the process described in the proof of Lemma 3.4 to eigenvectors

$$\mathbf{u}_i = \begin{pmatrix} 1 & \pm\lambda & \lambda^2 & \pm\lambda^3 \end{pmatrix}^t, \quad \mathbf{v}_i = \begin{pmatrix} 1 & \pm\lambda + \lambda^2 & \lambda^2 & \pm\lambda^3 - \lambda^2 - 9 \end{pmatrix}^t, \ i = 1, 2,$$

of A, C, respectively, corresponding to $\pm\lambda$.) Thus, $G_B = G_C = G_A$, the characteristic polynomial of A is irreducible, and the characteristic polynomial of B is not irreducible.

8. Applications

8.1. **$\mathbb{Z}^n$-odometers.** In this section we generalize our results in [S22] on application of groups G_A to $\mathbb{Z}^2$-odometers to the n-dimensional case. By definition, a $\mathbb{Z}^n$-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.

In the next lemma we analyze when G_A is dense in $\mathbb{Q}^n$. The result generalizes the case $n = 2$ [S22, Lemma 8.4]. Let $A \in \mathrm{M}_n(\mathbb{Z})$ be non-singular and let $h_A \in \mathbb{Z}[t]$ be the characteristic polynomial of A. Let $h_A = h_1 h_2 \cdots h_s$, where $h_1, \ldots, h_s \in \mathbb{Z}[t]$ are irreducible of degrees $n_1, \dots, n_s$, respectively. By Theorem 9.1 below, there exists $S \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$SAS^{-1} = \begin{pmatrix} A_1 & * & \cdots & * \\ 0 & A_2 & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_s \end{pmatrix}, \tag{8.1}$$

where each $A_i \in \mathrm{M}_{n_i}(\mathbb{Z})$ has characteristic polynomial h_i, $i \in \{1, 2, \dots, s\}$.

Lemma 8.1. *G_A is dense in $\mathbb{Q}^n$ if and only if $A_i \notin \mathrm{GL}_{n_i}(\mathbb{Z})$ for all $i \in \{1, 2, \dots, s\}$. Equivalently, G_A is dense in $\mathbb{Q}^n$ if and only if $\det A_i \neq \pm 1$ for all $i \in \{1, 2, \dots, s\}$ if and only if $h_i(0) \neq \pm 1$ for all $i \in \{1, 2, \dots, s\}$.*

Proof. As in the proof of Lemma 8.4 in [S22], G_A is dense in $\mathbb{Q}^n$ if and only if

$$A^{-i}\mathbf{y} \in \mathbb{Z}^n \text{ for any } i \in \mathbb{N}, \quad \mathbf{y} \in \mathbb{Z}^n, \tag{8.2}$$

implies $\mathbf{y} = \mathbf{0}$. We first show that if there exists $A_i \in \mathrm{GL}_{n_i}(\mathbb{Z})$, then G_A is not dense. Indeed, without loss of generality, we can assume that A itself has the block upper-triangular form (8.1) and that $A_1 \in \mathrm{GL}_{n_1}(\mathbb{Z})$. Then for any $\mathbf{y}_0 \in \mathbb{Z}^{n_1}$ and $i \in \mathbb{N}$, $A_1^{-i}\mathbf{y}_0 \in \mathbb{Z}^{n_1}$, so that there exists non-zero $\mathbf{y} = \begin{pmatrix} \mathbf{y}_0 & \mathbf{0} \end{pmatrix}^t \in \mathbb{Z}^n$ satisfying (8.2), and G_A is not dense.

We are now left to show that if G_A is not dense, then there exists $A_i \in \mathrm{GL}_{n_i}(\mathbb{Z})$. We first consider the case when h_A is irreducible. Assume G_A is not dense, hence there exists $\mathbf{y} \neq \mathbf{0}$ satisfying (8.2). Note that A is diagonalizable with eigenvectors $\mathbf{u}_1, \dots, \mathbf{u}_n \in \mathbb{C}^n$, linearly independent over $\mathbb{C}$, corresponding to eigenvectors $\lambda_1, \dots, \lambda_n \in \mathbb{C}$, respectively. Let $M = \begin{pmatrix} \mathbf{u}_1 & \dots & \mathbf{u}_n \end{pmatrix} \in \mathrm{GL}_n(\mathbb{C})$. Let K be a finite Galois extension of $\mathbb{Q}$ that contains all the eigenvalues of A and let $\mathcal{O}_K$ denote its ring of integers. Without loss of generality, we can assume that $M \in \mathrm{M}_n(\mathcal{O}_K)$, so that $\det M \in \mathcal{O}_K - \{0\}$. Let $\mathbf{y} \in \mathbb{Z}^n$ satisfy (8.2), $\mathbf{y} = \sum_{j=1}^n c_j \mathbf{u}_j$, $c_1, \dots, c_n \in K$, not all are zeroes. Then (8.2) implies

$$A^{-i}\mathbf{y} = M \cdot \begin{pmatrix} c_1\lambda_1^{-i} & c_2\lambda_2^{-i} & \dots & c_n\lambda_n^{-i} \end{pmatrix}^t \in \mathbb{Z}^n.$$

Thus, multiplying the last formula (on the left) by the adjoint matrix $\tilde{M} \in \mathrm{M}_n(\mathcal{O}_K)$ of M, we have

$$\det M c_j \lambda_j^{-i} \in \mathcal{O}_K \text{ for any } i \in \mathbb{N} \text{ and } j \in \{1, 2, \dots, s\}. \tag{8.3}$$

Since there exists $c_k \neq 0$ for some $k \in \{1, \dots, n\}$ and $\det M \neq 0$, we have $\lambda_k \in \mathcal{O}_K^\times$, *i.e.*, λ_k is a unit in $\mathcal{O}_K$. Indeed, otherwise there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ dividing λ_k. Then, writing, $c_k = \gamma_k/\delta_k$, $\gamma_k, \delta_k \in \mathcal{O}_K - \{0\}$, from (8.3) for $j = k$ we get that non-zero $\det M\gamma_k \in \mathcal{O}_K$ (which does not depend on i) is divisible by arbitrary powers $\mathfrak{p}^i$, $i \in \mathbb{N}$, which is impossible. Since h_A is irreducible by assumption, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts transitively on the set of eigenvalues of A. Thus, since there is one eigenvalue $\lambda_k \in \mathcal{O}_K^\times$, all the eigenvalues of A are units in $\mathcal{O}_K$ and their product $\lambda_1\lambda_2\cdots\lambda_n = \det A$ is a unit in $\mathbb{Z}$, *i.e.*, $\det A = \pm 1$ and $A \in \mathrm{GL}_n(\mathbb{Z})$.

We now assume that h_A is not irreducible. We need to show that if G_A is not dense, then there exists $A_i \in \mathrm{GL}_{n_i}(\mathbb{Z})$. Equivalently, if all $A_i \notin \mathrm{GL}_{n_i}(\mathbb{Z})$, then G_A is dense. Assume all $A_i \notin \mathrm{GL}_{n_i}(\mathbb{Z})$. We prove that this implies that G_A is dense by induction on the number of irreducible components of h_A; the base of the induction (the case of one irreducible component) is considered in the preceding paragraph. Let $h_A = h_1 h_2$, where $h_1, h_2 \in \mathbb{Z}[t]$ are monic polynomials of degrees $n_1, n_2 \in \mathbb{N}$, respectively. By Theorem 9.1 below, there exists $T \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$TAT^{-1} = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}, \tag{8.4}$$

where each $A_i \in \mathrm{M}_{n_i}(\mathbb{Z})$ has characteristic polynomial h_i, $i = 1, 2$. Without loss of generality, we can assume that A itself has the block triangular form (8.4). Clearly, $C \notin \mathrm{GL}(\mathbb{Z})$ for any "irreducible" block C of A_1, A_2. Then, by induction, G_{A_i} is dense in $\mathbb{Q}^{n_i}$, $i = 1, 2$. Namely, if $\mathbf{y} \in \mathbb{Z}^n$ satisfies (8.2) and $\mathbf{y} = \begin{pmatrix} \mathbf{y}_1 & \mathbf{y}_2 \end{pmatrix}^t$, $\mathbf{y}_i \in \mathbb{Z}^{n_i}$, $i = 1, 2$, then $A_2^{-i}\mathbf{y}_2 \in \mathbb{Z}^{n_2}$ for all $i \in \mathbb{N}$, and hence $\mathbf{y}_2 = \mathbf{0}$ by induction. Then, (8.2) implies $A_1^{-i}\mathbf{y}_1 \in \mathbb{Z}^{n_1}$ for all $i \in \mathbb{N}$, and hence $\mathbf{y}_1 = \mathbf{0}$ by induction as well. Thus, $\mathbf{y} = \mathbf{0}$ and G_A is dense in $\mathbb{Q}^n$.

The other two equivalent formulations follow from the facts that $A \in \mathrm{M}_n(\mathbb{Z})$ belongs to $\mathrm{GL}_n(\mathbb{Z})$ if and only if $\det A = \pm 1$ and if $h \in \mathbb{Z}[t]$ is the characteristic polynomial of A, then $\det A = (-1)^n h(0)$. □

Lemma 8.2. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$ be non-singular such that G_A (resp., G_B) is dense in $\mathbb{Q}^n$ (see Lemma 8.1). Then $\mathbb{Z}^n$-actions Y_A, Y_B are orbit equivalent if and only if* $\det A, \det B$ *have the same prime divisors.*

Proof. Follows from [GPS19, Theorem 1.5] and [S22, Lemma 8.5]. □

In [GPS19, Theorem 1.5], the authors give a characterization of various equivalences of $\mathbb{Z}^2$-odometers Y_H in terms of the corresponding groups H. In our subsequent paper, we extend their results to the n-dimensional case of $\mathbb{Z}^n$-odometers and apply them for odometers of the form Y_A defined by non-singular matrices $A \in \mathrm{M}_n(\mathbb{Z})$.

9. 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 with a slight modification, which is useful in calculating examples.

Theorem 9.1. *Let R be a PID with field of fractions of characteristic zero. For any $A \in \mathrm{M}_n(R)$ 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, $i \in \{1, 2, \dots, t\}$, $1 \le t \le n$.

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. It is well-known that L is the field of fractions of $R[\alpha]$. Let $\mathbf{u} \in (\overline{F})^n$ be an eigenvector of A corresponding to α. Without loss of generality, we can assume that $\mathbf{u} \in R[\alpha]^n$. Then

$$\mathbf{u} = C\omega, \quad \omega = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{k-1} \end{pmatrix}^t$$

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 $1, \alpha, \dots, \alpha^{k-1}$ is a basis of L over F. Since R is a PID, matrix C has a Smith normal form, *i.e.*, there exist $\lambda_1, \dots, \lambda_r \in R - \{0\}$, $U \in \mathrm{GL}_n(R)$, and $V \in \mathrm{GL}_k(R)$ such that

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

where $T \in \mathrm{M}_{n\times k}(R)$, $\Lambda = \mathrm{diag}(\lambda_1, \dots, \lambda_r)$ is a non-singular diagonal matrix, and $r \le k$. 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

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} V = \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} VB. \tag{9.1}$$

Thus, $A_3\Lambda = 0$ 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 (9.1) by ω on the right, we get

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} V\omega = \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} VB\omega = \alpha \begin{pmatrix} \Lambda & 0 \\ 0 & 0 \end{pmatrix} V\omega, \tag{9.2}$$

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 (9.2) 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. □

References

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

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

[D37] D. Derry, *Uber Eine Klasse von Abelschen Gruppen*, Proc. London Math. Soc. (2) 43 (1937), no. 7, 490–506.

[F73] L. Fuchs, Infinite abelian groups. Vol. II. Pure and Applied Mathematics. Vol. 36-II. Academic Press, New York-London, 1973.

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

[GM81] R. Gütling, O. Mutzbauer, *Classification of torsion free abelian minimax groups*, Rend. Sem. Mat. Univ. Padova 64 (1981), 193–199.

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database*, home page of the number field `4.0.144400.1`, https://www.lmfdb.org/NumberField/4.0.144400.1, 2022, [Online; accessed 8 June 2022].

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

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

[SAGE] William A. Stein et al. Sage Mathematics Software (Version 9.6), The Sage Development Team, 2022, http://www.sagemath.org.

[S22] M. Sabitova, *Generalized ideal classes in application to toroidal solenoids*, Pacific Journal of Mathematics 318-1 (2022), 189–228.

[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.