ALBANIAN JOURNAL OF MATHEMATICS
Volume 13, Number 1, Pages 211–218
ISSN: 1930-1235; (**2019**)

ON CONJUGACY OF DIAGONALIZABLE INTEGRAL MATRICES

GABRIELE NEBE

Lehrstuhl D für Mathematik,
RWTH Aachen University, Germany

Abstract. It is shown that under some additional assumption two diagonalizable integral matrices X and Y with only rational eigenvalues are conjugate in $\mathrm{GL}_n(\mathbb{Z})$ if and only if they are conjugate over all localizations. This is used to prove that for a prime $p \equiv 3 \pmod 4$ the adjacency matrices of the Paley graph and the Peisert graph on p^2 vertices are conjugate in $\mathrm{GL}_{p^2}(\mathbb{Z})$, answering a question by Peter Sin [9].

MSC 2010: 15B36, 11R65, 05B20
Keywords: conjugacy of integral matrices, lattices over orders, Payley graph, Peisert graph

1. Introduction

Let X, $Y \in \mathbb{Z}^{n\times n}$ be two integral matrices. Then $C(X) := \{A \in \mathbb{Z}^{n\times n} \mid AX = XA\}$ is a $\mathbb{Z}$-order and $C(X,Y) := \{A \in \mathbb{Z}^{n\times n} \mid AX = YA\}$ is a right module for $C(X)$. Faddeev [4] shows that X and Y are conjugate in $\mathrm{GL}_n(\mathbb{Z})$ if and only if $C(X,Y)$ is a free $C(X)$-module.

Local-global properties for similarity of matrices have been considered for lattices over orders in [6] and later in [5]. Using the above mentioned result by Faddeev both papers, [6, Satz 7] and [5, Theorem 7], show that two matrices over the ring of integers in an algebraic number field are conjugate over all localizations if and only if they are conjugate over the ring of integers in some finite field extension. In certain cases, there is no need to pass to an extension field. This paper gives an additional sufficient condition (see Assumption 2.1) for which a thorough analysis of [6] allows to prove Theorem 2.2 saying that, two diagonalizable integral matrices satisfying Assumption 2.1 are conjugate in $\mathrm{GL}_n(\mathbb{Z})$ if and only if they are conjugate over all localizations.

E-mail address: nebe@math.rwth-aachen.de.

The work on this paper started during the Hausdorff Trimester program "Logic and Algorithmic group theory". I thank the HIM for their support during this program and Eamonn O'Brien for communicating a question by Peter Sin which was the main motivation for this note. The recent paper [9] shows that for any prime $p \equiv 3 \pmod 4$ the adjacency matrices of the Paley graph $A(p^2)$ and the Peisert graph $A^*(p^2)$ on p^2 vertices are conjugate over all localizations of $\mathbb{Z}$ and asks whether these are also conjugate in $\mathrm{GL}_{p^2}(\mathbb{Z})$. As these adjacency matrices are rationally diagonalizable and satisfy Assumption 2.1 (see Section 4) Theorem 2.2 implies a positive answer to this question.

The paper contributes to the SFB TRR 195 "Symbolic Tools in Mathematics and their Application".

2. Notation and statement of main result

We denote by $\mathbb{Z}$ the ring of integers in the rationals $\mathbb{Q}$. For a prime p let

$$\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \text{ does not divide } b\}$$

denote the localization of $\mathbb{Z}$ at p. For $n \in \mathbb{N}$ let

$$\mathrm{GL}_n(\mathbb{Z}) := \{g \in \mathbb{Z}^{n\times n} \mid \det(g) \in \{\pm 1\}\}$$

be the group of invertible integral matrices of size n and

$$\mathrm{GL}_n(\mathbb{Z}_{(p)}) := \{g \in \mathbb{Z}_{(p)}^{n\times n} \mid p \text{ does not divide } \det(g)\}$$

the group of invertible matrices over $\mathbb{Z}_{(p)}$.

Let $A \in \mathbb{Z}^{n\times n}$. Then there are matrices $g, h \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$gAh = \mathrm{diag}(d_1, \ldots, d_r, 0, \ldots, 0), \text{ with } d_i \in \mathbb{N},\ d_1 \mid d_2 \mid \ldots \mid d_r.$$

Then the *abelian invariants* $(d_1, \ldots, d_r)$ of A are uniquely determined by A and the *Smith group* of A is the torsion part of the cokernel of the endomorphism A; as an abelian group this is isomorphic to $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$. Its exponent is d_r.

In this note we consider integral diagonalizable matrices $X, Y \in \mathbb{Z}^{n\times n}$ with the same minimal polynomial $\mu_X = \mu_Y = \prod_{i=1}^{k}(t - a_i) \in \mathbb{Z}[t]$ where $a_1, \ldots, a_k \in \mathbb{Z}$ are pairwise distinct integers. Then by Chinese Remainder Theorem the $\mathbb{Q}$-algebras $\mathbb{Q}[X]$ and also $\mathbb{Q}[Y]$ are isomorphic to a direct sum of copies of $\mathbb{Q}$

$$\mathbb{Q}[X] \cong \bigoplus_{i=1}^{k} \mathbb{Q}[t]/(t - a_i) \cong \bigoplus_{i=1}^{k} \mathbb{Q}.$$

Let $e_i \in \mathbb{Q}[X] \subseteq \mathbb{Q}^{n\times n}$ denote the primitive idempotents of this algebra ($1 \le i \le k$). Then there are minimal $q_i \in \mathbb{N}$ such that $E_i := q_i e_i \in \mathbb{Z}^{n\times n}$ for all i. For our proof of the main result we make the following assumption on the Smith group of E_i:

Assumption 2.1. *Assume that one of the following two statements holds:*

(a) *For all $1 \le i \le k$ the Smith group of E_i has exponent q_i.*
(b) $\mathrm{rk}(e_1) = 1$ *and for all $2 \le i \le k$ the Smith group of E_i has exponent q_i.*

Though the formulation of part (b) of the assumption does not seem to be natural, this is the situation that will occur quite frequently in graph theory. It is the one that we need in Section 4.

Theorem 2.2. *Let $X, Y \in \mathbb{Z}^{n\times n}$ be two matrices with minimal polynomial $\mu_X = \mu_Y = \prod_{i=1}^k (t-a_i) \in \mathbb{Z}[t]$ where $a_1,\ldots,a_k \in \mathbb{Z}$ are pairwise distinct integers. Assume that X satisfies Assumption 2.1. Then there is some $T \in \mathrm{GL}_n(\mathbb{Z})$ with $TXT^{-1} = Y$ if and only if for all primes p there are matrices $T_p \in \mathrm{GL}_n(\mathbb{Z}_{(p)})$ with $T_pXT_p^{-1} = Y$.*

Note that we could prove Theorem 2.2 under weaker hypotheses, for instance for minimal polynomials $\mu_X = \mu_Y = \prod_{i=1}^k f_i$ where all the pairwise distinct irreducible factors f_i have equation orders $\mathbb{Z}[t]/(f_i(t))$ that are principal ideal domains. Such an assumption on the equation orders is necessary as the following example shows: Put

$$Y := \begin{pmatrix} 0 & 1 \\ -6 & 0 \end{pmatrix},\ X := \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix},\ T_2 := \begin{pmatrix} 0 & -1 \\ 3 & 0 \end{pmatrix},\ T_p := \mathrm{diag}(1,2) \text{ for } p > 2.$$

Then $\mu_X = \mu_Y = t^2+6$ is irreducible but the equation order $\mathbb{Z}[t]/(t^2+6) \cong \mathbb{Z}[\sqrt{-6}]$ has class number 2. It is easy to see that X and Y are not conjugate in $\mathrm{GL}_2(\mathbb{Z})$ but for all primes p the matrix $T_p \in \mathrm{GL}_2(\mathbb{Z}_{(p)})$ satisfies $T_pXT_p^{-1} = Y$, so X and Y are conjugate over all localizations.

Also Assumption 2.1 cannot be completely omitted, as can be seen by taking

$$Y := \begin{pmatrix} 1 & 1 \\ 0 & 6 \end{pmatrix},\ X := \begin{pmatrix} 1 & 2 \\ 0 & 6 \end{pmatrix},\ T_2 := \begin{pmatrix} -1 & 1 \\ 0 & 3 \end{pmatrix},\ T_p := \mathrm{diag}(1,2) \text{ for } p > 2.$$

Here $\mu_X = \mu_Y = (t-1)(t-6)$ and $T_pXT_p^{-1} = Y$ for all primes p but X and Y are not conjugate over $\mathrm{GL}_2(\mathbb{Z})$. Note that neither X nor Y satisfies Assumption 2.1 as both matrices

$$E_1 = 5e_1 = X - 1, E_2 = 5e_2 = 6 - X$$

have trivial Smith group.

3. Proof of Theorem 2.2 based on [6]

For a ring O we put $\mathrm{SL}_n(O) := \{g \in O^{n\times n} \mid \det(g) = 1\}$.

Lemma 3.1. *(see [7, Theorem K.14]) Let $q \in \mathbb{Z}$ be such that $q \geq 2$. Then the entry-wise reduction map $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/q\mathbb{Z})$ is onto.*

It is clear that Lemma 3.1 cannot be true for GL_n, as the determinant of the reduction modulo q of a matrix in $\mathrm{GL}_n(\mathbb{Z})$ is ± 1 mod q.

One direction of Theorem 2.2 is obvious: If there is a matrix $T \in \mathrm{GL}_n(\mathbb{Z})$ with $TXT^{-1} = Y$ then we may put $T_p := T \in \mathrm{GL}_n(\mathbb{Z}_{(p)})$ for all primes p to see that the two matrices are also conjugate over all localizations.

To see the opposite direction we use [6, Satz 4]. I thank Peter Sin for simplifying my original approach.

The ring

$$R := \mathbb{Z}[t]/\prod_{i=1}^k (t-a_i)$$

is a $\mathbb{Z}$-order in the commutative split semisimple $\mathbb{Q}$-algebra

$$\mathcal{A} := \mathbb{Q}[t]/\prod_{i=1}^k (t-a_i) \cong \bigoplus_{i=1}^k \mathbb{Q}.$$

Let $e_1,\dots,e_k\in\mathcal{A}$ denote the primitive idempotents. Then the unique maximal order $\mathcal{O}$ in $\mathcal{A}$ is

$$\mathcal{O}=\bigoplus_{i=1}^{k} Re_i\cong\bigoplus_{i=1}^{k}\mathbb{Z}.$$

The two matrices X and Y in $\mathbb{Z}^{n\times n}$ with minimal polynomial $\mu_X=\mu_Y=\prod_{i=1}^{k}(t-a_i)$ define two R-module structures M_X and M_Y on $\mathbb{Z}^{1\times n}$ by letting t act as right multiplication by X respectively Y.

Remark 3.2. $C(X)=\{A\in\mathbb{Z}^{n\times n}\mid AX=XA\}\cong\mathrm{End}_R(M_X)$ and $C(X,Y)\cong\mathrm{Hom}_R(M_Y,M_X)$. In particular any isomorphism between the two R-modules M_X and M_Y is given by a matrix $T\in\mathrm{GL}_n(\mathbb{Z})$ conjugating X to Y.

Applying Remark 3.2 to the localizations of M_X and M_Y, the matrices $T_p\in\mathrm{GL}_n(\mathbb{Z}_{(p)})$ conjugating X to Y yield isomorphisms between these localizations for all primes p. So M_X and M_Y are in the same genus of R-lattices.

The $\mathcal{O}$-module

$$\Gamma:=M_X\mathcal{O}=\bigoplus_{i=1}^{k}M_Xe_i=:\bigoplus_{i=1}^{k}\Gamma_i$$

has endomorphism ring

$$\Delta:=\mathrm{End}_{\mathcal{O}}(\Gamma)\cong\bigoplus_{i=1}^{k}\mathbb{Z}^{n_i\times n_i}$$

where $n_i=\dim(\Gamma_i)$. In particular the genus of the Δ-lattice Γ consists of a single class, and hence by [6, Satz 3] the genus of the R-lattice M_X consists of a single narrow genus.

Put $\Lambda_i:=M_X\cap\Gamma_i$. Then

$$\Gamma=\bigoplus_{i=1}^{k}\Gamma_i\supseteq M_X\supseteq\bigoplus_{i=1}^{k}\Lambda_i$$

and X acts on Γ_i and on Λ_i as a scalar matrix, the multiplication by a_i. Recall that we choose $q_i\in\mathbb{N}$ to be minimal such that $E_i=q_ie_i\in\mathrm{End}_{\mathbb{Z}}(M_X)=\mathbb{Z}^{n\times n}$.

Remark 3.3. If $(d_1,\dots,d_{n_i})$ are the abelian invariants of E_i and $m_j:=q_i/d_j$ for $i=1,\dots,n_i$, then

$$\Gamma_i/\Lambda_i\cong\mathbb{Z}/m_1\mathbb{Z}\times\ldots\times\mathbb{Z}/m_{n_i}\mathbb{Z}.$$

To agree with the notation in [6] we put $H:=C(X)=\mathrm{End}_R(M_X)\subseteq\Delta$. Then Δ is a maximal order containing H and the maximal two-sided Δ-ideal contained in H is

$$\mathcal{F}:=\bigoplus_{i=1}^{k}E_i\Delta=\bigoplus_{i=1}^{k}q_i\mathbb{Z}^{n_i\times n_i}\subseteq C(X)\subseteq\Delta.$$

Moreover $M_X\mathcal{F}=\Gamma\mathcal{F}=\bigoplus_{i=1}^{k}q_i\Gamma_i$. In the notation preceding [6, Satz 4] we put

$$\tilde{\Delta}:=\Delta/\mathcal{F}\text{ and }\tilde{H}:=C(X)/\mathcal{F}.$$

Then $\tilde{H}\leq\tilde{\Delta}$. The respective groups of units are

$$\begin{aligned}
&U(\Delta)=\textstyle\prod_{i=1}^{k}\mathrm{GL}_{n_i}(\mathbb{Z})=\prod_{i=1}^{k}\mathrm{GL}(\Gamma_i),\\
&U(\tilde{\Delta})=\textstyle\prod_{i=1}^{k}\mathrm{GL}_{n_i}(\mathbb{Z}/q_i\mathbb{Z})=\mathrm{GL}(\Gamma/\mathcal{F}\Gamma),\text{ and}\\
&U(\tilde{H})=U(C(X)/\mathcal{F})=\{g\in U(\tilde{\Delta})\mid(M_X/M_X\mathcal{F})g=M_X/M_X\mathcal{F}\}.
\end{aligned}$$

We also put $\widetilde{U(\Delta)} := U(\Delta)/\mathcal{F} \leq U(\tilde{\Delta})$ to denote the reduction of the units of Δ modulo $\mathcal{F}$.

Then [6, Satz 4] tells us that the isomorphism classes of $C(X)$-lattices in the (narrow) genus of M_X correspond bijectively to the double cosets

$$U(\tilde{H})/U(\tilde{\Delta})\backslash\widetilde{U(\Delta)}.$$

So to prove Theorem 2.2 we need to show that this set consists of only one element.

Lemma 3.4. *In the situation of Theorem 2.2 we have* $|U(\tilde{H})/U(\tilde{\Delta})\backslash\widetilde{U(\Delta)}| = 1$.

Proof. Clearly $C(X) = H \leq \Delta$, so we may write any element B of H as a tuple $(B_1, \dots, B_k)$ of matrices $B_i \in \mathbb{Z}^{n_i\times n_i} = \mathrm{End}_{\mathbb{Z}}(\Gamma_i)$ which will be our canonical notation for the elements of $\Delta = \oplus_{i=1}^k \mathrm{End}_{\mathbb{Z}}(\Gamma_i)$. In particular

$$H = \{B := (B_1, \dots, B_k) \in \Delta \mid M_X B \subseteq M_X\}.$$

Let $\tilde{A} := (\tilde{A}_1, \dots, \tilde{A}_k) \in U(\tilde{\Delta})$ and choose a preimage $A = (A_1, \dots, A_k) \in \Delta$, so $A_i \in \mathbb{Z}^{n_i\times n_i}$ reducing modulo q_i to $\tilde{A}_i$. Then $d_i := \det(A_i) \in \mathbb{Z}$ maps onto a unit $\det(\tilde{A}_i) \in \mathbb{Z}/q_i\mathbb{Z}$. Let $d_i' \in \mathbb{Z}$ with $d_i d_i' \equiv 1 \pmod{q_i}$ be the corresponding inverse.

We construct $B = (B_1, \dots, B_k) \in H$ such that $\det(B_i) \equiv d_i' \pmod{q_i}$ for all i.

Assume that part (a) of Assumption 2.1 holds. If $m_1, \dots, m_{n_i}$ are as in Remark 3.3 there is a basis $(b_1^{(i)}, \dots, b_{n_i}^{(i)})$ of Γ_i such that

$$(m_1 b_1^{(i)}, \dots, m_{n_i} b_{n_i}^{(i)})$$

is a basis of Λ_i. By Assumption 2.1 we have $m_{n_i} = 1$ for all i. Put

$$K_i := \langle b_{n_i}^{(i)}\rangle \text{ and } K_i' := \langle b_1^{(i)}, \dots, b_{n_i-1}^{(i)}\rangle.$$

Then $\Gamma_i = K_i \oplus K_i'$ and $\Lambda_i = K_i \oplus (K_i' \cap \Lambda)$. Let

$$K := \bigoplus_{i=1}^k K_i \text{ and } K' := (\bigoplus_{i=1}^k K_i') \cap M_X.$$

Then $M_X = K \oplus K'$ is a direct sum of these two R-sublattices.

Let B be the endomorphism of M_X that is the identity on K' and the multiplication by d_i' on K_i for all $i = 1, \dots, k$. Then $B = (B_1, \dots, B_k) \in C(X)$ and $\det(B_i) = d_i'$ for all i.

If part (b) of Assumption 2.1 holds then we may first add a multiple of q_1 to d_1' such that d_1' is prime to q_i for all $i = 2, \dots, k$. With the same construction as before we then find $B' = (B_1', \dots, B_k') \in C(X)$ with $\det(B_i') \equiv d_i'/(d_1')^{n_i} \pmod{q_i}$ for all $i = 2, \dots, k$ and $\det(B_1') = 1$. Then $B := d_1' B' \in C(X)$ has the desired properties.

In both cases $\tilde{B} \in U(\tilde{H})$ and $BA = (B_1A_1, \dots, B_kA_k) \in \Delta$ satisfies $\det(B_iA_i) \equiv 1 \pmod{q_i}$, so $\widetilde{B_iA_i} \in \mathrm{SL}_{n_i}(\mathbb{Z}/q_i\mathbb{Z})$. By Lemma 3.1, there are matrices $C_i \in \mathrm{SL}_{n_i}(\mathbb{Z})$ with $\widetilde{C_i^{-1}} = \widetilde{B_iA_i}$ for all i. Then $C := (C_1, \dots, C_k) \in U(\Delta)$ satisfies $\tilde{B}\tilde{A}\tilde{C} = 1$.

□

4. PALEY AND PEISERT

This last section is dedicated to the proof that the adjacency matrices of the Paley and Peisert graphs satisfy Part (b) of Assumption 2.1.

Let p be a prime $p \equiv 3 \pmod 4$ and $q := p^{2t}$ be an even power of p. The Paley graph (see [2, p. 101]) and the Peisert graph [8] on q vertices are two cospectral Cayley graphs on an elementary abelian group of order q which are isomorphic if and only if $q = 9$ (see [9]). Choose a primitive element $\beta \in \mathbb{F}_q^\times$ and let $U := \langle \beta^4 \rangle \leq \mathbb{F}_q^\times$ denote the subgroup of fourth powers in the multiplicative group $\mathbb{F}_q^\times$ of the field with q elements. Then

$$\mathbb{F}_q^\times = U \cup \beta U \cup \beta^2 U \cup \beta^3 U.$$

The Paley graph $P(q)$ and the Peisert graph $P^*(q)$ have vertex set $\mathbb{F}_q$. Two vertices $i, j \in \mathbb{F}_q$ are joined in $P(q)$, if and only if $i-j \in U \cup \beta^2 U =: S = (\mathbb{F}_q^\times)^2$ and in $P^*(q)$ is and only if $i - j \in U \cup \beta U$. Let $A(q)$ respectively $A^*(q)$ denote the adjacency matrices of $P(q)$ respectively $P^*(q)$.

One main result of [9] is that for $q = p^2$ the adjacency matrices $A(q)$ and $A^*(q)$ are conjugate in $\mathrm{GL}_q(\mathbb{Z}_{(\ell)})$ for all primes ℓ.

Using Theorem 2.2 this allows us to show the following result:

Theorem 4.1. *The matrices $A(p^2)$ and $A^*(p^2)$ are conjugate in $\mathrm{GL}_{p^2}(\mathbb{Z})$.*

To prove the theorem we show that the matrix $X := A(p^2)$ satisfies part (b) of Assumption 2.1. Put

$$k := \frac{p^2-1}{2}, r := \frac{p-1}{2}, s := \frac{-p-1}{2}.$$

Then the eigenvalues of X are k, r, s with multiplicities $1, \frac{p^2-1}{2}, \frac{p^2-1}{2}$. Define

$$\begin{array}{lll} E_1 := & 2(X-rI)(X-sI)/k = & J \\ E_2 := & -(X-kI)(X-sI)/r = & sJ + pX - psI \\ E_3 := & -(X-kI)(X-rI)/s = & rJ - pX + prI \end{array}$$

where I denotes the unit matrix and J the all-ones matrix. Then elementary computations show that for $i \neq j \in \{1, 2, 3\}$

$$E_i^2 = p^2 E_i \text{ and } E_i E_j = 0.$$

In particular $e_i := \frac{1}{p^2} E_i$ are the primitive idempotents in $\mathbb{Q}[X]$ and $q_i = p^2$ for $i = 1, 2, 3$. Moreover $\mathrm{rk}(E_1) = 1$ and hence $\mathrm{rk}(E_2) = \mathrm{rk}(E_3) = k$. The next lemma shows that the E_i satisfy part (b) of Assumption 2.1. Therefore Theorem 2.2 together with the local considerations in [9] imply Theorem 4.1.

Lemma 4.2. *For $i = 2, 3$ the Smith group of E_i is*

$$\mathbb{Z}/\mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^{(p+1)^2/4-2} \oplus (\mathbb{Z}/p^2\mathbb{Z})^{(p-1)^2/4}.$$

Proof. We use the methods from [3]. We first note that the exponent of the Smith group of E_i divides p^2 by Remark 3.3. In particular we may pass to the p-adics. Let $R := \mathbb{Z}_p[\zeta_{q-1}]$ denote the ring of integers in the unramified extension of $\mathbb{Q}_p$ of degree 2. Then the adjacency matrix X of $P(p^2)$ is seen as an endomorphism of $R[\mathbb{F}_q]$. Recall that $S = \langle \beta^2 \rangle = (\mathbb{F}_q^\times)^2$. Then S acts on $R[\mathbb{F}_q]$ permuting the basis vectors $([x], s) \mapsto [xs]$ for all $x \in \mathbb{F}_q$, $s \in S$. As $|S| = \frac{q-1}{2} \in R^\times$ is invertible in R the RS-module $R[\mathbb{F}_q]$ is semisimple. Let $\tau : \mathbb{F}_q^\times \to R^\times$ denote the group monomorphism known as the Teichmüller character. The matrices $J : [x] \mapsto \sum_{y \in \mathbb{F}_q} [y]$ and X :

$[x] \mapsto \sum_{s\in S}[x+s]$ commute with the action of S and hence act on the homogeneous components

$$M_0 := \langle \mathbf{1} := \sum_{y\in\mathbb{F}_q}[y], [0], b_k := \sum_{s\in S}[s] - \sum_{x\in\mathbb{F}_q^\times\setminus S}[x]\rangle$$

and

$$M_j := \langle b_j, b_{j+k}\rangle,\ j = 1,\dots,k-1,\ \text{where } b_j := \sum_{x\in\mathbb{F}_q^\times}\tau^j(x^{-1})[x]$$

(see [3, Section 3]). For the action of E_i on M_0 we compute

$$E_1^{(0)} := \left(\begin{array}{ccc} p^2 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right),\ E_2^{(0)} := \frac{1}{2}\left(\begin{array}{ccc} 0 & 0 & 0 \\ -1 & p^2 & p \\ -p & p^3 & p^2 \end{array}\right),\ E_3^{(0)} = \frac{1}{2}\left(\begin{array}{ccc} 0 & 0 & 0 \\ -1 & p^2 & -p \\ p & -p^3 & p^2 \end{array}\right).$$

In particular the rank of $E_i^{(0)}$ is 1, contributing a 1 to the abelian invariants of E_i for $i = 1, 2, 3$. Clearly $J = E_1$ acts on M_j as 0 for $j \geq 1$. In the notation of [3] let $j > 0$ and $\alpha_j := J(\tau^{-j}, \tau^k)$ denote the Jacobi sum. Then [3, Lemma 3.1] shows that X acts on M_j as right multiplication by $X_j := \frac{1}{2}\left(\begin{array}{cc} -1 & \alpha_j \\ \alpha_{j+k} & -1 \end{array}\right)$ so E_2 and E_3 by right multiplication with $p(X_j - s)$ respectively $-p(X_j - r)$ in matrices

$$E_2^{(j)} := \frac{p}{2}\left(\begin{array}{cc} p & \alpha_j \\ \alpha_{j+k} & p \end{array}\right) \text{ and } E_3^{(j)} := \frac{p}{2}\left(\begin{array}{cc} p & -\alpha_j \\ -\alpha_{j+k} & p \end{array}\right).$$

As the rank of E_2 and E_3 is $(p^2-1)/2 = 1 + (k-1)$ and all $E_i^{(j)}$ are non-zero for $i = 2, 3,\ j = 1,\dots,k-1$ we obtain that all these $E_i^{(j)}$ have rank 1, in particular $\alpha_j\alpha_{j+k} = p^2$, for all $j = 1,\dots,k-1$. Now [3, Theorem 3.4] says that the p-adic valuation of α_i is

$$c(j) = \frac{1}{p-1}(s(j) + s(k) - s(j+k))$$

where $s(j) = a+b$ if $j \equiv ap+b \pmod{p^2}$ with $0 \leq a, b \leq p-1$. As $k = \frac{p-1}{2}p + \frac{p-1}{2}$ we have $s(k) = p-1$. Moreover for

$$1 \leq j = ap + b < \frac{p^2-1}{2} = k$$

we have $a \leq (p-1)/2$ and $a \leq (p-3)/2$ if $b \geq (p-1)/2$. Computing the digits of $j + k$ for these j we find

(0) $s(j+k) = s(j) + s(k)$ if $0 \leq a, b \leq \frac{p-1}{2}$, $(a, b) \notin \{(0, 0), (\frac{p-1}{2}, \frac{p-1}{2})\}$

(1) $s(j+k) = s(j) + s(k) - (p-1)$ if $\frac{p+1}{2} \leq b \leq p-1$ and $0 \leq a \leq \frac{p-3}{2}$.

So there are $(\frac{p+1}{2})^2 - 2$ such $1 \leq j < k$ with $c(j) = 0$ and $(\frac{p-1}{2})^2$ such j with $c(j) = 1$. For the j with $c(j) = 1$ (and hence also $c(j+k) = 1$ as $\alpha_j\alpha_{j+k} = p^2$) all entries of $E_i^{(j)}$ are divisible by p^2 so these j contribute a value p^2 to the abelian invariants of both, E_2 and E_3. If $c(j) = 0$ there is one entry of $E_i^{(j)}$ having valuation 1, so these j contribute a value p to the abelian invariants of E_2 and E_3.

□

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput. 24 (1997) 235-265.
[2] A.E. Brouwer, W.H. Haemers, *Spectra of Graphs.* Springer, New York, 2012.
[3] David B. Chandler, Peter Sin, Qing Xiang, The Smith and critical groups of Paley graphs. J. Algebraic Combin. 41 (2015) 1013–1022.
[4] D.K. Faddeev, On the equivalence of systems of integral matrices. Ezv. Akad. Nauk SSSR Ser. Mat., 30 (1966) 449-454
[5] Robert M. Guralnick, A note on the local-global principle for similarity of matrices. Linear Algebra Appl. 30 (1980) 241-245.
[6] H. Jacobinski, Über die Geschlechter von Gittern über Ordnungen. J. Reine u. Angewandte Mathematik 230 (1968) 29-39.
[7] J. C. Jantzen, J. Schwermer, *Algebra*, Springer (2006)
[8] Wojciech Peisert, All self-complementary symmetric graphs. J. Algebra 240 (2001) 209-229.
[9] Peter Sin, The critical groups of the Peisert graphs. J. Algebraic Combin. 48 (2018) 227-245.