$\mathbb{Z}^2$-ACTIONS BY SYMPLECTIC AUTOMORPHISMS OF A TORUS

CATHY CANNIZZO, ALEXANDER LEAF, NINA SAKHAROVA

Abstract. This paper will explore the $\mathbb{Z}$-conjugacy classes of symplectic matrices, through the framework of number fields. An integral matrix A may be thought of as an endomorphism on the n-dimensional torus $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$. In this paper we consider $\mathbb{Z}^2$-actions on the torus. A $\mathbb{Z}^2$-action is given by an embedding $\rho_\alpha : \mathbb{Z}^2 \to GL(n,\mathbb{Z})$ where α is given by two commuting integral matrices $A, B \in GL(n,\mathbb{Z})$. For $\mathbf{n} = (n_1, n_2) \in \mathbb{Z}^2$ we define

$$\rho_\alpha^{\mathbf{n}} = A^{n_1} B^{n_2}$$

One of the goals of the project was to find two actions α corresponding to A, B and α' corresponding to A', B' such that α and α' are conjugate only over $\mathbb{Q}$ and not $\mathbb{Z}$. We require that all four matrices are symplectic. We utilize a correspondence between ideal classes of $\mathbb{Z}[a]$ and $\mathbb{Z}$-conjugacy classes of matrices with characteristic polynomial $f(x)$, due to Latimer and MacDuffee.

Introduction

In this paper we construct integral matrices from number fields. An integral matrix A may be thought of as an endomorphism on the n-dimensional torus $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$. This is because if $x, y \in \mathbb{R}^n$ satisfy $x - y \in \mathbb{Z}^n$, that is x and y are equivalent in $\mathbb{R}^n/\mathbb{Z}^n$, then as A has integer entries it respects this equivalence relation and $Ax - Ay \in \mathbb{Z}^n$. In this paper we consider $\mathbb{Z}^2$-actions on the torus. For example, A. Katok, S. Katok and K. Schmidt (2002) in [4] consider general $\mathbb{Z}^d$ actions. A $\mathbb{Z}^2$-action is given by an embedding $\rho_\alpha : \mathbb{Z}^2 \to GL(n,\mathbb{Z})$ where α is given by two commuting integral matrices $A, B \in GL(n,\mathbb{Z})$ which are toral automorphisms. Note that if $A \in GL(n,\mathbb{Z})$, we must have $\det A = \pm 1$; this is because for A to be an automorphism of the torus, A must preserve measure. That is, we cannot scale the measure of the fundamental domain non-trivially, otherwise we do not have a bijective map when we quotient by $\mathbb{Z}^n$. For $\mathbf{n} = (n_1, n_2) \in \mathbb{Z}^2$ we define

$$\rho_\alpha^{\mathbf{n}} = A^{n_1} B^{n_2}$$

B commutes with A but is not a power of A; later we will see this corresponds to having multiplicatively independent units in a number field. As described in [4], we have notions of algebraically isomorphic and weakly algebraically isomorphic $\mathbb{Z}^2$-actions.

Definition 1. We say α and α' are *algebraically isomorphic* if there exists a group automorphism $\varphi : \mathbb{T}^n \to \mathbb{T}^{n'}$ such that $\varphi \circ \alpha(\mathbf{n}) = \alpha'(\mathbf{n}) \circ \varphi$ for all $\mathbf{n} \in \mathbb{Z}^2$.

To give the definition of weakly algebraically isomorphic we first define an algebraic factor.

Definition 2. An action α' on $\mathbb{T}^{n'}$ is an algebraic factor of an action α on $\mathbb{T}^n$ if there exists a surjective group homomorphism $\varphi : \mathbb{T}^n \to \mathbb{T}^{n'}$ such that $\varphi \circ \alpha(\mathbf{n}) = \alpha'(\mathbf{n}) \circ \varphi$ for all $\mathbf{n} \in \mathbb{Z}^2$. The *factor map* is φ.

Definition 3. We say two actions α and α' are *weakly algebraically isomorphic* if each is an algebraic factor of the other.

Weakly algebraically isomorphic implies the two tori are of the same dimension, i.e. $n = n'$, and each factor map has finite fibres. From the definition of weakly algebraically isomorphic, it is clear how the role of conjugation over $\mathbb{Q}$ comes into play. The factor map corresponds with conjugating one action over $\mathbb{Q}$ to the other. In [4, §2.3], they construct a one-to-one correspondence between algebraic factors with finite fibres of an algebraic action, and n-dimensional lattices containing $\mathbb{Z}^n$. Thus, we have that weakly algebraically isomorphic is equivalent to the pairs $\{A, B\}$ and $\{A', B'\}$ being simultaneously conjugate over $\mathbb{Q}$. If we take $\mathbf{n} = (1, 0)$ and $\mathbf{n} = (0, 1)$ then from the above definition we have there exists $C \in GL(n, \mathbb{Q})$ such that $C^{-1}AC = A'$ and $C^{-1}BC = B'$. Our goal is to find α, α' which are only weakly algebraically isomorphic and not algebraically isomorphic, and also so that all four commuting toral automorphisms $\{A, B, A', B'\}$ are symplectic.

Symplectic Matrices

We begin by fixing some notation. Let J be the fixed $2n$ by $2n$ skew-symmetric matrix, which, in block form, is

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

where I_n is the n by n identity matrix. Then, we say that a real matrix M is symplectic if

$$M^T J M = J$$

Now, we note the following about symplectic matrices:

(1) Given a $2n$ by $2n$ matrix M, which in block form, is

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where A, B, C, D are n by n blocks, M is symplectic if and only if the following conditions hold:
   (i) $A^T D - C^T B = I_n$
   (ii) $A^T C = C^T A$
   (iii) $D^T B = B^T D$

Proof. These conditions follow by explicitly multiplying out

$$\begin{aligned} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} &= \begin{pmatrix} A & B \\ C & D \end{pmatrix}^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \\ &= \begin{pmatrix} A^T & C^T \\ B^T & D^T \end{pmatrix} \begin{pmatrix} C & D \\ -A & -B \end{pmatrix} \\ &= \begin{pmatrix} A^T C - C^T A & A^T D - C^T B \\ B^T C - D^T A & B^T D - D^T B \end{pmatrix} \end{aligned}$$

and the above conditions follow. □

(2) As the name suggests, the concept of a symplectic matrix is closely related to that of a symplectic form on a symplectic vector space. A symplectic vector space is a $2n$-dimensional vector space V with a symplectic form (a non-degenerate, skew-symmetric bilinear form) ω. A symplectic transformation is a linear transformation $L : V \to V$ which preserves ω, i.e.

$$\omega(Lu, Lv) = \omega(u, v)$$

for all $u, v \in V$. Then, we can fix a basis for our symplectic vector space V, and get a matrix M for L and J for ω. Then, M is a symplectic matrix by our above definition.

(3) While we will use $J = \left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$ to represent our symplectic form in a given basis, one can let J be any skew-symmetric matrix with a non-zero determinant. Indeed, some authors choose a different skew-symmetric matrix, which leads to a different definition of a symplectic matrix. Nonetheless, symplectic matrices resulting from a different choice of J will only differ from each other by a change of basis.

(4) The eigenvalues of a symplectic matrix M come in reciprocal pairs.

Proof. By our definition of a symplectic matrix, $M^T JM = J$, so because J is invertible, M is invertible, so $M^T = JM^{-1}J^{-1}$, so

$$\begin{aligned} \det(M - xI_{2n}) &= \det(M^T - xI_{2n}) \\ &= \det(JM^{-1}J^{-1} - xI_{2n}) \\ &= \det(J)\det(M^{-1} - xI_{2n})\det(J^{-1}) \\ &= \det(M^{-1} - xI_{2n}) \end{aligned}$$

Thus, if λ is an eigenvalue of M of multiplicity j, then we can write

$$\det(M - xI_{2n}) = \det(M^{-1} - xI_{2n}) = (\lambda - x)^j q(x)$$

where $q(x)$ is an integer polynomial of degree $2n - j$ such that $(\lambda - x)$ does not divide $q(x)$. Thus, λ is an eigenvalue of M^{-1} of multiplicity j, so λ^{-1} is an eigenvalue of M of multiplicity j, as desired. □

From the above, it follows that $\det(M) = 1$. Additionally, if the characteristic polynomial of M is

$$f(x) = 1 + a_1 x + \cdots + a_j x^j + \cdots + a_{2n-1}x^{2n-1} + x^{2n}$$

and λ is an eigenvalue of M, then $f(\lambda) = f(\lambda^{-1}) = 0$, so it follows that $f(x) = x^{2n} f(x^{-1})$, so $a_j = a_{2n-j}$, i.e. f is a reciprocal polynomial.

(5) More generally, we can talk about symplectic matrices with complex entries with the following definition: a matrix M is symplectic if $M^* JM = J$. For our discussion, however, we will restrict ourselves to symplectic matrices with integers entries, so this definition will not be necessary.

(6) Let Γ be the set of $2n$ by $2n$ symplectic matrices with integer entries. Γ is a group.

Proof. We want to show that Γ is a subgroup of $GL(2n, \mathbb{Z})$. To show that Γ is closed under matrix multiplication, if $A, B \in \Gamma$, then

$$(AB)^T J(AB) = B^T(A^T JA)B = B^T JB = J$$

so $AB \in \Gamma$. Any symplectic matrix has determinant 1, so the inverse of a matrix $A \in \Gamma$ has integer entries. To show that A^{-1} is symplectic,

$$J = (AA^{-1})^T J(AA^{-1}) = (A^{-1})^T JA^{-1}$$

so $A^{-1} \in \Gamma$. Thus, Γ is a group. □

The Integral Symplectic Group and Its Generators. The next few results we give without proof. See the referenced papers for the full proofs.

Theorem 4. *The group* Γ *has the following generators:*

$$\mathfrak{T}_0 = \begin{pmatrix} I_n & S_0 \\ 0 & I_n \end{pmatrix}$$

$$\mathfrak{R}_1 = \begin{pmatrix} U_1 & 0 \\ 0 & {U_1}^{T^{-1}} \end{pmatrix}$$

$$\mathfrak{R}_2 = \begin{pmatrix} U_2 & 0 \\ 0 & {U_2}^{T^{-1}} \end{pmatrix}$$

$$\mathfrak{S}_0 = \begin{pmatrix} J_1 & I_n - J_1 \\ J_1 - I_n & J_1 \end{pmatrix}$$

where we have

$$S_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \qquad U_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

$$U_2 = \begin{pmatrix} 1 & 1 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \qquad J_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Proof. See Hua and Reiner (1946) [3]. □

Note that in Hua and Reiner, the above matrices are given as generators of Γ_0, the modular symplectic group, which is obtained from Γ by identifying $M \in \Gamma$ with $-M$. Nonetheless, they state the above matrices also generate Γ. The symplectic group generators have the following properties: $\mathfrak{T}_0$ and $\mathfrak{R}_2$ have the same characteristic polynomial $(x-1)^4$ and commute. Also note that $\mathfrak{R}_1$ has order 2 and $\mathfrak{S}_0$ has order 4.

Later in this paper, we will want to find symplectic matrices conjugate over $\mathbb{Q}$. If we look at irreducible characteristic polynomials, because $\mathbb{Q}$ has characteristic 0, they will have distinct eigenvalues. Thus, in this case, two matrices are conjugate over $\mathbb{Q}$ if and only if they have the same characteristic polynomial. A natural question to ask is whether, given a reciprocal polynomial f of degree $2n$, there exists a symplectic matrix M with f as its characteristic polynomial. The answer is,

in fact, yes. This answer follows from a proof by construction given in Margalit and Spallone (2007) [5, §3.2]. This is done by writing the companion matrix as a product of special matrices and reordering the matrices to obtain a symplectic matrix conjugate to the original companion matrix. We provide Mathematica code in the Appendix that follows this construction. Note that Margalit and Spallone make a different choice of J to define symplectic matrices, so it is necessary to do a change of basis to get a symplectic matrix by our definition. We provide another construction below for 4 by 4 matrices.

In order to find symplectic matrices, it is necessary that the irreducible polynomial f we start with is reciprocal by (4) above. Let $f(x) = x^4+1+m(x^3+x)+nx^2 \in \mathbb{Z}[x]$ be irreducible and let a be a root. Let $K = \mathbb{Q}(a)$ and suppose we choose m and n so that all roots of f are real and the ring of integers $\mathcal{O}_K$ has class number at least 2. In the examples considered here, $\mathcal{O}_K = \mathbb{Z}[a]$. The matrix representation of the map m_a, multiplication by a, with respect to the $\mathbb{Z}$-basis $\mathcal{B} = \{1, a, \ldots, a^{n-1}\}$ of $\mathcal{O}_K$, is the companion matrix of f, i.e.

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -m & -n & -m \end{pmatrix}$$

Consider the matrix $N = \mathfrak{R}_1\mathfrak{S}_0\mathfrak{R}_2^m\mathfrak{T}_0^n$. This has the following characteristic polynomial:

$$\chi_N(x) := x^4 + 1 + m(x + x^3) + nx^2 \tag{1}$$

so in this way we can construct any symplectic matrix with a given reciprocal characteristic polynomial. The symplectic matrix N is

$$N = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -m & 1 \\ -1 & -m & -n & 0 \end{pmatrix}$$

If we let

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -m & 1 \end{pmatrix} \qquad R^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & m & 1 \end{pmatrix}$$

then NR^{-1} adds m times the fourth column to the third column which zeros out the $-m$ in the third row of N. Then RNR^{-1} adds $-m$ times the third row to the fourth row, resulting in a bottom row of $(-1, -m, -n, -m)$. Thus RNR^{-1} is the companion matrix A mentioned above:

$$RNR^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -m & -n & -m \end{pmatrix} = A$$

Since $\det R = 1$ we have proved:

Theorem 5. *Given an irreducible reciprocal polynomial $f(x) = x^4 + 1 + m(x^3 + x) + nx^2 \in \mathbb{Z}[x]$ with root a, the matrix $\mathfrak{R}_1\mathfrak{S}_0\mathfrak{R}_2^m\mathfrak{T}_0^n$ has characteristic polynomial $f(x)$ and corresponds to the principal ideal class of $\mathbb{Z}[a]$.*

We provide one more result before we proceed to the algebraic discussion.

Theorem 6. *Two $2n$ by $2n$ complex symplectic matrices M_1, M_2 are conjugate over the group of complex symplectic matrices if and only if they are conjugate over $GL(2n, \mathbb{C})$.*

Proof. See Theorem 1.1 of Gongopadhyay (2009) [2]. □

The statement of the theorem in Gongopadhyay (2009) assumes that the entries of the matrices are over an algebraically closed field. At the present, we do not know if two symplectic matrices M_1, M_2 with rational entries are conjugate over the group of rational symplectic matrices if and only if they are conjugate over $GL(2n, \mathbb{Q})$.

Algebraic Number Theory

We will now use tools from algebraic number theory to find matrices corresponding to $\mathbb{Z}^2$-actions. Let $f(x)$ be a monic irreducible polynomial over $\mathbb{Z}$ of degree $2n$ with constant coefficient ± 1, and let a be a root of f. The roots of f are distinct because $\mathbb{Q}$ has characteristic 0. Consider the field $K = \mathbb{Q}(a)$ and let $\mathcal{O}_K$ be the ring of algebraic integers. Note that a is a unit in $\mathcal{O}_K$. We have the following theorem [7]:

Theorem 7 (Latimer-MacDuffee Theorem)**.** *Ideal classes of $\mathbb{Z}[a]$, where a is a root of an irreducible polynomial $f(x)$ over $\mathbb{Z}$, are in bijection with $\mathbb{Z}$-conjugacy classes of integral matrices with characteristic polynomial f.*

Proof. For a proof refer to [7, pg 52–53]. □

One important component in the proof is determining which ideal class an integral matrix corresponds to. Let $v = (v_1, \ldots, v_n)^T$ be an eigenvector of an integral matrix $A \in GL(n, \mathbb{Z})$ with characteristic polynomial $f(x)$, corresponding to eigenvalue a. That is, $Av = av$. Since f is irreducible we have four distinct roots so the four eigenspaces of A each have dimension 1. Hence v is unique up to a scalar multiple. Assume we have cleared denominators in the entries of v so that $v_i \in \mathbb{Z}[a]$ for $1 \leq i \leq n$. Then the $\mathbb{Z}$-span of $\{v_1, \ldots, v_n\}$ forms an integral ideal $I \subset \mathcal{O}_K = \mathbb{Z}[a]$ since $av_i = (av)_i = (Av)_i = \sum_{j=1}^n A_{ij}v_j$ which is a linear combination of the v_i over $\mathbb{Z}$ hence in I. Thus we have constructed an ideal corresponding to the matrix A.

Commuting Matrices. We can think of an ideal $I \subset \mathcal{O}_K$ with integral basis $e_1, \ldots, e_n$ as an n-dimensional lattice, isomorphic to $\mathbb{Z}^n \subset \mathbb{Q}^n$. The isomorphism is given by

$$\pi : e_i \mapsto (0, \ldots, 0, 1, 0, \ldots 0)^T =: h_i \tag{2}$$

where h_i has a 1 in the ith place. Multiplication by another unit $b \in \mathcal{O}_K$ similarly gives rise to a matrix B. We know $ab = ba$ since multiplication is commutative in K. So by the isomorphism π, we obtain two commuting matrices A, B from multiplication by a, b on the same integral basis of some ideal. Note that commuting matrices have the same eigenvectors. For assume b has an irreducible minimal polynomial $q(x)$ of degree n so B has characteristic polynomial $q(x)$ and distinct eigenvalues. Let v be an eigenvector of A corresponding to eigenvalue a. Then

$ABv = BAv = aBv$ so Bv is an eigenvector of A of eigenvalue a. The corresponding eigenspace has dimension 1 so Bv must be a scalar multiple of v, say $Bv = \lambda v$. Hence v is also an eigenvector of B.

Dirichlet's Unit Theorem. We require the commuting matrices A and B to correspond to multiplication by multiplicatively independent units in $\mathcal{O}_K$. To define multiplicatively independent we use

Theorem 8 (Dirichlet's Unit Theorem)**.** *Let K be a number field. Let r_1 and r_2 denote the number of real and complex conjugate pair embeddings of K into $\mathbb{C}$. Then the group of units $U_K \subset \mathcal{O}_K$ satisfies*

$$U_K \cong \mathbb{Z}^{r_1+r_2-1} \times \mu_K \tag{3}$$

where μ_K is the finite group of the roots of unity in K.

Proof. For a proof refer to Esmonde and Murty (2005) [6, pg. 104–105]. □

In the case of $K = \mathbb{Q}(a)$ where all the conjugates of a, i.e. roots of its minimal polynomial f, are real, we have $U_K \cong \mathbb{Z}^{n-1} \times \{\pm 1\}$ since we have $r_1 = n$ real embeddings and no complex embeddings. Thus each unit $u \in \mathcal{O}_K$ can be written uniquely as $\pm\epsilon_1^{s_1} \dots \epsilon_{n-1}^{s_{n-1}}$ where $\{\epsilon_1, \dots, \epsilon_{n-1}\}$ are the fundamental units. Assume $\epsilon_i > 1$ for $1 \leq i \leq n-1$. Two units $u = \operatorname{sgn}(u)\epsilon_1^{s_1} \dots \epsilon_{n-1}^{s_{n-1}}$ and $v = \operatorname{sgn}(v)\epsilon_1^{t_1} \dots \epsilon_{n-1}^{t_{n-1}}$ are multiplicatively independent if and only if one is not a power of the other up to a sign, i.e. $(s_1, \dots, s_{n-1})$ and $(t_1, \dots, t_{n-1})$ are linearly independent in $\mathbb{Z}^{n-1}$ so $(s_1, \dots, s_{n-1}) \neq q(t_1, \dots, t_{n-1})$ for any $q \in \mathbb{Z}$.

In constructing a second matrix B commuting with a given matrix A, we look at multiplication by some unit $b \in \mathcal{O}_K = \mathbb{Z}[a]$, assuming we have chosen f so $\mathcal{O}_K = \mathbb{Z}[a]$. (In general we only know $\mathbb{Z}[a] \subset \mathcal{O}_K$.) Thus b is a polynomial $r(a)$ for some $r(x) \in \mathbb{Z}[x]$ and by the isomorphism π in (2) above, $B = r(A)$.

Example

We would like to find a reciprocal polynomial $f(x) \in \mathbb{Z}[x]$ with the following properties:

(1) f is irreducible over $\mathbb{Z}$.
(2) f has all real roots.
(3) The class number of $K := \mathbb{Q}(a)$, for a a root of f, is greater than 1. This ensures we can find matrices conjugate over $\mathbb{Q}$ but not $\mathbb{Z}$, since we have more than one ideal class.
(4) The ring of integers $\mathcal{O}_K = \mathbb{Z}[a]$. (Sage does not currently have the capability to find the class group of orders other than $\mathcal{O}_K$ and the correspondence in the Latimer-MacDuffee theorem pertains to ideal classes in $\mathbb{Z}[a]$.)
(5) We can obtain $f(x)$ from a more complicated product of symplectic generators than $\mathfrak{R}_1\mathfrak{S}_0\mathfrak{R}_2^m\mathfrak{T}_0^n$, since the latter corresponds to the principal ideal class.

Finding an appropriate polynomial f. Recall from above that we have a symplectic matrix in the principal ideal class. It remains to find symplectic matrices which are in a $\mathbb{Z}$-conjugacy class corresponding to a non-trivial ideal class. One option is to obtain symplectic matrices of a given characteristic polynomial by taking more complicated combinations of the generators so that the result is not conjugate over $\mathbb{Z}$ to the companion matrix. Consider the following product of symplectic group generators:

$$M := \mathfrak{S}_0(\mathfrak{T}_0\mathfrak{S}_0\mathfrak{R}_2)^4(\mathfrak{R}_2\mathfrak{R}_1)^{-2}(\mathfrak{R}_2\mathfrak{R}_1\mathfrak{T}_0)^{-2} = \begin{pmatrix} 1 & -2 & 1 & 1 \\ -3 & 5 & 0 & -1 \\ -1 & 2 & -6 & -4 \\ -3 & 5 & -2 & -2 \end{pmatrix}$$

This has characteristic polynomial $f(x) = x^4 + 2x^3 - 36x^2 + 2x + 1$. Further, the corresponding number field obtained by adjoining a root a of f to $\mathbb{Q}$ has class number 4 and the ring of integers is $\mathcal{O}_K = \mathbb{Z}[a]$. One can carry out these calculations in a computer algebra system, such as Sage. The fundamental units are

$$[\epsilon_1, \epsilon_2, \epsilon_3] = \left[a, 4a^3 + 8a^2 - 148a - 21, 4a^3 - 15a^2 - 300a + 60\right]$$

In particular, the minimal polynomial of ϵ_3 is $x^4 + 1220x^3 - 134742x^2 + 1220x + 1$ which is reciprocal, so we can consider multiplication by $b := \epsilon_3$ to attempt to obtain a symplectic matrix commuting with matrices arising from multiplication by $\epsilon_1 = a$.

First $\mathbb{Z}^2$ action from trivial ideal class. First we look at matrices corresponding to the principal ideal class. The companion matrix, i.e. the matrix corresponding to multiplication by a on $\mathbb{Z}[a]$ is

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -2 & 36 & -2 \end{pmatrix}$$

This conjugates to the symplectic matrix N as described in (1) via the matrix R

$$N = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 1 \\ -1 & -2 & 36 & 0 \end{pmatrix} \qquad R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 1 \end{pmatrix}$$

$$R^{-1}AR = N$$

The matrix corresponding to multiplication by ϵ_3, the third fundamental unit, on the principal ideal class is:

$$B = \begin{pmatrix} 60 & -300 & -15 & 4 \\ -4 & 52 & -156 & -23 \\ 23 & 42 & -776 & -110 \\ 110 & 243 & -3918 & -556 \end{pmatrix}$$

Since $b = \epsilon_3 = a^3 - 15a^2 - 300a + 60$ we have $B = A^3 - 15A^2 - 300A + 60I$. One question which arose while working on this project is, if we can conjugate the companion matrix A to a symplectic matrix N by some $R \in GL(n, \mathbb{Z})$, is it true that R also conjugates any polynomial in A to a symplectic matrix? The answer to

this question is not immediately evident because the symplectic group is a group under multiplication but not necessarily addition. In this case, R does indeed also conjugate B to a symplectic matrix, giving the $\mathbb{Z}^2$-action corresponding with the trivial ideal class.

$$N_2 := R^{-1}BR = \begin{pmatrix} 60 & -300 & -23 & 4 \\ -4 & 52 & -110 & -23 \\ 23 & 42 & -556 & -110 \\ 156 & 327 & -3918 & -776 \end{pmatrix}$$

Finding second $\mathbb{Z}^2$ action from a non-trivial ideal class. We now have two symplectic matrices N and N_2 corresponding to multiplication by a and ϵ_3 on a principal ideal. We have another symplectic matrix, M as described at the start, which potentially corresponds to a non-trivial ideal class. We would like to find which $\mathbb{Z}$-conjugacy class M belongs to. There are four possibilities since we have class number 4. Using the following commands we obtain the generator for the ideal class group G:

```
sage: K.<a> = NumberField( 1 + x^4 + 2*(x^3+x) - 36*x^2)
sage: G=K.class_group(); G.0
```

Fractional ideal class $(6, a-1)$

So $I := (6, a-1)$ has ideal class of order 4 in the ideal class group. The $\mathbb{Z}$-conjugacy class of M must correspond with one of the ideal classes $1, [I], [I]^2, [I]^3$ (where $[I]$ is the element of the ideal class group containing the ideal I). Consider multiplication by a on the ideal I^2.

```
sage: J = ((G.0).ideal())^2; J
```

$\left(6, a^3 + 2a^2 - 37a + 4\right)$

To obtain the matrix representation of m_a we use:

```
sage: [mu1, mu2, mu3] = K.units(); # Obtains fundamental units
sage: [e1, e2, e3, e4] = J.integral_basis();
sage: num = mu1; # mu3 gives second pair of matrices
sage: J.coordinates(num*e1); J.coordinates(num*e2);
sage: J.coordinates(num*e3); J.coordinates(num*e4);
```

This gives the following matrix

$$M' := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 17 & 2 & -6 & 6 \\ 14 & 2 & -5 & 5 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

In Sage we can consider the linear map on $M_4(\mathbb{Z})$ given by $S \mapsto M'S - SM$ and find a basis for the kernel. Then we can test a few linear combinations of the basis elements to see if we obtain an integral matrix S of determinant ± 1 in the kernel.

Indeed we find such an S of determinant -1.

$$S = \begin{pmatrix} 3 & 2 & 2 & -1 \\ -2 & 3 & -7 & -5 \\ 3 & 3 & -5 & -3 \\ -3 & -7 & 0 & 7 \end{pmatrix}$$

$$S^{-1}M'S = M$$

So the symplectic matrix M corresponds to a non-principal ideal class and cannot be conjugate over $\mathbb{Z}$ to N which was in the $\mathbb{Z}$-conjugacy class of the companion matrix of f. We construct the final fourth matrix M_2 by taking the appropriate polynomial in M; recall $\epsilon_3 = 4a^3 - 15a^2 - 300a + 60$. Also, M_2 is symplectic.

Alternate construction via eigenspaces. Alternatively we can look at M directly to determine which ideal class it corresponds to. Recall from the Algebraic Number Theory section above that the ideal class corresponding to a matrix is found from the $\mathbb{Z}$-span of the entries of an appropriately scaled eigenvector. With the following commands

```
sage: H = MatrixSpace(K,4,4);
sage: M = H([1,-2,1,1, -3,5,0,-1, -1,2,-6,-4, -3,5,-2,-2]);
sage: Mt = M.transpose();
sage: Mt.eigenspaces()
```

we obtain the eigenspace corresponding to a is

$$\text{Span}_{\mathbb{Q}(a)}\left(1, \quad -\tfrac{4}{3}a^3 - 3a^2 + 47a + \tfrac{22}{3}, \quad \tfrac{11}{3}a^3 + 8a^2 - 130a - \tfrac{56}{3}, \quad -\tfrac{19}{3}a^3 - 14a^2 + 225a + \tfrac{97}{3} \right)$$

In particular, clearing denominators by multiplying by three and taking the resulting entries as our integral basis, we find that 3 is in the ideal. This suggests we look at the prime ideal factorization of the ideal $3\mathcal{O}_K$ and see if multiplication by a on a prime ideal in the factorization gives a matrix in the same $\mathbb{Z}$-conjugacy class as M.

```
sage: ideal3 = K.ideal(3);
sage: factideal = factor(ideal3); factideal
```

$((3, a-1))^4$

Let J be the ideal $(3, a-1)$. We check if J is principal since we would like M not to correspond to the principal ideal class. It turns out J^2 is principal but J is not (and hence J is in the element of the ideal class group $[I]^2$).

```
sage: J = K.ideal(3,a-1);
sage: J.integral_basis(); J.is_principal()
```

$\left[3, a+2, a^3+2a^2-36a+3, a^3+3a^2-33a-16\right]$

False

Finally we determine a matrix representation for multiplication by a on J.

```
sage: [e1, e2, e3, e4] = J.integral_basis();
sage: num = mu1; # mu3 gives second pair of matrices
sage: J.coordinates(num*e1); J.coordinates(num*e2);
sage: J.coordinates(num*e3); J.coordinates(num*e4);
```

This gives

$$M'' := \begin{pmatrix} -2 & 3 & 0 & 0 \\ 7 & -1 & -1 & 1 \\ -1 & 1 & 0 & 0 \\ -5 & 15 & 0 & 1 \end{pmatrix}$$

We can consider the linear map $S \mapsto M''S - SM$ as above. Sage finds the following matrix in the kernel with determinant 1:

$$S_2 = \begin{pmatrix} 2 & -1 & 0 & 1 \\ 2 & -2 & 0 & 1 \\ 4 & 2 & 1 & -1 \\ -3 & -2 & 1 & -5 \end{pmatrix}$$

$$S_2^{-1} M'' S_2 = M$$

So M and M'' are in the same $\mathbb{Z}$-conjugacy class and again the symplectic matrix M corresponds to a non-trivial ideal class.

Thus we have two $\mathbb{Z}^2$ actions, α given by N, N_2 and α' given by M, M_2 which are only weakly algebraically isomorphic and not isomorphic, i.e. they are simultaneously conjugate over $\mathbb{Q}$ but not $\mathbb{Z}$.

$$N = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -2 & 1 \\ -1 & -2 & 36 & 0 \end{pmatrix} \qquad N_2 = \begin{pmatrix} 60 & -300 & -23 & 4 \\ -4 & 52 & -110 & -23 \\ 23 & 42 & -556 & -110 \\ 156 & 327 & -3918 & -776 \end{pmatrix}$$

$$M = \begin{pmatrix} 1 & -2 & 1 & 1 \\ -3 & 5 & 0 & -1 \\ -1 & 2 & -6 & -4 \\ -3 & 5 & -2 & -2 \end{pmatrix} \qquad M_2 = \begin{pmatrix} -149 & 435 & 9 & -87 \\ 829 & -1318 & 27 & 290 \\ -101 & 136 & -5 & -31 \\ 706 & -1151 & 21 & 252 \end{pmatrix}$$

We considered some further examples as well. We found symplectic matrices corresponding to the principal ideal class but it remains to prove that for class number at least two, we can always find a symplectic matrix in a non-trivial $\mathbb{Z}$-conjugacy class. See Further Questions for further discussion. For another example for which it is still unknown if a non-trivial ideal class corresponds with a $\mathbb{Z}$-conjugacy class containing a symplectic matrix, see the Appendix.

Remaining Questions

Several questions remain from this paper. While we have given specific constructions of symplectic matrices with the desired properties, several obstacles remain to doing a general construction. Many of these questions pertain to the relationship between conjugacy classes of integer (or rational) symplectic matrices over $GL(2n, \mathbb{Z})$ (or $GL(2n, \mathbb{Q})$) and conjugacy classes of integer (or rational) symplectic

matrices over symplectic matrices.

(1) In our construction, we were able to conjugate two commuting matrices, representing multiplication by two multiplicatively independent units in the same integral basis, by the same matrix in $GL(2n, \mathbb{Z})$ to obtain two symplectic matrices. However, we do not have a theorem to guarantee that this phenomenon will always hold. In other words, we can ask, what conditions must we put on two matrices $M_1, M_2 \in GL(2n, \mathbb{Z})$ such that if $S \in GL(2n, \mathbb{Z})$ and $S^{-1}M_1S$ is symplectic, then $S^{-1}M_2S$ will be symplectic as well? Given these conditions, we might be able to generalize our construction to produce matrices with the desired properties, given any number field (with large enough ideal class group) generated by the root of an irreducible reciprocal polynomial.

(2) More specifically, we can ask the following: what restrictions must we place on symplectic matrices M_1, M_2 with integer entries such that if $S \in GL(2n, \mathbb{Z})$ and $S^{-1}M_1S$ is symplectic, then $S^{-1}M_2S$ symplectic as well? We can state this question equivalently as follows: suppose there exists $S_1 \in GL(2n, \mathbb{Z})$ such that ${S_1}^{-1}M_1S_1$ and ${S_1}^{-1}M_2S_1$ are symplectic, i.e. S_1 conjugates both M_1 and M_2 to symplectic matrices. If $S_2 \in GL(2n, \mathbb{Z})$ and ${S_2}^{-1}M_1S_2$ is symplectic, what conditions on M_1 and M_2 would guarantee that ${S_2}^{-1}M_2S_2$ is symplectic?

(3) Another question is whether conjugacy classes of symplectic matrices over conjugation by matrices in $GL(2n, \mathbb{Z})$ are equivalent to conjugacy classes of symplectic matrices over conjugacy by matrices in Γ. In other words, given a symplectic matrix A, is the set of symplectic matrices that can be written as $S^{-1}AS$ with $S \in GL(2n, \mathbb{Z})$ equal to the set of symplectic matrices that can be written $S^{-1}AS$ with $S \in \Gamma$? Equivalently, if A is symplectic and $S^{-1}AS$ with $S \in GL(2n, \mathbb{Z})$ is symplectic, does there exist $M \in \Gamma$ such that $M^{-1}AM = S^{-1}AS$?

(4) In this paper, we were mainly concerned with matrices with irreducible characteristic polynomials. We know that given any reciprocal irreducible characteristic polynomial $f(x)$, there is a symplectic matrix with characteristic polynomial $f(x)$, which means that the $\mathbb{Q}$-conjugacy class containing matrices with that characteristic polynomial contains a symplectic matrix. This leaves us with a few questions. Must a symplectic matrix be contained in any $\mathbb{Z}$-conjugacy class contained in such a $\mathbb{Q}$-conjugacy class? Additionally, for a $\mathbb{Q}$-conjugacy class containing matrices with a reducible reciprocal characteristic polynomial, must that conjugacy class contain a symplectic matrix? (We know that we can construct a symplectic matrix with any reducible reciprocal polynomial as its characteristic polynomial, but not all matrices with that same characteristic polynomial have the same Jordan normal form.)

(5) Another possible direction is to use geometric properties to obtain symplectic matrices from the start. One question we can ask is, how can one

choose a $\mathbb{Z}$-basis for an appropriately chosen ideal in an ideal class, such that the matrix constructed is symplectic? We thought we could consider the matrix representation of a given basis and try to get this to be symplectic. Such a property may give us a way of obtaining symplectic matrices, without having to conjugate over $\mathbb{Z}$ to get to them.

Acknowledgments

First we would like to thank Dr. Misha Guysinsky for his guidance on our project and coordination of the 2011 Pennsylvania State University REU. We would also like to thank Prof. Leonid Vaserstein for discussions about symplectic matrices, Prof. John Clemens for help with the use of Sage, and Helge Dietert for help with Sage and Python programming.

Appendix

Mod p test. One method that can show if two matrices are not conjugate over $\mathbb{Z}$ is the following.

Theorem 9. *Given two integral matrices A, B, let A', B' be A and B respectively with the entries in each taken mod p (for some prime p). Then, if A', B' are not conjugate over $GL(2n, \mathbb{Z}/p\mathbb{Z})$, A and B are not conjugate over $\mathbb{Z}$.*

Proof. If A and B were conjugate over $\mathbb{Z}$, then by definition there exists $S \in GL(2n, \mathbb{Z})$ such that $S^{-1}AS = B$. Let S' be the matrix S with entries taken mod p, so $S' \in GL(2n, \mathbb{Z}/p\mathbb{Z})$. Then, ${S'}^{-1}A'S' = B'$, so A', B' are conjugate over $GL(2n, \mathbb{Z}/p\mathbb{Z})$. □

Note that the above condition is sufficient but not necessary. However, it can sometimes be useful. Consider the following examples. Let

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$$
$$B = \begin{pmatrix} 1 & 4 \\ 1 & 5 \end{pmatrix}$$

Both A and B have characteristic polynomial $(x-1)(x-5)-4 = x^2-6x+1$, which is irreducible over $\mathbb{Q}$ and hence has distinct roots. However, if we take A', B' to be A, B respectively with entries mod 2, then we have

$$A' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$B' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Then, because A' is the identity polynomial and B' is not, A' and B' are not conjugate over $GL(2, \mathbb{Z}/2\mathbb{Z})$, so A and B are not conjugate over $\mathbb{Z}$.

Overall, this method is useful if one can readily see that the two matrices are not conjugate over $GL(2n, \mathbb{Z}/p\mathbb{Z})$ (e.g. when one is the identity matrix and the other is not). Working with 4 by 4 matrices, as we do later in this paper, this method can be used to check conjugacy over $GL(4, \mathbb{Z}/2\mathbb{Z})$, because one need only check for every element of $GL(4, \mathbb{Z}/2\mathbb{Z})$ (and $|GL(4, \mathbb{Z}/2\mathbb{Z})| = 20106$). However, even checking over $GL(4, \mathbb{Z}/3\mathbb{Z})$ is too computationally expensive to do in this brute force manner.

Additional Example. Below is one example of an attempt of the same construction given above in the Example section. It did not satisfy all of the conditions specified at the beginning of that section. Only two of the four matrices are symplectic. As stated in the Further Questions section, we do not know if every $\mathbb{Z}$-conjugacy class contains a symplectic matrix.

Consider

$$f(x) = x^4 - 13x^2 + 1$$

Let a be a root. The roots are $\pm a$ and $\pm(a^3 - 13a)$. The fundamental units are:

$$[\epsilon_1, \epsilon_2, \epsilon_3] = [a, a^3 - 14a + 4, 3a^3 - 36a + 10]$$

Multiplication by ϵ_1 on the principal and non-principal ideals gives symplectic matrix A and non-symplectic matrix A' both of which have characteristic polynomial $f(x)$.

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 13 & 0 \end{pmatrix} \qquad A' = \begin{pmatrix} -3 & 5 & 0 & 0 \\ -1 & 3 & 0 & 1 \\ -2 & 3 & 0 & 0 \\ -6 & 9 & 1 & 0 \end{pmatrix}$$

Multiplication by $\epsilon_1\epsilon_3$ on these ideals also gives a symplectic matrix B and a non-symplectic matrix B'. Note that the minimal polynomial of $\epsilon_1\epsilon_3$ is reciprocal, as expected:

$$g(x) := x^4 + 1 - 66(x + x^3) - 409x^2$$

This is the characteristic polynomial of B and B'.

$$B = \begin{pmatrix} -3 & 10 & 3 & 0 \\ 0 & -3 & 10 & 3 \\ -3 & 0 & 36 & 10 \\ -10 & -3 & 130 & 36 \end{pmatrix} \qquad B' = \begin{pmatrix} -21 & 50 & 0 & 15 \\ -28 & 66 & 3 & 19 \\ -11 & 27 & -3 & 9 \\ -39 & 90 & 10 & 24 \end{pmatrix}$$

Code. Below is the code based on the construction in [5] of obtaining a symplectic matrix with a given characteristic polynomial.

```
(* This defines the function GetSymp[m,n], which obtains a
4 by 4 symplectic matrix with given characteristic polynomial
x^4 + 1 + m(x^3+x) + nx^2. The method is from Margalit and
Spallone (2007) *)

X1[n_Integer, m_Integer] := {{1, -n, 0, 0}, {0, 1, 0, 0},
{0, 0, 1, 0}, {0, 0, 0,1}};
X2[n_Integer, m_Integer] := {{1, 0, 0, 0}, {0, 1, m, 0},
{0, 0, 1, 0}, {0, 0, 0,1}};
X3[n_Integer, m_Integer] := {{1, 0, 0, 0}, {0, 1, 0, 0},
{0, 0, 1, -n}, {0, 0, 0,1}};

N12 = {{0, -1, 0, 0}, {1, 0, 0, 0}, {0, 0, 1, 0}, {0, 0, 0, 1}};
N23 = {{1, 0, 0, 0}, {0, 0, -1, 0}, {0, 1, 0, 0}, {0, 0, 0, 1}};
N34 = {{1, 0, 0, 0}, {0, 1, 0, 0}, {0, 0, 0, -1}, {0, 0, 1, 0}};
```

```
Y1[n_Integer, m_Integer] := X1[n, m].N12;
Y2[n_Integer, m_Integer] := X2[n, m].N23;
Y3[n_Integer, m_Integer] := X3[n, m].N34;
Aq[n_Integer, m_Integer] := Y1[n, m].Y2[n, m].Y3[n, m];
(* Aq is the companion matrix of the char poly *)

Bq[n_Integer, m_Integer] := Y1[n, m].Y3[n, m].Y2[n, m];
(* Bq is a reordering of the Yi, still conjugate to Aq hence it has
the same char poly *)

ch1 = {{1, 0, 0, 0}, {0, 0, 1, 0}, {0, 1, 0, 0}, {0, 0, 0, 1}};
ch2 = {{1, 0, 0, 0}, {0, 0, 0, 1}, {0, 0, 1, 0}, {0, 1, 0, 0}};
A = Transpose[ch1.ch2];
(* the matrix A conjugates the matrix J given in the
paper to the matrix J we have defined *)

GetSymp[n_Integer, m_Integer] := Inverse[A].Bq[n, m].A;
(* output matrix is symplectic with desired char poly *)
```

References

[1] Keith Conrad, *Ideal classes and matrix conjugation over* $\mathbb{Z}$.
[2] Krishnendu Gongopadhyay, *On the conjugacy classes in the orthogonal and symplectic groups over algebraically closed fields*, Expositiones Mathematicae **28** (2010), 351–356.
[3] L.K. Hua and I. Reiner, *On the generators of the symplectic modular group*, Transactions of the American Mathematical Society **65** (1949), no. 3, 415–426.
[4] Anatole Katok, Svetlana Katok, and Klaus Schmidt, *Rigidity of measurable structure for* $\mathbb{Z}^d$*-actions by automorphisms of a torus*, Comment. Math. Helv. **77** (2002), 718–745.
[5] Dan Margalit and Steven Spallone, *A homological recipe for pseudo-anosovs*, Math. Res. Lett. **14** (2007), no. 5, 853–863.
[6] M. Ram Murty and Jody Esmonde, *Problems in algebraic number theory*, 2 ed., Springer, New York, 2005.
[7] Morris Newman, *Integral matrices*, Academic Press, New York, 1972.