Conjugacy classes in integral symplectic groups

Qingjie Yang *

School of Information, Renmin University of China, Beijing 100872, China

Received 8 September 2005; accepted 1 March 2006
Available online 5 May 2006
Submitted by H. Schneider

Abstract

We study the conjugacy classification of integral symplectic matrices with a given separable, irreducible and palindromic monic polynomial as their characteristic polynomial.

AMS classification: 15A36; 20H25

Keywords: Integral symplectic groups; Conjugacy classes; Class number; Cyclotomic polynomials

1. Introduction

The problem that we consider in this paper is the conjugacy classification of matrix, which has a given separable and irreducible polynomial as its characteristic polynomial, in \( SP_{2n}(\mathcal{D}) \), the integral symplectic groups over \( \mathcal{D} \), where \( \mathcal{D} \) is a principal ideal domain with characteristic not 2.

Classification up to conjugacy plays an important role in group theory. The symplectic groups are of importance because they have numerous applications to number theory and the theory of modular functions of many variables, especially as developed by Seigel in [6] and in numerous other papers. But our original motivation for studying this problem came not from algebra but rather from Riemann surfaces. Sjerve and Yang already discussed the special case that \( p \)-torsion in \( SP_{p-1}(\mathbb{Z}) \), see [10]. We develop these methods and study the problem for general \( \mathcal{D} \).
To explain our results we need to develop some notation. Throughout the paper \( \mathscr{D} \) will be a principal ideal domain with characteristic not 2. Let \( \mathcal{F} \) denote the quotient field of \( \mathscr{D} \). Let \( M_n(\mathscr{D}) \) be the set of \( n \times n \) matrices over \( \mathscr{D} \). Let \( I_n \) be the identity matrix in \( M_n(\mathscr{D}) \) and

\[
J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.
\]

**Definition 1.** The set of \( 2n \times 2n \) unimodular matrices \( X \) in \( M_{2n}(\mathscr{D}) \) such that

\[
X'JX = J,
\]

where \( X' \) is the transpose of \( X \), is called the symplectic group of genus \( n \) over \( \mathscr{D} \) and is denoted by \( \text{SP}_{2n}(\mathscr{D}) \). Two symplectic matrices \( X, Y \) of \( \text{SP}_{2n}(\mathscr{D}) \) are said to be conjugate or similar, denoted by \( X \sim Y \), if there is a matrix \( Q \in \text{SP}_{2n}(\mathscr{D}) \) such that \( Y = Q^{-1}XQ \). Let \( \langle X \rangle \) denote the conjugacy class of \( X \).

**Remark.** The definition is meaningful and clearly \( \text{SP}_{2n}(\mathscr{D}) \) is a subgroup of \( \text{GL}_{2n}(\mathscr{D}) \), the general linear group with entries in \( \mathscr{D} \). It is well known that every symplectic matrix in \( \text{SP}_{2n}(\mathscr{D}) \) has determinant one, see Artin [1]. It is readily verified that \( X \) belongs to \( \text{SP}_{2n}(\mathscr{D}) \) if and only if \( X' \) belongs to \( \text{SP}_{2n}(\mathscr{D}) \).

Given a matrix \( X \in M_{2n}(\mathscr{D}) \), we denote the characteristic polynomial of \( X \) by

\[
f_X(x) = |xI - X|.
\]

If \( X \in \text{SP}_{2n}(\mathscr{D}) \), then \( f_X(x) \) is “palindromic” and monic, that is

\[
x^{2n}f \left( \frac{1}{x} \right) = f(x) \quad \text{and} \quad f(0) = 1.
\]

We always assume that \( f(x) \in \mathscr{D}[x] \) is a separable, irreducible and palindromic monic polynomial of degree \( 2n \) in this paper. Let \( M_f \) be the set of all symplectic matrices, whose characteristic polynomials are \( f(x) \), over \( \mathscr{D} \), that is

\[
M_f = \{ X \in \text{SP}_{2n}(\mathscr{D})| f_X(x) = f(x) \}.
\]

We use \( \mathcal{M}_f \) to denote the set of the conjugacy classes of \( M_f \) in \( \text{SP}_{2n}(\mathscr{D}) \).

Let \( \zeta \) be a fixed root of \( f(x) \). Let \( \mathcal{H} = \mathscr{D}[\zeta], \mathcal{I} = \mathcal{F}[\zeta] \). Then \( \mathcal{I} \) is the quotient field of \( \mathcal{H} \). An ideal (fractional ideal) in \( \mathcal{I} \) is a finitely generated \( \mathcal{H} \)-submodule of \( \mathcal{I} \) which is a free \( \mathscr{D} \)-module of rank \( 2n \). An integral ideal is an ideal which is contained in \( \mathcal{H} \).

Two ideal \( a, b \) are equivalent if there are non-zero elements \( \lambda, \mu \in \mathcal{H} \) such that \( \lambda a = \mu b \). We denote the equivalence class of \( a \) by \( \langle a \rangle \) and let \( \mathcal{C} \) denote the collection of equivalence classes of ideals. \( \mathcal{C} \) is a commutative monoid with respect to multiplication of ideals. The identity is \( \langle \mathcal{H} \rangle \).

Note that \( 1/\zeta \) is another root of \( f(x) \) and we have conjugate in \( \mathcal{I} \) such that \( \tilde{\zeta} = \frac{1}{\zeta} \). Then \( \tilde{a} = [\tilde{a}| a \in a] \) is also an integral ideal. Let \( P_f \) be the set of pairs \( (a, a) \) consisting of an integral ideal \( a \) and an element \( a \in \mathcal{H} \) such that \( \tilde{a} = a\Delta a' \) and \( a = \tilde{a} \), where \( \Delta = \zeta^{1-n}f'(\zeta) \) and \( a' \) is the complementary ideal. Two such pairs \( (a, a) \) and \( (b, b) \) are said to be equivalent if there are non-zero elements \( \lambda, \mu \in \mathcal{H} \) such that \( \lambda a = \mu b \) and \( \lambda \tilde{a} a = \mu \tilde{b} b \). We denote by \( \langle a, a \rangle \) the equivalence class of \( (a, a) \). Let \( \mathcal{P}_f \) denote the set of all classes of \( P_f \).

Suppose \( X \in M_f \). There is an eigenvector \( a = (a_1, a_2, \ldots, a_{2n})' \in \mathcal{H}^{2n} \) corresponding to \( \zeta \), that is \( Xa = \zeta a \). Let \( a \) be the \( \mathcal{H} \)-module generated by \( a_1, a_2, \ldots, a_{2n} \), and let \( a = \Delta^{-1}a'J\tilde{a} \). It is easy to check that \( a \) is an integral ideal in \( \mathcal{H} \) and \( a = \tilde{a} \). Thus \( a_1, a_2, \ldots, a_{2n} \) are
independent over $\mathcal{D}$. Furthermore we will prove that $(a, a) \in P_f$ and that the mapping $\Psi : M_f \rightarrow P_f, (X) \mapsto (a, a)$ is well defined.

**Theorem 1.1.** $\Psi$ is bijection.

Thus we can count conjugacy classes of $M_f$ by enumerating the elements of $P_f$. Since $\mathcal{R} = \Delta \mathcal{R}'$ we have $(\mathcal{R}, 1) \in P_f$, and

**Corollary 1.** $M_f \neq \emptyset$.

If $\mathcal{R}$ is integrally closed, then $\mathcal{C}$ is an abelian group. The inverse of $(a)$ is $(\Delta a')$. Also we have that $P_f = \{(a, a)|a\bar{a} = (a)$ and $a = \bar{a}\}$ and $P_f$ turns out to be an abelian group where multiplication is given by $\langle a, a\rangle \langle b, 1 \rangle = \langle ab, ab \rangle$. Let $C_0$ denote the subgroup of integral ideal classes defined by

$$C_0 = \{a \in \mathcal{C}|a\bar{a} = (a), a = \bar{a} \text{ for some } a \in \mathcal{R}\}. \quad (4)$$

Let $U^+ = \{u \in U|u = \bar{u}\}$ and $C = \{u\bar{u}|u \in U\}$, where $U$ is the group of units in $\mathcal{R}$. Clearly, $C \subset U^+$ and they are subgroups of $U$. We shall show

**Theorem 1.2.** There is a natural short exact sequence of abelian groups

$$1 \rightarrow U^+/C \xrightarrow{\phi} P_f \xrightarrow{\psi} C_0 \rightarrow 1, \quad (5)$$

where $\phi(u) = \langle \mathcal{R}, u \rangle$ and $\psi(a, a) = \langle a \rangle$.

Consequently, for the special case $\mathcal{D} = \mathbb{Z}$, let $\mathcal{C}_1$ be the set of integral ideal classes $a$ with $a\bar{a}$ a principal ideal,

$$\mathcal{C}_1 = \{a \in \mathcal{C}|a\bar{a} = (a) \text{ for some } a \in \mathcal{R}\}. \quad (6)$$

We shall show

**Theorem 1.3.** Let $q_m$ be the number of elements in $M_f$, where $f(x)$ is the $m$th cyclotomic polynomial. Then

$$q_m = \begin{cases} \frac{q_m}{2} & m \equiv 2 \pmod 4, \\ 2^{\frac{\phi(m)}{2}} h_1 & m \not\equiv 2 \pmod 4, \text{ and } m \text{ is prime power}, \\ 2^{\frac{\phi(m)}{2}-1} h_1 & m \not\equiv 2 \pmod 4, \text{ and } m \text{ is not prime power,} \end{cases}$$

where $\phi(m)$ is the Euler totient function and $h_1 = |\mathcal{C}_1|$ is the first factor of class number.

The idea for proving Theorem 1.1 comes from the results of Latimer and MacDuffee [3] and Taussky [7,8]. First in Section 2 we shall review some results of ideal classes, most of them can be found in Lang [2], Marcus [4] and any book about ideal theory. In Section 3 we introduce the $S$-pairs and prove Theorem 1.1. In Section 4 we shall show Theorem 1.2. Finally, in Section 5 we shall consider the rational integer case and prove Theorem 1.3.
2. Preliminaries

Let \( \mathcal{K} \) be the splitting field over \( \mathcal{F} \) of \( f(x) \). Then \( B \subset C \subset \mathcal{K} \). We also denote the set of non-zero elements of \( B \) by \( B^* \).

If \( \zeta_i \) is a root of \( f(x) \), then \( \frac{1}{\zeta_i} \) is also a root of \( f(x) \) and \( \frac{1}{\zeta_i} \in \mathcal{F}(\zeta_i) \). Without loss of generality we assume that the \( 2n \) roots \( \zeta_1, \zeta_2, \ldots, \zeta_{2n} \) of \( f(x) \) satisfy \( \zeta_{2i-1} \zeta_{2i} = 1 \), for \( i = 1, \ldots, n \).

Let \( \alpha = a_0 + a_1 \zeta + \cdots + a_{2n-1} \zeta^{2n-1} \in \mathcal{F} \). The \( i \)-th conjugate of \( \alpha \) is defined by \( \alpha^{(i)} = a_0 + a_1 \zeta^i + \cdots + a_{2n-1} \zeta^{2n-1} \). Then the trace of an element \( \alpha \) is as follows:

\[
\text{Tr}(\alpha) = \sum_{i=1}^{2n} \alpha^{(i)} \in \mathcal{F}.
\]

(7)

It is clear that if \( \alpha \in B \), then \( \text{Tr}(\alpha) \in \mathcal{F} \).

Suppose \( \alpha_1, \alpha_2, \ldots, \alpha_{2n} \in \mathcal{F} \), the discriminant of \( \alpha_1, \alpha_2, \ldots, \alpha_{2n} \) is

\[
\Delta(\alpha_1, \alpha_2, \ldots, \alpha_{2n}) = \det \begin{pmatrix}
\alpha_1^{(1)} & \alpha_1^{(2)} & \cdots & \alpha_1^{(2n)} \\
\alpha_2^{(1)} & \alpha_2^{(2)} & \cdots & \alpha_2^{(2n)} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha_{2n}^{(1)} & \alpha_{2n}^{(2)} & \cdots & \alpha_{2n}^{(2n)}
\end{pmatrix}.
\]

(8)

Lemma 1. \( \alpha_1, \alpha_2, \ldots, \alpha_{2n} \) are independent over \( \mathcal{F} \) if, and only if \( \Delta(\alpha_1, \alpha_2, \ldots, \alpha_{2n}) \neq 0 \).

For a proof see Lang [2].

According to Galois Theory, there are at least \( 2n \) automorphisms \( \eta_1 = 1, \ldots, \eta_{2n} \) of \( \mathcal{K} \) in \( \text{Gal}(\mathcal{K}/\mathcal{F}) \), the Galois group of the extension field \( \mathcal{K}/\mathcal{F} \), such that \( \eta_i(\zeta) = \zeta_i \). Then the \( i \)-conjugate of \( \alpha \in \mathcal{F} \) has the form \( \alpha^{(i)} = \eta_i(\alpha) \), for \( i = 1, \ldots, 2n \). We also use \( \alpha^{(i)} \) to denote \( \eta_i(\alpha) \) if \( \alpha \in \mathcal{K} \).

It is obvious that \( \eta_2 \) is an involution on the extension field \( \mathcal{F} \). We use \( \tilde{\alpha} \) instead of \( \eta_2(\alpha) \) if \( \alpha \in \mathcal{F} \). It is easy to check that

\[
\eta_{2i-1}(\tilde{\alpha}) = \eta_{2i}(\alpha) \quad \text{and} \quad \eta_{2i}(\tilde{\alpha}) = \eta_{2i-1}(\alpha)
\]

(9)

for \( \alpha \in \mathcal{F} \). Some notation is needed for the sake of convenience. We let

\[
\tilde{A} = (\tilde{\alpha}_{ij}) \quad \text{and} \quad \eta_k(B) = B^{(k)} = (\beta_{ij}^{(k)})
\]

(10)

if \( A = (\alpha_{ij}) \) and \( B = (\beta_{ij}) \) are matrices with entries in \( \mathcal{F} \) and \( \mathcal{K} \) respectively.

The following lemmas are very useful.

Lemma 2. Suppose \( M \in M_{2n}(\mathcal{F}) \) and \( \alpha, \beta \in \mathcal{F}^{2n} \) are two vectors. Then for any \( 1 \leq i, j \leq 2n \), there is \( 1 \leq k \leq 2n \), where \( k \) depends on \( i, j \), such that \( \alpha^{(i)} M \beta^{(j)} = (\alpha' M \beta^{(k)})^{(i)} \).

Proof. Since \( \eta_1, \ldots, \eta_{2n} \) are permutations of the roots of \( f(x) \), for any \( 1 \leq i, j \leq 2n \), \( \eta_{i-1}^{-1} \eta_j(\zeta) \) is a root of \( f(x) \), say \( \zeta_k \). We have \( \eta_k(\zeta) = \eta_k^{-1}(\eta_j(\zeta)) \), therefore \( \eta_j(a) = \eta_k(\eta_j(a)) \), for any \( a \in \mathcal{F} \).

Hence \( (\alpha' M \beta^{(k)})^{(i)} = \eta_i(\alpha' M \eta_k(\beta)) = \eta_i(\alpha') M \eta_k(\beta) = (\alpha') M \beta^{(k)} \). \( \square \)

Lemma 3. Suppose \( M, N \in M_{2n}(\mathcal{F}) \) and \( \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2n})' \in \mathcal{F}^{2n} \), where \( \alpha_1, \ldots, \alpha_{2n} \) are independent over \( \mathcal{F} \), and \( \alpha' M \tilde{\alpha}^{(i)} = \alpha' N \tilde{\alpha}^{(i)} \) (for \( i = 1, \ldots, 2n \)). Then \( M = N \).
Proof. We only prove the special case $N = 0$. By Lemma 2, for any $1 \leq i, j \leq 2n$, there is $1 \leq k \leq 2n$ such that $\alpha^{(i)} M \tilde{\alpha}^{(j)} = (\alpha' M \tilde{\alpha}^{(k)})^{(i)} = 0$. That is $A' M B = 0$, where $A = (\alpha^{(j)})$ and $B = (\tilde{\alpha}^{(j)})$ are $2n \times 2n$ matrices. By Lemma 1, $\det A \neq 0$ and $\det B \neq 0$, since $\alpha_1, \alpha_2, \ldots, \alpha_{2n}$ are independent over $\mathcal{D}$, therefore $M = 0$. □

Let $\alpha$ be an ideal in $\mathcal{D}$. The complementary ideal of $\alpha$ is

$$
\alpha' = \{ \alpha \in \mathcal{D} | \text{Tr}(\alpha \alpha) \subset \mathcal{D} \}.
$$

Let $\alpha_1, \alpha_2, \ldots, \alpha_{2n}$ be a $\mathcal{D}$-basis of $\alpha$. There is a dual basis $\alpha'_1, \alpha'_2, \ldots, \alpha'_{2n}$ in $\mathcal{D}$, that is a basis such that $\text{Tr}(\alpha'_i \alpha_j) = \delta_{ij}$, where $\delta_{ij}$ is the Kronecker symbol. This is equivalent to either of the following equations:

$$
\sum_k \alpha_i^{(k)} \alpha_j^{(k)} = \delta_{ij} \quad \text{or} \quad \sum_k \alpha_k^{(i)} \alpha_k^{(j)} = \delta_{ij}.
$$

We also have

$$
\alpha' = \mathcal{D} \alpha'_1 + \mathcal{D} \alpha'_2 + \cdots + \mathcal{D} \alpha'_{2n}
$$

and $\mathcal{R} = \mathcal{A} \mathcal{R}'$, that is $P_f \neq \emptyset$.

3. The Correspondence $\Psi$

First in this section we define $S$-pairs.

Definition 2. A pair $(\alpha, a)$ consisting of an integral ideal $\alpha$ and an element $a \in \mathcal{R}$ is said to be an $S$-pair, if there is a basis $\alpha_1, \alpha_2, \ldots, \alpha_{2n}$ of $\alpha$, such that

$$
\alpha' J \tilde{\alpha}^{(i)} = \delta_{1i} a \Delta, \quad i = 1, \ldots, 2n,
$$

where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2n})'$. The basis $\alpha_1, \alpha_2, \ldots, \alpha_{2n}$ is called a $J$-orthogonal basis of $\alpha$ with respect to $a$, and the vector $\alpha$ is called a $J$-vector with respect to $S$-pair $(\alpha, a)$.

Remark. By Lemma 2, we see that (14) is equivalent to

$$
\alpha'^{(i)} J \tilde{\alpha}^{(j)} = \delta_{ij} a \Delta^{(i)}.
$$

If $\lambda = \alpha' J \tilde{\alpha}$, then $\tilde{\lambda} = \lambda \tilde{J} \tilde{\alpha} = \alpha' J \alpha = (\alpha' J \alpha)' = -\alpha' J \tilde{\alpha} = -\lambda$. Since $\tilde{\Delta} = -\Delta$ it follows that if $(\alpha, a)$ is an $S$-pair, then $\alpha = \tilde{\alpha}$.

Lemma 4. A pair $(\alpha, a)$ is an $S$-pair if, and only if $(\alpha, a) \in P_f$.

Proof. Suppose $(\alpha, a)$ is an $S$-pair. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2n})'$ be a $J$-vector with respect to $(\alpha, a)$. Let $\beta = (\beta_1, \beta_2, \ldots, \beta_{2n})' = \frac{1}{a \Delta} J \tilde{\alpha}$. Then $\alpha'^{(i)} \beta^{(j)} = \delta_{ij}$, which implies $\text{Tr}(\alpha_i \beta_j) = \delta_{ij}$, so $\beta_1, \beta_2, \ldots, \beta_{2n}$ is the dual basis of $\alpha_1, \alpha_2, \ldots, \alpha_{2n}$. Since $\det(J) = 1$, we see that $\beta_1, \beta_2, \ldots, \beta_{2n}$ is also a basis of $\frac{1}{a \Delta} \tilde{\alpha}$. Hence $\tilde{\alpha} = a \Delta \alpha'$.

For the converse, suppose $(\alpha, a) \in P_f$. If $\beta_1, \beta_2, \ldots, \beta_{2n}$ is a basis of $\alpha$ then $\tilde{\beta}_1, \tilde{\beta}_2, \ldots, \tilde{\beta}_{2n}$ is a basis of $\tilde{\alpha}$. Let $\gamma_1, \gamma_2, \ldots, \gamma_{2n}$ be the dual basis of $\beta_1, \beta_2, \ldots, \beta_{2n}$. Then $\text{Tr}(\beta_1 \gamma_j) = \delta_{ij}$, and we have $\beta'^{(i)} \gamma^{(j)} = \delta_{ij}$, where $\beta = (\beta_1, \beta_2, \ldots, \beta_{2n})', \gamma = (\gamma_1, \gamma_2, \ldots, \gamma_{2n})'$. Since $\tilde{\alpha} = a \Delta \alpha'$, there is $M \in GL_{2n}(\mathcal{D})$ such that $M \tilde{\beta} = a \Delta \gamma$. Then

$$
\beta' M \tilde{\beta}^{(i)} = a^{(i)} \Delta^{(i)} \beta' \gamma^{(i)} = \delta_{1i} a \Delta.
$$

(15)
and
\[ \beta'M' \tilde{\beta}^{(i)} = \tilde{\alpha}A\gamma' \eta_i(\tilde{\beta}) = -aA\eta_2(\gamma')\eta_2(\beta) = -\delta_{i1}aA. \] (16)

For the last equality, we use Formula (9). Thus \( \beta'M' \tilde{\beta}^{(i)} = -\beta'M' \tilde{\beta}^{(i)} \) (for \( i = 1, \ldots, 2n \)), and so \( M' = -M \) (by Lemma 3). According to Newman [5], there is \( Q \in GL_{2n}(\mathcal{D}) \) such that \( M = Q'JQ \). If \( \alpha = Q\beta \), then
\[ \alpha'J\tilde{\alpha}^{(i)} = \beta'M \tilde{\beta}^{(i)} = \delta_{i1}aA. \]

So \( \alpha \) is a \( J \)-vector with respect to \( (a, a) \). \( \square \)

Recall that \( M_f \) is the set of all the matrices in \( SP_{2n}(\mathcal{D}) \) with characteristic polynomial \( f(x) \), and \( \mathcal{M} \) is the set of the similarity classes in \( M_f \) over \( SP_{2n}(\mathcal{D}) \). Suppose \( X \in M_f \). There is an eigenvector \( \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2n})' \in \mathbb{R}^{2n} \) corresponding to \( \zeta \), that is \( X\alpha = \zeta \alpha \). Let \( a \) be the \( \mathcal{D} \)-module generated by \( \alpha_1, \alpha_2, \ldots, \alpha_{2n} \), i.e.
\[ a = \mathcal{D}\alpha_1 + \mathcal{D}\alpha_2 + \cdots + \mathcal{D}\alpha_{2n} \]
and \( a = \Delta^{-1}\alpha'J\tilde{\alpha} \). It is easy to check that \( a \) is an integral ideal in \( \mathbb{R} \) and \( a = \tilde{a} \). Thus \( \alpha_1, \alpha_2, \ldots, \alpha_{2n} \) are independent over \( \mathcal{D} \). Furthermore, we have

**Lemma 5.** The pair \( (a, a) \) is an \( S \)-pair.

**Proof.** We only need to prove \( \alpha'J\tilde{\alpha}^{(i)} = 0 \) (for \( i = 2, \ldots, 2n \)). Assume \( 2 \leq i \leq 2n \). From \( X\alpha = \zeta \alpha \) and \( X \in SP_{2n}(\mathcal{D}) \), we have \( X\alpha^{(i)} = \zeta_i\alpha^{(i)} \) and \( X\tilde{\alpha}^{(i)} = 1_i\tilde{\alpha}^{(i)} \). Hence
\[ \alpha'J\tilde{\alpha}^{(i)} = \frac{\zeta_i}{\zeta} \alpha'XJX\tilde{\alpha}^{(i)} = \frac{\zeta_i}{\zeta} \alpha'J\tilde{\alpha}^{(i)}. \] (17)

The last equality follows from the fact that \( X \in SP_{2n}(\mathcal{D}) \). Since \( \zeta \neq \zeta_i \), we get \( \alpha'J\tilde{\alpha}^{(i)} = 0 \). \( \square \)

Suppose \( Y \) is another element of \( M_f \), and \( \beta = (\beta_1, \beta_2, \ldots, \beta_{2n})' \in \mathbb{R}^{2n} \) is an eigenvector corresponding to \( \zeta \), that is \( Y\beta = \zeta \beta \). Let \( b \) be the integral ideal generated by \( \beta_1, \beta_2, \ldots, \beta_{2n} \) and \( b = \Delta^{-1}\beta'J\tilde{\beta} \).

**Lemma 6.** \( X \sim Y \) if, and only if \( (a, a) = (b, b) \).

**Proof.** **Necessity.** Suppose there is \( Q \in SP_{2n}(\mathcal{D}) \) such that \( Y = Q^{-1}XQ \). Then \( QY = XQ \) and therefore \( XQ\beta = QY\beta = \zeta Q\beta \), that is \( Q\beta \) is an eigenvector of \( X \). There are \( \lambda, \mu \in \mathbb{R}^* \) such that \( \lambda\alpha = \mu Q\beta = Q\mu\beta \). So \( \lambda\alpha = \mu b \), and
\[ \lambda\tilde{\alpha} = \Delta^{-1}\lambda\alpha'J\tilde{\alpha} = \Delta^{-1}(\mu Q\beta)'J\tilde{\mu}Q\beta = \Delta^{-1}\mu\tilde{\mu}Q'JQ\tilde{\beta} = \Delta^{-1}\mu\tilde{\mu}\beta'J\tilde{\beta} = \mu\tilde{\mu}b. \]

Therefore \( (a, a) = (b, b) \).

**Sufficiency.** Suppose \( \lambda, \mu \in \mathbb{R}^* \) are such that \( \lambda\alpha = \mu b \) and \( \lambda\tilde{\alpha} = \mu \tilde{\mu}b \). Then there is \( Q \in GL_{2n}(\mathcal{D}) \) such that \( \lambda\alpha = \mu Q\beta \), and thus
\[ \mu QY\beta = \mu Q\zeta\beta = \zeta \mu Q\beta = \zeta \lambda\alpha = \lambda X\alpha = \mu XQ\beta, \]
hence \( QY\beta = XQ\beta \). Therefore \( QY = XQ \), i.e. \( Y = Q^{-1}XQ \).
It remains to prove that $Q \in SP_{2n}(\mathcal{D})$. If $i = 2, \ldots, 2n$, then

$$
\beta' Q' J Q \tilde{\beta}(i) = \frac{\lambda \tilde{\alpha}(i)}{\mu \tilde{\alpha}(i)} \alpha' J \tilde{\alpha}(i) = 0 = \beta' J \tilde{\beta}(i).
$$

If $i = 1$, then

$$
\beta' Q' J Q \tilde{\beta}(i) = \frac{\lambda \tilde{\alpha}(i)}{\mu \tilde{\alpha}(i)} \alpha' J \tilde{\alpha} = \frac{b}{a} \alpha' J \tilde{\alpha} = \beta' J \tilde{\beta}.
$$

Hence $Q' J Q = J$ (by Lemma 3). □

Let $\Psi$ denote the correspondence from $\mathcal{M}$ to $\mathcal{P}_f$ defined as above. Lemma 6 guarantees $\Psi$ is well defined and injective. The proof of Theorem 1.1 is completed by following lemma.

**Lemma 7.** $\Psi$ is surjective.

**Proof.** Let $(a, a) \in P_f$ and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2n})'$ be a $J$-vector with respect to $(a, a)$. Then we see that $\zeta \alpha_1, \zeta \alpha_2, \ldots, \zeta \alpha_{2n}$ is another basis of $a$, and so there is $X \in GL_{2n}(\mathcal{D})$, such that $X \alpha = \zeta \alpha$. It is clear that $f_X(x) = f(x)$. We only need to prove that $X \in SP_{2n}(\mathcal{D})$. We have

$$
\alpha' X' J X \tilde{\alpha}(i) = \frac{\zeta}{\tilde{\alpha}(i)} \alpha' J \tilde{\alpha} = \delta_{ij} a, \Delta.
$$

Hence $\alpha' X' J X \tilde{\alpha}(i) = \alpha' J \tilde{\alpha}(i)$ (for $i = 1, \ldots, 2n$). By Lemma 3, $X' J X = J$. This completes the proof. □

4. Class number of $\mathcal{P}_f$

In this section we prove Theorem 1.2. Suppose $\mathcal{R}$ is integrally closed in $\mathcal{P}$. Then $\mathcal{C}$ is turned to be a group, the identity is $\mathcal{R}$ and $\mathcal{a}^{-1} = \Delta a'$, see Lang [2]. We easily see that $(a, a) \in P_f$ if and only if $\tilde{a}a = (a)$ and $a = \tilde{a}$. Then $\mathcal{P}_f$ is a group if we define multiplication in $\mathcal{P}_f$ by

$$
\langle a, a \rangle \langle b, b \rangle = \langle ab, ab \rangle.
$$

The identity is $\langle \mathcal{R}, 1 \rangle$ and the inverse of $\langle a, a \rangle$ is $\langle \tilde{a}, a \rangle$.

For the proof of Theorem 1.2 we will need the following lemmas.

**Lemma 8.** Suppose $(a, a) \in P_f$, $\lambda \in \mathcal{R}^*$. Then

1. $\langle \lambda a, \lambda \tilde{a} a \rangle \in P_f$.
2. $(a, \lambda a) \in P_f$ if and only if $\lambda \in U^+$.

**Proof.** The first part is because $\langle \lambda a \rangle' = \frac{1}{\lambda} a'$, and hence $\tilde{\lambda} \alpha = \tilde{\lambda} \tilde{\alpha} = \tilde{\lambda} a \Delta a' = \lambda \tilde{\lambda} a (\lambda a)'$.

For the second part, we have $\tilde{a} = a \Delta a$ and $a = \tilde{a}$. If $(a, \lambda a) \in P$, then $\tilde{a} = \lambda a \Delta a'$ and $\lambda a = \tilde{\lambda} a$. Hence $\langle \lambda a \rangle = (a)$ and $\lambda = \tilde{\lambda}$, this means $\lambda \in U^+$. The converse is quite simple. □

**Lemma 9.** Suppose $(a, a), (a, b) \in P_f$. Then $\langle a, a \rangle = \langle a, b \rangle$ if and only if $\frac{a}{b} \in C$.

**Proof.** Suppose $\langle a, a \rangle = \langle a, b \rangle$. There are $\lambda, \mu \in \mathcal{R}^*$ such that $\lambda a = \mu a$ and $\lambda \tilde{\lambda} a = \mu \tilde{\mu} b$. If $u = \frac{\mu}{\lambda}$, then $u \in U$ and $\frac{u}{b} = u \tilde{u}$, that is $\frac{u}{b} \in C$. 


Conversely, suppose \( \frac{a}{b} = u\bar{u} \) for some \( u \in U \). Then \( \langle a, a \rangle = \langle a, u\bar{u}b \rangle = \langle u\bar{a}, u\bar{u}b \rangle = \langle a, b \rangle \). \( \square \)

**Lemma 10.** Let \((a, a), (b, b) \in P_f, \) and \( \lambda a = \mu b, \) for some \( \lambda, \mu \in \mathbb{R}^* \). Then \( \langle a, a \rangle = \langle b, ub \rangle \) for some \( u \in U^+ \).

**Proof.** If \( \lambda a = \mu b \), then \( \lambda \bar{a} = \mu \bar{b} \). Hence \( \langle \lambda \bar{a}, \lambda \bar{a} \rangle = \lambda \mu \bar{a} \bar{b} = \langle \mu \bar{b}, \mu \bar{b} \rangle \). Then there is a unit \( u \in U^+ \), such that \( \lambda \bar{a} = \mu \bar{a} u \). Therefore \( \langle a, a \rangle = \langle \lambda a, \lambda \bar{a} \rangle = \langle \mu b, \mu \bar{b} \rangle = \langle b, ub \rangle \). \( \square \)

Now we can prove Theorem 1.2; namely there is a short exact sequence

\[
1 \to U^+/C \xrightarrow{\phi} P_f \xrightarrow{\psi} \mathbb{C}_0 \to 1,
\]
where \( \phi(u) = \langle \mathbb{R}, u \rangle \) and \( \psi(a, a) = \langle a \rangle \).

**Proof of Theorem 1.2.** Clearly, \( \phi \) is well defined and a group monomorphism (by Lemma 9). \( \psi \) is also well defined and a group epimorphism (by Lemma 4). \( \psi \phi(u) = \phi \langle \mathbb{R}, u \rangle = \langle \mathbb{R} \rangle \) (by definition) and \( \text{Ker} \psi = \text{Im} \phi \) (by Lemma 10). This completes the proof. \( \square \)

**Remark.** These three Lemmas are also true even if \( \mathbb{R} \) is not integrally closed in \( \mathbb{P} \). So there is a bijective mapping between \( P_f \) and \( \mathbb{C}_0 \times U^+/C \).

**Corollary 2.** If \( \mathbb{D} \) is the rational field \( \mathbb{Q} \), then there is an one-to-one correspondence between \( \mathbb{M}_f \) and \( \mathbb{R}^+/C \), where \( \mathbb{R}^+ = \{ a \in \mathbb{R}^* | a = \bar{a} \} \) and \( C = \{ a\bar{a} | a \in \mathbb{R}^* \} \), where the bar denotes complex conjugation.

**Proposition 1.** If \( f(x) = x^2 + x + 1 \), then the number of conjugacy classes of \( M_f \) in \( SP_2(\mathbb{Q}) \) is infinity.

**Proof.** Let \( \mathbb{R} = \mathbb{Q}[\xi], \xi = e^{\frac{2\pi i}{3}} \). Let \( p, q \) are different primes with \( p \equiv q \equiv 2 \) (mod 3). We want to show \([p] \neq [q]\) in \( \mathbb{R}^+/C \).

Suppose \([p] = [q]\). There are \( \lambda = x_1 + y_1 \xi, \mu = x_2 + y_2 \xi \in \mathbb{Z}[\xi] \) such that \( \lambda \bar{\lambda} p = \mu \bar{\mu} q \), that is

\[
(x_1^2 - x_1 y_1 + y_1^2)p = (x_2^2 - x_2 y_2 + y_2^2)q.
\]

Then there is an integer \( k \) such that

\[
\begin{align*}
x_1^2 - x_1 y_1 + y_1^2 &= kq, \\
x_2^2 - x_2 y_2 + y_2^2 &= kp.
\end{align*}
\]

(18)

This is impossible due to the fact that if the Diophantine equation \( x^2 - xy + y^2 = kp^r \), where \( p \equiv 2 \) (mod 3) and \( p \nmid k \), has solution, then \( r \) is even.

By a theorem of Dirichlet, there are infinite primes of form \( 3k + 2 \), and so we prove that \( \mathbb{R}^+/C \) is an infinite group. \( \square \)

In general we have

**Conjecture.** Let \( f(x) = x^{p-1} + \cdots + x + 1 \), \( p \) an odd prime. Then the number of conjugacy classes of \( M_f \) in \( SP_{p-1}(\mathbb{Q}) \) is infinite.
5. The rational integer case

In this section, we assume $\mathcal{D} = \mathbb{Z}$ and $\mathcal{F} = \mathbb{Q}$. Using the fact that the number of ideal classes is finite, the unit group $U$ is a finite generated abelian group and $U^+ \subset C$, we get

**Proposition 2.** If $\mathcal{R}$ is integrally closed in $\mathcal{D}$, then $\mathcal{M}_f$ is finite.

From now on we consider the $m$th ($m > 2$) cyclotomic polynomial

$$\Phi_m(x) = (x - \zeta_1)(x - \zeta_2) \ldots (x - \zeta_{\phi(m)}), \tag{19}$$

where $\zeta_1, \zeta_2, \ldots, \zeta_{\phi(m)}$ are the primitive $m$th roots of unity and $\phi(m)$ is the Euler totient function. It is well known that the $\Phi_m(x)$ has integral coefficients and is irreducible over $\mathbb{Q}$. We simply denote $M_{\Phi_m}$ and $\mathcal{M}_{\Phi_m}$ by $M_m$ and $\mathcal{M}_m$.

Let $\zeta = \zeta_m = e^{2\pi i / m}$, $\mathcal{R}_m = \mathbb{Z}[\zeta_m]$. Then the involution on $\mathcal{R}_m$ is just complex conjugation. We denote $\zeta_m$ by $\tilde{\zeta}_m$.

**Proposition 3.** For any $X \in M_m$, we have $X \not\sim X^{-1}$.

**Proof.** Let $\alpha \in \mathcal{R}_m^{\Phi(m)}$ be an eigenvector of $X$ corresponding to $\zeta$, $X\alpha = \zeta\alpha$. Then $X^{-1} \tilde{\alpha} = \bar{\zeta} \tilde{\alpha}$. Hence $\Psi(X) = \langle \alpha, \Delta^{-1} \alpha' J \tilde{\alpha} \rangle$ and $\Psi(X^{-1}) = \langle \bar{\alpha}, \Delta^{-1} \bar{\alpha}' \tilde{\alpha} \rangle$. Since $\Delta^{-1} \alpha' J \tilde{\alpha} = -\Delta^{-1} \bar{\alpha}' J \alpha$, and for any $\lambda \in \mathcal{R}_m$, $\lambda \tilde{\lambda} \neq -1$, we have $\Psi(X) \neq \Psi(X^{-1})$. □

Recall that $\mathcal{C}_1$ is the set of integral ideal classes $a$ with $\tilde{a}a$ a principal ideal. It is easy to check that $\mathcal{C}_0 \subset \mathcal{C}_1$. To show that $\mathcal{C}_0 = \mathcal{C}_1$ we need

**Lemma 11.** Suppose $\zeta$ is a primitive $m$th root of unity. Then $(1 - \zeta)$ is a prime ideal of $\mathcal{R}_m$ if $m$ is a prime power and $1 - \zeta$ is a unit of $\mathcal{R}_m$ if $m$ has at least two distinct prime factors.

See Washington [9].

**Lemma 12.** $\mathcal{C}_0 = \mathcal{C}_1$.

**Proof.** Suppose $\tilde{a}a = (a_0)$ where $a_0 \in \mathcal{R}_m^n$. We need to find a unit $u \in U$ such that $ua_0 = \bar{u}a_0$. Let $u_0 = \bar{a}_0 / a_0$. We see that $u_0$ is a unit because $(a_0) = (\bar{a}_0)$, and $u_0 \bar{u}_0 = 1$. According to Washington [9] $u_0 = \pm \zeta^k$, for some integer $k$. If $u_0 = \zeta^{2l}$, for some integer $l$, then we can choose $u = \zeta^l$. Now we suppose $u_0 \neq \zeta^{2l}$, for any integer $l$.

Note that

$$a \equiv \tilde{a} \pmod{1 - \zeta^2} \tag{20}$$

for any $a \in \mathcal{R}_m$.

**Case 1.** If $m$ is odd, then $u_0 = -\zeta^k$, for some integer $k$. This is because if $u_0 = \zeta^{2k+1}$ then $u_0 = \zeta^{2k+1 - m}$, where $2k - m$ is even. By Lemma 11, either $(1 - \zeta)$ is a prime ideal in $\mathcal{R}_m$ or $1 - \zeta$ is a unit in $\mathcal{R}_m$. If $1 - \zeta$ is a unit, then $\frac{(1 - \zeta)a_0}{(1 - \zeta)a_0} = \zeta^{-k-1} = \zeta^{2l}$, for some integer $l$. We can choose $u = (1 - \zeta)\zeta^l$.

Consider the case where $(1 - \zeta)$ is a prime ideal in $\mathcal{R}_m$. We want to show that $u_0 \neq -\zeta^k$ for any integer $k$. 

If \( a_0 \in (1 - \zeta) \), then \( \tilde{a} \subset (1 - \zeta) \) since \( \tilde{a} = (a_0) \). So either \( a \subset (1 - \zeta) \) or \( \tilde{a} \subset (1 - \zeta) \).
Both cases are the same and imply \( (a_0) \subset (1 - \zeta)(1 - \zeta) \). Let \( a_1 = \frac{a_0}{(1-\zeta)(1-\zeta)} \). Then \( a_1 \in \mathbb{R}_m^* \) and \( u_0 = \frac{\tilde{a}_1}{\tilde{a}_1} \).
Continuing this procedure, there is \( a \in \mathbb{R}_m^* \) and \( \tilde{a} \) such that \( u_0 = \frac{\tilde{a}}{\tilde{a}} \).

Now suppose \( u_0 = -\zeta^k \). Then, by (20), \( a \equiv \tilde{a} = -\zeta^k a \equiv -a \mod (1 - \zeta) \), therefore we get \( 2a \equiv 0 \mod (1 - \zeta) \). Since (2) is a prime ideal different from \( (1 - \zeta) \) we have \( a \equiv 0 \mod (1 - \zeta) \), that is \( a \equiv (1 - \zeta) \).

\[ \text{Contradiction.} \]

\text{Case 2.} If \( m \) is even, then \( u_0 = \zeta^{2k+1} \), for some integer \( k \), since \( -1 = \zeta^m \). Note that \(-\zeta\) is also a primitive \( m \)th root of unity, so either \( (1 + \zeta) \) is a prime ideal of \( \mathbb{R}_m \) or \( 1 + \zeta \) is a unit in \( \mathbb{R}_m \). If \( 1 + \zeta \) is a unit in \( \mathbb{R}_m \), then we use \( u = (1 + \zeta)^k \).

In the case that \( (1 + \zeta) \) is a prime ideal of \( \mathbb{R}_m \), we want to prove that \( u_0 \neq \zeta^{2k+1} \) for any integer \( k \). For a similar reason as in Case 1, there is \( a \in \mathbb{R}_m^* \), \( \tilde{a} \neq (1 + \zeta) \), such that \( u_0 = \frac{\tilde{a}}{\tilde{a}} \).

Suppose \( u_0 = \zeta^{2k+1} \). By (20) we have \( \tilde{a} = \zeta^{2l+1 + 1} a \equiv \zeta^{2l+1+1} \) \( \mod (1 - \zeta^2) \). This implies \( (\zeta - 1)(\zeta^{2l+1+1} + \cdots + \zeta + 1) a \equiv 0 \mod (1 - \zeta^2) \), thus \( (\zeta^{2l+2l+1+1} + \cdots + \zeta + 1) a \equiv 0 \mod (1 + \zeta) \). We know that \( \zeta^{2l+2l+1+1} + \cdots + \zeta + 1 \notin (1 + \zeta) \), hence \( \tilde{a} \in (1 + \zeta) \). \( \text{Contradiction.} \)

Now we want compute the index \([U^+ : C]\) of \( C \) in \( U^+ \), that is the order of \( U^+ / C \). Since for \( m \equiv 2 \mod (4) \), \( \mathbb{R}_m = \mathbb{R}_m^* \), we assume that \( m \neq 2 \mod (4) \). First, we quote some results of number theory (see Marcus [4] and Washington [9]). Let \( W = \{ \pm \zeta_m \} \), a finite cyclic group consisting of the roots of the index \( \mathbb{R}_m \).

**Lemma 13 (Dirichlet).** The unit group \( U \) of \( \mathbb{R}_m \) is the direct product of \( W \times V \), where \( V \) is a free abelian group of rank \( \frac{\phi(m)}{2} - 1 \).

**Lemma 14**

\[ [U : WU^+] = \begin{cases} 
1, & \text{m prime power}, \\
2, & \text{m not prime power}.
\end{cases} \]

**Lemma 15.** If \( m \) is not a prime power, then \( 1 - \zeta_m \notin WU^+ \) and \( (1 - \zeta_m)(1 - \zeta_m) \notin U^2 + 2 \).

**Proof.** If there is an integer \( l \) such that \( \zeta_m^l(1 - \zeta_m) \in U^+ \), then \( (1 - \zeta_m)(1 - \zeta_m) \notin U^2 + 2 \). Thus \( 4l - 2 \equiv 0 \mod (m) \) and \( m \) is even. Since \( m \neq 2 \mod (4) \), we have \( m \equiv 0 \mod (4) \). Thus \( 4l - 2 \equiv 0 \mod (4) \), which is impossible. This completes the proof. \( \Box \)

**Lemma 16.** Let \( k_m = [U^+ : C] \). Then

\[ k_m = \begin{cases} 
2^{\frac{\phi(m)}{2}}, & \text{m prime power}, \\
2^{\frac{\phi(m)}{2} - 1}, & \text{m not prime power}.
\end{cases} \]

**Proof.** By Lemmas 13 and 15, we see that \( U^+ \) is the direct product of \( \mathbb{Z}_2 \) and a free abelian group with rank \( \frac{\phi(m)}{2} - 1 \), and then we get \([U^+ : U^2 + 2] = 2^{\frac{\phi(m)}{2}} \).

Lemma 14 tells us that if \( m \) is a prime power, then \( C = U^2 + 2 \), and we obtain \( k_m = 2^{\frac{\phi(m)}{2}} \).
If \( m \) is not a prime power, then \( U = WU^+ \cup (1 - \zeta)WU^+ \) (by Lemmas 14 and 15). We get \( C = U^{+2} \cup (1 - \zeta)(1 - \bar{\zeta})U^{+2} \), which implies \([C : U^{+2}] = 2\). Thus \( k_m = 2^{\phi(m)/2} - 1 \), since \([U^+ : U^{+2}] = [U^+ : C][C : U^{+2}]\). □

This completes the proof of Theorem 1.3 (by applying Theorem 1.2).

**Example 1.** Let \( m = 5 \). Then \( h_1 = 1, \phi(5) = 4 \), and hence \( q_5 = 4 \). There are 4 classes of \( M_5 \) in \( SP_4(\mathbb{Z}) \). Here is a list of canonical matrices of \( M_5 \),

\[
X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 \\ 1 & 1 & -1 & 0 \end{pmatrix}, \quad X^2 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 \end{pmatrix},
\]

\[
X^3 = \begin{pmatrix} 0 & 0 & 1 & -1 \\ -1 & -1 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \end{pmatrix}, \quad X^4 = \begin{pmatrix} -1 & -1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 \end{pmatrix}.
\]

Similarly a list of canonical matrices of \( M_{10} \) in \( SP_4(\mathbb{Z}) \) is \(-X, -X^2, -X^3, -X^4\).

**Example 2.** Let \( m = 8 \). Then \( h_1 = 1, \phi(8) = 4 \), and hence \( q_8 = 4 \). There are four classes in \( M_8 \). A complete set of conjugacy classes of 8-torsion in \( SP_4(\mathbb{Z}) \) is

\[
I \circ J, \quad I \circ (-J), \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.
\]

**Example 3.** Let \( m = 12 \). Then \( h_1 = 1, \phi(12) = 4 \), and hence \( q_{12} = 2 \). There are two classes of \( X \in SP_4(\mathbb{Z}) \) with characteristic polynomial \( f(x) = x^4 - x^2 + 1 \). Two non-conjugacy matrices are \( C_f \) and \( C_f^{-1} \), where \( C_f \) is the companion matrix of \( f(x) \).

**References**