THE INTEGRAL SYMPLECTIC GROUPS AND THE EICHLER TRACE OF $\mathbb{Z}_P$ ACTIONS OF RIEMANN SURFACES

by

QINGJIE YANG

B.Sc. (Mathematics) Peking University, 1982
M.Sc. (Mathematics) Academia Sinica, 1985

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

THE FACULTY OF GRADUATE STUDIES

Department of Mathematics

We accept this thesis as conforming
to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

March 1997

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Mathematics
The University of British Columbia
Vancouver, Canada

Date April 15, 1997

Abstract

Every conformal automorphism on a compact connected Riemann surface S of genus g gives rise to a matrix A in the integral symplectic group $SP_{2g}(\mathbb{Z})$ by passing to the first homology group. If $g \geq 2$ then A has the same order as the automorphism. We consider the converse problem, namely which elements of finite order in $SP_{2g}(\mathbb{Z})$ are induced by some automorphism on some Riemann surface S of genus g? A related problem is the determination of the conjugacy classes of torsion in $SP_{2g}(\mathbb{Z})$. To explain one of our main results let $f(x) \in \mathbb{Z}[x]$ be an irreducible "palindromic" monic polynomial of degree $2g$, that is one satisfying $x^{2g}f(1/x) = f(x)$ and $f(0) = 1$, and let ζ be a fixed root of $f(x)$. Then there is a one-to-one correspondence between the conjugacy classes of integral symplectic matrices with characteristic polynomial $f(x)$ and the classes of certain pairs $(\mathfrak{a}, a)$, where $\mathfrak{a}$ is an ideal of $\mathbb{Z}[\zeta]$ and a is an element of $\mathbb{Z}[\zeta]$ satisfying certain conditions. In the special case where $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$, p is an odd prime, this result says that the number of conjugacy classes of elements of order p in $SP_{p-1}(\mathbb{Z})$ is $2^{(p-1)/2}h_1$, where h_1 is the first factor of the class number of the cyclotomic extension.

If $X \in SP_{2g}(\mathbb{Z})$ has a reducible characteristic polynomial of the form $f(x)g(x)$, where $f(x)$ and $g(x)$ are integral "palindromic" polynomials and coprime with coefficients in $\mathbb{Z}$, then we prove that X is conjugate to a matrix of the form $X_1 * X_2$, where the star operation is an analogue of orthogonal direct sum.

We determine completely those conjugacy classes of elements of order p in $SP_{p-1}(\mathbb{Z})$ which can be induced by some automorphism on a Riemann surface with genus $(p-1)/2$.

A complete list of the conjugacy classes of torsion in $SP_4(\mathbb{Z})$ is obtained. We give a complete set of realizable conjugacy classes in $SP_4(\mathbb{Z})$.

We also study the Eichler trace of $\mathbb{Z}_p$ actions on Riemann surfaces. If $\widehat{A}$ denotes the set of all Eichler traces of all possible actions modulo integers and $\widehat{B} = \{\chi \in \mathbb{Z}[\zeta] | \chi + \overline{\chi} \in \mathbb{Z}\}/\mathbb{Z}$, we prove that the index of $\widehat{A}$ in $\widehat{B}$ is h_1. There is group isomorphism between $\widehat{A}$ and Ω, the group

of equivariant cobordism classes of $\mathbb{Z}_p$ actions. Finally, we determine which dihedral subgroups of $GL_g(\mathbb{C})$ can be realized by an action on a Riemann surfaces of genus g.

Table of Contents

List of Figures

Acknowledgement

It gives me great pleasure to thank my supervisor Dr. Denis Sjerve. Throughout my research, he carefully and patiently directed every step. He spent countless hours discussing the problem with me, and made numerous constructive suggestions to keep me in progress.

I must also thank Professors K. Y. Lam and E. Luft for their valuable comments and advice. The financial support of UGF and Department of Mathematics is very much appreciated.

Finally, I thank my wife Grace for her support and encouragement. This work is respectfully dedicated to Grace Gao.

Chapter 1
Introduction

This thesis consists of two parts. The first part is the conjugacy classification of elements of the symplectic group over a principal ideal domain and the realizability of integer symplectic matrices by analytic automorphisms of compact connected Riemann surfaces. The second part is about the "Eichler trace" of group actions of $\mathbb{Z}_p$, the cyclic group of odd prime order p, and D_{2p}, the dihedral group of order $2p$, on compact connected Riemann surfaces.

1.1 Motivations

The first problem that we consider in this thesis is the determination of the conjugacy classes of matrices in the integral symplectic groups $SP_{2n}(\mathcal{D})$, where $\mathcal{D}$ is a principal ideal domain, with a given characteristic polynomial. 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 Siegel in [32] and in numerous other papers. But our original motivation for studying this problem came not from algebra but rather from Riemann surfaces.

Let S be a connected compact Riemann surface of genus g ($g \geq 2$) without boundary. Let $T \in \mathrm{Aut}(S)$, the group of analytic automorphisms of S. Then T induces an isomorphism of $H_1(S) = H_1(S, \mathbb{Z})$, the first homology group of S,

$$T_*: \; H_1(S) \to H_1(S).$$

Let $\{a, b\} = \{a_1, \ldots, a_g, b_1, \ldots, b_g\}$ be a canonical basis of $H_1(S)$, that is the intersection matrix for $\{a, b\}$ is

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

where I_g is the identity matrix of degree g. Let X be the matrix of T_* with respect to the basis $\{a, b\}$, i.e.

$$T_*(a_1, \ldots, a_g, b_1, \ldots, b_g) = (a_1, \ldots, a_g, b_1, \ldots, b_g)X.$$

Since T_* preserves intersection numbers, $X'JX = J$, where X' is the transpose of X. Hence $X \in SP_{2g}(\mathbb{Z})$, the symplectic group of genus g over $\mathbb{Z}$. If we fix a canonical basis of $H_1(S)$, there is a natural group monomorphism

$$\mathrm{Aut}\,(S) \to SP_{2g}(\mathbb{Z}),$$

see [13]. Clearly, the matrices of T_* with respect to different canonical basis are conjugate in $SP_{2g}(\mathbb{Z})$.

Definition 1.1. A matrix $X \in SP_{2g}(\mathbb{Z})$ is said to be realizable if there is $T \in \mathrm{Aut}\,(S)$ for some Riemann surface S such that X is the matrix of T_* with respect to some canonical basis of $H_1(S)$.

Two questions naturally arise.

1: Can every $X \in SP_{2g}(\mathbb{Z})$ be realized?

2: If the answer to Question 1 is no, which ones can be realized?

Note that $\mathrm{Aut}\,(S)$ is finite, so we only consider torsion elements of $SP_{2g}(\mathbb{Z})$. To answer these questions, we need some knowledge of the conjugacy classification of $SP_{2g}(\mathbb{Z})$.

For example, consider elements of order p, where p is odd prime. Any action of $\mathbb{Z}_p$ on S determines a representation $\rho : \mathbb{Z}_p \to GL_g(\mathbb{V})$, where $\mathbb{V}$ is the vector space of holomorphic differentials on S. If T is a preferred generator of $\mathbb{Z}_p$ then this representation yields a matrix $\rho(T) \in GL_g(\mathbb{C})$. The trace of this matrix, $\chi = \mathrm{tr}\,(T)$, is referred to as the Eichler trace. It is an element of the ring of integers $\mathbb{Z}[\zeta]$, where $\zeta = e^{\frac{2\pi i}{p}}$. Suppose there are t fixed points $P_1, \ldots, P_t$ of T. The fixed point data is described as a set of integers modulo p, $\{a_1, \ldots, a_t\}$, one for each fixed point P_j, such that T^{a_j} acts on the tangent space at P_j by counterclockwise rotation through $2\pi/p$. The Eichler Trace Formula then determines the Eichler trace of T as

$$\chi = 1 + \sum_{j=1}^{t} \frac{1}{\zeta^{k_j} - 1} \tag{1.1}$$

where the k_j are determined by the equations $k_j a_j \equiv 1 \pmod{p}$, $1 \leq j \leq t$. See [13] for a proof of this result.

Suppose we have two such automorphisms of order p,

$$T_1 : S_1 \to S_1, \quad T_2 : S_2 \to S_2,$$

where S_1 and S_2 have the same genus g. Let X_1, X_2 be the symplectic matrices induced by T_1, T_2 respectively. Then X_1 and X_2 are conjugate in $SP_{2g}(\mathbb{Z})$ if and only if their Eichler traces $\chi(T_1)$ and $\chi(T_2)$ are the same, see A. Edmonds & J. Ewing [5] and P. Symonds [35].

The Riemann-Hurwitz formula for an order p element $T \in \mathrm{Aut}\,(S)$ is

$$g = pg_0 + \tfrac{p-1}{2}(t-2) \tag{1.2}$$

where $g_0 = \mathrm{g}\,(S/T)$, the genus of S/T, and $t = \mathrm{Fix}\,(T)$, the number of fixed points of T. We shall show that $a_1 + \cdots + a_t \equiv 0 \pmod{p}$ is a necessary and sufficient condition that there be some T with order p and fixed point data $\{a_1, \ldots, a_t\}$. This implies there are only finitely many possibilities for the Eichler trace for fixed g. Therefore, there are only finitely many classes of order p matrices in $SP_{2g}(\mathbb{Z})$ which can be realized. The minimal polynomial of an element of order p is $x^{p-1} + x^{p-2} + \cdots + x + 1$, which is irreducible over integer ring $\mathbb{Z}$. Hence the minimum g such that there is a element of order p in $SP_{2g}(\mathbb{Z})$ is $g = \frac{p-1}{2} > 1$. We consider this special case, only $\frac{p^2-1}{6}$ classes of order p matrices in $SP_{p-1}(\mathbb{Z})$ can be realized. But we shall show that the number of conjugacy classes of order p matrices in $SP_{p-1}(\mathbb{Z})$ is $2^{\frac{p-1}{2}} h_1$, where h_1 is the first factor of the class number h of $\mathbb{Z}[\zeta]$. So in general most of the order p matrices in $SP_{p-1}(\mathbb{Z})$ is not realizable. Furthermore, we shall answer Question 2 for this case.

The second problem we consider is to determine how much information about the action of $\mathbb{Z}_p$ is captured by the Eichler trace. We want to answer the following two questions.

Question 3: What element $\chi \in \mathbb{Z}[\zeta]$ can be realized as the trace of some action?

Question 4: What is the relationship between two actions, not necessarily on the same surface, if they have the same trace?

The primary motivation for these two questions are the papers of J. Ewing ([6], [7]).

1.2 Main Results

In this section we will give main results of our thesis. All theorems in this section except for Theorem 8 and Theorem 9 are completely original. Proofs of the results in Theorem 8 and Theorem 9 have appeared previously (see [6], [7], [35]), but our approach is entirely new. To explain our results we need to develop some notation. Throughout this thesis $\mathcal{D}$ will be a principal ideal domain with characteristic not 2, that means $\mathcal{D}$ is a commutative ring without zero divisors, containing 1, in which every ideal is a principal ideal. Let $\mathcal{F}$ denote the quotient field of $\mathcal{D}$. Let $M_{n\times m}(\mathcal{D})$ be the set of $n\times m$ matrices over $\mathcal{D}$. For sake of simplicity we denote $M_{n\times m}(\mathcal{D})$ by $M_n(\mathcal{D})$ when $n = m$, and let I_n be the identity matrix in $M_n(\mathcal{D})$.

For $A \in M_{n_1}(\mathcal{D})$, $B \in M_{n_2}(\mathcal{D})$, we define the direct sum of A and B as

$$A \dot{+} B = \begin{pmatrix} A & \\ & B \end{pmatrix} \in M_{n_1+n_2}(\mathcal{D}). \tag{1.3}$$

Definition 1.2. The set of $2n\times 2n$ unimodular matrices X in $M_{2n}(\mathcal{D})$ such that

$$X'JX = J \tag{1.4}$$

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

Remark. The definition is meaningful and clearly $SP_{2n}(\mathcal{D})$ is a subgroup of $GL_{2n}(\mathcal{D})$, the general linear group with entries in $\mathcal{D}$. It is well known that every symplectic matrix in $SP_{2n}(\mathcal{D})$ has determinant one [1].

It is readily verified that X belongs to $SP_{2n}(\mathcal{D})$ if and only if X' belongs to $SP_{2n}(\mathcal{D})$. Let

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

where A, B, C, $D \in M_n(\mathcal{D})$. If $X \in SP_{2n}(\mathcal{D})$ the following conditions are satisfied:

$$AB' = BA', \quad CD' = DC' \quad \text{and} \quad AD' - BC' = I \tag{1.5}$$

as well as

$$A'B = B'A, \quad C'D = D'C \quad \text{and} \quad A'D - C'B = I. \tag{1.6}$$

Conversely, if one of (1.5) or (1.6) is true then $X \in SP_{2n}(\mathcal{D})$.

Given two matrices

$$X_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in M_{2n_1}(\mathcal{D}) \quad \text{and} \quad X_2 = \begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} \in M_{2n_2}(\mathcal{D}),$$

we define the symplectic direct sum of X_1 and X_2 by

$$X_1 * X_2 = \begin{pmatrix} A_1 & 0 & B_1 & 0 \\ 0 & A_2 & 0 & B_2 \\ C_1 & 0 & D_1 & 0 \\ 0 & C_2 & 0 & D_2 \end{pmatrix} \in M_{2(n_1+n_2)}(\mathcal{D}). \tag{1.7}$$

It is easy to check that $X_1 * X_2 \in SP_{2(n_1+n_2)}(\mathcal{D})$ if and only if $X_i \in SP_{2n_i}(\mathcal{D})$, for $i = 1, 2$.

Given two matrices

$$Y_1 = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} \in M_{2n_1 \times 2n_2}(\mathcal{D}) \quad \text{and} \quad Y_2 = \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix} \in M_{2n_2 \times 2n_1}(\mathcal{D})$$

where $C_{ij} \in M_{n_1 \times n_2}(\mathcal{D})$, $D_{ij} \in M_{n_2 \times n_1}(\mathcal{D})$, we define the quasi-direct sum by

$$Y_1 \circ Y_2 = \begin{pmatrix} 0 & C_{11} & 0 & C_{12} \\ D_{11} & 0 & D_{12} & 0 \\ 0 & C_{21} & 0 & C_{22} \\ D_{21} & 0 & D_{22} & 0 \end{pmatrix} \in M_{2(n_1+n_2)}(\mathcal{D}). \tag{1.8}$$

By an easy calculation we see that if $n_1 = n_2 = n$, then $Y_1 \circ Y_2 \in SP_{4n}(\mathcal{D})$ if and only if $Y_1, Y_2 \in SP_{2n}(\mathcal{D})$.

Definition 1.3. A matrix $X \in SP_{2n}(\mathcal{D})$ is said to be decomposable if it is conjugate to a symplectic direct sum of two symplectic matrices which have smaller genera; otherwise, X is said to be indecomposable. When n is even, X is said to be quasi-decomposable if it is conjugate to $X_1 \circ X_2$ for some $X_1, X_2 \in SP_n(\mathcal{D})$.

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

$$f_X(x) = |xI - X|.$$

If $X \in SP_{2n}(\mathcal{D})$, then $f_X(x)$ is "palindromic" and monic, that is

$$x^{2n} f(\tfrac{1}{x}) = f(x) \quad \text{and} \quad f(0) = 1. \tag{1.9}$$

This is because $X'JX = J$, $X' = JX^{-1}J^{-1}$,

$$\begin{aligned} f_X(x) &= |xI - X| \\ &= |xI - X'| \\ &= |xI - X^{-1}| \\ &= x^{2n}|X - \tfrac{1}{x}I||X^{-1}| \\ &= x^{2n} f_X(\tfrac{1}{x}) \end{aligned}$$

and $f(0) = \det(X) = 1$.

Definition 1.4. A polynomial $f(x)$ in $\mathcal{D}[x]$ of degree $2n$ ($n \geq 1$) is called an S-polynomial if it is a palindromic monic polynomial. An S-polynomial $f(x) \in \mathcal{D}[x]$ is said to be irreducible over $\mathcal{D}$, or is an irreducible S-polynomial in $\mathcal{D}[x]$, if it can not be expressed as the product of two S-polynomials (in $\mathcal{D}[x]$) of positive degree. Otherwise, $f(x)$ is termed reducible over $\mathcal{D}$. An S-polynomial of type-I is an irreducible S-polynomial which is also irreducible in the common sense, all other irreducible S-polynomials are said to be of type-II.

Given a separable S-polynomial $f(x)$ of degree $2n$, let M_f be the set of all symplectic matrices, whose characteristic polynomials are $f(x)$, over $\mathcal{D}$, that is

$$M_f = \{X \in SP_{2n}(\mathcal{D}) \mid f_X(x) = f(x)\}. \tag{1.10}$$

We use $\mathcal{M}_f$ to denote the set of the conjugacy classes of M_f in $SP_{2n}(\mathcal{D})$.

In Chapter 3 we deal with the case that $f(x)$ is a separable S-polynomial of type-I. Let ζ be a fixed root of $f(x)$. Then $1/\zeta$ is also a root of $f(x)$. Let $\mathcal{R} = \mathcal{D}[\zeta]$, $\mathcal{S} = \mathcal{F}[\zeta]$. Then $\mathcal{S}$ is the quotient field of $\mathcal{R}$. An ideal (fractional ideal) in $\mathcal{S}$ is a finitely generated $\mathcal{R}$-submodule of $\mathcal{S}$ which is a free $\mathcal{D}$-module of rank $2n$. An integral ideal is an ideal which is contained in $\mathcal{R}$.

Two ideals $\mathfrak{a}$, $\mathfrak{b}$ are equivalent if there are non-zero elements $\lambda, \mu \in \mathcal{R}$ such that $\lambda\mathfrak{a} = \mu\mathfrak{b}$. We denote the equivalence class of $\mathfrak{a}$ by $[\mathfrak{a}]$ and let $\mathcal{C}$ denote the collection of equivalence classes of ideals. $\mathcal{C}$ is an commutative monoid with respect to multiplication of ideals. The identity is $[\mathcal{R}]$.

Let P_f be the set of pairs $(\mathfrak{a}, a)$ consisting of an integral ideal $\mathfrak{a}$ and an element $a \in \mathcal{R}$ such that $\widetilde{\mathfrak{a}} = a\Delta\mathfrak{a}'$ and $a = \widetilde{a}$, where the tilde denotes that conjugate such that $\widetilde{\zeta} = \frac{1}{\zeta}$, $\widetilde{\mathfrak{a}} = \{\alpha \mid \alpha \in \mathfrak{a}\}$, $\Delta = \zeta^{1-n}f'(\zeta)$ and $\mathfrak{a}'$ is the complementary ideal. Two such pairs $(\mathfrak{a}, a)$ and $(\mathfrak{b}, b)$ are said to be equivalent if there are non-zero elements $\lambda, \mu \in \mathcal{R}$ such that $\lambda\mathfrak{a} = \mu\mathfrak{b}$ and $\lambda\widetilde{\lambda}a = \mu\widetilde{\mu}b$. We denote by $\langle\mathfrak{a}, a\rangle$ the equivalence class of $(\mathfrak{a}, a)$. Let $\mathcal{P}_f$ denote the set of all classes of P_f.

Suppose $X \in M_f$. There is an eigenvector $\alpha = (\alpha_1, \ldots, \alpha_{2n})' \in \mathcal{R}^{2n}$ corresponding to ζ, that is $X\zeta = \zeta\alpha$. Let $\mathfrak{a}$ be the $\mathcal{D}$-module generated by $\alpha_1, \ldots, \alpha_{2n}$, and let $a = \Delta^{-1}\alpha' J\widetilde{\alpha}$. It is easy to check that $\mathfrak{a}$ is an integral ideal in $\mathcal{R}$ and $a = \widetilde{a}$. Furthermore we will prove that $(\mathfrak{a}, a) \in P$ and that the correspondence $\Psi : \mathcal{M}_f \to \mathcal{P}_f$, $\langle X \rangle \to \langle \mathfrak{a}, a \rangle$, is well defined (cf. Section 3.3).

Theorem 1. *Ψ is bijection.*

Theorem 2. *If $f(x)$ is a separable S-polynomial, then $M_f \neq \emptyset$.*

If $\mathcal{R}$ is integrally closed, then $\mathcal{C}$ is an abelian group. Also we have that

$$P_f = \{(\mathfrak{a}, a) \mid \mathfrak{a}\widetilde{\mathfrak{a}} = (a) \text{ and } a = \widetilde{a}\}$$

and $\mathcal{P}$ turns out to be an abelian group where multiplication is given by $\langle \mathfrak{a}, a \rangle \langle \mathfrak{b}, b \rangle = \langle \mathfrak{a}\mathfrak{b}, ab \rangle$ (cf. Section 3.4). Let $\mathcal{C}_0$ denote the subgroup of integral ideal classes defined by

$$\mathcal{C}_0 = \left\{ \mathfrak{a} \in \mathcal{C} \mid \mathfrak{a}\widetilde{\mathfrak{a}} = (a), a = \widetilde{a} \text{ for some } a \in \mathcal{R} \right\} \tag{1.11}$$

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

Theorem 3. *There is a natural short exact sequence*

$$1 \to U^+/C \xrightarrow{\phi} \mathcal{P}_f \xrightarrow{\psi} \mathcal{C}_0 \to 1 \tag{1.12}$$

where $\phi([u]) = \langle \mathcal{D}[\zeta], u \rangle$ and $\psi(\langle \mathfrak{a}, a \rangle) = [\mathfrak{a}]$.

Consequently, for the special case $\mathcal{D} = \mathbb{Z}$, we shall show

Theorem 4. *Let q_m be the number of elements in $\mathcal{M}_f$, where $f(x)$ is the m-th cyclotomic polynomial. Then*

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

where $\phi(m)$ is the Euler totient function.

If m is an odd prime p, then $\phi(p) = p - 1$. Hence we have

Corollary 1.1. *The number of conjugacy classes of order p elements in $SP_{p-1}(\mathbb{Z})$ is $2^{\frac{p-1}{2}} h_1$.*

In Chapter 4 we introduce symplectic spaces and symplectic group spaces. Let V be a symplectic space of rank $2n$. In Section 4.1 we define (l,k)-normal sets of V and prove

Theorem 5. *Let the $l+k$ elements $\alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_k$ be an (l,k)-normal set of V. Then there are $2n - l - k$ elements $\alpha_{l+1}, \ldots, \alpha_n, \beta_{k+1}, \ldots, \beta_n$ in V such that*

$$\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$$

is a symplectic basis of V.

We relate symplectic matrices to symplectic transformations, and shall give a necessary and sufficient condition for decomposition. Let $f(x)$ be a reducible S-polynomial in $\mathcal{D}[x]$,

$$f(x) = p_1(x) \cdots p_m(x),$$

where $p_1(x), \ldots, p_m \in \mathcal{D}[x]$ are mutually coprime S-polynomials. Then there are m polynomials $u_1(x), \ldots, u_m(x) \in \mathcal{F}[x]$ such that

$$u_1(x)q_1(x) + \cdots + u_m(x)q_m(x) = 1,$$

where $q_i(x) = f(x)/p_i(x)$, for $i = 1, \ldots, m$. We shall show

Theorem 6. *Let $X \in M_f$. Then $X \sim X_1 * \cdots * X_m$, for some $X_i \in M_{p_i}$, $i = 1, \ldots, m$, if and only if $u_i(X)q_i(X) \in M_{2n}(\mathcal{D})$, for $i = 1, \ldots, m$.*

To every S-pair $(\mathfrak{a}, a)$, defined in Section 3.2, we shall assign a symplectic structure and a G_m action on $\mathfrak{a}$, where G_m is the cyclic group on a fixed generator g of order m (cf. Section 4.3). Therefore $\mathfrak{a}$ becomes a symplectic G_m-space, denoted by $[\mathfrak{a}, a]$.

Theorem 7. *Two symplectic direct sums $[\mathfrak{a}_1, a_1] * \cdots * [\mathfrak{a}_r, a_r]$ and $[\mathfrak{b}_1, b_1] * \cdots * [\mathfrak{b}_s, b_s]$ are isomorphic as symplectic G_m-spaces if and only if $r = s$, and there is an $r \times r$ invertible matrix*

$Q = (q_{ij})$, $q_{ij} \in \mathcal{F}[\zeta]$, *satisfying the conditions* $q_{ij}\mathfrak{a}_j \subset \mathfrak{b}_i$ *(for* $i, j = 1, \ldots, r$*) and*

$$\begin{pmatrix} \frac{1}{a_1} & & \\ & \ddots & \\ & & \frac{1}{a_r} \end{pmatrix} = Q' \begin{pmatrix} \frac{1}{b_1} & & \\ & \ddots & \\ & & \frac{1}{b_s} \end{pmatrix} \widetilde{Q}, \tag{1.13}$$

where $\widetilde{Q} = (\widetilde{q}_{ij})$.

In Chapter 5 we consider order p matrices in $SP_{p-1}(\mathbb{Z})$. The proof of Theorem 1 gives us a way to find symplectic matrices of order p. First in this section we find a symplectic matrix X of order p such that $\Psi(X) = \langle \mathbb{Z}[\zeta], 1\rangle$, where $\zeta = e^{\frac{2\pi i}{p}}$. Then we give a complete answer to Question 2 for order p elements in $SP_{p-1}(\mathbb{Z})$. Let

$$u_k = \frac{\sin \frac{k\pi}{p}}{\sin \frac{\pi}{p}}, \quad \text{for } (k, p) = 1, \tag{1.14}$$

be the cyclotomic units of $\mathbb{Z}[\zeta]$. By the Riemann-Hurwitz formula, an automorphism $T : S \to S$ of order p, where S has genus $\frac{p-1}{2}$, has exactly 3 fixed points. Let the fixed point data of T be $\{a, b, c\}$, where $1 \le a, b, c \le p-1$, and $a + b + c \equiv 0 \pmod{p}$. We use $M(a, b, c)$ to denote the symplectic matrix represented by T_*.

Theorem 8. $\Psi(M(a, b, c)) = \langle \mathbb{Z}[\zeta], u_a u_b u_{a+b}\rangle$

This is similar to a result of P. Symonds[35] which was proved by using the G-signature. But we use an entirely different method to approach it.

Corollary 1.2. *Let* $X \in SP_{p-1}(\mathbb{Z})$ *be of order* p*. Then* X *is realizable if and only if*

$$\Psi(X) = \langle \mathbb{Z}[\zeta], u_a u_b u_{a+b}\rangle.$$

for some integers a*,* b *with* $1 \le a, b \le p-1$ *and* $a + b \ne p$*.*

In Chapter 6 we shall give a complete set of conjugacy classes of torsion in $SP_4(\mathbb{Z})$. In addition, a list of realizable classes in $SP_4(\mathbb{Z})$ is obtained.

In Chapter 7 we shall answer Questions 3 and 4. Let A denote the set of all Eichler traces of all possible actions, that is

$$A = \left\{ \chi \in \mathbb{Z}[\zeta] \;\middle|\; \chi = \mathrm{tr}\,(T) \right\} \tag{1.15}$$

where T is any automorphism of order p on any compact connected Riemann surface S. A simple calculation with the Eichler Trace Formula (1.1) shows that $\chi + \bar{\chi} = 2 - t$ for any $\chi \in A$, where $\bar{\chi}$ denotes the complex conjugate of χ. Thus $A \subset B$, where

$$B = \left\{ \chi \in \mathbb{Z}[\zeta] \;\middle|\; \chi + \bar{\chi} \in \mathbb{Z} \right\}. \tag{1.16}$$

In Section 7.1 we shall show that B is a free abelian subgroup of $\mathbb{Z}[\zeta]$ of rank $(p+1)/2$ and determine a basis. Thus a reasonable first step in describing A is to determine the "index" of A in B. Unfortunately, it turns out that A is not a subgroup of B, so this does not make sense. On the other hand, the quotient set $\widehat{A} = A/\mathbb{Z}$, that is the elements of A modulo the integers, is a group, in fact a subgroup of $\widehat{B} = B/\mathbb{Z}$. We prove that $\widehat{B}$ is a free abelian group of rank $(p-1)/2$ and that the index of $\widehat{A}$ in $\widehat{B}$ is finite.

Theorem 9. *The index of $\widehat{A}$ in $\widehat{B}$ is h_1.*

This theorem has appeared previously, see the two papers [6] and [7] of J. Ewing. The first paper is quite technical. It contains Theorem 9, but stated in terms of Witt classes and G-signatures. The second paper is an elegant exposition of the first. Theorem 9 gives a partial answer to Question 3. We shall find free generators of $\widehat{A}$, thereby answering completely Question 3. See Theorem 11.

To an automorphism $T \colon S \to S$ of order p we associate a "vector" $[g; k_1, \dots, k_t]$, where g is the genus of the orbit surface $S/\mathbb{Z}_p$, t is the number of fixed points, and the k_j are the rotation numbers. The rotation numbers are unique modulo p, but their order is not determined. From the Eichler Trace Formula (1.1) it is clear that $\chi = \mathrm{tr}\,(T)$ does not depend on g or on the order of the k_j. If a cancelling pair $\{k, p-k\}$, where $1 \leq k \leq p-1$, appears amongst the set of rotation numbers $\{k_1, \cdots, k_t\}$, then an easy calculation shows that their contribution to the

Eichler trace is

$$\frac{1}{\zeta^k - 1} + \frac{1}{\zeta^{p-k} - 1} = -1.$$

Thus we can replace the cancelling pair $\{k, p-k\}$ by any other cancelling pair $\{l, p-l\}$ and not change the Eichler trace.

Given two such automorphisms

$$T_1 \colon S_1 \to S_1, \; T_2 \colon S_2 \to S_2$$

we have two "vectors" $[g; k_1, \dots, k_t]$, $[h; l_1, \dots, l_u]$. Let χ_1 and χ_2 denote the respective Eichler traces.

Theorem 10. *$\chi_1 = \chi_2$ if, and only if, $t = u$ and the set of rotation numbers $\{k_1, \dots, k_t\}$ agrees with $\{l_1, \dots, l_u\}$ up to permutations and replacements of cancelling pairs.*

Theorem 11. *$\widehat{A}$ is a free abelian group of rank $(p-1)/2$. It is freely generated by the mod $\mathbb{Z}$ representatives of the $(p-1)/2$ elements:*

$$\chi_{r,s} = \frac{1}{\zeta - 1} + \frac{1}{\zeta^r - 1} + \frac{1}{\zeta^s - 1}, \text{ where } 1 \le r \le s \le p-1 \text{ and } 1 + r + s \equiv 0 \pmod{p}.$$

We shall give some geometric content to these theorems by relating equivariant cobordism of $\mathbb{Z}_p$ actions on compact connected Riemann surfaces to $\widehat{A}$. To explain this let Ω denote the group of equivariant cobordism classes of $\mathbb{Z}_p$ actions. We show that the Eichler trace induces a natural group homomorphism $\phi : \widehat{A} \to \Omega$.

Theorem 12. *$\phi : \widehat{A} \to \Omega$ is a group isomorphism.*

Finally, in Section 7.3 we study the realizability problem for dihedral groups in $GL_g(\mathbb{C})$. This is a special case of a general problem. A group G of analytic automorphisms of a Riemann surface S of genus $g > 1$ can be represented as a subgroup $R(S, G)$ of $GL_g(\mathbb{C})$ by passing to the induced action on the vector space $\mathbb{V}$ of holomorphic differentials. The problem is to determine those subgroups of $GL_g(\mathbb{C})$ which are conjugate to $R(S, G)$ for some S and some G. In 1983, I. Kuribayashi proved that an element A of prime order in $GL_g(\mathbb{C})$ is realizable if and only if A satisfies the "Eichler trace formula" [14]. In 1986 and 1990, I. Kuribayashi and A. Kuribayashi determined all realizable subgroups of $GL_g(\mathbb{C})$ for $g \leq 5$ (see [15], [16], [17] and [18]). We consider the dihedral group D_{2p}. Let D_{2p} be a subgroup of $GL_g(\mathbb{C})$, and let A and B be generators with orders p and 2 respectively. D_{2p} is called an IR-group if $\mathrm{tr}(A)$, $\mathrm{tr}(B)$ are integers ≤ 1. If D_{2p} is an IR-group for some choice of A, B then it is an IR-group for all choices. We shall prove

Theorem 13. *D_{2p} is realizable if and only if it is an IR-group.*

Chapter 2
Preliminaries

In this chapter we collect some of the preliminaries needed for later chapters.

2.1 Direct Sum of Symplectic Matrices

First we state some properties of symplectic direct sum and quasi-direct sum,

$$(X_1 * X_2)' = X_1' * X_2', \tag{2.1}$$

$$(Y_1 \circ Y_2)' = Y_2' \circ Y_1', \tag{2.2}$$

$$(X_1 * X_2)(Y_1 \circ Y_2) = (X_1Y_1) \circ (X_2Y_2), \tag{2.3}$$

$$(X_1 \circ X_2)(Y_1 * Y_2) = (X_1Y_2) \circ (X_2Y_1), \tag{2.4}$$

$$(X_1 * X_2)(Y_1 * Y_2) = (X_1Y_1) * (X_2Y_2), \tag{2.5}$$

$$(X_1 \circ X_2)(Y_1 \circ Y_2) = (X_1Y_2) * (X_2Y_1). \tag{2.6}$$

We assume that all matrix multiplications are suitable.

Lemma 2.1. *Let X_1, X_2, X_3, Y_1, Y_2 be symplectic matrices. Then*

1. $X_1 * X_2 \sim X_2 * X_1$.

2. $(X_1 * X_2) * X_3 = X_1 * (X_2 * X_3)$.

3. *If $X_1 \sim Y_1$ and $X_2 \sim Y_2$, then $X_1 * X_2 \sim Y_1 * Y_2$.*

   In the following we assume X_1 and X_2 have the same genus

4. $X_1 \circ X_2 \sim X_2 \circ X_1$.

5. $X_1 \circ X_2 \sim (-X_1) \circ (-X_2)$.

6. *If* $X_1 \sim X_2$, *then* $I \circ X_1 \sim I \circ X_2$.

Proof. (2) and (3) are easy. To prove (1) we let $Q = I_{2n_1} \circ I_{2n_2} \in SP_{2(n_1+n_2)}(\mathbb{Z})$, where n_i is the genus of X_i, $i = 1, 2$. Then $Q^{-1}(X_1 * X_2)Q = X_2 * X_1$. Similarly we prove (4) by using $Q = I \circ I$, (5) by using $Q = I*(-I)$. For (6), if $X_2 = Q^{-1}X_1Q$, then $(Q^{-1}*Q^{-1})(I \circ X_1)(Q*Q) = I \circ X_2$. $\square$

In general the converse of (3) in Lemma 2.1 is not true, but we have

Lemma 2.2. *Suppose* X_1, X_2, Y_1 *and* Y_2 *are symplectic matrices,* $f_{X_i}(x) = f_{Y_i}(x) = f_i(x)$, *for* $i = 1, 2$. *Suppose* $f_1(x)$ *and* $f_2(x)$ *are coprime. Then* $X_1 * X_2 \sim Y_1 * Y_2$ *if and only if* $X_1 \sim Y_1$ *and* $X_2 \sim Y_2$.

Proof. The sufficiency part has been proved. We consider the necessity.

Note that any $P \in M_{2(n_1+n_2)}(\mathcal{D})$ can be expressed in the form

$$P = P_1 * P_2 + P_3 \circ P_4,$$

where $P_1 \in M_{2n_1}(\mathcal{D})$, $P_2 \in M_{2n_2}(\mathcal{D})$, $P_3 \in M_{2n_1 \times 2n_2}(\mathcal{D})$, and $P_4 \in M_{2n_2 \times 2n_1}(\mathcal{D})$ are blocks of P. Let P be a symplectic matrix such that $(X_1 * X_2)P = P(Y_1 * Y_2)$. We obtain $X_1P_1 = P_1Y_1$, $X_2P_2 = P_2Y_2$, $X_1P_3 = P_3Y_2$ and $X_2P_4 = P_4Y_2$. Then $f_2(X_1)P_3 = P_3f_2(Y_1) = 0$, which yields $P_3 = 0$ since $f_2(X_1)$ is invertible. Similarly, we get $P_4 = 0$. Hence P_1, P_2 are symplectic, therefore $X_1 \sim Y_1$ and $X_2 \sim Y_2$. $\square$

2.2 S-Polynomials

Before we prove the following lemmas we make a Remark.

Remark. Let $f(x) = g(x)h(x)$, where $f(x), g(x)$ and $h(x)$ are polynomials over $\mathcal{D}$. Then if two of them are S-polynomials so is the third.

Lemma 2.3. *Suppose that* $p(x)$ *is an irreducible monic polynomial of degree* n.

1 If $x^n p(\frac{1}{x}) = p(x)$, then $p(x)$ is S-polynomial of type-I or $p(x) = x + 1$.

2 If $x^n p(\frac{1}{x}) = -p(x)$, then $p(x) = x - 1$.

Proof. (1) If n is even then $p(x)$ is an S-polynomial of type-I. Assume n be odd. Then $p(-1) = 0$, so $x + 1$ is a factor of $p(x)$; but $p(x)$ is irreducible, hence $p(x) = x + 1$.

(2) Similar to the proof of (1) since $p(1) = 0$. □

Lemma 2.4. *Let $f(x)$ be an S-polynomial and assume $f(\pm 1) = 0$. Then*

$$f(x) = (x \mp 1)^2 g(x)$$

where $g(x)$ is also a S-polynomial.

Proof. Differentiate both sides of $x^{2n} f(\frac{1}{x}) = f(x)$ to see that

$$2nx^{2n-1} f(\tfrac{1}{x}) - x^{2n-2} f'(\tfrac{1}{x}) = f'(x). \tag{2.7}$$

But $f(\pm 1) = 0$, hence $f'(\pm 1) = 0$, $f(x) = (x \mp 1)^2 g(x)$. It is obvious that $g(x)$ is an S-polynomial by the above Remark. □

Lemma 2.5. *Suppose $f(x)$ is an S-polynomial of type-II of degree $2n$. Then*

$$f(x) = p(0) x^n p(x) p(\frac{1}{x})$$

where $p(x)$ is an irreducible monic polynomial with degree n.

Proof. We will prove this by using the Unique Factorization Theorem.

If $f(\pm 1) = 0$ then $f(x) = (x \mp 1)^2$, by Lemma 2.4. We can choose $p(x) = x \mp 1$.

Now we consider the case $f(1) \neq 0$ and $f(-1) \neq 0$. Suppose that $f(x) = p_1(x) \cdots p_m(x)$, where $p_1(x), \ldots, p_m(x)$ are irreducible monic polynomials of positive degrees $n_1, \ldots, n_m$. By the

Remark, none of $p_1(x)\dots p_m(x)$ is an S-polynomial since $f(x)$ is an irreducible S-polynomial. Since $f(x)$ is an S-polynomial,

$$f(x) = x^{2n} f(\tfrac{1}{x}) = x^{n_1} p_1(\tfrac{1}{x}) \cdots x^{n_m} p_m(\tfrac{1}{x}).$$

Note that $x^{n_1} p_1(\frac{1}{x})$ is an irreducible polynomial, and neither $x+1$ nor $x-1$ are factors of $f(x)$. There is $k \neq 1$, say $k = 2$, such that $x^{n_1} p_1(\frac{1}{x}) = p_1(0) p_2(x)$. It is easy to verify that $p_1(x)p_2(x)$ is an S-polynomial, and therefore $f(x) = p_1(x)p_2(x)$. Let $p(x) = p_1(x)$. Then $p_2(x) = p(0) x^n p(\frac{1}{x})$, and $f(x) = p(0) x^n p(\frac{1}{x}) p(x)$. □

Proposition 2.1. *Every S-polynomial $f(x)$ is a product of irreducible S-polynomials. Apart from the order of the factors, this factorization is unique.*

Proof. Without loss of generality we assume that neither $x+1$ nor $x-1$ are factors of $f(x)$, because of Lemma 2.4. We know that $f(x)$ can be written as a product of irreducible monic polynomials,

$$f(x) = p_1(x)p_2(x)\cdots p_k(x) q_1(x) q_2(x) \cdots q_l(x)$$

where the $p_i(x)$ $(i = 1,\dots,k)$ are S-polynomials of degree $2r_i$ and $q_j(x)$ $(j = 1,\dots,l)$ are of degree s_j. Then

$$\begin{aligned} x^n f(\tfrac{1}{x}) &= x^{2r_1} p_1(\tfrac{1}{x}) x^{2r_2} p_2(\tfrac{1}{x}) \cdots x^{2r_k} p_k(\tfrac{1}{x}) x^{s_1} q_1(\tfrac{1}{x}) x^{s_2} q_2(\tfrac{1}{x}) \cdots x^{s_l} q_l(\tfrac{1}{x}) \\ &= p_1(x)p_2(x)\cdots p_k(x) x^{s_1} q_1(\tfrac{1}{x}) x^{s_2} q_2(\tfrac{1}{x}) \cdots x^{s_l} q_l(\tfrac{1}{x}) \end{aligned}$$

So we have

$$q_1(x)q_2(x)\cdots q_l(x) = x^{s_1} q_1(\tfrac{1}{x}) x^{s_2} q_2(\tfrac{1}{x}) \cdots x^{s_n} q_l(\tfrac{1}{x})$$

Note that $x^{s_j} q_j(\frac{1}{x})$ $(j = 1,\dots,l)$ are irreducible polynomials. Then for each $x^{s_j} q_j(\frac{1}{x})$, there is $l_j \neq j$ such that $x^{s_j} q_j(\frac{1}{x}) = q_j(0) q_{l_j}(x)$. It is easy to check that $q_j(0) q_j(x) x^{s_j} q_j(\frac{1}{x})$ is an irreducible S-polynomial. By rearranging the order of $q_j(x)$ we get

$$f(x) = p_1(x)p_2(x)\cdots p_k(x)\ q_1(0) q_1(x) x^{s_1} q_1(\tfrac{1}{x})\ \cdots\ q_m(0) q_m(x) x^{s_m} q_m(\tfrac{1}{x})$$

The second part is simple. □

2.3 Strictly Coprime Polynomials

We consider two polynomials

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \\ g(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0, \end{aligned}$$

in $\mathcal{D}[x]$. Assume $m > 0$, $n > 0$, and $a_n \neq 0$, $b_m \neq 0$.

Definition 2.1. $f(x)$ and $g(x)$ are said to be strictly coprime over $\mathcal{D}$ if there are polynomials $u(x)$ and $v(x)$ in $\mathcal{D}[x]$ such that

$$u(x)f(x) + v(x)g(x) = 1 \tag{2.8}$$

Example. Let $p_n(x) = x^{n-1} + x^{n-2} + \cdots + 1$. Then $p_m(x)$, $p_n(x)$ are strictly coprime over $\mathbb{Z}$ if and only if m, n are coprime. And $p_m(x)$ and $p_n(x)$ have a common factor of positive degree in $\mathbb{Z}[x]$ if and only if m, n have common factor great than 1.

Recall that the resultant of $f(x)$ and $g(x)$ is

$$\operatorname{Res}(f,g) = \det \begin{pmatrix} a_n & a_{n-1} & \cdot & \cdot & \cdot & a_0 & 0 & \cdot & \cdots & \cdot \\ 0 & a_n & a_{n-1} & \cdot & \cdot & \cdot & a_0 & 0 & \cdots & \cdot \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdot & \cdot & 0 & a_n & a_{n-1} & \cdot & \cdot & \cdot & \cdots & a_0 \\ b_m & b_{m-1} & \cdot & \cdot & b_0 & 0 & \cdot & \cdot & \cdots & \cdot \\ 0 & b_m & b_{m-1} & \cdot & \cdot & b_0 & 0 & \cdot & \cdots & \cdot \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdot & \cdot & \cdot & 0 & b_m & b_{m-1} & \cdot & \cdot & \cdots & b_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} n \text{ rows} \end{matrix} \tag{2.9}$$

The result we want to establish is

Proposition 2.2. *Suppose either $f(x)$ or $g(x)$ is monic, that is either $a_n = 1$ or $b_m = 1$. Then $f(x)$ and $g(x)$ are strictly coprime if, and only if $\operatorname{Res}(f,g)$ is a unit in $\mathcal{D}$.*

Proof. Without loss of generality, let $a_n = 1$. If $f(x)$ and $g(x)$ are strictly coprime, then $x^k u(x)f(x) + x^k v(x)g(x) = x^k$ for any $0 \le k \le m+n-1$. Any $x^k v(x)$ can be written as $x^k v(x) = q_k(x)f(x) + v_k(x)$, where $q_k(x), v_k(x) \in \mathcal{D}[x]$, and $v_k(x)$ has degree less than n or $v_k(x) = 0$. We set $u_k(x) = x^k u(x) + q_k(x)g(x) \in \mathcal{D}[x]$, then

$$u_k(x)f(x) + v_k(x)g(x) = x^k \tag{2.10}$$

and $u_k(x)$ has degree less than m or $u_k(x) = 0$. We may write

$$\begin{aligned} u_k(x) &= c_{m-1}^{(k)} x^{m-1} + c_{m-2}^{(k)} x^{m-2} + \cdots + c_0^{(k)}, \\ v_k(x) &= d_{n-1}^{(k)} x^{n-1} + d_{n-2}^{(k)} x^{n-2} + \cdots + d_0^{(k)}. \end{aligned}$$

If we equate the coefficients of x^{m+n-1}, x^{m+n-2}, ..., 1 in Equations (2.10), we obtain the following equations:

$$\sum_{\substack{i+j=l \\ 0\le i\le n \\ 0\le j\le m-1}} a_i c_j^{(k)} + \sum_{\substack{i+j=l \\ 0\le i\le m \\ 0\le j\le n-1}} b_i d_j^{(k)} = \begin{cases} 1, & l = k, \\ 0, & l \ne k. \end{cases} \tag{2.11}$$

Considering this as a system of $m+n$ linear equations in the $c^{(k)}$'s and $d^{(k)}$'s, taken in the order $c_{m-1}^{(k)}, \cdots, c_0^{(k)}, d_{n-1}^{(k)}, \cdots, d_0^{(k)}$, we see that $D \cdot \operatorname{Res}(f,g) = 1$, where the D is the determinant

$$D = \det \begin{pmatrix} c_{m-1}^{(m+n-1)} & \cdots & c_0^{(m+n-1)} & d_{n-1}^{(m+n-1)} & \cdots & d_0^{(m+n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{m-1}^{(1)} & \cdots & c_0^{(1)} & d_{n-1}^{(1)} & \cdots & d_0^{(1)} \\ c_{m-1}^{(0)} & \cdots & c_0^{(0)} & d_{n-1}^{(0)} & \cdots & d_0^{(0)} \end{pmatrix}.$$

Since $D \in \mathcal{D}$, $\operatorname{Res}(f,g)$ is a unit.

Conversely, assume $\operatorname{Res}(f,g)$ is a unit in $\mathcal{D}$. Then we can retrace the steps through (2.11) and (2.10) for $k = 0$ and conclude that there exist integral polynomials $u_0(x)$, $v_0(x)$ such that $u_0(x)f(x) + v_0(x)g(x) = 1$. □

Remark. It is well known that $f(x)$, $g(x)$ have a common factor if and only if the $\operatorname{Res}(f,g) = 0$.

We apply Proposition 2.2 to $L_{m,n}$, the $(m+n-2)\times(m+n-2)$ matrix defined by

$$m\left\{\begin{pmatrix} 1 & & & 1 & & & \\ 1 & \ddots & & \vdots & \ddots & & \\ \vdots & \ddots & 1 & 1 & \ddots & \ddots & \\ \vdots & \ddots & 1 & 1 & \ddots & \ddots & 1 \\ 1 & \ddots & \vdots & & \ddots & \ddots & \vdots \\ & \ddots & \vdots & & & \ddots & 1 \\ & & 1 & & & & 1 \end{pmatrix}\right\}n \tag{2.12}$$

where the entries are given by

$$l_{ij}=\begin{cases} 1, & j\le i\le j+m-1, 1\le j\le n-1 \text{ or } j-n+1\le i\le j, n\le j\le m+n-2,\\ 0, & \text{otherwise.}\end{cases}$$

It is easy to see that

$$\det(L_{m,n})=\operatorname{Res}(p_m,p_n)=\begin{cases}\pm 1, & (m,n)=1,\\ 0, & (m,n)\neq 1.\end{cases} \tag{2.13}$$

2.4 Group Actions on Riemann Surfaces

Throughout the thesis all Riemann surfaces S will be connected, orientable and without boundary. By the uniformization theorem the universal covering space $\mathbb{U}$ of S is one of three possibilities: the extended complex plane $\widehat{\mathbb{C}}$, the complex plane $\mathbb{C}$, or the upper half plane $\mathbb{H}$. The letter $\mathbb{U}$ will always denote one of these three.

If G is a finite group acting topologically on a surface S by orientation preserving homeomorphisms then the positive solution of the Nielsen Realization Problem guarantees that there exists a complex analytic structure on S for which the action of G is by analytic automorphisms (see [27], [11], [9] or [25]). Thus there is no loss of generality in assuming that the action of G is complex analytic to begin with, and we will tacitly do so.

The orbit space $\bar{S} = S/G$ of the action of G is also a Riemann surface and the orbit map $\pi : S \to \bar{S}$ is a branched covering, with all branching occurring at fixed points of the action. If $x \in \bar{S}$ is a branch point then each point in $\pi^{-1}(x)$ has a non-trivial stabilizer subgroup in G.

To any action of G on S we associate a short exact sequence of groups

$$1 \to \Pi \to \Gamma \xrightarrow{\theta} G \to 1, \tag{2.14}$$

with Γ being a discrete subgroup of $\mathrm{Aut}\,(\mathbb{U})$ and Π a torsion free normal subgroup of Γ, as follows. Let $\pi : \mathbb{U} \to S$ denote the covering map. Then Γ is defined by

$$\Gamma = \big\{\gamma \in \mathrm{Aut}\,(\mathbb{U}) \bigm| \pi \circ \gamma = g \circ \pi,\ g \in G\big\}. \tag{2.15}$$

In other words Γ consists of all lifts $\gamma \colon \mathbb{U} \to \mathbb{U}$ of all automorphisms $g \colon S \to S$, $g \in G$. The subgroup Γ is unique up to conjugation in $\mathrm{Aut}\,(\mathbb{U})$. See the commutative diagram below.

$$\begin{array}{ccc} \mathbb{U} & \xrightarrow{\gamma} & \mathbb{U} \\ \big\downarrow & & \big\downarrow \\ S & \xrightarrow{g} & S \end{array}$$

The epimorphism $\theta \colon \Gamma \to G$ is defined by $\theta(\gamma) = g$, where γ and g are as in (2.15). The kernel of $\theta \colon \Gamma \to G$ is Π, the fundamental group of S, and is therefore torsion free. The Riemann surface $S = \mathbb{U}/\Pi$ and the action of G on $\mathbb{U}/\Pi$ is given by $g[z]_\Pi = [\gamma(z)]_\Pi$, where $z \in \mathbb{U}$, $g \in G$, and $\gamma \in \Gamma$ is any element such that $\theta(\gamma) = g$. Here the square brackets denote the orbits under the action of Π. The orbit surface $\bar{S} = \mathbb{U}/\Gamma$, and the branched covering $\pi \colon S \to \bar{S}$ is just the natural map $\mathbb{U}/\Pi \to \mathbb{U}/\Gamma$, $[z]_\Pi \mapsto [z]_\Gamma$.

Conversely, suppose $1 \to \Pi \to \Gamma \xrightarrow{\theta} G \to 1$ is a given short exact sequence of groups, where Γ is a discrete subgroup of $\mathrm{Aut}\,(\mathbb{U})$ and Π is torsion free. Then this short exact sequence corresponds to the one arising from the action of G on the Riemann surface $S = \mathbb{U}/\Pi$ defined above.

Thus there is a one-to-one correspondence between analytic conjugacy classes of analytic actions by the finite group G on compact connected Riemann surfaces and short exact sequences

(2.14), where Γ is a discrete subgroup of $\mathrm{Aut}\,(\mathbb{U})$, unique only up to conjugation in $\mathrm{Aut}\,(\mathbb{U})$, and Π is a torsion free subgroup of Γ.

It is known that the signature of Γ must have form $(g; m_1, \ldots, m_t)$, where g is non-negative integer, each m_i is an integer great than 1 and a factor of $|G|$, the order of G. As an abstract group Γ has a presentation of the following standard form (see [33] or [10]):

(i) $t + 2g$ generators $A_1, \ldots, A_t$, $X_1, Y_1, \ldots, X_g, Y_g$.

(ii) $t + 1$ relations $A_1^{m_1} = \cdots = A_t^{m_t} = A_1, \ldots, A_t[X_1, Y_1] \cdots [X_g, X_g] = 1$.

For brevity, we refer to Γ by $\Gamma(g; m_1, \ldots, m_t)$. Moreover, consideration of non-Euclidean area implies the Riemann-Hurwitz formula

$$\frac{2(\gamma - 1)}{|G|} = 2(g-1) + \sum_{i=1}^{t} \left(1 - \frac{1}{m_i}\right) \tag{2.16}$$

where γ is the genus of $\mathbb{U}/\Pi$.

Now suppose G is the cyclic group $\mathbb{Z}_p$ and $T \in \mathbb{Z}_p$ denotes a fixed generator. Actions of $\mathbb{Z}_p$ on Riemann surfaces correspond to short exact sequences $1 \to \Pi \to \Gamma \xrightarrow{\theta} \mathbb{Z}_p \to 1$. We see that Γ must have the form $\Gamma(g; \overbrace{p, \ldots, p}^{t \text{ times}})$, where g and t are non-negative integers. That is, as an abstract group Γ has the following presentation

(i) $t + 2g$ generators $A_1, \ldots, A_t, X_1, Y_1, \ldots, X_g, Y_g$.

(ii) $t + 1$ relations $A_1^p = \cdots = A_t^p = A_1 \cdots A_t[X_1, Y_1] \cdots [X_g, Y_g] = 1$.

Any such group can be embedded in $\mathrm{Aut}\,(\mathbb{U})$ as a discrete subgroup in many different ways up to conjugation. In fact the set of conjugacy classes of embedding is a cell of dimension

$$d(\Gamma) = 6g - 6 + 2t \text{ so long as } 6g - 6 + 2t \geq 0.$$

See [3] and [4]. The genus of the orbit surface $S/\mathbb{Z}_p$ is g and the number of fixed points is t.

Figure 2.1 illustrates a fundamental domain for a particular embedding when $g = 0$ and $t = 3$. It consists of a regular 3-gon P, all of whose angles are π/p, together with a copy of

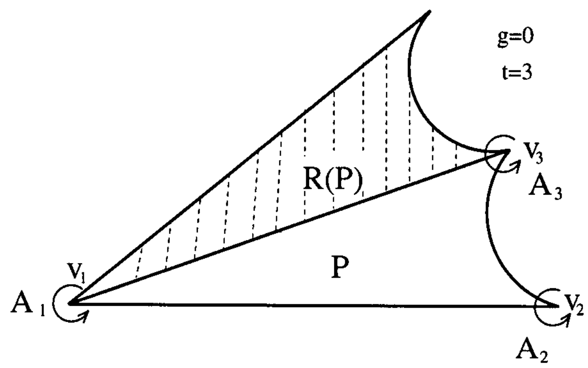

Figure 2.1: Fundamental Domain

P obtained by reflection in one of its sides. The generators A_1, A_2, A_3 are the rotations by $2\pi/p$ about consecutive vertices, ordered in the counterclockwise sense. In this case the cell dimension is $d(\Gamma) = 6g - 6 + 2t = 0$, in other words, up to conjugacy in Aut $(\mathbb{U})$ there is a unique subgroup of signature $(0; p, p, p)$.

In a similar manner, when $g = 0$ and $t > 3$, a fundamental domain for a particular Fuchsian group Γ of signature $(0; \overbrace{p, \ldots, p}^{t \text{ times}})$ is given by $P \cup R(P)$, where P is a regular t-gon all of whose angles are π/p and R is a reflection in one of its sides. In this case Γ is the Fuchsian group generated by the rotations $A_1, \ldots, A_t$ through $2\pi/p$ about consecutive vertices. The dimension of the cell is $d(\Gamma) = 6g - 6 + 2t = -6 + 2t > 0$. Thus the embedding is not unique up to conjugacy in Aut $(\mathbb{U})$.

Let Γ be any Fuchsian group of signature $(g; \overbrace{p, \ldots, p}^{t \text{ times}})$. Then an epimorphism $\theta \colon \Gamma \to \mathbb{Z}_p$ is determined by the images of the generators. The relations in Γ must be preserved and the kernel of θ must be torsion free, so θ is determined by the equations

$$\theta(A_j) = T^{a_j},\ 1 \le j \le t;\ \theta(X_k) = T^{b_k},\ \theta(Y_k) = T^{c_k}, 1 \le k \le g.$$

The following restrictions must hold:

(i) The a_j are integers such that $1 \le a_j \le p - 1$ and $\sum_{j=1}^{t} a_j \equiv 0 \pmod p$.

(ii) The b_k, c_k are arbitrary integers mod p, except that at least one of them is non-zero if $t = 0$ (this guarantees that θ is an epimorphism).

It follows from the first restriction that the only possible values of t are $t = 0, 2, 3, \dots$.

Conversely, given integers a_j, b_k, c_k satisfying conditions (i) and (ii), there is an epimorphism $\theta\colon \Gamma \to \mathbb{Z}_p$ with torsion free kernel Π and a corresponding $\mathbb{Z}_p$ action $T\colon S \to S$, where $S = \mathbb{U}/\Pi$.

The integer t equals the number of fixed points of $T\colon S \to S$ and g is the genus of the orbit surface $S/\mathbb{Z}_p$. A well known result of Nielsen [27] says that the topological conjugacy class of $T\colon S \to S$ is completely determined by g and the unordered sequence $(a_1, \dots, a_t)$. We use the notation $[g \mid a_1, \dots, a_t]$ to denote the topological conjugacy class of the homeomorphism $T\colon S \to S$ determined by this data. If $g = 0$ we use the notation $[a_1, \dots, a_t]$, and usually order the a_j so that $1 \le a_1 \le \ldots \le a_t \le p-1$.

Of particular interest is the case $g = 0$. Then the orbit surface $S/\mathbb{Z}_p$ is the extended complex plane $\widehat{\mathbb{C}}$ and Γ has the presentation

(i) t generators $A_1, \dots, A_t$.

(ii) $t+1$ relations $A_1^p = \cdots = A_t^p = A_1 \cdots A_t = 1$.

The epimorphism θ is given by the equations

$$\theta(A_j) = T^{a_j}, \tag{2.17}$$

where $a_1, \dots, a_t$ satisfy the conditions

$$1 \le a_1 \le \ldots \le a_t \le p-1, \text{ and } \sum_{j=1}^{t} a_j \equiv 0 \pmod{p}. \tag{2.18}$$

Proposition 2.3. *There is a one-to-one correspondence between the set of topological conjugacy classes of automorphisms $T\colon S \to S$ of order p and orbit genus 0, where S is an arbitrary compact connected Riemann surface, and sequences $[a_1, \dots, a_t]$ satisfying the conditions in (2.18). The integer t is the number of fixed points and the rotation numbers k_j are determined by the equations $k_j a_j \equiv 1 \pmod{p}$, $1 \le j \le t$.*

Proof. It follows from the above that we can associate to an automorphism $T\colon S \to S$ of order p, where S is any compact connected Riemann surface such that the genus of $S/\mathbb{Z}_p$ is 0, a sequence $[a_1, \dots, a_t]$ satisfying the conditions in (2.18). According to the results of Nielsen two such automorphisms are topologically conjugate if, and only if, the associated sequences are identical.

Conversely, given any sequence $[a_1, \dots, a_t]$ satisfying (2.18) we can construct an automorphism $T\colon S \to S$ of order p and orbit genus 0 as follows. Let Γ be any discrete subgroup of $\mathrm{Aut}\,(\mathbb{U})$ of signature $(0; \overbrace{p, \dots, p}^{t \text{ times}})$. Then Equation (2.17) defines an epimorphism $\theta\colon \Gamma \to \mathbb{Z}_p$ with a torsion free kernel Π, and this in turn determines an automorphism T of order p on $S = \mathbb{U}/\Pi$. The topological conjugacy class of T does not depend on the embedding of Γ, only on the signature and the sequence $[a_1, \dots, a_t]$. Thus the correspondence is one-to-one on the level of topological conjugacy.

A particular embedding of Γ in $\mathrm{Aut}\,(\mathbb{U})$ is the one indicated above; that is, Γ is the subgroup generated by $A_1, \dots, A_t$, where the A_j are rotations by $2\pi/p$ about the vertices of a regular t-gon P, all of whose angles are π/p. See Figure 2.1 for the case where $t = 3$. The fixed points of this action correspond to the orbits of the vertices, and thus there are t of them, $P_1, \dots, P_t$, where P_j is the orbit of the vertex of rotation for the generator A_j. The epimorphism θ satisfies $\theta(A_j) = T^{a_j}$, and therefore $\theta(A_j^{k_j}) = T$, where the k_j satisfy $k_j a_j \equiv 1 \pmod{p}$, $1 \leq j \leq t$. This implies that the automorphism $T\colon S \to S$ in a small neighborhood of P_j is represented by $A_j^{k_j}$, a rotation about P_j by an angle of $2k_j\pi/p$. In other words the rotation numbers are the k_j for this particular embedding. This completes the proof since the number of fixed points and their rotation numbers are invariants of topological conjugacy. $\square$

We conclude this section by answering Question 3 in the introduction. This is just a matter of determining the possible sets of rotation numbers. Thus let $\{k_1, \cdots, k_t\}$ be any set of t numbers satisfying $1 \leq k_j \leq p-1$, $1 \leq j \leq t$, and let a_j denote that number such that $k_j a_j \equiv 1 \pmod{p}$ and $1 \leq a_j \leq p-1$.

Proposition 2.4. $1+\sum_{j=1}^{t}\frac{1}{\zeta^{k_j}-1}\in A$, *if, and only if,* $\sum_{j=1}^{t}a_j\equiv 0 \pmod p$.

Proof. First suppose that $\chi = 1+\sum_{j=1}^{t}\frac{1}{\zeta^{k_j}-1}\in A$. Thus there is an automorphism of order p, $T\colon S\to S$, on some compact, connected Riemann surface S, such that $\chi(T)=\chi$. In fact we can assume that the genus of $S/\mathbb{Z}_p$ is zero. According to the results of this chapter the action of $\mathbb{Z}_p$ on S corresponds to a short exact sequence $1\to\Pi\to\Gamma\xrightarrow{\theta}\mathbb{Z}_p\to 1$. Here Γ is abstractly isomorphic to the group presented by t generators $A_1,\dots,A_t$ and $t+1$ relations $A_1^p=\cdots=A_t^p=A_1\cdots A_t=1$. The epimorphism θ is determined by the equations $\theta(A_j)=T^{a_j}$, $1\le k_j\le p-1$. In order that θ be well defined it is necessary that $\sum_{j=1}^{t}a_j\equiv 0 \pmod p$.

Next suppose that we are given a set $\{k_1,\cdots,k_t\}$ satisfying the conditions of the proposition. Then the short exact sequence above determines a Riemann surface S and an automorphism $T\colon S\to S$ realizing χ as an Eichler trace. $\square$

Chapter 3
The Conjugacy Classes of Type-I

It is well known that there is an one-to-one correspondence between the conjugacy classes of matrices of rational integers with a given irreducible characteristic polynomial $f(x)$ and the classes of ideals in $\mathbb{Z}[x]/(f(x))$ [22], [31], [36]. It is also known that under some conditions, the matrix class generated by the transpose of X corresponds to the inverse ideal class, [37]. E. Bender generalized this correspondence to matrices over an integral domain [2]. In this chapter we extend these methods and study symplectic matrices over $\mathcal{D}$ with a given separable characteristic polynomial of type-I. In particular, we give the the conjugacy class number of cyclic matrices with characteristic polynomial a cyclotomic polynomial in the integral symplectic groups. In Section 3.1 we shall review some results of ideal classes, most of them can be found in [19], [23] or any book on ideal theory. In Section 3.2 we introduce S-pairs. We prove Theorem 1 and Theorem 2 in Section 3.3. In Section 3.4 we shall prove Theorem 3. Finally, in Section 3.5 we shall consider the rational integer case and prove Theorem 4.

3.1 Ideal Classes

Let $f(x) \in \mathcal{D}_n[x]$ be a monic irreducible and separable polynomial with degree n and ζ be a fixed root of $f(x)$. Let $\mathcal{F}$ be the quotient field of $\mathcal{D}$ and $\mathcal{K}$ be the splitting field over $\mathcal{F}$ of $f(x)$. Let $\mathcal{R} = \mathcal{D}[\zeta]$ and $\mathcal{S} = \mathcal{F}[\zeta]$. Then $\mathcal{S}$ is the quotient field of $\mathcal{R}$ and $\mathcal{R} \subset \mathcal{S} \subset \mathcal{K}$. We also denote the set of non-zero elements of $\mathcal{R}$ by $\mathcal{R}^*$.

The trace of an element α in $\mathcal{S}$ is defined as follows. Suppose the n different roots of $f(x)$ are $\zeta_1, \dots, \zeta_n \in \mathcal{K}$ with $\zeta_1 = \zeta$. Let $\alpha = a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1} \in \mathcal{S}$. The i-th conjugate of

α is defined by $\alpha^{(i)} = a_0 + a_1\zeta_i + \cdots + a_{n-1}\zeta_i^{n-1}$. Then the trace of α is

$$\mathrm{Tr}\,(\alpha) = \sum_{i=1}^{n} \alpha^{(i)} \quad \in \mathcal{F}. \tag{3.1}$$

It is clear that if $\alpha \in \mathcal{R}$, then $\mathrm{Tr}\,(\alpha) \in \mathcal{D}$.

Suppose $\alpha_1, \ldots, \alpha_n \in \mathcal{S}$. Then the discriminant of $\alpha_1, \ldots, \alpha_n$ is defined to be

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix} \alpha_1^{(1)} & \alpha_1^{(2)} & \cdots & \alpha_1^{(n)} \\ \alpha_2^{(1)} & \alpha_2^{(2)} & \cdots & \alpha_2^{(n)} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_n^{(1)} & \alpha_n^{(2)} & \cdots & \alpha_n^{(n)} \end{pmatrix}. \tag{3.2}$$

A standard result is that $\Delta^2(\alpha_1, \ldots, \alpha_n) = \det\left(\mathrm{Tr}\,(\alpha_i\alpha_j)\right)$.

Lemma 3.1. *$\alpha_1, \ldots, \alpha_n$ are independent over $\mathcal{F}$ if, and only if* $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.

For a proof see [19].

An ideal (fractional ideal) in $\mathcal{S}$ is a non-zero finitely generated $\mathcal{R}$-submodule of $\mathcal{S}$ which is a free $\mathcal{D}$-module of rank n. An integral ideal is an ideal which is contained in $\mathcal{R}$.

Assume that $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in $\mathcal{S}$. The product $\mathfrak{a}\mathfrak{b}$ is the collection of all possible finite sums of products ab, where $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. With this definition $\mathfrak{a}\mathfrak{b}$ indeed becomes an ideal in $\mathcal{S}$.

Let $\alpha_1, \ldots, \alpha_r \in \mathcal{S}$. Then $\mathfrak{a} = \{\xi_1\alpha_1 + \cdots + \xi_r\alpha_r \mid \xi_i \in \mathcal{R}\}$ is an ideal in $\mathcal{S}$. We denote this ideal by $(\alpha_1, \ldots, \alpha_r)$. It is clear that

$$(\alpha_1, \ldots, \alpha_r)(\beta_1, \ldots, \beta_s) = (\alpha_1\beta_1, \ldots, \alpha_1\beta_s, \ldots, \alpha_r\beta_1, \ldots, \alpha_r\beta_s). \tag{3.3}$$

An ideal $\mathfrak{a}$ is called a principal ideal if there is an α in $\mathcal{S}$ such that $\mathfrak{a} = (\alpha)$. If α, $\beta \in \mathcal{S}$, then $(\alpha) = (\beta)$ if and only if α and β are associates, i.e. they differ only by a unit factor.

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be equivalent if there exist non-zero elements $\lambda, \mu \in \mathcal{R}$, such that $\lambda\mathfrak{a} = \mu\mathfrak{b}$. In fact the collection $\mathcal{C}$ of equivalence classes of integral ideals forms a monoid.

Let $\mathfrak{a}$ be an ideal in $\mathcal{S}$. The complementary ideal of $\mathfrak{a}$ is

$$\mathfrak{a}' = \left\{ \alpha \in \mathcal{S} \;\middle|\; \mathrm{Tr}\,(\alpha\mathfrak{a}) \subset \mathcal{D} \right\}. \tag{3.4}$$

Let $\alpha_1, \ldots, \alpha_n$ be a $\mathcal{D}$-basis of $\mathfrak{a}$. There is a dual basis $\alpha'_1, \ldots, \alpha'_n$ in $\mathcal{S}$, that is a basis such that $\mathrm{Tr}\,(\alpha'_i\alpha_j) = \delta_{ij}$, where δ_{ij} is the Kronecker symbol. This is equivalent to either of the following equations

$$\sum_k \alpha'^{(k)}_i \alpha^{(k)}_j = \delta_{ij} \quad \text{or} \quad \sum_k \alpha^{(i)}_k \alpha'^{(j)}_k = \delta_{ij}. \tag{3.5}$$

We also have

$$\mathfrak{a}' = \mathcal{D}\alpha'_1 + \cdots + \mathcal{D}\alpha'_n \tag{3.6}$$

because if $\beta = \sum a_i \alpha'_i$ with $a_i \in \mathcal{F}$, then $a_i = \mathrm{Tr}\,(\beta\alpha_i)$.

The following lemmas are given here without proof (for reference see [19]).

Lemma 3.2. *Let $f'(x)$ be the derivative of $f(x)$, and $\frac{f(x)}{x-\zeta} = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$. Then the dual basis of $1, \zeta, \ldots, \zeta^{n-1}$ is*

$$\frac{b_0}{f'(\zeta)}, \; \ldots, \; \frac{b_{n-1}}{f'(\zeta)}. \tag{3.7}$$

Lemma 3.3. $\mathcal{R}' = \mathcal{R}/\left(f'(\zeta)\right)$.

Lemma 3.4. $\mathfrak{a}\mathfrak{a}' \subset \mathcal{R}'$.

3.2 S-Pairs

In this section we assume that $f(x)$ is a separable S-polynomial of type-I and degree $2n$. If ζ_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 $\zeta_1 = \zeta, \; \zeta_2, \; \ldots, \; \zeta_{2n}$ of $f(x)$ satisfy $\zeta_{2i-1}\zeta_{2i} = 1$, for $i = 1, \ldots, n$.

According to Galois Theory, there are $2n$ automorphisms $\eta_1 = 1, \; \ldots, \; \eta_{2n}$ of $\mathcal{K}$ in $\mathrm{Gal}\,(\mathcal{K}/\mathcal{F})$, the Galois group of the extension field $\mathcal{K}/\mathcal{F}$, such that $\eta_i(\zeta) = \zeta_i$. Then the i-conjugate of $\alpha \in \mathcal{S}$ has the form $\alpha^{(i)} = \eta_i(\alpha)$, for $i = 1, \ldots, 2n$.

It is obvious that η_2 is an involution on the extension field $\mathcal{S}$. We use $\widetilde{\alpha}$ instead of $\eta_2(\alpha)$ if $\alpha \in \mathcal{S}$. It is easy to check that

$$\eta_{2i-1}(\widetilde{\alpha}) = \eta_{2i}(\alpha) \quad \text{and} \quad \eta_{2i}(\widetilde{\alpha}) = \eta_{2i-1}(\alpha) \tag{3.8}$$

for $\alpha \in \mathcal{S}$.

Some notation is needed for the sake of convenience. We let

$$\widetilde{A} = (\widetilde{\alpha}_{ij}) \quad \text{and} \quad \eta_k(A) = A^{(k)} = \left(\alpha_{ij}^{(k)}\right) \tag{3.9}$$

if $A = (\alpha_{ij})$ is a matrix with entries in $\mathcal{S}$, and $\widetilde{\mathfrak{a}} = \{\widetilde{\alpha} \mid \alpha \in \mathfrak{a}\}$ for any ideal $\mathfrak{a}$ in $\mathcal{S}$. It is clear that $\widetilde{\mathfrak{a}}$ is also an ideal in $\mathcal{S}$.

The following lemmas are very useful.

Lemma 3.5. *Suppose $M \in M_{2n}(\mathcal{F})$ and $\alpha, \beta \in \mathcal{S}^{2n}$ 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 $\alpha'^{(i)} M \beta^{(j)} = \left(\alpha' M \beta^{(k)}\right)^{(i)}$.*

Proof. Since $\eta_1, \dots, \eta_{2n}$ are permutations of the roots of $f(x)$, for any $1 \leq i, j \leq 2n$, $\eta_i^{-1}\eta_j(\zeta)$ is a root of $f(x)$, say ζ_k. We have $\eta_k(\zeta) = \eta_i^{-1}\eta_j(\zeta)$, therefore $\eta_j(a) = \eta_i\eta_k(a)$, for any $a \in \mathcal{S}$. Hence $\left(\alpha' M \beta^{(k)}\right)^{(i)} = \eta_i\left(\alpha' M \eta_k(\beta)\right) = \eta_i(\alpha') M \eta_i\eta_k(\beta) = \alpha'^{(i)} M \beta^{(j)}$. □

Lemma 3.6. *Suppose $M, N \in M_{2n}(\mathcal{F})$ and $\alpha = (\alpha_1, \dots, \alpha_{2n})' \in \mathcal{S}^{2n}$, where $\alpha_1, \dots, \alpha_{2n}$ are independent over $\mathcal{D}$, and $\alpha' M \widetilde{\alpha}^{(i)} = \alpha' N \widetilde{\alpha}^{(i)}$ (for $i = 1, \dots, 2n$). Then $M = N$.*

Proof. We only prove the special case $N = 0$. By Lemma 3.5, for any $1 \leq i, j \leq 2n$, there is $1 \leq k \leq 2n$ such that $\alpha'^{(i)} M \widetilde{\alpha}^{(j)} = (\alpha' M \widetilde{\alpha}^{(k)})^{(i)} = 0$. i.e. $A' M B = 0$, where $A = \left(\alpha_i^{(j)}\right)$ and $B = \left(\widetilde{\alpha}_i^{(j)}\right)$ are $2n \times 2n$ matrices. By Lemma 3.1, $\det A \neq 0$ and $\det B \neq 0$, since $\alpha_1, \dots, \alpha_{2n}$ are independent over $\mathcal{D}$, and therefore $M = 0$. □

Let $\Delta = \zeta^{1-n} f'(\zeta)$. Clearly $\widetilde{\Delta} = -\Delta$ by (2.7) and $f(\frac{1}{\zeta}) = 0$. Note that the pair $(\mathfrak{a}, a)$ of an integral ideal $\mathfrak{a}$ and an element $a \in \mathcal{R}$ is an element of P_f if, and only if $\widetilde{\mathfrak{a}} = a\Delta\mathfrak{a}'$ and $a = \widetilde{a}$. From Lemma 3.3, we have $\mathcal{R}' = \mathcal{R}/\Delta$ and that is $(\mathcal{R}, 1) \in P_f$. Thus $P_f \neq \emptyset$.

Definition 3.1. A pair $(\mathfrak{a}, a)$ consisting of an ideal $\mathfrak{a}$ and an element a in $\mathcal{S}$ is said to be an S-pair, if there is a basis $\alpha_1, \ldots, \alpha_{2n}$ of $\mathfrak{a}$, such that

$$\alpha' J \widetilde{\alpha}^{(i)} = \delta_{1i}\, a\Delta, \quad \text{for } i = 1, \ldots, 2n, \tag{3.10}$$

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

Remark. By Lemma 3.5, we see that (3.10) is equivalent to

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

The bilinear form defined on column vectors $\alpha = (\alpha_1, \ldots, \alpha_{2n})'$ and $\beta = (\beta_1, \ldots, \beta_{2n})'$ by $\langle \alpha, \beta \rangle = \alpha' J \widetilde{\beta}$ is a non-degenerate skew-hermitian form. In particular, if $\lambda = \alpha' J \widetilde{\alpha}$, then $\widetilde{\lambda} = -\lambda$. Since $\widetilde{\Delta} = -\Delta$ it follows that if $(\mathfrak{a}, a)$ is an S-pair, then $a = \widetilde{a}$.

Lemma 3.7. *A pair $(\mathfrak{a}, a)$ is an S-pair if, and only if*

$$\widetilde{\mathfrak{a}} = a\Delta\mathfrak{a}' \quad \textit{and} \quad a = \widetilde{a}. \tag{3.11}$$

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

For the converse, suppose (3.11). If $\beta_1, \ldots, \beta_{2n}$ is a basis of $\mathfrak{a}$ then $\widetilde{\beta}_1, \ldots, \widetilde{\beta}_{2n}$ is a basis of $\widetilde{\mathfrak{a}}$. Let $\gamma_1, \ldots, \gamma_{2n}$ be the dual basis of $\beta_1, \ldots, \beta_{2n}$. Then $\mathrm{Tr}\,(\beta_i \gamma_j) = \delta_{ij}$, and we have $\beta'^{(i)} \gamma^{(j)} = \delta_{ij}$, where $\beta = (\beta_1, \ldots, \beta_{2n})'$, $\gamma = (\gamma_1, \ldots, \gamma_{2n})'$. Since $\widetilde{\mathfrak{a}} = a\Delta\mathfrak{a}'$, there is $M \in GL_{2n}(\mathcal{D})$ such that $M\widetilde{\beta} = a\Delta\gamma$. Then

$$\beta' M \widetilde{\beta}^{(i)} = a^{(i)} \Delta^{(i)} \beta' \gamma^{(i)} = \delta_{1i}\, a\Delta \tag{3.12}$$

and

$$\beta' M' \widetilde{\beta}^{(i)} = \widetilde{a}\widetilde{\Delta}\widetilde{\gamma}' \eta_i(\widetilde{\beta}) = -a\Delta\eta_2(\gamma')\eta_i\eta_2(\beta) = -\delta_{1i}\, a\Delta \tag{3.13}$$

For the last equality, we use Formula (3.8). Thus $\beta' M \widetilde{\beta}^{(i)} = -\beta' M' \widetilde{\beta}^{(i)}$ (for $i = 1, \ldots, 2n$), and so $M' = -M$ (by Lemma 3.6). According to [26] there is $Q \in GL_{2n}(\mathcal{D})$ such that $M = Q'JQ$. If $\alpha = Q\beta$, then

$$\alpha' J \widetilde{\alpha}^{(i)} = \beta' M \widetilde{\beta}^{(i)} = \delta_{1i}\, a\Delta.$$

So α is a J-vector with respect to $(\mathfrak{a}, a)$. $\square$

Corollary 3.1. *Suppose $\mathfrak{a}$ is an integral ideal. Then $(\mathfrak{a}, a) \in P_f$ if and only of $(\mathfrak{a}, a)$ is an S-pair.*

Proof. Suppose $(\mathfrak{a}, a)$ is an S-pair. We need to show that $a \in \mathcal{R}$. Since $\mathfrak{a} \subset \mathcal{R}$, then $\frac{\mathcal{R}}{\Delta} = \mathcal{R}' \subset \mathfrak{a}'$. But $a\Delta\mathfrak{a}' = \widetilde{\mathfrak{a}}$, so $a\mathcal{R} \subset \widetilde{\mathfrak{a}}$, thus $a \in \mathcal{R}$.

The converse is clear. $\square$

3.3 The Correspondence Ψ

In this section we prove Theorem 1 and Theorem 2. Recall that M_f is the set of all the matrices in $SP_{2n}(\mathcal{D})$ with characteristic polynomial $f(x)$, and $\mathcal{M}_f$ is the set of the similarity classes in M_f over $SP_{2n}(\mathcal{D})$. Suppose $X \in M_f$. There is an eigenvector $\alpha = (\alpha_1, \ldots, \alpha_{2n})' \in \mathcal{R}^{2n}$ corresponding to ζ, that is $X\alpha = \zeta\alpha$. Let $\mathfrak{a}$ be the $\mathcal{D}$-module generated by $\alpha_1, \ldots, \alpha_{2n}$, i.e.

$$\mathfrak{a} = \mathcal{D}\alpha_1 + \cdots + \mathcal{D}\alpha_{2n}$$

and $a = \Delta^{-1}\alpha' J \widetilde{\alpha}$. It is easy to check that $\mathfrak{a}$ is an integral ideal in $\mathcal{R}$ and $a = \widetilde{a}$. Thus $\alpha_1, \ldots, \alpha_{2n}$ are independent over $\mathcal{D}$. Furthermore we have

Lemma 3.8. *The pair $(\mathfrak{a}, a)$ is an S-pair.*

Proof. We only need to prove that $\alpha' J \widetilde{\alpha}^{(i)} = 0$ (for $i = 2, \ldots, 2n$). Assume $2 \leq i \leq 2n$. From $X\alpha = \zeta\alpha$ we have $X\alpha^{(i)} = \zeta_i \alpha^{(i)}$ and $X\widetilde{\alpha}^{(i)} = \frac{1}{\zeta_i}\widetilde{\alpha}^{(i)}$. Hence

$$\alpha' J \widetilde{\alpha}^{(i)} = \frac{\zeta_i}{\zeta} \alpha' X' J X \widetilde{\alpha}^{(i)} = \frac{\zeta_i}{\zeta} \alpha' J \widetilde{\alpha}^{(i)}. \tag{3.14}$$

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

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

Lemma 3.9. *$X \sim Y$ if, and only if $\langle \mathfrak{a}, a\rangle = \langle \mathfrak{b}, b\rangle$.*

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 λ, $\mu \in \mathcal{R}^*$ such that $\lambda\alpha = \mu Q\beta = Q\mu\beta$. So $\lambda\mathfrak{a} = \mu\mathfrak{b}$, and

$$\begin{aligned}\lambda\widetilde{\lambda}a &= \Delta^{-1}\lambda\alpha' J\widetilde{\lambda\alpha} = \Delta^{-1}(\mu Q\beta)' J\widetilde{\mu Q\beta} \\ &= \Delta^{-1}\mu\widetilde{\mu}\beta' Q' JQ\widetilde{\beta} = \Delta^{-1}\mu\widetilde{\mu}\beta' J\widetilde{\beta} = \mu\widetilde{\mu}b.\end{aligned}$$

Therefore $\langle \mathfrak{a}, a\rangle = \langle \mathfrak{b}, b\rangle$.

Sufficiency. Suppose λ, $\mu \in \mathcal{R}^*$ are such that $\lambda\mathfrak{a} = \mu\mathfrak{b}$ and $\lambda\widetilde{\lambda}a = \mu\widetilde{\mu}b$. 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

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

If $i = 1$, then

$$\beta' Q' JQ\widetilde{\beta} = \frac{\lambda\widetilde{\lambda}}{\mu\widetilde{\mu}}\alpha' J\widetilde{\alpha} = \frac{b}{a}\alpha' J\widetilde{\alpha} = \beta' J\widetilde{\beta}.$$

Hence $Q' JQ = J$ (by Lemma 3.6). $\square$

Let Ψ denote the correspondence from $\mathcal{M}_f$ to $\mathcal{P}_f$ defined as above. Lemma 3.9 guarantees Ψ is well defined and injective. The proof of Theorem 1 is completed by following lemma.

Lemma 3.10. *Ψ is surjective.*

Proof. Let $(\mathfrak{a}, a) \in P_f$ and $\alpha = (\alpha_1, \ldots, \alpha_{2n})'$ be a J-vector with respect to $(\mathfrak{a}, a)$. Then $\zeta\alpha_1, \ldots, \zeta\alpha_{2n}$ is another basis of $\mathfrak{a}$, 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

$$\alpha' X' J X \widetilde{\alpha}^{(i)} = \frac{\zeta}{\zeta_i} \alpha' J \widetilde{\alpha}^{(i)} = \delta_{1i}\, a\Delta.$$

Hence $\alpha' X' J X \widetilde{\alpha}^{(i)} = \alpha' J \widetilde{\alpha}^{(i)}$ (for $i = 1, \ldots, 2n$). By Lemma 3.6, $X'JX = J$. This completes the proof. □

We now prove the Theorem 2.

Proof of Theorem 2. By Proposition 2.1, $f(x)$ is a product of irreducible S-polynomials,

$$f(x) = (x-1)^{2k}(x+1)^{2l} p_1(x) \cdots p_s(x).$$

If $p_i(x)$ is of type-I, then $P_{p_i} \neq \emptyset$, thus there exists $X_i \in M_{p_i}$. On the other hand, if $p_j(x)$ is of type-II, then $p_j(x) = q(0)x^{n_i} q(x) q(\frac{1}{x})$, where $q(x)$ is an irreducible monic polynomial with degree n_i (by Lemma 2.5). Let C_q be the companion matrix of $q(x)$. Then $X_j = C_q' + C_q^{-1} \in M_{p_j}$. Hence

$$I_{2l} * (-I_{2k}) * X_1 * \cdots X_s \in M_f.$$

That is $M_f \neq \emptyset$. □

3.4 Class Number of $\mathcal{P}_f$

In this section we prove Theorem 3. Suppose $\mathcal{R}$ is integrally closed in $\mathcal{S}$. Then $\mathfrak{a}\widetilde{\mathfrak{a}} = (a)$ if and only if $\widetilde{\mathfrak{a}} = a\Delta\mathfrak{a}'$, see [19]. So $\mathcal{C}$ is a group, the identity is $\mathcal{R}$ and $\mathfrak{a}^{-1} = \Delta\mathfrak{a}'$. We easily see that $(\mathfrak{a}, a) \in P_f$ if and only if $\mathfrak{a}\widetilde{\mathfrak{a}} = (a)$ and $a = \widetilde{a}$. Then $\mathcal{P}_f$ is a group if we define multiplication in $\mathcal{P}_f$ by

$$\langle \mathfrak{a}, a\rangle \langle \mathfrak{b}, b\rangle = \langle \mathfrak{a}\mathfrak{b}, ab\rangle.$$

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

For the proof of Theorem 3 we will need the following lemmas.

Lemma 3.11. *Suppose* $(\mathfrak{a}, a) \in P_f$, $\lambda \in \mathcal{R}^*$. *Then*

1. $(\lambda\mathfrak{a}, \lambda\widetilde{\lambda}a) \in P_f$.

2. $(\mathfrak{a}, \lambda a) \in P_f$ *if and only if* $\lambda \in U^+$.

Proof. For the first part we have $\lambda\mathfrak{a}\widetilde{\lambda\mathfrak{a}} = \lambda\widetilde{\lambda}\mathfrak{a}\widetilde{\mathfrak{a}} = \left(\lambda\widetilde{\lambda}a\right)$ and $\widetilde{\lambda\widetilde{\lambda}a} = \widetilde{\lambda}\lambda\widetilde{a} = \lambda\widetilde{\lambda}a$. Hence $(\lambda\mathfrak{a}, \lambda\widetilde{\lambda}a) \in P_f$.

For the second part, if $(\mathfrak{a}, \lambda a) \in P_f$ then $\mathfrak{a}\widetilde{\mathfrak{a}} = (\lambda a) = (a)$; so $\lambda \in U$. We also have $\widetilde{\lambda}a = \widetilde{\lambda a} = \lambda a$, and so $\widetilde{\lambda} = \lambda$. The converse is quite simple. $\square$

Lemma 3.12. *Suppose* $(\mathfrak{a}, a)$, $(\mathfrak{a}, b) \in P_f$. *Then* $\langle\mathfrak{a}, a\rangle = \langle\mathfrak{a}, b\rangle$ *if and only if* $\frac{a}{b} \in C$.

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

Conversely, suppose $\frac{a}{b} = u\widetilde{u}$ for some $u \in U$. Then $\langle\mathfrak{a}, a\rangle = \langle\mathfrak{a}, u\widetilde{u}b\rangle = \langle u\mathfrak{a}, u\widetilde{u}b\rangle = \langle\mathfrak{a}, b\rangle$. $\square$

Lemma 3.13. *Let* $(\mathfrak{a}, a), (\mathfrak{b}, b) \in P_f$, *and* $\lambda\mathfrak{a} = \mu\mathfrak{b}$, *for some* λ, $\mu \in \mathcal{R}^*$. *Then* $\langle\mathfrak{a}, a\rangle = \langle\mathfrak{b}, ub\rangle$ *for some* $u \in U^+$.

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

Now we can prove Theorem 3; namely there is a short exact sequence

$$1 \to U^+/C \xrightarrow{\phi} \mathcal{P}_f \xrightarrow{\psi} \mathcal{C}_0 \to 1$$

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

Proof of Theorem 3. Clearly, ϕ is well defined and a group monomorphism (by Lemma 3.12). ψ is also well defined and a group epimorphism (by Lemma 3.7). $\psi\phi([u]) = \psi(\langle\mathcal{R}, u\rangle) = [\mathcal{R}]$ (by definition) and Ker $\psi =$ Im ϕ (by Lemma 3.13). This completes the proof. $\square$

Remark. Lemma 3.11, Lemma 3.12 and Lemma 3.13 are also true even if $\mathcal{R}$ is not integrally closed in $\mathcal{S}$. There is a bijective mapping between $\mathcal{P}_f$ and $\mathcal{C}_0 \times U^+/C$.

Corollary 3.2. *If $\mathcal{D}$ is the rational field $\mathbb{Q}$, then there is an one-to-one correspondence between $\mathcal{M}_f$ and $\mathcal{R}^+/C$, where $\mathcal{R}^+ = \{a \in \mathcal{R}^* \mid a = \tilde{a}\}$ and $C = \{a\tilde{a} \mid a \in \mathcal{R}^*\}$.*

Proposition 3.1. *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 $\mathcal{R} = \mathbb{Q}[\zeta]$, $\zeta = e^{\frac{2\pi i}{3}}$. Let p, q be different primes with $p \equiv q \equiv 2 \pmod 3$. We want to show $[p] \neq [q]$ in $\mathcal{R}^+/C$.

Suppose $[p] = [q]$. There are $\lambda = x_1 + y_1\zeta$, $\mu = x_2 + y_2\zeta \in \mathbb{Z}[\zeta]$ such that $\lambda\overline{\lambda}p = \mu\overline{\mu}q$, that is

$$(x_1^2 - x_1y_1 + y_1^2)p = (x_2^2 - x_2y_2 + y_2^2)q.$$

Then there is an integer k such that

$$\begin{cases} x_1^2 - x_1y_1 + y_1^2 = kq \\ x_2^2 - x_2y_2 + y_2^2 = kp \end{cases} \tag{3.15}$$

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

By a theorem of Dirichlet, there are infinitely many primes of the form $3k + 2$, and so we have proved that $\mathcal{R}^+/C$ 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.

3.5 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 finitely generated abelian group and $U^{+2} \subset C$, we get

Proposition 3.2. *$\mathcal{M}_f$ is finite.*

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

$$\Phi_m(x) = (x - \zeta_1) \dots (x - \zeta_{\phi(m)}) \tag{3.16}$$

where $\zeta_1, \dots, \zeta_{\phi(m)}$ 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 $\mathbb{Q}$. Also $\Phi_m(x)$ is an S-polynomial. We simply denote M_{Φ_m} and $\mathcal{M}_{\Phi_m}$ by M_m and $\mathcal{M}_m$.

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

Proposition 3.3. *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 ζ, $X\alpha = \zeta\alpha$. Then $X^{-1}\overline{\alpha} = \zeta\overline{\alpha}$. Hence $\Psi(X) = \langle \mathfrak{a}, \Delta^{-1}\alpha' J\overline{\alpha}\rangle$ and $\Psi(X^{-1}) = \langle \overline{\mathfrak{a}}, \Delta^{-1}\overline{\alpha}' J\alpha\rangle$. If X were conjugate to X^{-1} we would have $\langle \mathfrak{a}, \Delta^{-1}\alpha' J\overline{\alpha}\rangle = \langle \overline{\mathfrak{a}}, \Delta^{-1}\overline{\alpha}' J\alpha\rangle$, that is we could find non-zero elements $\lambda, \mu \in \mathcal{R}$ such that $\lambda\mathfrak{a} = \mu\overline{\mathfrak{a}}$ and $\frac{\lambda\overline{\lambda}}{\Delta}\alpha' J\overline{\alpha} = \frac{\mu\overline{\mu}}{\Delta}\overline{\alpha}' J\alpha$. But this is impossible since $\alpha' J\overline{\alpha} = -\overline{\alpha}' J\alpha$. □

Let $\mathcal{C}_1$ be the set of integral ideal classes $\mathfrak{a}$ such that $\mathfrak{a}\overline{\mathfrak{a}}$ is a principal ideal,

$$\mathcal{C}_1 = \left\{\mathfrak{a} \in \mathcal{C} \mid \mathfrak{a}\overline{\mathfrak{a}} = (a) \text{ for some } a \in \mathcal{R}_m\right\}. \tag{3.17}$$

$\mathcal{C}_1$ is a subgroup of $\mathcal{C}$ and by definition $h_1 = |\mathcal{C}_1|$. 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 3.14. *Suppose ζ 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 [39].

Lemma 3.15. $\mathcal{C}_0 = \mathcal{C}_1$.

Proof. Suppose $\mathfrak{a}\overline{\mathfrak{a}} = (a_0)$ where $a_0 \in \mathcal{R}_m^*$. We need to find a unit $u \in U$ such that $ua_0 = \overline{ua_0}$. Let $u_0 = \frac{\overline{a}_0}{a_0}$. We see that u_0 is a unit because $(a_0) = (\overline{a}_0)$, and $u_0\overline{u}_0 = 1$. According to [39] $u_0 = \pm\zeta^k$, 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

$$a \equiv \overline{a} \pmod{1-\zeta^2} \tag{3.18}$$

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 $2k-1+m$ is even. By Lemma 3.14, 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 $\frac{\overline{(1-\zeta)a_0}}{(1-\zeta)a_0} = \zeta^{k-1} = \zeta^{2l}$, 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 $\mathfrak{a}\overline{\mathfrak{a}} \subset (1-\zeta)$ since $\mathfrak{a}\overline{\mathfrak{a}} = (a_0)$. So either $\mathfrak{a} \subset (1-\zeta)$ or $\overline{\mathfrak{a}} \subset (1-\zeta)$. Both cases are the same and imply $(a_0) \subset (1-\zeta)(1-\overline{\zeta})$. Let $a_1 = \frac{a_0}{(1-\zeta)(1-\overline{\zeta})}$. Then $a_1 \in \mathcal{R}_m^*$ and $u_0 = \frac{\overline{a}_1}{a_1}$. Continuing this procedure, there is $a \in \mathcal{R}_m^*$ with $a \notin (1-\zeta)$ such that $u_0 = \frac{\overline{a}}{a}$.

Now suppose $u_0 = -\zeta^k$. Then, by (3.18), $a \equiv \overline{a} = -\zeta^k a \equiv -a \pmod{1-\zeta}$, hence $2a \equiv 0 \pmod{1-\zeta}$. Since (2) is a prime ideal different from $(1-\zeta)$ we have $a \equiv 0 \pmod{1-\zeta}$, that is $a \in (1-\zeta)$. Contradiction.

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

In the case that $(1+\zeta)$ is a prime ideal of $\mathcal{R}_m$, 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 $a \in \mathcal{R}_m^*$, $\overline{a} \notin (1+\zeta)$, such that $u_0 = \frac{\overline{a}}{a}$.

Suppose $u_0 = \zeta^{2k+1}$. By (3.18) we have $\overline{a} = \zeta^{2l+1}a \equiv \zeta^{-(2l+1)}\overline{a} \pmod{1-\zeta^2}$. This implies $(\zeta-1)(\zeta^{2l}+\cdots+\zeta+1)\overline{a} \equiv 0 \pmod{1-\zeta^2}$, thus $(\zeta^{2l}+\cdots+\zeta+1)\overline{a} \equiv 0 \pmod{1+\zeta}$. We know that $\zeta^{2l}+\cdots+\zeta+1 \notin (1+\zeta)$, hence $\overline{a} \in (1+\zeta)$. Contradiction. $\square$

Now we want compute the index $[U^+ : C]$ of C in U^+, that is the order of U^+/C. Since for $m \equiv 2 \pmod 4$, $\mathcal{R}_m = \mathcal{R}_{\frac{m}{2}}$, we assume that $m \not\equiv 2 \pmod 4$. First, we quote some results of number theory (see [23] and [39]). Let $W = \{\pm\zeta_m^l\}$, a finite cyclic group consisting of the roots of 1 in $\mathcal{R}$.

Lemma 3.16 (Dirichlet). *The unit group U of $\mathcal{R}_m$ is the direct product $W \times V$, where V is a free abelian group of rank $\frac{\phi(m)}{2} - 1$.*

Lemma 3.17.

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

Lemma 3.18. *If m is not a prime power, then $1-\zeta_m \notin WU^+$ and $(1-\zeta_m)(1-\overline{\zeta}_m) \notin U^{+2}$.*

Proof. If there is an integer l such that $\zeta_m^l(1-\zeta_m) \in U^+$, then $(1-\zeta_m)(1-\overline{\zeta}_m) \in U^{+2}$. So we only need to show that $\frac{1-\zeta_m}{1-\overline{\zeta}_m} = -\zeta_m \notin U^2$. For this purpose we suppose $-\zeta_m \in U^2$. Then $-\zeta_m = \zeta_m^{2l}$ for some l, which implies $4l-2 \equiv 0 \pmod m$ and m is even. Since $m \not\equiv 2 \pmod 4$, we have $m \equiv 0 \pmod 4$. Thus $4l-2 \equiv 0 \pmod 4$, which is impossible. This completes the proof. $\square$

Lemma 3.19. *Let $k_m = [U^+ : C]$. Then*

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

Proof. By Lemma 3.16 and Lemma 3.17, 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 $[U^+ : U^{+2}] = 2^{\frac{\phi(m)}{2}}$.

If m is a prime power, then $C = U^{+2}$ (Lemma 3.17), 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 Lemma 3.17 and Lemma 3.18). We get $C = U^{+2} \cup (1-\zeta)(1-\overline{\zeta})U^{+2}$, which implies $[C : U^{+2}] = 2$. Thus $k_m = 2^{\frac{\phi(m)}{2}-1}$, since $[U^+ : U^{+2}] = [U^+ : C][C : U^{+2}]$. $\square$

This completes the proof of Theorem 4 (by applying Theorem 3).

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

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

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

Chapter 4
Symplectic Spaces

If a symplectic matrix X is decomposable, then its characteristic polynomial $f(x)$ is a reducible S-polynomial. In general, the converse is not true. In this section we want to find sufficient and necessary conditions for X to be decomposable. First, in Section 4.1 we introduce symplectic spaces and prove Theorem 5. In Section 4.2 we relate symplectic matrices to symplectic transformations and then prove Theorem 6. Finally, in Section 4.3 we shall discuss symplectic group spaces and prove Theorem 7. Some of the material in this chapter is known, see [12].

4.1 The Symplectic Spaces

We start with a definition:

Definition 4.1. Let V be a free $\mathcal{D}$-module with rank $2n$ and suppose there is a skew symmetric inner product $\langle\,,\,\rangle$ on it. V is called a symplectic space over $\mathcal{D}$ if there are $2n$ elements $v_1, \ldots, v_{2n}$ of V such that their inner product matrix

$$M(v_1, \ldots, v_{2n}) = \big(\langle v_i, v_j\rangle\big)_{2n\times 2n} = J. \tag{4.1}$$

The ordered elements $v_1, \ldots, v_{2n}$ form a symplectic basis of V. Two symplectic spaces are said to be isomorphic if there is a $\mathcal{D}$-module isomorphism σ which preserves their inner products. σ is called a symplectic isomorphism.

Example. Let S be a Riemann surface with genus $g \geq 1$. Then $H_1(S)$ with the intersection form is a symplectic space over $\mathbb{Z}$, with rank $2g$.

The following lemma says that a symplectic basis is a $\mathcal{D}$-basis.

Lemma 4.1. *Suppose V is a symplectic space over $\mathcal{D}$ with rank $2n$. Then every symplectic basis is a $\mathcal{D}$-basis of V.*

Proof. Suppose $v_1, \ldots, v_{2n}$ is a symplectic basis of V. If $w_1, \ldots, w_{2n}$ is a $\mathcal{D}$-basis of V, then

$$\begin{cases} v_1 = a_{1\,1}w_1 + \cdots + a_{1\,2n}w_{2n}, \\ v_2 = a_{2\,1}w_1 + \cdots + a_{2\,2n}w_{2n}, \\ \quad \cdots \\ v_{2n} = a_{2n\,1}w_1 + \cdots + a_{2n\,2n}w_{2n} \end{cases} \tag{4.2}$$

where $a_{ij} \in \mathcal{D}$ $(i, j = 1, \ldots, 2n)$. Let $A = \left(a_{ij}\right)$ be the coefficient matrix. It is obvious that

$$AM(w_1, \ldots, w_{2n})A' = M(v_1, \ldots, v_{2n}) = J.$$

Hence the determinant of A is a unit in $\mathcal{D}$, therefore $v_1, \ldots, v_{2n}$ is a $\mathcal{D}$-basis of V. □

Lemma 4.2. *Two symplectic spaces over $\mathcal{D}$ are isomorphic if and only if they have the same $\mathcal{D}$-ranks.*

Proof. The necessity is clear.

For sufficiency, suppose $v_1, \ldots, v_{2n}$ is a symplectic basis of V and $w_1, \ldots, w_{2n}$ is a symplectic basis of W. If we define $\sigma : V \to W$ by $\sigma(v_i) = w_i$ (for $i = 1, \ldots, 2n$), then σ is a symplectic isomorphism. □

Lemma 4.3. *Suppose two symplectic spaces V and W have the same $\mathcal{D}$-ranks. Then a $\mathcal{D}$-linear mapping $\sigma : V \to W$ which preserves inner products is a symplectic isomorphism.*

Proof. Let $v_1, \ldots, v_{2n}$ is a symplectic basis of V. Then

$$M\big(\sigma(v_1), \ldots, \sigma(v_{2n})\big) = M(v_1, \ldots, v_{2n}) = J.$$

By Lemma 4.1, $\sigma(v_1), \ldots, \sigma(v_{2n})$ is a basis of W. Hence σ is a $\mathcal{D}$-module isomorphism and therefore a symplectic isomorphism. □

Consider $\mathcal{D}^{2n}$, the $\mathcal{D}$-module of $2n$-tuple over $\mathcal{D}$. For any two column vectors $\alpha, \beta \in \mathcal{D}^{2n}$, we define a skew symmetric inner product on $\mathcal{D}^{2n}$ by $\langle \alpha, \beta \rangle = \alpha' J \beta$. It is easy to verify that $\mathcal{D}^{2n}$ with this inner product becomes a symplectic space, which we call the canonical symplectic space. Furthermore, if we put

$$e_i = (0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0)', \quad \text{for } i = 1, \ldots, 2n, \tag{4.3}$$

then $e_1, \ldots, e_{2n}$ is a symplectic basis of $\mathcal{D}^{2n}$, which we call the standard symplectic basis.

In this section, we always assume that V is a symplectic space over $\mathcal{D}$ with rank $2n$ and $v_1, \ldots, v_{2n}$ is a symplectic basis of V. Let $v,\ w \in V$, and

$$v = a_1 v_1 + \cdots + a_{2n} v_{2n} \quad \text{and} \quad w = b_1 v_1 + \cdots + b_{2n} v_{2n}. \tag{4.4}$$

We set $\alpha = (a_1, \ldots, a_{2n})'$ and $\beta = (b_1, \ldots, b_{2n})'$, the coordinate vectors of v and w under the basis $v_1, \ldots, v_{2n}$. Clearly, we have $\langle v, w \rangle = \alpha' J \beta$.

Suppose V_1, V_2 are $\mathcal{D}$-submodules of V. We use $V_1 \oplus V_2$ to denote the module sum $V_1 + V_2$ if $V_1 \cap V_2 = \{0\}$. V_1 and V_2 are said to be orthogonal, written as $V_1 \perp V_2$, if $\langle v_1, v_2 \rangle = 0$, for any elements $v_1 \in V_1$, $v_2 \in V_2$. Furthermore, suppose V_1, V_2 are symplectic subspaces of V. Then $V_1 \oplus V_2$ is called the symplectic direct sum of V_1 and V_2, denoted by $V_1 * V_2$.

Let $a_1, \ldots, a_k$ be elements of $\mathcal{D}$. It is convenient to denote any greatest common divisor of $a_1, \ldots, a_k$ by g.c.d$\,(a_1, \ldots, a_k)$. We know that g.c.d$\,(a_1, \ldots, a_k) = 1$ if and only if there exist $r_1, \ldots, r_k \in \mathcal{D}$ such that $r_1 a_1 + \cdots + r_k a_k = 1$. In this case, we say that $a_1, \ldots, a_k$ are relatively prime.

Definition 4.2. An element v ($v \neq 0$) of V is said to be primitive, if $v = c\, w$, where $c \in \mathcal{D}$ and $w \in V$, implies c is a unit in $\mathcal{D}$. Let $\alpha_1, \ldots, \alpha_k \in V$. We say that $\alpha_1, \ldots, \alpha_k$ are coprimitive if for any relatively prime elements $a_1, \ldots, a_k \in \mathcal{D}$, the linear combination $a_1\alpha_1 + \cdots + a_k\alpha_k$ is primitive. An ordered set of $l + k$ ($0 \leq k, l \leq n$) coprimitive elements $\alpha_1, \ldots, \alpha_l$, $\beta_1, \ldots, \beta_k$ is said to form an (l, k)-normal set if

$$\langle \alpha_i, \beta_j \rangle = \delta_{ij}, \quad \langle \alpha_i, \alpha_j \rangle = \langle \beta_i, \beta_j \rangle = 0, \tag{4.5}$$

for all possible i and j.

If $\alpha_1, \ldots, \alpha_l$, $\beta_1, \ldots, \beta_k$ form a (l,k)-normal set, then their inner product matrix is

$$M(\alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_k) = \begin{pmatrix} 0 & A \\ -A' & 0 \end{pmatrix} \tag{4.6}$$

where $A = (I_l, 0)$ or $\begin{pmatrix} I_k \\ 0 \end{pmatrix}$ depending on whether $l \leq k$ or $l \geq k$.

Remark. If $\alpha_1, \ldots, \alpha_k$ are coprimitive, then every α_i is primitive. Let $\alpha_1, \ldots, \alpha_{2n}$ be a $\mathcal{D}$-basis. Then $\alpha_1, \ldots, \alpha_{2n}$ are coprimitive. Thus an element of any $\mathcal{D}$-basis is primitive. A primitive element forms an $(1,0)$-normal set or a $(0,1)$-normal set. An ordered set of $2n$ elements is a symplectic basis if, and only if, it forms an (n,n)-normal set.

Lemma 4.4. *An element $v = a_1 v_1 + \cdots + a_{2n} v_{2n}$ is primitive if and only if the greatest common divisor* g.c.d $(a_1, \ldots, a_{2n}) = 1$.

Lemma 4.5. *Let $v \in V$ be primitive, $w \in V$ and a, b be non-zero elements in $\mathcal{D}$. If $aw = bv$, then $a \mid b$.*

Lemma 4.6. *Let $\alpha_1, \ldots, \alpha_k$ be coprimitive. Then $\alpha_1, \ldots, \alpha_k$ are independent and can be extended to a $\mathcal{D}$-basis of V.*

Proof. It is clear that $\alpha_1, \ldots, \alpha_k$ are independent.

To complete the proof we need to show that V/W, where W is the subspace generated by $\alpha_1, \ldots, \alpha_k$, is torsion free. Let v be a non-zero element in V and a be a non-zero element in $\mathcal{D}$. Suppose av is zero in V/W, that is $av \in W$. Then $av = a_1\alpha_1 + \cdots + a_k\alpha_k$ for some $a_1, \ldots, a_k \in \mathcal{D}$. Let g.c.d $(a_1, \ldots, a_k) = b$. We have $a_i = bc_i$, where $c_i \in \mathcal{D}$ and g.c.d $(c_1, \ldots, c_k) = 1$. Then $av = b(c_1\alpha_1 + \cdots + c_k\alpha_k)$ and $c_1\alpha_1 + \cdots + c_k\alpha_k$ is primitive. Hence $a \mid b$ and therefore $v \in W$. $\square$

Lemma 4.7. *An element v is primitive if, and only if there is an element $w \in V$ such that $\langle v, w \rangle = 1$, that is v, w form an $(1,1)$-normal set.*

Proof. By Lemma 4.4, if v is primitive then g.c.d $(a_1, \ldots, a_{2n}) = 1$. There are $c_1, \ldots, c_{2n} \in \mathcal{D}$ such that $\sum_{i=1}^{2n} a_i c_i = 1$. Let w be an element of V such that the coefficient vector of w is $\beta = -J\gamma$, where $\gamma = (c_1, \ldots, c_{2n})'$. Then $\langle v, w \rangle = \alpha' J(-J\gamma) = \alpha'\gamma = 1$.

The converse is clear. □

Lemma 4.8. *If W is $\mathcal{D}$-module summand of V, then there is a primitive element w in W.*

Proof. This is because every $\mathcal{D}$-basis of W can be extended to a $\mathcal{D}$-basis of V. □

Proposition 4.1. *If $V = V_1 + V_2$ and $V_1 \perp V_2$, then $V = V_1 * V_2$.*

Proof. First, we prove that $V_1 \cap V_2 = \{0\}$. Let $v \in V_1 \cap V_2$. Then for any $w = w_1 + w_2$, where $w_1 \in V_1$ and $w_2 \in V_2$, we have $\langle v, w \rangle = \langle v, w_1 \rangle + \langle v, w_2 \rangle = 0$. Hence $v = 0$, that is $V = V_1 \oplus V_2$.

Now we prove that V_1 is a symplectic subspace of V by induction on rank (V_1), the rank of V_1. If rank $(V_1) = 1$, then $V_1 \perp V_1$, and so $V_1 \perp V$. Thus $V_1 = \{0\}$, this is contrary to rank $(V_1) = 1$. Hence rank $(V_1) = 1$ is impossible. Suppose rank $(V_1) \geq 2$. Since $V_1 \perp V_2$, there are two primitive elements w_1, w_2 of V_1 such that $\langle w_1, w_2 \rangle = 1$ (by Lemma 4.8 and Lemma 4.7). Let W be the symplectic subspace generated by w_1 and w_2. If rank $(V_1) = 2$, we see that $V_1 = W$ is a symplectic space. Suppose rank $(V_1) > 2$. We let $U = \{v \in V_1 \mid \langle v, w \rangle = 0 \text{ for } w \in W\}$. If $v \in V_1$, then $v - \langle v, w_2 \rangle w_1 + \langle v, w_1 \rangle w_2 \in U$. We see that $V_1 = U + W$. By the same argument as above, $V_1 = W \oplus U$. Thus $V = U \oplus (W \oplus V_2)$. Also $U \perp (W + V_2)$ and rank $(U) =$ rank $(V_1) - 2$ by the definition of U. By induction, U is a symplectic subspace, and therefore $V_1 = W * U$ is a symplectic subspace too.

By the same reasoning, V_2 is a symplectic space. □

Corollary 4.1. *Suppose $V_1, \ldots, V_m$ are subspaces of V with*

1. $V = V_1 + \cdots + V_m$,

2. $V_i \perp V_j$ *for* $i \neq j$.

Then $V = V_1 * \cdots * V_m$.

Lemma 4.9. *Let* $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_k, \gamma_0$, $\gamma_1, \ldots, \gamma_l$ *be a* $\mathcal{D}$*-basis of* V *such that* $\langle \alpha_i, \beta_j \rangle = \delta_{ij}$ *and* $\langle \alpha_i, \alpha_j \rangle = \langle \alpha_i, \gamma_j \rangle = 0$. *Then* $\text{g.c.d}\left(\langle \gamma_0, \gamma_1 \rangle, \ldots, \langle \gamma_0, \gamma_l \rangle\right) = 1$.

Proof. Suppose there is a non-unit $c \in D$ such that

$$c \,|\, \langle \gamma_0, \gamma_j \rangle, \quad \text{for } j = 1, \ldots, l. \tag{4.7}$$

Let $\gamma = \gamma_0 - \langle \gamma_0, \beta_1 \rangle \alpha_1 - \cdots - \langle \gamma_0, \beta_k \rangle \alpha_k$. Then γ is primitive since γ_0 is primitive and γ_0, $\alpha_1, \ldots, \alpha_k$ are independent over $\mathcal{D}$. Any $v \in V$ can be expressed by

$$v = \sum_{i=1}^{k} \left(a_i \alpha_i + b_i \beta_i\right) + \sum_{j=0}^{l} c_j \gamma_j$$

where $a_i, b_i, c_j \in \mathcal{D}$. Hence

$$\begin{aligned}
\langle \gamma, v \rangle &= \langle \gamma_0 - \sum_{i=1}^{k} \langle \gamma_0, \beta_i \rangle \alpha_i, \sum_{i=1}^{k} \left(a_i \alpha_i + b_i \beta_i\right) + \sum_{j=0}^{l} c_j \gamma_j \rangle \\
&= \sum_{j=1}^{k} b_j \langle \gamma_0, \beta_j \rangle + \sum_{j=1}^{l} c_j \langle \gamma_0, \gamma_j \rangle - \sum_{i=1}^{k} \sum_{j=1}^{k} b_j \langle \gamma_0, \beta_i \rangle \langle \alpha_i, \beta_j \rangle \\
&= c_1 \langle \gamma_0, \gamma_1 \rangle + \cdots + c_l \langle \gamma_0, \gamma_l \rangle
\end{aligned}$$

which implies $c \,|\, \langle \gamma, v \rangle$ by (4.7). This is contrary to Lemma 4.7. □

Lemma 4.10. *Let* $\alpha_1, \ldots, \alpha_l$ *be an* $(l, 0)$*-normal set of* V. *Then for any* $0 \leq k \leq l$, *there are* $\beta_1, \ldots, \beta_k$, $\gamma_1, \ldots, \gamma_m$, *where* $m = 2n - k - l$, *in* V *such that*

1. $\alpha_1, \ldots, \alpha_l$, $\beta_1, \ldots, \beta_k$, $\gamma_1, \ldots, \gamma_m$ *is a* $\mathcal{D}$*-basis of* V

2. $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_k$ *form a* (k, k)*-normal set.*

Proof. We prove this lemma by induction on k.

For $k = 0$ it is obvious (by Lemma 4.6).

Suppose it is true for $k-1$. We have elements $\beta_1, \dots, \beta_{k-1}$, $\gamma_1, \dots, \gamma_{m+1}$ satisfying these two conditions. Set

$$\gamma_1' = \gamma_1 - \sum_{j=1}^{k-1} \langle \alpha_j, \gamma_1 \rangle \beta_j + \sum_{j=1}^{k-1} \langle \beta_j, \gamma_1 \rangle \alpha_j,$$
$$\gamma_2' = \gamma_2 - \sum_{j=1}^{k-1} \langle \alpha_j, \gamma_2 \rangle \beta_j + \sum_{j=1}^{k-1} \langle \beta_j, \gamma_2 \rangle \alpha_j,$$
$$\dots \quad \dots$$
$$\gamma_{m+1}' = \gamma_{m+1} - \sum_{j=1}^{k-1} \langle \alpha_j, \gamma_{m+1} \rangle \beta_j + \sum_{j=1}^{k-1} \langle \beta_j, \gamma_{m+1} \rangle \alpha_j.$$

We have

$$\langle \alpha_i, \gamma_j' \rangle = 0 \quad \text{and} \quad \langle \beta_i, \gamma_j' \rangle = 0 \tag{4.8}$$

for $i = 1, \dots, k-1$ and $j = 1, \dots, m+1$. Applying Lemma 4.9 to $\alpha_1, \dots, \alpha_{k-1}$, $\beta_1, \dots, \beta_{k-1}$, $\alpha_k, \dots, \alpha_l$, $\gamma_1', \dots, \gamma_{m+1}'$, we see that there are $c_1, \dots, c_{m+1}$ in $\mathcal{D}$ such that

$$c_1 \langle \alpha_k, \gamma_1' \rangle + \dots + c_{m+1} \langle \alpha_k, \gamma_{m+1}' \rangle = 1. \tag{4.9}$$

Note that here we use the fact $\langle \alpha_k, \alpha_j \rangle = 0$ for $j = 1, \dots, l$.

Now we can find a unit matrix $A = (a_{ij})$ in $GL_{m+1}(\mathcal{D})$ with $c_1, \dots, c_{m+1}$ as its first row, see [26]. Let

$$\begin{aligned}
\beta_k &= c_1 \gamma_1' + \dots + c_{m+1} \gamma_{m+1}', \\
\gamma_1'' &= a_{21} \gamma_1' + \dots + a_{2m+1} \gamma_{m+1}', \\
\dots & \quad \dots \quad \dots \\
\gamma_m'' &= a_{m+11} \gamma_1' + \dots + a_{m+1m+1} \gamma_{m+1}'.
\end{aligned}$$

Clearly, $\alpha_1, \dots, \alpha_l$, $\beta_1, \dots, \beta_k$, $\gamma_1'', \dots, \gamma_m''$ forms a $\mathcal{D}$-basis of V. Furthermore, let

$$\begin{aligned}
\beta_1' &= \beta_1 - \langle \alpha_k, \beta_1 \rangle \beta_k, \\
\dots & \quad \dots
\end{aligned}$$

$$
\begin{aligned}
\beta'_{k-1} &= \beta_{k-1} - \langle \alpha_k, \beta_{k-1} \rangle \beta_k, \\
\beta'_k &= \beta_k.
\end{aligned}
$$

Then $\alpha_1, \dots, \alpha_l$, $\beta'_1, \dots, \beta'_k$, $\gamma''_1, \dots, \gamma''_m$ is also a $\mathcal{D}$-basis of V. We shall verify that $\alpha_1, \dots, \alpha_k$, $\beta'_1, \dots, \beta'_k$ form a (k, k)-normal set by using (4.8) and (4.9)

Case 1. For $i, j = 1, \dots, k-1$,

$$
\begin{aligned}
\langle \alpha_i, \beta'_j \rangle &= \langle \alpha_i, \beta_j - \langle \alpha_k, \beta_j \rangle \beta_k \rangle = \langle \alpha_i, \beta_j \rangle - \langle \alpha_k, \beta_j \rangle \langle \alpha_i, \beta_k \rangle \\
&= \langle \alpha_i, \beta_j \rangle - \langle \alpha_k, \beta_j \rangle \sum_{s=1}^{m+1} c_s \langle \alpha_i, \gamma'_s \rangle = \langle \alpha_i, \beta_j \rangle = \delta_{ij}.
\end{aligned}
$$

Case 2. For $i = 1, \dots, k$, $j = k$,

$$
\langle \alpha_i, \beta'_k \rangle = \langle \alpha_i, \beta_k \rangle = \sum_{s=1}^{m+1} c_s \langle \alpha_i, \gamma'_s \rangle = \delta_{ik}.
$$

Case 3. For $i = k$, $j = 1, \dots, k-1$,

$$
\langle \alpha_k, \beta'_j \rangle = \langle \alpha_k, \beta_j \rangle - \langle \alpha_k, \beta_j \rangle \langle \alpha_k, \beta_k \rangle = 0.
$$

Case 4. For $j = 1, \dots, k-1$,

$$
\langle \beta'_j, \beta'_k \rangle = \langle \beta_j - \langle \alpha_k, \beta_j \rangle \beta_k, \beta_k \rangle = \langle \beta_j, \beta_k \rangle = \sum_{s=1}^{m+1} c_s \langle \beta_j, \gamma'_s \rangle = 0.
$$

This completes the proof. $\square$

Proof of Theorem 5. Without loss of generality we can assume that $k \le l$. Let V_1 be the symplectic subspace generated by $\alpha_1, \dots, \alpha_k$, $\beta_1, \dots, \beta_k$, and $V_2 = V_1^{\perp}$.

If $v \in V$, let

$$
w = v - \sum_{i=1}^{k} \langle v, \beta_i \rangle \alpha_i + \sum_{i=1}^{k} \langle v, \alpha_i \rangle \beta_i.
$$

It is easy to see that $w \in V_2$. Hence $V = V_1 + V_2$. By Proposition 4.1, we see that V_2 is a symplectic subspace and $V = V_1 * V_2$.

If $k < l$, then $\alpha_{k+1}, \dots, \alpha_l$ form a $(l-k, 0)$-normal set of V_2. By Lemma 4.10 we can find $\beta_{k+1}, \dots, \beta_l$ in V_2 such that $\alpha_{k+1}, \dots, \alpha_l$, $\beta_{k+1}, \dots, \beta_l$ form a $(l-k, l-k)$-normal set. Then $\alpha_1, \dots, \alpha_l$, $\beta_1, \dots, \beta_l$ form an (l, l)-normal set. So we can suppose $k = l$.

If $k = l$ then a combination of $\alpha_1, \dots, \alpha_k$, $\beta_1, \dots, \beta_k$ and a symplectic basis of V_2 is a symplectic basis of V. □

Remark. This theorem gives another way to prove that every normal array can be completed to a matrix in $SP_{2n}(\mathcal{D})$, see [29].

4.2 Symplectic Transformations

Definition 4.3. A linear transformation σ of a symplectic space V is called a symplectic transformation if it preserves the inner product.

A symplectic transformation σ is reducible if there is a non-trivial σ-invariant subspace of V; otherwise it is called irreducible. A symplectic transformation σ is decomposable if V can be decomposed as a symplectic direct sum of two non-zero symplectic σ-invariant subspaces; otherwise it is indecomposable.

Remark. It is easy to see that every symplectic transformation maps a (k, l)-normal set to a (k, l)-normal set. Thus a symplectic transformation is a $\mathcal{D}$-module isomorphism.

Clearly, a decomposable symplectic transformation must be reducible. Now we shall see that the converse is also true.

Lemma 4.11. *A symplectic transformation is decomposable if, and only if it is reducible.*

Proof. Suppose V_1 is a non-trivial σ-invariant symplectic subspace. Then $\sigma(V_1) = V_1$. By Theorem 5, there is a non-trivial subspace V_2, such that $V = V_1 * V_2$. V_2 is σ-invariant since $\langle \sigma(V_1), \sigma(V_2) \rangle = \langle V_1, V_2 \rangle = 0$, □

Let σ be a linear transformation of V and X be the matrix of σ with respect to a symplectic basis $v_1, \ldots, v_{2n}$, i.e.

$$\sigma(v_1, \ldots, v_{2n}) = \big(\sigma(v_1), \ldots, \sigma(v_{2n})\big) = (v_1, \ldots, v_{2n})X. \tag{4.10}$$

We know that the inner product matrix of $\sigma(v_1), \ldots, \sigma(v_{2n})$ is $M\big(\sigma(v_1), \ldots, \sigma(v_{2n})\big) = X'JX$. Hence σ is a symplectic transformation if and only if $X \in SP_{2n}(\mathcal{D})$. Suppose σ is a symplectic transformation. Let $v_1, \ldots, v_{2n}$ and $w_1, \ldots, w_{2n}$ be two symplectic bases of V. Then there is a symplectic matrix $Q \in SP_{2n}(\mathcal{D})$ such that $(w_1, \ldots, w_{2n}) = (v_1, \ldots, v_{2n})Q$. Let X and Y be the symplectic matrices of σ with respect to the bases $v_1, \ldots, v_{2n}$ and $w_1, \ldots, w_{2n}$. A simple calculation tells us $Y = Q^{-1}XQ$, that is $X \sim Y$.

Proposition 4.2. *Suppose σ is a symplectic transformation of V. Then σ is decomposable if and only if X is decomposable. Furthermore, suppose $V_1, \ldots, V_m$ are σ-invariant symplectic subspaces of V, and $V = V_1 * \cdots * V_m$. Then $X \sim X_1 * \cdots * X_m$ where $X_1, \ldots, X_m$ are the matrices of $\sigma|V_1, \ldots, \sigma|V_m$ respectively.*

Proof. Let $\operatorname{rank}(V_i) = 2n_i$, and $\alpha_{i1}, \ldots, \alpha_{in_i}, \beta_{i1}, \ldots, \beta_{in_i}$ be a symplectic basis of V_i. Let X_i be the matrix of $\sigma|V_i$ with respect to the basis $\alpha_{i1}, \ldots, \alpha_{in_i}, \beta_{i1}, \ldots, \beta_{in_i}$. We see that

$$\alpha_{11}, \ldots, \alpha_{1n_1}, \beta_{11}, \ldots, \beta_{1n_1}, \ldots, \alpha_{m1}, \ldots, \alpha_{mn_m}, \beta_{m1}, \ldots, \beta_{mn_m} \tag{4.11}$$

is a symplectic basis of V, and the matrix of σ with respect to the basis (4.11) is $X_1 * \cdots * X_m$.

For the converse, we assume that $X = X_1 * \cdots * X_m$. Let V_i be the subspace generated by $(v_1, \ldots, v_{2n})[0 * \cdots * X_i * \cdots * 0]$. It is easy to see that V_i is a σ-invariant symplectic subspace of V and $V_1 + \cdots + V_m = V$. Thus $V = V_1 * \cdots * V_m$. $\square$

Lemma 4.12. *Let σ be a symplectic transformation of V, let $p(x)$, $q(x) \in \mathcal{D}[x]$ be mutually coprime polynomials, and let one of them be an S-polynomial. If $\alpha, \beta \in V$ are such that $p(\sigma)(\alpha) = 0$ and $q(\sigma)(\beta) = 0$, then $\langle \alpha, \beta \rangle = 0$.*

Proof. Without lost of generality we assume that $q(x)$ is an S-polynomial. There are two polynomials $u(x), v(x) \in \mathcal{D}[x]$ such that $u(x)p(x) + v(x)q(x) = c$, where $c \in \mathcal{D}$, $c \neq 0$. Then

$c\ \alpha = v(\sigma)q(\sigma)(\alpha)$, and

$$c\ \langle \alpha, \beta \rangle = \langle v(\sigma)q(\sigma)(\alpha), \beta \rangle = \langle v(\sigma)(\alpha), q(\sigma^{-1})(\beta) \rangle = \langle v(\sigma)(\alpha), 0 \rangle = 0$$

since $q(\sigma)(\beta) = 0$, and $q(\sigma^{-1}) = \sigma^{-2m} q(\sigma)$, where m is the degree of $q(x)$. Here we use the fact $\langle \sigma(\alpha), \beta \rangle = \langle \alpha, \sigma^{-1}(\beta) \rangle$. $\square$

Let V be the canonical symplectic space $\mathcal{D}^{2n}$. Given any $X \in SP_{2n}(\mathcal{D})$, we can define a symplectic transformation σ as follows,

$$\sigma(\alpha) = X\alpha \quad \left(\text{for } \alpha \in \mathcal{D}^{2n}\right).$$

It is well known that the matrix of σ with respect to the standard basis $e_1, \ldots, e_{2n}$ is X.

Corollary 4.2. *Let $\mathcal{K}$ be an extension field of $\mathcal{F}$ and λ, $\mu \in \mathcal{K}$ with $\lambda \neq \mu$ and $\lambda\mu \neq 1$. If $X \in SP_{2n}(\mathcal{K})$ and α, $\beta \in \mathcal{K}^{2n}$ are such that*

$$(X - \lambda I)^r \alpha = 0 \quad \textit{and} \quad (X - \mu I)^s \beta = 0,$$

for some integers r, s, then $\alpha' J \beta = 0$.

Proof. We apply Lemma 4.12 to X. Note that $(x - \lambda)^r$ and $(x - \mu)^s (x - \frac{1}{\mu})^s$ are mutually coprime, and the latter is an S-polynomial. $\square$

Now we are ready to complete the proof of Theorem 6.

Proof of Theorem 6. Suppose $f(x)$ is a reducible S-polynomial and

$$f(x) = \prod_{i=1}^{m} p_i(x)$$

where $p_1(x), \ldots, p_m(x)$ are mutually coprime S-polynomials. Let $q_i(x) = f(x)/p_i(x)$. There are m polynomials, $u_1(x), \ldots, u_m(x) \in \mathcal{F}[x]$, such that

$$u_1(x)q_1(x) + \cdots + u_m(x)q_m(x) = 1. \tag{4.12}$$

Suppose $X \sim X_1 * \cdots * X_m$, where $X_i \in M_{p_i}$ (for $i = 1, \ldots, m$). There is $Q \in SP_{2n}(\mathcal{D})$ such that $X = Q^{-1}(X_1 * \cdots * X_m)Q$. Then $g(X) = Q^{-1}[g(X_1) * \cdots * g(X_m)]Q$, for any polynomial $g(x)$. By (4.12) and the fact that $p_i(X_i) = 0$ (for $i = 1, \ldots, m$), we obtain

$$u_i(X_j)q_i(X_j) = \begin{cases} I, & i = j, \\ 0, & i \neq j. \end{cases}$$

Hence $u_i(X)q_i(X) = Q^{-1}[0 * \cdots * \overset{i}{I} * \cdots * 0]Q \in M_{2n}(\mathcal{D})$.

For the converse, we regard X as the symplectic transformation $\alpha \to X\alpha$ of the canonical symplectic space $\mathcal{D}^{2n}$. Let

$$V_i = u_i(X)q_i(X)\left(\mathcal{D}^{2n}\right) \quad \text{for } i = 1, \ldots, m. \tag{4.13}$$

Then for each $1 \leq i \leq m$, we have

1. V_i is submodule of $\mathcal{D}^{2n}$, because $u_i(X)q_i(X) \in M_{2n}(D)$;

2. V_i is X-invariant, for $X(V_i) = X\left(u_i(X)q_i(X)\left(\mathcal{D}^{2n}\right)\right) = u_i(X)q_i(X)\left(X\left(\mathcal{D}^{2n}\right)\right) = V_i$;

3. $\mathcal{D}^{2n} = V_1 + \cdots + V_m$, for $\sum u_i(X)q_i(X) = I$;

4. $V_i \perp V_j$ $(i \neq j)$, by Lemma 4.12 and $p_i(X)V_i = \{0\}$.

Applying Proposition 4.2, we can complete the proof. □

Corollary 4.3. *Suppose $f(x)$ and $g(x)$ are strictly coprime S-polynomials, and $X \in M_{fg}$. Then X is decomposable.*

Example. Consider the case $D = \mathbb{Z}$. Let

$$X_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} \quad \text{and} \quad X_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & -1 & 0 \end{pmatrix}.$$

$X_1, X_2 \in SP_4(\mathbb{Z})$, and $f_{X_1}(x) = f_{X_2}(x) = (x^2+x+1)(x^2-x+1)$. We know that

$$\tfrac{1}{2}(x+1)(x^2-x+1) - \tfrac{1}{2}(x-1)(x^2+x+1) = 1.$$

Clearly, X_1 is decomposable and $\frac{1}{2}(X_1+I)(X_1^2-X_1+I) \in M_4(\mathbb{Z})$. But X_2 is indecomposable, since $\frac{1}{2}(X_2+I)(X_2^2-X_2+I) \notin M_4(\mathbb{Z})$.

Example. Let $f(x) = (x^2+1)(x^2 \pm x + 1)$. Any $X \in M_f$ is decomposable, since

$$(x \pm 1)(x^2+1) - x(x^2 \pm x + 1) = \pm 1.$$

4.3 Symplectic Group Spaces

Definition 4.4. Given a group G, a symplectic space V is called a symplectic G-space, or G-space, if G acts on V and every element of G preserves the inner product.

Relative to a symplectic basis, V affords a symplectic representation of G. Let G be the cyclic group G_m, generated by a fixed element g of order m, where m is a finite integer or infinity. To specify a G_m-space V, it suffices to give a symplectic matrix X. The characteristic polynomial of X is independent of the representation, we call it the characteristic polynomial of the G_m-space. The set of all symplectic G_m-spaces with characteristic polynomial $f(x)$ is denoted by V_f.

Definition 4.5. Two G-spaces V and W are equivalent, denoted by $V \cong W$, if there is a symplectic isomorphism $\sigma : V \to W$ such that the diagram

$$\begin{array}{ccc} G \times V & \longrightarrow & V \\ \big\downarrow{\scriptstyle id\times\sigma} & & \big\downarrow{\scriptstyle \sigma} \\ G \times W & \longrightarrow & W \end{array}$$

is commutative, that is $\sigma(g \circ v) = g \circ (\sigma(v))$.

Remark. Let $\mathcal{V}_f$ denote the set of equivalence classes in V_f. We have a natural one-to-one correspondence Σ, defined as above, between $\mathcal{V}_f$ and $\mathcal{M}_f$.

A G-space is decomposable if it is expressible as a symplectic direct sum of two non-zero G-subspaces; otherwise, it is indecomposable. A G-space is reducible if it contains a non-zero G-subspace of smaller rank. A non-zero G-space which is not reducible is called irreducible.

An analogue of Lemma 4.11 is

Proposition 4.3. *V is decomposable if and only if it is reducible.*

Example. If we have a group G acting on a Riemann surface S, then $H_1(S)$ is a symplectic G-space by passing the action to homology.

Suppose $f(x)$ is an S-polynomial of type-I, and ζ is a fixed root. Given any S-pair $(\mathfrak{a}, a) \in P_f$ (cf. Section 3.3), we know that $\mathfrak{a}$ is a $\mathcal{D}$-module since it is an ideal. We define a skew symmetric inner product as follows,

$$\langle \alpha, \beta \rangle = \mathrm{Tr}\left(\frac{1}{a\Delta}\alpha\widetilde{\beta}\right).$$

Let m = order of ζ. We define the action of G_m on $\mathfrak{a}$ by $g \circ x = x/\zeta$, for all $x \in \mathfrak{a}$. Note that $\widetilde{\mathfrak{a}} = a\Delta\mathfrak{a}'$. Let $\alpha = (\alpha_1, \ldots, \alpha_{2n})'$, where $\alpha_1, \ldots, \alpha_{2n}$ is a J-orthogonal basis of $\mathfrak{a}$ with respect to a. Then the components of $\frac{1}{a\Delta}J\widetilde{\alpha}$ form the dual basis of $\alpha_1, \ldots, \alpha_{2n}$. This means the matrix $\mathrm{Tr}\left(\frac{\alpha\widetilde{\alpha}'}{a\Delta}J'\right)$ is the identity matrix. On the other hand, $\mathrm{Tr}\left(\frac{\alpha\widetilde{\alpha}'}{a\Delta}J'\right) = \mathrm{Tr}\left(\frac{\alpha\widetilde{\alpha}'}{a\Delta}\right)J'$, hence $\mathrm{Tr}\left(\frac{\alpha\widetilde{\alpha}'}{a\Delta}\right) = J'^{-1} = J$. Therefore we obtain a symplectic space, denoted by $[\mathfrak{a}, a]$, and $\alpha_1, \ldots, \alpha_{2n}$ is a symplectic basis. Also, it is easy to verify that g preserves the inner product and its characteristic polynomial is $f(x)$. We have $[\mathfrak{a}, a] \in V_f$.

Before we prove the Theorem 7, we give the following lemmas,

Lemma 4.13. *If $\mathrm{Tr}(ax) = \mathrm{Tr}(bx)$ for all $x \in \mathfrak{a}$, then $a = b$.*

Proof. Tr is additive, so we only prove the special case where $b = 0$. Let $x_1, \ldots, x_{2n}$ be a $\mathcal{D}$-basis of $\mathfrak{a}$. We obtain a system of $2n$ equations in the $a^{(i)}$'s,

$$a^{(1)}x_1^{(1)} + \cdots + a^{(2n)}x_1^{(2n)} = 0,$$
$$a^{(1)}x_2^{(1)} + \cdots + a^{(2n)}x_2^{(2n)} = 0,$$

$$\cdots$$

$$a^{(1)}x_{2n}^{(1)} + \cdots + a^{(2n)}x_{2n}^{(2n)} = 0,$$

which only has the 0 solution. Hence $a^{(1)} = \cdots = a^{(2n)} = 0$, so $a = 0$. $\square$

Lemma 4.14. *Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathcal{R}$, and $\sigma : \mathfrak{a} \to \mathfrak{b}$ is a $\mathcal{D}$-linear mapping with $\sigma(g \circ x) = g \circ \sigma(x)$. Then there is a unique element q of $\mathcal{S}$ such that*

$$\sigma(x) = qx \quad \textit{for all } x \in \mathfrak{a}. \tag{4.14}$$

Proof. First note that σ is $\mathcal{R}$-linear. To prove this we write any element α of $\mathcal{R}$ as a $\mathcal{D}$-linear combination of $1, 1/\zeta, 1/\zeta^2, \ldots, 1/\zeta^{2n-1}$. It is easy to verify that $\sigma(\alpha x) = \alpha\sigma(x)$.

Let $\alpha_0 \in \mathfrak{a}$. Then $\alpha_0\sigma(x) = \sigma(\alpha_0 x) = \sigma(\alpha_0)x$. Set $q = \sigma(\alpha_0)/\alpha_0$, we see that (4.14) is true. $\square$

Proof of Theorem 7. Suppose σ is an symplectic isomorphism from the symplectic G_m-space $[\mathfrak{a}_1, a_1] * \cdots * [\mathfrak{a}_r, a_r]$ to $[\mathfrak{b}_1, b_1] * \cdots * [\mathfrak{b}_s, b_s]$. Thus there is an $r \times s$ matrix $Q = (q_{ij})$ with entries in $\mathcal{S}$ so that

$$\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_s \end{pmatrix} = Q \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix},$$

for all $(x_1, \ldots, x_r)' \in \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$, and $(y_1, \ldots, y_s)' \in \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$. Since σ is an isomorphism, Q has an inverse, and hence $r = s$. If we choose all $x_1, \ldots, x_r$ to be zero except x_j, we obtain $q_{ij}x_j \in \mathfrak{b}_i$. Thus $q_{ij}\mathfrak{a}_j \subset \mathfrak{b}_i$ for $i, j = 1, \ldots, r$.

If $\alpha = (\alpha_1, \ldots, \alpha_r)'$ and $\beta = (\beta_1, \ldots, \beta_r)'$ are in $[\mathfrak{a}_1, a_1] * \cdots * [\mathfrak{a}_r, a_r]$, then

$$\langle \alpha, \beta \rangle = \sum_{i=1}^{r} \langle \alpha_i, \beta_i \rangle = \mathrm{Tr} \left(\frac{1}{\Delta} \alpha' \begin{pmatrix} \frac{1}{a_1} & & \\ & \ddots & \\ & & \frac{1}{a_r} \end{pmatrix} \widetilde{\beta} \right), \tag{4.15}$$

and similarly

$$\langle \sigma(\alpha), \sigma(\beta) \rangle = \operatorname{Tr}\left(\frac{1}{\Delta}\alpha' Q' \begin{pmatrix} \frac{1}{b_1} & & \\ & \ddots & \\ & & \frac{1}{b_s} \end{pmatrix} \widetilde{Q}\widetilde{\beta} \right). \tag{4.16}$$

Comparing each entry of (4.15) to (4.16), and using Lemma 4.13, we complete the proof of the first half.

To prove the second half, we define σ by

$$\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = Q \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}.$$

σ is a $\mathcal{D}$-linear mapping from $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ to $\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_r$ and preserves the inner product, hence σ is isomorphism by Lemma 4.3. $\square$

Corollary 4.4. *If* $[\mathfrak{a}_1, a_1] * \cdots * [\mathfrak{a}_r, a_r] \cong [\mathfrak{b}_1, b_1] * \cdots * [\mathfrak{b}_r, b_r]$, *then*

$$\langle \mathfrak{a}_1 \cdots \mathfrak{a}_r, a_1 \cdots a_r \rangle = \langle \mathfrak{b}_1 \cdots \mathfrak{b}_r, b_1 \cdots b_r \rangle.$$

Proof. For each generator $a_1 \cdots a_r$ of $\mathfrak{a}_1 \cdots \mathfrak{a}_r$, the product $(\det Q) a_1 \cdots a_r$ can be expressed as the determinant of the product matrix

$$Q \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_r \end{pmatrix}$$

whose i-th row consists completely of elements $q_{ij}a_j$ of $\mathfrak{b}_i$. This proves that

$$(\det Q)\mathfrak{a}_1 \cdots \mathfrak{a}_r \subset \mathfrak{b}_1 \cdots \mathfrak{b}_r.$$

A similar argument shows that

$$(\det Q^{-1})\mathfrak{b}_1 \cdots \mathfrak{b}_r \subset \mathfrak{a}_1 \cdots \mathfrak{a}_r.$$

Multiplying this last inclusion by $\det Q$ and comparing, it follows that $\mathfrak{b}_1 \cdots \mathfrak{b}_r$ is equal to $(\det Q)\mathfrak{a}_1 \cdots \mathfrak{a}_r$; and it is easy to verify that $b_1 \cdots b_r = (\det Q)(\det \widetilde{Q}) a_1 \cdots a_r$. This completes the proof. $\square$

Now we give some applications of Theorem 7. When $r = 1$, we have

Corollary 4.5. $[\mathfrak{a}, a] \cong [\mathfrak{b}, b]$ *if, and only if* $\langle \mathfrak{a}, a \rangle = \langle \mathfrak{b}, b \rangle$.

Proof. By Theorem 7, $[\mathfrak{a}, a] \cong [\mathfrak{b}, b]$ if and only if there is $\lambda \in \mathcal{S}$ such that $\lambda\mathfrak{a} \subset \mathfrak{b}$ and $b = \lambda\widetilde{\lambda}a$, which is equivalent to $\langle \mathfrak{a}, a \rangle = \langle \mathfrak{b}, b \rangle$. $\square$

From this corollary, we obtain a natural injective correspondence $\Phi : \langle \mathfrak{a}, a \rangle \to [\mathfrak{a}, a]$ from $\mathcal{P}_f$ to $\mathcal{V}_f$. The following lemma says Φ is surjective.

Lemma 4.15. *For any* $V \in V_f$*, there is an S-pair* $(\mathfrak{a}, a) \in \mathcal{P}_f$ *such that* $V \cong [\mathfrak{a}, a]$.

Proof. Let $v_1, \ldots, v_{2n}$ be a symplectic basis of V. The action of g on V has a representative $X \in SP_{2n}(\mathcal{D})$. We choose $(\mathfrak{a}, a) \in \mathcal{P}_f$ such that $\Psi(X'^{-1}) = \langle \mathfrak{a}, a \rangle$. Suppose

$$X'^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_{2n} \end{pmatrix} = \zeta \begin{pmatrix} x_1 \\ \vdots \\ x_{2n} \end{pmatrix},$$

where $x_1, \ldots, x_{2n}$ is a J-orthogonal basis with respect to $(\mathfrak{a}, a)$. We define the isomorphism $\phi : V \to \mathfrak{a}$ by $\phi(v_j) = x_j$. It follows that $\langle x_i, x_j \rangle = \operatorname{Tr}\left(\frac{1}{a\Delta} x_i \widetilde{x}_j\right) = \delta_{ij} = \langle v_i, v_j \rangle$. That is, ϕ preserves the inner product. $\square$

Furthermore, we have one-to-one correspondences Ψ between $\mathcal{M}_f$ and $\mathcal{P}_f$ and Σ between $\mathcal{V}_f$ and $\mathcal{M}_f$. More precisely, we have

Proposition 4.4. *The correspondence* $\Psi \circ \Sigma \circ \Phi$ *is the identity of* $\mathcal{P}_f$.

Proof. Let $(\mathfrak{a}, a) \in P_f$, and $\alpha = (\alpha_1, \ldots, \alpha_{2n})'$ be a J-vector with respect to $(\mathfrak{a}, a)$. Then $\alpha_1, \ldots, \alpha_{2n}$ is a symplectic basis of $[\mathfrak{a}, a]$. Let X be the matrix of g with respect to $\alpha_1, \ldots, \alpha_{2n}$. We need to prove that $\Psi(X) = \langle \mathfrak{a}, a \rangle$. Since $g \circ (\alpha_1, \ldots, \alpha_{2n}) = \frac{1}{\zeta}(\alpha_1, \ldots, \alpha_{2n}) = (\alpha_1, \ldots, \alpha_{2n})X$, and $X'^{-1}\alpha = \zeta\alpha$, we get $\Psi(X'^{-1}) = \langle \mathfrak{a}, a \rangle$. Hence $\Psi(X) = \Psi(X'^{-1}) = \langle \mathfrak{a}, a \rangle$. □

The following proposition gives a method to compute $\Pi \circ \Sigma(V)$, for a symplectic G_m-space $V \in V_f$ without needing to know a symplectic basis of V.

Proposition 4.5. *Suppose $V \in \mathcal{V}_f$. Let $a_1, \ldots, a_{2n}$ be a $\mathcal{D}$-basis of V, not necessarily symplectic. Let M be the inner product matrix of $a_1, \ldots, a_{2n}$, and X be the matrix of g with respect to $a_1, \ldots, a_{2n}$. Let $\alpha = (\alpha_1, \ldots, \alpha_{2n})' \in \mathcal{D}^{2n}$ be an eigenvector of X with respect to ζ. Then $\Psi \circ \Sigma(V) = \langle \mathfrak{a}, a \rangle$, where $\mathfrak{a}$ is the ideal generated by $\alpha_1, \ldots, \alpha_{2n}$ and $a = \Delta^{-1}\alpha' M\widetilde{\alpha}$.*

Proof. We choose a symplectic basis $v_1, \ldots, v_{2n}$ of V and let Y be the matrix of g with respect to $v_1, \ldots, v_{2n}$. There is $Q \in GL_{2n}(\mathcal{D})$ such that $(a_1, \ldots, a_{2n}) = (v_1, \ldots, v_{2n})Q$. It follows that $Y = QXQ^{-1}$ and $M = Q'JQ$.

If $\beta = Q\alpha$, then $Y\beta = QXQ^{-1}(Q\alpha) = QX\alpha = Q\zeta\alpha = \zeta Q\alpha = \zeta\beta$. We see that β is an eigenvector of Y with respect to ζ. Now we need to show that β is a J-vector with respect to of $(\mathfrak{a}, a)$. From the fact that Q is invertible, we see that the components of β form a $\mathcal{D}$-basis of $\mathfrak{a}$, and

$$a = \Delta^{-1}\alpha' M\widetilde{\alpha} = \Delta^{-1}\alpha' Q' JQ\widetilde{\alpha} = \Delta^{-1}\beta' J\widetilde{\beta}.$$

So $\Psi \circ \Sigma(V) = \Psi(Y) = \langle \mathfrak{a}, a \rangle$. □

For $r = 2$, we have

Corollary 4.6. $[\mathfrak{a}, a] * [\mathfrak{b}, b] \cong [\mathcal{R}, 1] * [\mathfrak{ab}, ab]$ *if and only if there are $u \in \mathfrak{a}$ and $v \in \mathfrak{b}$ such that*

$$\frac{u\widetilde{u}}{a} + \frac{v\widetilde{v}}{b} = 1. \tag{4.17}$$

Proof. Suppose $[\mathfrak{a}, a] * [\mathfrak{b}, b] \cong [\mathcal{R}, 1] * [\mathfrak{ab}, ab]$. There is a 2×2 matrix $Q = (q_{ij})$ with entries in $\mathcal{S}$, so that $q_{11}\mathcal{R} \subset \mathfrak{a}$, $q_{21}\mathcal{R} \subset \mathfrak{b}$ and

$$\begin{pmatrix} 1 & \\ & \frac{1}{ab} \end{pmatrix} = Q' \begin{pmatrix} \frac{1}{a} & \\ & \frac{1}{b} \end{pmatrix} \widetilde{Q}. \tag{4.18}$$

Set $u = q_{11}$, $v = q_{21}$ and then compare the top left entries of both sides of Equation (4.18).

For the converse, suppose there are $u \in \mathfrak{a}$, $v \in \mathfrak{b}$ such that (4.17) holds. Let $Q = \begin{pmatrix} u & -\frac{\widetilde{v}}{b} \\ v & \frac{\widetilde{u}}{a} \end{pmatrix}$. It follows that Q satisfies (4.18). Now we need to verify that $-\frac{\widetilde{v}}{b}\mathfrak{ab} \subset \mathfrak{a}$ and $\frac{\widetilde{u}}{a}\mathfrak{ab} \subset \mathfrak{b}$. Since $v \in \mathfrak{b}$, then $-\widetilde{v} \in \widetilde{\mathfrak{b}}$, which implies $-\widetilde{v}\mathfrak{b} \subset \mathfrak{b}\widetilde{\mathfrak{b}} = b\Delta\mathfrak{b}\mathfrak{b}' \subset b\mathcal{R}$, and thus $-\frac{\widetilde{v}}{b}\mathfrak{b} \subset \mathcal{R}$. It follows that $\frac{\widetilde{v}}{b}\mathfrak{ab} \subset \mathfrak{a}$. Similarly, $\frac{\widetilde{u}}{a}\mathfrak{ab} \subset \mathfrak{b}$. Therefore $[\mathfrak{a}, a] * [\mathfrak{b}, b] \cong [\mathcal{R}, 1] * [\mathfrak{ab}, ab]$ by Theorem 7.

This completes the proof. □

Example. Let $\mathcal{R}_m$ be as in Section 3.5. Then $[\mathcal{R}_m, -1] * [\mathcal{R}_m, -1] \ncong [\mathcal{R}_m, 1] * [\mathcal{R}_m, 1]$.

Chapter 5
Order p elements in $SP_{p-1}(\mathbb{Z})$

First, in Section 5.1 we will give examples of elements of order p in $SP_{p-1}(\mathbb{Z})$. Then in Section 5.2 we will discuss the cyclotomic units of the cyclotomic field $\mathbb{Q}[\zeta]$, where $\zeta = e^{\frac{2\pi i}{p}}$. And finally, in Section 5.3 we shall prove Theorem 8.

5.1 An Example

Theorem 1 gives us a way to find representatives for each cyclic matrix class in $SP_{2n}(\mathcal{D})$ with characteristic polynomial $f(x)$ irreducible and separable in $\mathcal{D}$. Suppose we have an S-pair $(\mathfrak{a}, a)$ and a basis $\beta_1, \ldots, \beta_{2n}$ of $\mathfrak{a}$, which is not necessarily J-orthogonal. The following steps will find a symplectic matrix $X \in SP_{2n}(\mathcal{D})$ such that $\Psi(X) = \langle \mathfrak{a}, a \rangle$.

1. Find the dual basis $\gamma_1, \ldots, \gamma_{2n}$ of $\beta_1, \ldots, \beta_{2n}$, that is solve the linear system
$$\gamma' \beta^{(i)} = \delta_{1i} \tag{5.1}$$
where $\beta = (\beta_1, \ldots, \beta_{2n})'$ and $\gamma = (\gamma_1, \ldots, \gamma_{2n})'$;
2. Find the integral matrix $Y \in GL_{2n}(\mathcal{D})$ such that $Y\beta = \zeta\beta$;
3. Find the skew symmetric matrix $M \in GL_{2n}(\mathcal{D})$ such that $M\widetilde{\beta} = a\Delta\gamma$;
4. Find a matrix $Q \in GL_{2n}(\mathcal{D})$ such that $M = Q'JQ$;
5. Let $X = QYQ^{-1}$. Then $X \in SP_{2n}(\mathcal{D})$ and $\Psi(X) = \langle \mathfrak{a}, a \rangle$.

Let $\mathcal{R} = \mathbb{Z}[\zeta]$. We shall apply this method to find X in $SP_{p-1}(\mathbb{Z})$ of order p and such that $\Psi(X) = \langle \mathcal{R}, 1 \rangle$. We know that $1, \zeta, \ldots, \zeta^{p-2}$ is a basis of $\mathcal{R}$.

Lemma 5.1. *The dual basis of* $1, \zeta, \ldots, \zeta^{p-2}$ *is* $\gamma_1, \ldots, \gamma_{p-1}$*, where*

$$\gamma_i = \frac{(\zeta-1)\zeta}{p}\left(1+\cdots+\zeta^{p-1-i}\right), \quad i = 1, \ldots, p-1. \tag{5.2}$$

Proof. By Lemma 3.2, we need to verify

$$f(x) = f'(\zeta)(x-\zeta)\left(\sum_{i=0}^{p-2}\gamma_{i+1}x^i\right)$$

where $f(x) = x^{p-1}+\cdots+x+1$, and $f'(\zeta) = \frac{p}{(\zeta-1)\zeta}$. Let $\gamma_0 = \gamma_p = 0$.

$$\begin{aligned}(x-\zeta)\sum_{i=0}^{p-2}\gamma_{i+1}x^i &= \sum_{i=0}^{p-2}\gamma_{i+1}x^{i+1} - \sum_{i=0}^{p-2}\gamma_{i+1}\zeta x^i = \sum_{i=1}^{p-1}\gamma_i x^i - \sum_{i=0}^{p-2}\gamma_{i+1}\zeta x^i \\ &= \sum_{i=0}^{p-1}(\gamma_i - \gamma_{i+1}\zeta)x^i = \sum_{i=0}^{p-1}\frac{(\zeta-1)\zeta}{p}x^i = \frac{f(x)}{f'(\zeta)}.\end{aligned}$$

Thereby proving our assertion. □

Let $\beta = \left(1, \zeta, \ldots, \zeta^{p-2}\right)'$ and $\gamma = (\gamma_1, \ldots, \gamma_{p-1})'$. Then Y is the companion matrix

$$C_{p-1} = \begin{pmatrix} 0 & 1 & & \\ & & \ddots & \\ & & & 1 \\ -1 & -1 & \ldots & -1 \end{pmatrix}$$

and

$$\overline{\beta} = \begin{pmatrix} 1 \\ \zeta^{p-1} \\ \vdots \\ \zeta^2 \end{pmatrix} \quad \text{and} \quad \gamma = \frac{\zeta-1}{p}\begin{pmatrix} -1 & & & \\ -1 & -1 & & \\ \vdots & \vdots & \ddots & \\ -1 & -1 & \ldots & -1 \end{pmatrix}\overline{\beta} = \frac{\zeta-1}{p}L_{p-1}\overline{\beta} \tag{5.3}$$

where L_n is the $n \times n$ matrix whose entries above the diagonal are 0 and the others are -1. Since $\zeta\beta = C_{p-1}\beta$ we have $\zeta\overline{\beta} = C_{p-1}^{-1}\overline{\beta}$. Note that $\Delta = \frac{p\zeta^{(p+1)/2}}{\zeta-1}$ we see that

$$\Delta\gamma = \zeta^{\frac{p+1}{2}}L_{p-1}\overline{\beta} = L_{p-1}C_{p-1}^{-\frac{p+1}{2}}\overline{\beta}.$$

Let $M = L_{p-1}C_{p-1}^{-\frac{p+1}{2}}$. By a long but routine computation, we see that

$$M = \begin{pmatrix} & L_{\frac{p-1}{2}} \\ -L'_{\frac{p-1}{2}} & \end{pmatrix}$$

is a skew symmetric matrix, and $M = Q'_{p-1}J_{p-1}Q_{p-1}$, where $Q_{p-1} = I \dotplus L_{\frac{p-1}{2}} \in GL_{p-1}(\mathbb{Z})$. Therefore we have shown

Proposition 5.1. *Let*

$$X_p = Q_{p-1}C_{p-1}Q_{p-1}^{-1} = \left(\begin{array}{cccc|cccc} 0 & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & 0 & -1 & & & \\ \hline & & & & -1 & 1 & & \\ & & & & -1 & & \ddots & \\ & & & & \vdots & & & 1 \\ 1 & 1 & \dots & 1 & -1 & & & 0 \end{array}\right) \tag{5.4}$$

where each block is a $\frac{p-1}{2} \times \frac{p-1}{2}$ matrix. Then $X_p \in SP_{p-1}(\mathbb{Z})$ with order p and $\Phi(X_p) = \langle \mathcal{R}, 1 \rangle$.

Example. When $p = 3$, we see that $X = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ is an element of order 3 in $SP_2(\mathbb{Z})$.

In Section 5.3 we shall see that all X_p are realizable if $p \geq 5$, that is X_p is the matrix of T_* with respect to some canonical basis of $H_1(S)$, for some analytic automorphism T of some compact connected Riemann surface S.

5.2 Cyclotomic Units

The cyclotomic units in $\mathcal{R}$ are

$$u_k = \frac{\sin \frac{k\pi}{p}}{\sin \frac{\pi}{p}}, \quad \text{for } (k,p) = 1. \tag{5.5}$$

Since

$$\frac{1-\zeta^k}{1-\zeta} = \lambda^{k-1}u_k, \quad \text{where } \lambda = -\zeta^{\frac{p+1}{2}} \tag{5.6}$$

and $\frac{1-\zeta^k}{1-\zeta}$ is a unit, we conclude that $u_k \in U^+$. The following properties of the cyclotomic units are easy to verify:

$$u_1 = 1 \quad \text{and} \quad u_{mp+k} = -u_{mp-k} = (-1)^m u_k \tag{5.7}$$

$$\begin{cases} u_k > 0, & 1 \le k \le p-1, \\ u_k < 0, & p+1 \le k \le 2p-1. \end{cases} \tag{5.8}$$

Lemma 5.2. $\sum_{j=1}^{k} u_{2j+l} = u_k u_{k+l+1}$.

Proof. We use the trigonometric formulas,

$$\begin{aligned}
\sum_{j=1}^{k} u_{2j+l} &= \sum_{j=1}^{k} \frac{\sin\frac{(2j+l)\pi}{p}\sin\frac{\pi}{p}}{\sin^2\frac{\pi}{p}} \\
&= \frac{1}{\sin^2\frac{\pi}{p}}\sum_{j=1}^{k}\frac{1}{2}\left(\cos\frac{(2j+l-1)\pi}{p} - \cos\frac{(2j+l+1)\pi}{p}\right) \\
&= \frac{\cos\frac{(l+1)\pi}{p} - \cos\frac{(2k+l+1)\pi}{p}}{2\sin^2\frac{\pi}{p}} \\
&= \frac{\sin\frac{k\pi}{p}\sin\frac{(k+l+1)\pi}{p}}{\sin^2\frac{\pi}{p}} = u_k u_{k+l+1}
\end{aligned}$$

□

From now on we let the i-th conjugate of ζ be ζ^i. We have

Lemma 5.3. $u_k^{(i)} = (-1)^{(k-1)(i+1)} u_{ik} u_i^{-1}$.

Proof. Using (5.6), we see that

$$u_k^{(i)} = (-\zeta^{i\frac{p+1}{2}})^{-(k-1)}\frac{1-\zeta^{ik}}{1-\zeta^i}$$

$$
\begin{aligned}
&= (-1)^{k-1}\zeta^{i(k-1)(\frac{p-1}{2})}\frac{1-\zeta^{ik}}{1-\zeta}\frac{1-\zeta}{1-\zeta^{i}} \\
&= (-1)^{k-1}\zeta^{i(k-1)(\frac{p-1}{2})}(-\zeta^{\frac{p+1}{2}})^{ik-i}u_{ik}u_i^{-1} \\
&= (-1)^{(k-1)(i+1)}u_{ik}u_i^{-1}
\end{aligned}
$$

□

Lemma 5.4. $\Delta^{(i)} = (-1)^{i-1}u_i^{-1}\Delta$.

Proof. Since $\Delta = \frac{p\zeta^{\frac{p+1}{2}}}{\zeta-1}$, $\Delta^{(i)} = \frac{p\zeta^{\frac{i(p+1)}{2}}}{\zeta^{i}-1}$. We obtain $\frac{\Delta^{(i)}}{\Delta} = \frac{\zeta-1}{\zeta^{i}-1}\zeta^{\frac{(i-1)(p+1)}{2}} = (-1)^{i-1}u_i^{-1}$. □

Lemma 5.5. *Suppose $X \in SP_{p-1}(\mathbb{Z})$ has order p, and $\Psi(X) = \langle \mathfrak{a}, a\rangle$. Then*

$$\Psi(X^k) = \left\langle \mathfrak{a}^{(k')}, (-1)^{k'-1}u_{k'}a^{(k')}\right\rangle,$$

where $1 \le k \le p-1$, k' is the inverse of k modulo p, and $\mathfrak{a}^{(k')} = \left\{\alpha^{(k')} \;\middle|\; \alpha \in \mathfrak{a}\right\}$.

Proof. Suppose α is a J-vector with respect to $(\mathfrak{a}, a)$ and $X\alpha = \zeta\alpha$. Then $a = \Delta^{-1}\alpha' J\overline{\alpha}$ and $X^k\alpha^{(k')} = \zeta^{kk'}\alpha^{(k')} = \zeta\alpha^{(k')}$, hence $\Psi(X^k) = \left\langle \mathfrak{a}^{(k')}, a_k\right\rangle$, where

$$a_k = \Delta^{-1}\alpha'^{(k')}J\overline{\alpha}^{(k')} = \frac{\Delta^{(k')}}{\Delta}(\Delta^{-1}\alpha' J\overline{\alpha})^{(k')} = (-1)^{k'-1}u_{k'}^{-1}a^{(k')}$$

(By Lemma 5.4). This completes the proof. □

Lemma 5.6. $u_k \notin C$, *for* $2 \le k \le p-2$.

Proof. We only consider $2 \le k \le \frac{p-1}{2}$.

Case I: k is even. For $4 \le 2k \le p-1$, we get $u_k^{(2)} = -u_{2k}u_2^{-1} < 0$, and so $u_k \notin C$.

Case II: k is odd. There is $1 \le i \le p-1$ such that $p+1 \le ki \le 2p-1$. Then we have $u_k^{(i)} = u_{ki}u_i^{-1} < 0$, hence $u_k \notin C$. □

Lemma 5.7. $u_k u_l^{-1}$, $u_k u_l \notin C$, *for* $1 \le k, l \le \frac{p-1}{2}$ *and* $k \ne l$.

Proof. There is $2 \leq i \leq p-2$, such that $il \equiv k \pmod p$. Then $u_k u_l^{-1} = \pm u_{il} u_l^{-1} = \pm u_i^{(l)}$. But $\pm u_i^{(l)}$ does not belong to C since if it did we would have $\pm u_i \in C$ by choosing the appropriate conjugate. This contradicts Lemma 5.6. Then $u_k u_l = (u_k u_l^{-1}) u_l^2 \notin C$ (since $u_l^2 \in C$). $\square$

By Lemma 5.5, Lemma 5.6 and Lemma 5.7, the following corollary and Proposition 5.2 are easy to prove.

Corollary 5.1. *The $p-1$ elements $[\pm 1], [\pm u_2], \ldots, [\pm u_{\frac{p-1}{2}}]$ are distinct in U^+/C.*

Proposition 5.2. *Let X_p be the matrix given by Equation (5.4). Then $X_p, X_p^2, \ldots, X_p^{p-1}$ are not similar to each other.*

Proposition 5.3. *If $\frac{p-1}{2}$ is odd, then there is an $X \in SP_{p-1}(\mathbb{Z})$ of order p, such that there are just two different classes amongst $X, \ldots, X^{p-1}$.*

Proof. Let $a = u_2 \cdots u_{\frac{p-1}{2}}$. There is $X \in SP_{p-1}(\mathbb{Z})$ of order p such that $\Psi(X) = \langle \mathcal{R}, a \rangle$. Suppose $\alpha \in \mathcal{R}^{p-1}$ $(\alpha \neq 0)$, $X\alpha = \zeta\alpha$ and $a = \Delta^{-1}\alpha' J \bar{\alpha}$. From Lemma 5.5 and the fact that $\mathcal{R}^{(k)} = \mathcal{R}$ we get $\Psi(X^k) = \langle \mathcal{R}, a_k \rangle$, where $a_k = (-1)^{k'-1} u_{k'}^{-1} a^{(k')}$ and k' is the inverse of k. Note that

$$a^{(k')} = \pm u_{2k'} u_{k'}^{-1} \cdots u_{\frac{p-1}{2}k'} u_{k'}^{-1} = \pm u_2 \cdots u_{\frac{p-1}{2}} u_{k'}^{-\frac{p-1}{2}} = \pm a u_{k'}^{-\frac{p-1}{2}},$$

hence $a/a_k = \pm u_{k'}^{\frac{p+1}{2}} \in C \cup (-C)$. Therefore

$$\Psi(X^k) = \begin{cases} \Psi(X), & \text{if } a/a_k \in C, \\ \Psi(X^{-1}), & \text{if } a/a_k \in -C. \end{cases}$$

i.e. $X, \ldots, X^{p-1}$ are in two different classes. $\square$

Example. Let $p = 7$. Let

$$X = \begin{pmatrix} 0 & 0 & 0 & -1 & -1 & 0 \\ 1 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \qquad \alpha = \begin{pmatrix} \zeta^4 + \zeta^3 + \zeta^2 \\ \zeta^3 + \zeta - 1 \\ -\zeta^6 \\ \zeta^2 + 1 \\ \zeta^6 + \zeta \\ 1 \end{pmatrix}$$

Then one can easily check that $X\alpha = \zeta\alpha$, $X \in SP_6(\mathbb{Z})$ and $X^7 = I$. One can also check that $a = \Delta^{-1}\alpha' J\overline{\alpha} = \zeta^6 + \zeta = u_2^{-1}u_3$. By computing, we get

$$X \sim X^2 \sim X^4 \quad \text{and} \quad X^3 \sim X^5 \sim X^6.$$

Proposition 5.4. *Suppose $p \equiv 1 \pmod 3$. There is $X \in SP_{p-1}(\mathbb{Z})$ of order p such that $X \sim X^k$, where k is the least positive solution of $k^2 + k + 1 \equiv 0 \pmod p$.*

Proof. Since $p \equiv 1 \pmod 3$, then $x^2 + x + 1 \equiv 0 \pmod p$ has a solution. Let k be the minimal positive solution. There is an $X \in SP_{p-1}(\mathbb{Z})$, of order p, with $\Psi(X) = \langle \mathcal{R}, u_k u_{k+1} \rangle$. Then by applying Lemma 5.5 we get $\Psi(X^k) = \langle \mathcal{R}, u \rangle$, where

$$\begin{aligned} u &= (-1)^{p-k} u_{p-k-1} u_k^{(p-k-1)} u_{k+1}^{(p-k-1)} \\ &= (-1)^{p-k} u_{k+1} (-1)^{(k-1)(p-k)} u_{k(p-k-1)} u_{p-k-1}^{-1} (-1)^{k(p-k)} u_{(k+1)(p-k-1)} u_{p-k-1}^{-1} \\ &= u_k u_{k+1}^{-1}. \end{aligned}$$

Note that $k(p-k-1) = mp + 1$ and $(k+1)(p-k-1) = (m+1)p - k$. Hence $X \sim X^k$. $\square$

To finish this section we give a proposition:

Proposition 5.5. *There are integers $k_1, \ldots, k_n$, such that $2 \le k_1 < \cdots < k_n \le \frac{p-1}{2}$, and $u_{k_1} \cdots u_{k_n} \in C$ if and only if h_2, the second factor of the class number of $\mathcal{R}$, is even.*

Proof. Let C_1 be the group generated by $\pm 1, u_2, \ldots, u_{\frac{p-1}{2}}$. Then $[U^+ : C_1] = h_2$, see [20]. Suppose $u_{k_1} \cdots u_{k_n} = u^2 \in C$ and $u \in U^+$. We see that $u \notin C_1$ since $u_2, \ldots, u_{\frac{p-1}{2}}$ are free generators. Let C_2 be the group generated by $\pm 1, u, u_2, \ldots, u_{\frac{p-1}{2}}$. Clearly, $C_1 \subset C_2 \subset U^+$ and $[C_2 : C_1] = 2$, so $2 | h_2$.

If h_2 is even, there is $u \in U^+$, $u \notin C_1$, but $u^2 \in C_1$. Then $u^2 = u_1^{r_1} \cdots u_{\frac{p-1}{2}}^{r_{\frac{p-1}{2}}}$ where not all of r_j are even. Thus $u^2 = u_{k_1} \cdots u_{k_n} v^2$ for some distinct integers $2 \le k_j \le \frac{p-1}{2}$ and some $v \in C_1$. It follows that $u_{k_1} \cdots u_{k_n} \in C$. $\square$

Remark. In case that h_2 is odd, the $2^{\frac{p-1}{2}}$ elements $[\pm u_{k_1}u_{k_2}\cdots u_{k_n}]$, where $2 \le k_1 < \cdots < k_n \le \frac{p-1}{2}$, are all distinct. They are in fact the elements of U^+/C.

5.3 Realizable Elements of Order p

Theorem 8 is similar to a result of P. Symonds[35], but our approach is new. We consider short exact sequences of Fuchsian groups

$$1 \to \Pi \to \Gamma(0; p, p, p) \xrightarrow{\theta} \mathbb{Z}_p \to 1$$

where $\Gamma(0; p, p, p) = \langle A_1, A_2, A_3 \mid A_1A_2A_3 = A_1^p = A_2^p = A_3^p = 1\rangle$. If Π is torsion free, then we get an action of $\mathbb{Z}_p$ on $S = \mathbb{U}/\Pi$, with genus $\frac{p-1}{2}$. Now we indicate how to find all epimorphisms θ with torsion free kernel.

The epimorphism $\theta : \Gamma \to \mathbb{Z}_p$ is determined by the images of the generators. The relations in Γ must be preserved and the kernel of θ must be torsion free, therefore θ is determined by the equations

$$\theta : \begin{cases} A_1 \to T^a, \\ A_2 \to T^b, \\ A_3 \to T^c, \end{cases}$$

where T is a fixed generator of $\mathbb{Z}_p$, $1 \le a, b, c \le p-1$ and $a + b + c \equiv 0 \pmod{p}$. We use $M(a, b, c)$ to denote the matrix class which is induced by T. Let $V(a, b, c)$ denote the symplectic $\mathbb{Z}_p$-space $H_1(S)$ where the action of T on $H_1(S)$ is given by T_*. Then $\Sigma\big(V(a, b, c)\big) = M(a, b, c)$.

The proof of Theorem 8 is based on Proposition 4.5. Suppose $a_1, \ldots, a_{p-1}$ is a basis of $H_1(S)$, and M is the intersection matrix of $a_1, \ldots, a_{p-1}$. Let X be the matrix of T_* with respect to $a_1, \ldots, a_{p-1}$. Let $\alpha = (\alpha_1, \ldots, \alpha_{p-1})' \in \mathcal{R}^{p-1}$ be an eigenvector of X with respect to ζ. It is easy to check that $\Psi\big(M(a, b, c)\big) = \Psi \circ \Sigma\big(V(a, b, c)\big) = \big\langle \mathfrak{a}, \Delta^{-1}\alpha' M \overline{\alpha}\big\rangle$, where $\mathfrak{a}$ is the ideal generated by $\alpha_1, \ldots, \alpha_{p-1}$.

Remark. If we prove the special case where $a = 1$ and $1 \le b \le \frac{p-1}{2}$, that is if we show that

$$\Psi(M(1, b, c)) = \langle \mathcal{R}, u_b u_{b+1} \rangle,$$

then Theorem 8 will follow. This is because $M(1,b,c) = M(1,c,b)$ and $M(a,b,c)$ is the a'-th power of $M(1,b_1,c_1)$, where $aa' \equiv 1 \pmod p$, $b_1 \equiv a'b \pmod p$, $c_1 \equiv a'c \pmod p$. Applying Lemma 5.5, we would get

$$\Psi(M(a,b,c)) = \left\langle \mathcal{R}, (-1)^{a-1} u_a (u_{b_1} u_{b_1+1})^{(a)} \right\rangle$$

and by Lemma 5.3, we could then have

$$\begin{aligned} u &= (-1)^{a-1} u_a (u_{b_1} u_{b_1+1})^{(a)} \\ &= (-1)^{a-1} u_a (-1)^{(b_1-1)(a+1)} u_{b_1 a} u_a^{-1} (-1)^{b_1(a+1)} u_{(b_1+1)a} u_a^{-1} \\ &= u_a^{-1} u_{mp+b} u_{mp+a+b} \\ &= u_a^{-1} (-1)^m u_b (-1)^m u_{a+b} = u_a^{-1} u_b u_{a+b} \end{aligned}$$

where m satisfies $b_1 a = mp + b$. We see that $u/u_a u_b u_{a+b} = u_a^{-2} \in C$.

Thus we assume $a = 1$ and $1 \le b \le \frac{p-1}{2}$. Then $\frac{p-1}{2} \le c \le p-2$. We choose a particular embedding of Γ in Aut $(\mathbb{U})$, namely Γ is the subgroup generated by A_1, A_2, A_3, where A_1, A_2, A_3 are rotations by $2\pi/p$ about the vertices v_1, v_2, v_3 of a regular triangle P, all of whose angles are π/p, see Figure 2.1. A fundamental domain of Γ consists of P together with a copy of P obtained by reflection in its side v_1v_3. Then a fundamental domain D of Π is the $2p$-gon consisting of p copies of the fundamental domain of Γ obtained by the p rotations A_1^k $(k = 0, \ldots, p-1)$, see Figure 5.1. Let $e_1, \ldots, e_{2p}$ be the $2p$ sides of D, and $\eta_i = e_{2i-1} + e_{2i}$ (for $i = 1. \ldots, p$). Then $\eta_1, \ldots, \eta_p$ are closed paths on S and $[\eta_1], \ldots, [\eta_{p-1}]$ forms a basis of $H_1(S)$, see [24]. The intersection matrix of $[\eta_1], \ldots, [\eta_{p-1}]$ is somewhat complex, so we need to find another basis.

Since $\theta(A_1^{c+i-1} A_3^{-1} A_1^{1-i}) = 1$, then $\gamma = A_1^{c+i-1} A_3^{-1} A_1^{1-i} \in \Pi$ is a boundary substitution of D and so $[e_{2i-1}]_\Pi = [-e_{2c+2i}]_\Pi$. In the interior of each side e_i, we choose a point E_i such that $[E_{2i-1}]_\Pi = [E_{2c+2i}]_\Pi$. Let f_i denote the straight line segment from v_1 to E_i in D. Let $\xi_i = f_{2i-1} - f_{2c+2i}$. Then ξ_i is a closed path on S.

It is clear that $[\xi_i] = [\eta_i] + \cdots + [\eta_{c+i}]$ and $[\eta_1] + \cdots + [\eta_p] = 0$ in the homology group $H_1(S)$.

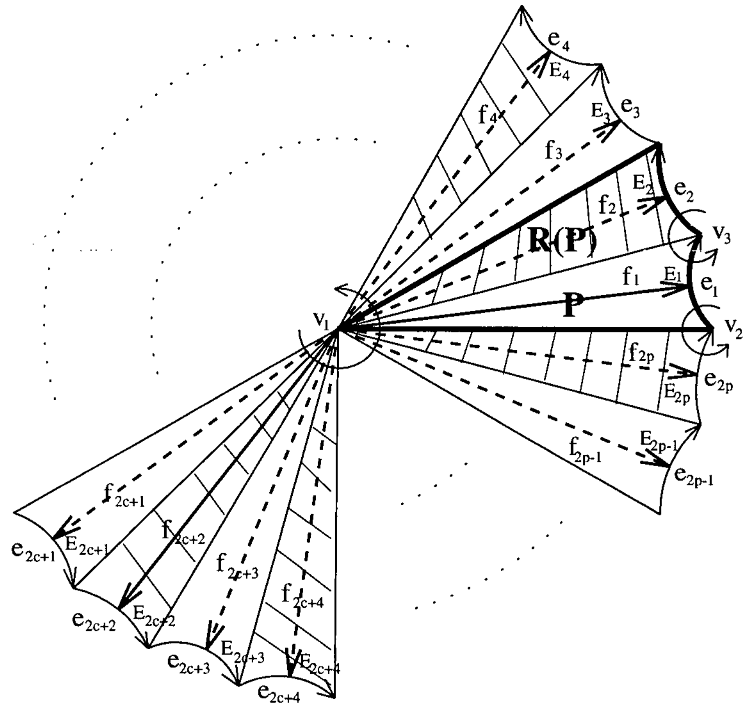

Figure 5.1: Fundamental Domain (order p)

Hence the transform matrix from $[\eta]$'s to $[\xi]$'s is the $(p-1)\times(p-1)$ matrix

$$
\begin{array}{c}
c+1 \left\{ \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \right. \\ \\ \\
\end{array}
\begin{pmatrix}
1 & & & -1 & & & \\
\vdots & \ddots & & \vdots & \ddots & & \\
\vdots & & 1 & -1 & & \ddots & \\
\vdots & & \vdots & & \ddots & & -1 \\
1 & & \vdots & & & \ddots & \vdots \\
 & \ddots & \vdots & & & & -1 \\
 & & 1 & & & & 0
\end{pmatrix}
\begin{array}{c}
\\ \\ \\ \left. \begin{array}{c} \\ \\ \\ \end{array} \right\} p-c-1 \\ \\
\end{array}
$$

where the entries x_{ij} are given by

$$
x_{ij} = \begin{cases}
1, & 1 \le j \le p-c-1 \text{ and } j \le i \le j+c, \\
-1, & p-c \le j \le p-1 \text{ and } j+c+1-p \le i \le j-1, \\
0, & \text{otherwise.}
\end{cases}
$$

By applying the Laplace expansion theorem to the last row we see that the determinant of this matrix is just the determinant of the $(p-2)\times(p-2)$ matrix $L_{c+1,p-c-1}$, see Equation (2.9). Since p is an odd prime and $1 \le c \le p-2$, then $c+1$, $p-c-1$ are coprime, and therefore $|\det L_{c+1,p-c-1}| = 1$ (See Section 2.3). Hence $[\xi_1], \dots, [\xi_{p-1}]$ is a basis of $H_1(S)$.

Lemma 5.8. *The matrix of T_* with respect to $[\xi_1], \dots, [\xi_{p-1}]$ is*

$$C'_{p-1} = \begin{pmatrix} 0 & & & & -1 \\ 1 & & & & -1 \\ & 1 & & & -1 \\ & & \ddots & & \vdots \\ & & & 1 & -1 \end{pmatrix}.$$

Proof. Let $f_{2p+i} = f_i$ and $\xi_{p+k} = \xi_k$. Since $\theta(A_1) = T$, we get $T([f_i]_\Pi) = [A_1(f_i)]_\Pi = [f_{i+2}]_\Pi$, for $i = 1, \dots, 2p$. Then

$$\begin{aligned} T([\xi_k]_\Pi) &= T([f_{2k-1}]_\Pi - [f_{2c+2k}]_\Pi) \\ &= [f_{2k+1}]_\Pi - [f_{2c+2k+2}]_\Pi = [\xi_{k+1}]_\Pi \end{aligned}$$

for $k = 1, \dots, p$. Therefore $T_*([\xi_k]) = [\xi_{k+1}]$, for $k = 1, \dots, p-1$. But $[\xi_1] + \cdots + [\xi_p] = 0$ and therefore

$$\begin{aligned} T_*([\xi_1]) &= [\xi_2], \\ T_*([\xi_2]) &= [\xi_3], \\ &\cdots\cdots \\ T_*([\xi_{p-2}]) &= [\xi_{p-1}], \\ T_*([\xi_{p-1}]) &= -[\xi_1] - [\xi_2] - \cdots - [\xi_{p-1}]. \end{aligned}$$

This proves the lemma. ∎

Now we compute the intersection matrix M of $[\xi_1], \dots, [\xi_{p-1}]$. Let $m_{i,j}$ be the intersection number $\xi_i \cdot \xi_j$ of $[\xi_i]$ and $[\xi_j]$. We have

Lemma 5.9. *For any* $1 \le i, j \le p-1$, $m_{i,j} = m_{i+1,j+1}$ *and* $m_{1,j+1} = -m_{1,p-j+1}$.

Proof. T_* preserves the intersection number of closed chains. By Lemma 5.8,

$$m_{i,j} = \xi_i \cdot \xi_j = T_*(\xi_i) \cdot T_*(\xi_j) = \xi_{i+1} \cdot \xi_{j+1} = m_{i+1,j+1}.$$

Iterating this formula we see that $m_{1,p-j+1} = m_{j+1,p+1} = m_{j+1,1} = -m_{1,j+1}$. □

Let $k_j = m_{1,j+1}$. Then $m_{i,i+j} = k_j$. Hence the intersection matrix is of the form

$$M = k_1 M_1 + \cdots + k_{p-2} M_{p-2},$$

where the M_j is the $(p-1) \times (p-1)$ matrix

$$M_j = \begin{pmatrix} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & \ddots & & \vdots \\ 0 & & & & & \ddots & 0 \\ -1 & & & & & & 1 \\ 0 & \ddots & & & & & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \dots & 0 & -1 & 0 & \dots & 0 \end{pmatrix}.$$

The entries $x_{kl}^{(j)}$ of M_j are given by

$$x_{kl}^{(j)} = \begin{cases} 1, & l - k = j, \\ -1, & k - l = j, \\ 0, & \text{otherwise.} \end{cases}$$

By Lemma 5.9, we see that $k_j = m_{1,j+1} = -m_{1,p+1-j} = -k_{p-j}$, and therefore

$$M = k_1 M_1 + k_2(M_2 - M_{p-2}) + \cdots + k_{\frac{p-1}{2}} \left(M_{\frac{p-1}{2}} - M_{\frac{p+1}{2}} \right).$$

Lemma 5.10.

$$k_j = \begin{cases} 1, & 1 \le j \le p - c - 1, \\ 0, & p - c \le j \le \frac{p-1}{2}. \end{cases} \tag{5.9}$$

Proof. It is clear that the intersection of ξ_1 and ξ_{j+1} ($j = 1, \dots, \frac{p-1}{2}$) is only one point, namely the vertex v_1. The verification of (5.9) is straightforward by referring to Figure 5.2 and 5.3. $\square$

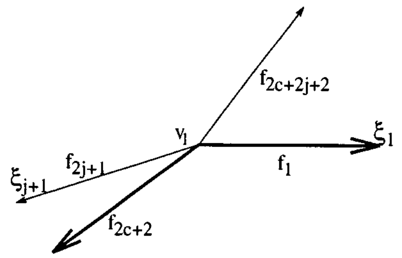

Figure 5.2: $p - c \leq j \leq (p-1)/2$

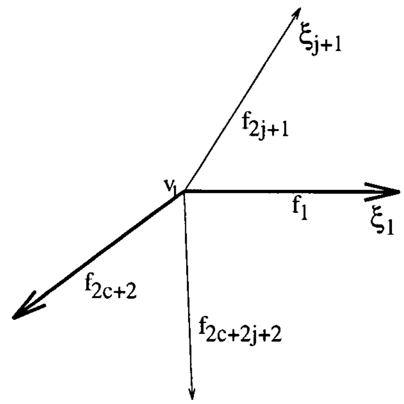

Figure 5.3: $1 \leq j \leq p - c - 1$

Let

$$\alpha = \begin{pmatrix} 1 + \zeta + \cdots + \zeta^{p-2} \\ 1 + \zeta + \cdots + \zeta^{p-3} \\ \vdots \\ 1 + \zeta \\ 1 \end{pmatrix}.$$

α is an eigenvector of C'_{p-1} with respect to the eigenvalue ζ, that is $C'_{p-1}\alpha = \zeta\alpha$.

Lemma 5.11. *Let*

$$y_j = \begin{cases} \Delta^{-1}\alpha' M_1 \overline{\alpha}, & j = 1, \\ \Delta^{-1}\alpha'(M_j - M_{p-j})\overline{\alpha}, & j = 2, \dots, \frac{p-1}{2}. \end{cases}$$

Then $y_j = u_{2j}$.

Proof. Let $\beta = (1 - \zeta)\alpha$. We see that $\beta_k = 1 - \zeta^{p-k}$.

$$\begin{aligned} \beta' M_j \overline{\beta} = \sum_{k=1}^{p-1}\sum_{l=1}^{p-1} \beta_k x_{kl}^{(j)} \overline{\beta}_l &= \sum_{l-k=j} \beta_k \overline{\beta}_l - \sum_{k-l=j} \beta_k \overline{\beta}_l \\ = \sum_{k=1}^{p-1-j} \beta_k \overline{\beta}_{k+j} - \sum_{k=j+1}^{p-1} \beta_k \overline{\beta}_{k-j} &= \sum_{k=1}^{p-1-j} \beta_k \overline{\beta}_{k+j} - \sum_{k=1}^{p-1-j} \beta_{k+j} \overline{\beta}_k \end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=1}^{p-1-j} \left(1-\zeta^{p-k}\right)\left(1-\overline{\zeta}^{p-k-j}\right) - \sum_{k=1}^{p-1-j} \left(1-\zeta^{p-k-j}\right)\left(1-\overline{\zeta}^{p-k}\right) \\
&= \sum_{k=1}^{p-1-j} \left(1-\zeta^{p-k}-\overline{\zeta}^{p-k-j}+\zeta^{j}\right) - \sum_{k=1}^{p-1-j} \left(1-\zeta^{p-j-k}-\overline{\zeta}^{p-k}+\overline{\zeta}^{j}\right) \\
&= \sum_{k=1}^{p-1-j} \left(\overline{\zeta}^{p-k}-\zeta^{p-k}+\zeta^{p-j-k}-\overline{\zeta}^{p-j-k}\right) + (p-1-j)\left(\zeta^{j}-\overline{\zeta}^{j}\right) \\
&= \sum_{k=1}^{j} 2\left(\zeta^{k}-\overline{\zeta}^{k}\right) + (p-1-j)\left(\zeta^{j}-\overline{\zeta}^{j}\right) \\
&= \sum_{k=1}^{j-1} 2\left(\zeta^{k}-\overline{\zeta}^{k}\right) + (p+1-j)\left(\zeta^{j}-\overline{\zeta}^{j}\right).
\end{aligned}
$$

Hence for $j=1$, $\beta' M_1 \overline{\beta} = p\left(\zeta - \overline{\zeta}\right)$.

For $j = 2, \ldots, \frac{p-1}{2}$, we have

$$
\begin{aligned}
\beta' M_j \overline{\beta} - \beta' M_{p-j} \overline{\beta} &= \sum_{k=1}^{j} 2\left(\zeta^{k}-\overline{\zeta}^{k}\right) + (p-1-j)\left(\zeta^{j}-\overline{\zeta}^{j}\right) \\
&\quad - \sum_{k=1}^{p-j-1} 2\left(\zeta^{k}-\overline{\zeta}^{k}\right) - (p+1-p+j)\left(\zeta^{p-j}-\overline{\zeta}^{p-j}\right) \\
&= p\left(\zeta^{j}-\overline{\zeta}^{j}\right) - \sum_{k=j+1}^{p-j-1} 2\left(\zeta^{k}-\overline{\zeta}^{k}\right) \\
&= p\left(\zeta^{j}-\overline{\zeta}^{j}\right).
\end{aligned}
$$

So we get

$$
y_j = \frac{\zeta^{\frac{p+1}{2}}}{(1-\zeta)\,p} p\left(\zeta^{j}-\overline{\zeta}^{j}\right) = \frac{\zeta^{\frac{p+1}{2}}\zeta^{-j}\left(\zeta^{2j}-1\right)}{1-\zeta} = -\zeta^{\frac{p+1}{2}}\zeta^{-j}\left(-\zeta^{\frac{p+1}{2}}\right)^{2j-1} u_{2j} = u_{2j}.
$$

□

Proof of Theorem 8. Let $\mathfrak{a}$ be the ideal generated by the components of α. It is clear that $\mathfrak{a} = \mathcal{R}$ since $1 \in \mathfrak{a}$. Now applying Lemma 5.2 and Lemma 5.11, we obtain $\Delta^{-1}\alpha' M \overline{\alpha} = u_b u_{b+1}$. This completes the proof of Theorem 8. □

Chapter 6
Torsion in $SP_4(\mathbb{Z})$

We consider torsion elements of $SP_4(\mathbb{Z})$. The first question we consider is: for what positive integers $d\,(d \geq 2)$, is there a matrix $X \in SP_{2n}(\mathbb{Z})$ having order d? If X has order d, then its minimal polynomial $m_X(x)$ is a factor of $x^d - 1$, i.e. $m_X(x)$ is a product of some different cyclotomic polynomials, and its characteristic polynomial $f_X(x)$ is a product of some cyclotomic polynomials. Suppose $d = p_1^{s_1} \cdots p_t^{s_t}$ where $p_1, \ldots, p_t$ are different primes. According to a result of D. Sjerve [34], the degree of $f_X(x)$ is not less then $\phi(p_1^{s_1}) + \cdots + \phi(p_t^{s_t}) - 1$, so

$$\phi(p_1^{s_1}) + \cdots + \phi(p_t^{s_t}) \leq 2n + 1.$$

We get

If $n = 1$, then d must be 2, 3, 4, 6.

If $n = 2$, then d must be 2, 3, 4, 5, 6, 8, 10, 12.

Let $W_\lambda = \begin{pmatrix} 0 & -1 \\ 1 & -\lambda \end{pmatrix}$ and $W = W_1$. Clearly, $W_{-\lambda} = -W_\lambda'$ and $W_0 = -J_2$.

Proposition 6.1. *Suppose $X \in SP_2(\mathbb{Z})$ has order 3, 4, or 6. Then $f_X(x) = m_X(x) = x^2 + \lambda x + 1$, and $X \sim W_\lambda$ or W_λ', where $\lambda = 1$ (resp. 0, -1) if the order is 3 (resp. 4, 6).*

This is an application of Theorem 1 or a corollary of Lemma 6.5.

We denote by T_d the set of elements of order d in $SP_4(\mathbb{Z})$. I. Reiner gave a complete list of representatives of the conjugacy classes of involutions in all symplectic groups $SP_{2n}(\mathbb{Z})$ [30]. We state the special case for T_2 here without proof.

Proposition 6.2. *Any $X \in T_2$ is conjugate to one of the three following matrices*

$$-I_4, \qquad I_2 * (-I_2) \quad \text{or} \quad U \dotplus U' \tag{6.1}$$

where $U = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$.

Now we suppose that $d \geq 3$. Let $X \in T_d$. The possible minimal polynomials $m_X(x)$ and characteristic polynomials $f_X(x)$ are as follows:

When $d = 3$,

$$m(x) = (x^2 + x + 1), \qquad f(x) = (x^2 + x + 1)^2, \tag{6.2}$$

$$m(x) = (x - 1)(x^2 + x + 1), \qquad f(x) = (x - 1)^2(x^2 + x + 1). \tag{6.3}$$

When $d = 4$,

$$m(x) = (x^2 + 1), \qquad f(x) = (x^2 + 1)^2, \tag{6.4}$$

$$m(x) = (x - 1)(x^2 + 1), \qquad f(x) = (x - 1)^2(x^2 + 1), \tag{6.5}$$

$$m(x) = (x + 1)(x^2 + 1), \qquad f(x) = (x + 1)^2(x^2 + 1). \tag{6.6}$$

When $d = 5$,

$$m(x) = f(x) = x^4 + x^3 + x^2 + x^1 + 1. \tag{6.7}$$

When $d = 6$,

$$m(x) = (x^2 - x + 1), \qquad f(x) = (x^2 - x + 1)^2, \tag{6.8}$$

$$m(x) = (x - 1)(x^2 - x + 1), \qquad f(x) = (x - 1)^2(x^2 - x + 1), \tag{6.9}$$

$$m(x) = (x + 1)(x^2 - x + 1), \qquad f(x) = (x + 1)^2(x^2 - x + 1), \tag{6.10}$$

$$m(x) = (x + 1)(x^2 + x + 1), \qquad f(x) = (x + 1)^2(x^2 + x + 1), \tag{6.11}$$

$$m(x) = (x^2 - x + 1)(x^2 + x + 1), \qquad f(x) = (x^2 - x + 1)(x^2 + x + 1). \tag{6.12}$$

When $d = 8$,

$$m(x) = f(x) = x^4 + 1. \tag{6.13}$$

When $d = 10$,

$$m(x) = f(x) = x^4 - x^3 + x^2 - x + 1, \tag{6.14}$$

When $d = 12$,

$$m(x) = f(x) = (x^4 - x^2 + 1), \tag{6.15}$$

$$m(x) = f(x) = (x^2 + 1)(x^2 + x + 1), \tag{6.16}$$

$$m(x) = f(x) = (x^2 + 1)(x^2 - x + 1). \tag{6.17}$$

Remark. The characteristic polynomials (6.7), (6.13), (6.14) and (6.15) are irreducible over $\mathbb{Z}$. We have given a complete set of conjugacy classes for these cases (see Examples in Section 3.5).

Remark. The characteristic polynomials (6.16) and (6.17) are products of two strictly coprime S-polynomials. According to Theorem 6, all matrices with characteristic polynomials (6.16) or (6.17) are decomposable (see Section 4.2).

By Lemma 2.2 and Proposition 6.1, and the Remarks above, we obtain

Proposition 6.3. *The number of conjugacy classes in T_{12} is 10. A complete set of non-conjugate classes is given by*

$$I_2 \circ (-W), \quad I_2 \circ (-W'); \tag{6.18}$$

$$J_2 * W, \quad J_2 * W', \quad J_2' * W, \quad J_2' * W'; \tag{6.19}$$

$$J_2 * (-W), \quad J_2 * (-W'), \quad J_2' * (-W), \quad J_2' * (-W'); \tag{6.20}$$

with respect to characteristic polynomials (6.15), (6.16), (6.17).

For all other cases, we need to develop some new tools. In Section 6.1 we shall use symplectic complements to study the case where ± 1 is an eigenvalue of X. In Section 6.2 we discuss the case of characteristic polynomials (6.2), (6.4) and (6.8). Then in Section 6.3 we consider the last case of (6.12). Finally, in Section 6.4 we shall give a list of conjugacy classes which are realizable. We use the program Maple V to calculate most of our results in this chapter.

6.1 Symplectic Complements

A primitive integral $2n \times (j+k)$ matrix

$$\begin{pmatrix} A_{2n\times j} & B_{2n\times k} \end{pmatrix} \qquad j, k \leq n$$

which satisfies the conditions

$$A'JA = 0, \qquad B'JB = 0, \quad \text{and} \quad A'JB = \begin{pmatrix} I_k \\ 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} I_j & 0 \end{pmatrix}$$

(depending on whether $j \geq k$ or $j \leq k$) will be called a normal (j,k)-array. According to Theorem 5 every normal (j,k)-array can be completed to a symplectic matrix by placing $n-j$ columns after the first j columns and $n-k$ columns after the last k columns.

Remark. Let α, $\beta \in \mathbb{Z}^{2n}$. Clearly, α is $(1,0)$-array if and only if α is a primitive vector, and (α, β) is a normal $(1,1)$-array if and only if $\alpha' J \beta = 1$.

Lemma 6.1. *Suppose that $X \in SP_{2n}(\mathbb{Z})$ and $f_X(1) = 0$. Then*

$$X \sim \begin{pmatrix} 1 & \gamma' & a & \delta' \\ 0 & A & \alpha & B \\ 0 & 0 & 1 & 0 \\ 0 & C & \beta & D \end{pmatrix}$$

where $Y = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_{2(n-1)}(\mathbb{Z})$, $f_X(x) = (x-1)^2 f_Y(x)$, $a \in \mathbb{Z}$, and α, β, γ, $\delta \in \mathbb{Z}^{n-1}$ with

$$\begin{cases} \alpha &= A\delta - B\gamma, \\ \beta &= C\delta - D\gamma, \\ \gamma &= C'\alpha - A'\beta, \\ \delta &= D'\alpha - B'\beta. \end{cases} \tag{6.21}$$

Furthermore, if $Y \sim Y_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$, *then*

$$X \sim \begin{pmatrix} 1 & \gamma_1' & a_1 & \delta_1' \\ 0 & A_1 & \alpha_1 & B_1 \\ 0 & 0 & 1 & 0 \\ 0 & C_1 & \beta_1 & D_1 \end{pmatrix}.$$

Proof. Since 1 is an eigenvalue of X, there is a primitive vector $\eta \in \mathbb{Z}^{2n}$ such that $X\eta = \eta$. By Theorem 5, we can find a integer symplectic matrix P with η as its first column. Then

$$P^{-1}XP = X_1 = \begin{pmatrix} 1 & \gamma' & a & \delta' \\ 0 & A & \alpha & B \\ 0 & * & b & * \\ 0 & C & \beta & D \end{pmatrix} \in SP_{2n}(\mathbb{Z}).$$

By computing we can see that the $*$'s are 0, $b = 1$, $Y = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_{2(n-1)}(\mathbb{Z})$, and α, β, γ, δ satisfy (6.21). Thus $f_X(x) = (x-1)^2 g_Y(x)$.

The second part is easy, merely conjugate by $I*Q$, where $Q \in SP_2(\mathcal{D})$ and $Q^{-1}YQ = Y_1$. $\square$

Lemma 6.2. *Suppose* $X \in SP_4(\mathbb{Z})$, $m_X(x) = (x-1)(x^2 + \lambda x + 1)$ *where* $\lambda = 0, \pm 1$. *Then* X *is conjugate to one of*

$$I * W_\lambda \quad \text{and} \quad I * W_\lambda',$$

Moreover, these matrices are not conjugate.

Proof. It is clear that $I * W_\lambda \nsim I * W_\lambda'$ (cf. Lemma 2.2).

By Lemma 6.1, we get

$$X \sim X_1 = \begin{pmatrix} 1 & a_1 & b_1 & c_1 \\ 0 & A & d_1 & B \\ 0 & 0 & 1 & 0 \\ 0 & C & e_1 & D \end{pmatrix},$$

where $Y = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_2(\mathbb{Z})$ with $f_Y(x) = x^2 + \lambda x + 1$. Then, from Proposition 6.1, $Y \sim W_\lambda$ or W'_λ. Without loss the generality we assume $Y \sim W_\lambda$. Then

$$X \sim X_2 = \begin{pmatrix} 1 & a_2 & b_2 & c_2 \\ 0 & 0 & a_2 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & \lambda a_2 + c_2 & -\lambda \end{pmatrix} \sim X_3 = \begin{pmatrix} 1 & 0 & b & c \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & c & -\lambda \end{pmatrix},$$

where the last conjugacy is achieved by $Q = \begin{pmatrix} 1 & -a_2 \\ 0 & 1 \end{pmatrix} \dot{+} \begin{pmatrix} 1 & 0 \\ a_2 & 1 \end{pmatrix} \in SP_4(\mathbb{Z})$. We obtain $(\lambda + 2)b + c^2 = 0$ since $m_X(x) = (x - 1)(x^2 + \lambda x + 1)$. This implies $(\lambda + 2) \mid c$. Now we use Theorem 6 to see that X_3 is decomposable and use Proposition 6.1 to complete the proof. In fact let

$$P = \begin{pmatrix} 1 & k & & k \\ & -1 & -k & \\ & & 1 & \\ & & k & -1 \end{pmatrix} \in SP_4(\mathbb{Z})$$

where $k = \frac{c}{\lambda+2} \in \mathbb{Z}$. It is easy to check that $P^{-1} X_3 P = I * W_\lambda$. □

Similarly, we have

Lemma 6.3. *Suppose $X \in SP_4(\mathbb{Z})$, $m_X(x) = (x + 1)(x^2 + \lambda x + 1)$ where $\lambda = 0, \pm 1$. Then X is conjugate to one of*

$$(-I) * W_\lambda \quad \textit{and} \quad (-I) * W'_\lambda,$$

and these matrices are not conjugate.

Proof. Since $m_{-X}(x) = (x-1)(x^2 - \lambda x + 1)$, we have $-X \sim I * W_{-\lambda}$ or $I * W'_{-\lambda}$. Note that $-W_\lambda = W'_\lambda$. This complete the proof. $\square$

6.2 Minimal Representatives

Let $X \in SP_{2n}(\mathbb{Z})$ and $\eta = (x_1, \ldots, x_{2n})' \in \mathbb{Z}^{2n}$. If $a = \eta' JX\eta$ then we say that X represents a. The set of values represented by X will be denoted by $q(X)$. It is clear that $q(X)$ is a conjugacy invariant, for if $Y = Q^{-1}XQ$, where $Q \in SP_{2n}(\mathbb{Z})$, then

$$q(Y) = q(Q^{-1}XQ) = \left\{\eta' JQ^{-1}XQ\eta \mid \eta \in \mathbb{Z}^{2n}\right\},$$

and so putting $\xi = Q\eta$ gives

$$\xi' JX\xi = \eta' Q' JXQ\eta = \eta' JQ^{-1}XQ\eta = \eta' JY\eta.$$

Thus $q(Y) = q(X)$. Unfortunately, the converse is not necessarily true.

The set $q(X)$ is a set of integers, and consequently there is a non-zero η_0 in $\mathbb{Z}^{2n}$ such that $|\eta_0' JX\eta_0|$ is least. If both $\eta_0' JX\eta_0$ and $-\eta_0' JX\eta_0 = \eta_1' JX\eta_1$ occur, we resolve the ambiguity by choosing the non-negative value. We write $\mu(X) = \eta_0' JX\eta_0$. Clearly, if $\mu(X) \neq 0$, the minimizing vector x_0 must be primitive, and if $\mu(X) = 0$, we also can choose a primitive vector η_0 such that $\eta_0' JX\eta_0 = 0$.

Example. If X is quasi-decomposable, then $\mu(X) = 0$ since JX will have zero entries on the diagonal.

Lemma 6.4. *Let $f(x) = f_X(x)$ be the characteristic polynomial of X. Then*

$$|\mu(X)| \leq \left(\frac{4}{3}\right)^{n-\frac{1}{2}} \frac{|f(1)f(-1)|^{\frac{1}{2n}}}{2}. \tag{6.22}$$

Proof. Note that $\eta' JX\eta$ is a quadratic form over $\mathbb{Z}$. If M is a symmetric matrix belonging to $M_n(\mathbb{Z})$, and $a = \min\left\{|\eta' M\eta| \mid \eta \in \mathbb{Z}^{(n)}, \eta \neq 0\right\}$, then

$$a \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} |\det M|^{\frac{1}{n}}.$$

See [26]. Clearly, it is also true if M is a rational symmetric matrix.

We know that $\eta' JX\eta = \frac{1}{2}\eta'(JX + (JX)')\eta$, where $\frac{1}{2}(JX + (JX)')$ is a rational symmetric matrix. Because $(JX)' = X'J' = -X'J = -JX^{-1}$, and $|J| = |X| = 1$, we see that $|JX + (JX)'| = |JX - JX^{-1}| = |J||X^{-1}||X^2 - I| = f(1)f(-1)$. Hence

$$|\mu(X)| \leq \left(\frac{4}{3}\right)^{n-\frac{1}{2}} \frac{|f(1)f(-1)|^{\frac{1}{2n}}}{2}.$$

$\square$

Remark. Note if $X \in SP_4(\mathbb{Z})$ is a torsion element, then $|\mu(X)| \leq 1$ since $|\mu(X)|$ is integer and the maximum of $|f(1)f(-1)|$ is 16.

Lemma 6.5. *Suppose $X \in SP_{2n}(\mathbb{Z})$, and $1 \in q(X)$. Then*

$$X \sim \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & A & \alpha & B \\ 1 & \gamma' & a & \delta' \\ 0 & C & \beta & D \end{pmatrix},$$

where $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_{2(n-1)}(\mathbb{Z})$, $a \in \mathbb{Z}$, and $\alpha, \beta, \gamma, \delta \in \mathbb{Z}^{n-1}$ satisfy (6.21).

Proof. Since there is a primitive vector $\eta \in \mathbb{Z}^{2n}$ such that $\eta' JX\eta = 1$, we see that $(\eta, X\eta)$ is a normal $(1,1)$-array. Let P be the completion of the normal $(1,1)$-array $(\eta, X\eta)$ to a symplectic matrix. Then

$$P = \begin{pmatrix} \vdots & * & \vdots & * \\ \eta & * & X\eta & * \\ \vdots & * & \vdots & * \end{pmatrix}$$

and therefore

$$P^{-1}XP = X_1 = \begin{pmatrix} 0 & * & b & * \\ 0 & A & \alpha & B \\ 1 & \gamma' & a & \delta' \\ 0 & C & \beta & D \end{pmatrix} \in SP_{2n}(\mathbb{Z}).$$

The remainder of the proof is similar to that of Lemma 6.1. $\square$

Corollary 6.1. *Suppose $X \in SP_{2n}(\mathbb{Z})$, $m_X(x) = x^2+\lambda x+1$, with $1 \in q(X)$. Then $X \sim W_\lambda * Y$, where $Y \in SP_{2(n-1)}(\mathbb{Z})$ with $m_Y(x) = m_X(x)$.*

Proof. Since $X^2\eta = -\lambda X\eta - \eta$, we see that the entries of the matrix in Lemma 6.5 are: $a = -\lambda$, $\alpha = 0$, $\beta = 0$, and so $\gamma = 0$, $\delta = 0$. $\square$

Lemma 6.6. *Suppose $X \in SP_{2n}(\mathbb{Z})$, and $\mu(X) = 0$. Then*

$$X \sim \begin{pmatrix} 0 & A & \alpha & B \\ 1 & \gamma' & a & \delta \\ 0 & C & \beta & D \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

where $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SP_{2(n-1)}(\mathbb{Z})$, $a \in \mathbb{Z}$, and $\alpha, \beta, \gamma, \delta \in \mathbb{Z}^{n-1}$ satisfy (6.21).

Proof. Note that we have a normal $(2,0)$-array $(\eta, X\eta)$, where $\eta \in \mathbb{Z}^{2n}$ is primitive. $\square$

Lemma 6.7. *Suppose $X \in SP_4(\mathbb{Z})$, with $m_X(x) = x^2 + \lambda x + 1$, where $\lambda = 0, \pm 1$. Then*

1. *If $\mu(X) = 1$, then $X \sim W_\lambda * W_\lambda$.*
2. *If $\mu(X) = -1$, then $X \sim W'_\lambda * W'_\lambda$.*
3. *If $\mu(X) = 0$ and $\lambda = \pm 1$, then $X \sim W_\lambda * W'_\lambda$.*
4. *If $\mu(X) = 0$, $\lambda = 0$, and $1 \in q(X)$, then $X \sim W_0 * W'_0 = (-J_2) * J_2$.*
5. *If $\mu(X) = 0$, $\lambda = 0$, and $1 \notin q(X)$, then $X \sim W_0 \dotplus W_0 = (-I_2) \circ I_2$,*

Proof. (1) If $\mu(X) = 1$, then by Corollary 6.1, $X \sim W_\lambda * Y$, for some $Y \in SP_2(\mathbb{Z})$, with $m_Y(x) = x^2 + \lambda x + 1$. From Proposition 6.1, $Y \sim W_\lambda$ or W'_λ. Then $X \sim W_\lambda * W_\lambda$ or $W_\lambda * W'_\lambda$. But $\mu(W_\lambda * W'_\lambda) = 0$, hence $X \sim W_\lambda * W_\lambda$.

(2) If $\mu(X) = -1$, then $\mu(-X) = 1$. It is clear that $m_{-X}(x) = x^2 - \lambda x + 1$, hence $-X \sim W_{-\lambda} * W_{-\lambda}$, and thus $X \sim -(W_{-\lambda} * W_{-\lambda}) = W'_\lambda * W'_\lambda$.

(3)–(5) In the following we assume that $\mu(X) = 0$. By Lemma 6.6 we get

$$X \sim X_1 = \begin{pmatrix} W_\lambda & Y \\ 0 & W'^{-1}_\lambda \end{pmatrix}$$

where $Y = \begin{pmatrix} a & b \\ b & \lambda b - a \end{pmatrix}$, $a,\ b \in \mathbb{Z}$. Let $P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Then $P^{-1}X_1P = X(a)$, where $X(a) = \begin{pmatrix} 0 & -1 & a & 0 \\ 1 & -\lambda & 0 & -a \\ 0 & 0 & -\lambda & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. Let $Q = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Then $Q^{-1}X(a)Q = X(a-2)$. So we obtain $X \sim X(0)$ or $X(1)$.

It is clear that $1 \in q(X(0))$ if and only if λ is odd, and always $1 \in q(X(1))$. For the case where $1 \in q(X)$, we get $X \sim W_\lambda * W'_\lambda$. This completes the proofs of (3), (4) and (5). □

From Lemma 6.2, Lemma 6.3, and Lemma 6.7 we obtain the following two Propositions.

Proposition 6.4. *The number of conjugacy classes in T_3 is 5. A complete set of non-conjugate classes is given by*

$$W * W, \quad W' * W', \quad W * W'; \tag{6.23}$$

$$I_2 * W, \quad I_2 * W'. \tag{6.24}$$

with respect to characteristic polynomials (6.2), (6.3).

Proposition 6.5. *The number of conjugacy classes in T_4 is 8. A complete set of non-conjugate classes is given by*

$$J_2 * J_2, \qquad J'_2 * J'_2, \qquad J_2 * J'_2, \quad (-I_2) \circ I_2; \tag{6.25}$$

$$I_2 * J_2, \qquad I_2 * J_2'; \tag{6.26}$$

$$(-I_2) * J_2, \quad (-I_2) * J_2'. \tag{6.27}$$

with respect to characteristic polynomials (6.4), (6.5), (6.6).

6.3 The Case of $f(x) = x^4 + x^2 + 1$

In this section we discuss the case that $X \in SP_4(\mathbb{Z})$ has $f_X(x) = x^4 + x^2 + 1$. From Theorem 6 it follows that:

Lemma 6.8. *If X is decomposable, then X is conjugate to one of four non-conjugate matrices,*

$$W * (-W), \quad W * (-W'), \quad W' * (-W), \quad W' * (-W'). \tag{6.28}$$

Note that $m_{X^2}(x) = x^2 + x + 1$, hence X^2 is conjugate to one of three non-conjugate matrices

$$W * W, \quad W^2 * W^2, \quad W * W^2.$$

Without loss of generality we assume that $X^2 = X_1 * X_2$, where X_1 and X_2 are either W or W^2. We can express X as

$$X = P_1 * P_2 + P_3 \circ P_4 \tag{6.29}$$

where the P_i's are 2×2 matrices. Then

$$X^3 = X(X_1 * X_2) = P_1X_1 * P_2X_2 + P_3X_2 \circ P_4X_1,$$

$$X^3 = (X_1 * X_2)X = X_1P_1 * X_2P_2 + X_1P_3 \circ X_2P_4.$$

Note that X has order 6. Then $(JX^3)' = X'^3J' = -JX^{-3} = -JX^3$. Therefore we have

$$P_1 = aX_1^2, \quad P_2 = -aX_2^2, \quad P_3P_4 = (1-a^2)X_1, \quad P_4P_3 = (1-a^2)X_2, \tag{6.30}$$

and $\det P_3 = \det P_4 = 1 - a^2$ for some $a \in \mathbb{Z}$. Also, since $X \in SP_4(\mathbb{Z})$, we have

$$\begin{cases} P_1'JP_1 + P_4'JP_4 = J, \\ P_2'JP_2 + P_3'JP_3 = J, \\ P_1'JP_3 + P_4'JP_2 = 0, \end{cases} \quad \text{and} \quad \begin{cases} P_1JP_1' + P_3JP_3' = J, \\ P_2JP_2' + P_4JP_4' = J, \\ P_1JP_4' + P_3JP_2' = 0. \end{cases} \tag{6.31}$$

We state the following lemmas without proof. They are very easy to verify. Let P be a 2×2 matrix.

Lemma 6.9. *If $PW = WP$, then P has form $P = aI + bW$.*

Lemma 6.10. *If $PW + WP = 0$ then $P = 0$.*

Lemma 6.11. *If $PW = W^2P$, then $P = \begin{pmatrix} a & b \\ a+b & -a \end{pmatrix}$.*

Clearly, if $P = aI + bW$, then $\det(P) = a^2 - ab + b^2$.

Now suppose that $X^2 = W^l * W^l$. From Equation (6.30), we see that $P_3 = bI + cW$, where $b^2 - bc + c^2 = 1 - a^2$. Hence $a = -1, 0, 1$.

If $a = \pm 1$, then $b = c = 0$, thus X is decomposable.

If $a = 0$, then $P_1 = P_2 = 0$, hence $X = P_3 \circ P_4$ is quasi-decomposable. We know that the Diophantine equation $b^2 - bc + c^2 = 1$ has six integral solutions.

1. $b = 1$, $c = 0$, then $P_3 = I$, $P_4 = W^l$;
2. $b = 1$, $c = 1$, then $P_3 = -W^2$, $P_4 = -W^{l+1}$;
3. $b = 0$, $c = 1$, then $P_3 = W$, $P_4 = W^{l-1}$;
4. $b = 0$, $c = -1$, then $P_3 = -W$, $P_4 = -W^{l-1}$;
5. $b = -1$, $c = 0$, then $P_3 = -I$, $P_4 = -W^l$;
6. $b = -1$, $c = -1$, then $P_3 = W^2$, $P_4 = W^{l+1}$.

By Lemma 2.1 and $I \circ W^l \sim W^{2l} \circ W^{2l}$ (use $I * W^l$ as the conjugating matrix) we see that the matrices $P_3 \circ P_4$, in all 6 cases, are conjugate. So we obtain

Lemma 6.12. *Suppose $X^2 \sim W^l * W^l$, $l = 1, 2$. If X is indecomposable, then it is quasi-decomposable and conjugate to $I \circ W^l$.*

Now we consider the case that $X^2 = W * W^2$.

Lemma 6.13. *Suppose $X^2 \sim W * W^2$. Then $X \sim X(a, b, c)$, where*

$$X(a,b,c) = \begin{pmatrix} a & b & -a & c \\ -c & 0 & b+c & -a \\ a & b+c & 0 & -b \\ b & a & c & -a \end{pmatrix} \tag{6.32}$$

for integers a, b, c satisfying $a^2 - 1 = b^2 + bc + c^2$.

Proof. From (6.30), we see that $X = (-aW^2) * (aW) + P_3P_4$, where $P_3P_4 = (1-a^2)W$ and $P_3W = P_3W^2$. Applying Lemma 6.11, we get

$$P_3 = \begin{pmatrix} b & c \\ b+c & -b \end{pmatrix} \quad \text{and} \quad P_4 = \begin{pmatrix} -c & b+c \\ b & c \end{pmatrix}.$$

It is clear that $\det P_3 = -(b^2 + bc + c^2) = 1 - a^2$. ◻

Remark. For any integral solution of $a^2 - 1 = b^2 + bc + c^2$, $X(a, b, c) \in SP_4(\mathbb{Z})$, and its characteristic polynomial is (6.12). Clearly, $a \neq 0$.

Remark. An easy calculation proves that $X^5(a, b, c) \sim X(-a, b, c)$.

Lemma 6.14. *$X(a, b, c)$ is decomposable if and only if a is odd.*

Proof. It is easy to check that $\frac{1}{2}(X^3 - I) \in M_4(\mathbb{Z})$ if and only if a is odd. ◻

Lemma 6.15. *$\mu(X(a, b, c))$ has the same sign as the non-zero number a.*

Proof. Let $M = JX(a, b, c) + (JX(a, b, c))'$. We want to prove that M is positive definite if

$a > 0$, and M is negative definite if $a < 0$. We see that

$$M = \begin{pmatrix} 2a & 2b+c & -a & -b+c \\ 2b+c & 2a & -b+c & -a \\ -a & -b+c & 2a & -b-2c \\ -b+c & -a & -b-2c & 2a \end{pmatrix}.$$

Its principal minors are:

$$M_1 = 2a,$$

$$M_2 = \det \begin{pmatrix} 2a & 2b+c \\ 2b+c & 2a \end{pmatrix} = 4a^2 - 4b^2 - 4bc - c^2 = 4 + 3c^2 > 0,$$

$$M_3 = \det \begin{pmatrix} 2a & 2b+c & -a \\ 2b+c & 2a & -b+c \\ -a & -b+c & 2a \end{pmatrix} = 6(a^3 - ab^2 - abc - ac^2) = 6a,$$

$$M_4 = \det A = 9.$$

Hence M is positive or negative definite dependent according as $a > 0$ or $a < 0$, $\square$

Corollary 6.2. *$X(a, b, c)$ is quasi-indecomposable.*

Corollary 6.3. *$X(a_1, b_1, c_1) \not\sim X(a_2, b_2, c_2)$ if $a_1 a_2 < 0$.*

If a is even, then $X(a, b, c)$ is also indecomposable. It is known that the Diophantine equation $a^2 - 1 = b^2 + bc + c^2$ has infinitely many solutions with a even. There are infinitely many $X \in SP_4(\mathbb{Z})$, which are neither quasi-decomposable nor decomposable, of the form $X(a, b, c)$. In the following, we want to show that there are just two classes amongst $X(a, b, c)$, where a is even. For this purpose, we let

$$V(x, y, z) = \begin{pmatrix} 2x & 0 & -y & x \\ 0 & -2x & -x & -z \\ z & x & -x & z \\ -x & y & y & x \end{pmatrix}$$

where

$$\begin{cases} x = a - b - c, \\ y = 2a - 2b - c, \\ z = 2a - b - 2c, \end{cases} \qquad \text{or} \qquad \begin{cases} a = -3x + y + z, \\ b = -2x + z, \\ c = -2x + y. \end{cases}$$

Then $V(x, y, z) = QX(a, b, c)Q^{-1}$, where

$$Q = \begin{pmatrix} 1 & 1 & -1 & 0 \\ 0 & -1 & -1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

It is easy to see that $a^2 - 1 = b^2 + bc + c^2$ if and only if $yz = 3x^2 + 1$, and a is even if and only if $x + y + z$ is even, and also $a > 0$ if and only if $y > 0$. Furthermore, we have

Lemma 6.16. *Let x, y, z be integers satisfy $yz = 3x^2 + 1$ and $x + y + z$ is even. Then*

1. *If $y > 0$, then $V(x, y, z) \sim V(0, 1, 1)$;*

2. *If $y < 0$, then $V(x, y, z) \sim V(0, -1, -1)$.*

Proof. Suppose $yz = 3x^2 + 1$, and $x + y + z$ is even. If y is even, then $y = 4k$, where k is odd. The reason for this is that x is odd, and then z is odd and $3x^2 + 1 = 4l$ where l is odd. If p is an odd prime and $y \equiv 0 \pmod{p}$, then $p \equiv 1 \pmod{3}$. This is because $p \neq 3$, and $3x^2 + 1 \equiv 0 \pmod{p}$. Thus we see that y has the form

$$y = \pm 4^r p_1^{r_1} \cdots p_t^{r_t}$$

where $r = 0, 1$, $r_i \geq 0$, and the p_i are primes of the form $3k + 1$.

Now suppose $y > 0$. First we want to prove there is a solution (u, v) of the Diophantine equation $y = 3u^2 + v^2$ satisfying $u + xv \equiv 0 \pmod{y}$.

If $y = 1$ then $(0, 1)$ is a such solution.

If $y = 4$, then $x \equiv \pm 1 \pmod 4$. A solution is $(1, \mp 1)$.

If y is an odd prime and $y \equiv 1 \pmod 3$ then it is well known that there are $a, b \in \mathbb{Z}$ such that $3a^2 + b^2 = y$, which implies $(a - xb)(a + xb) = a^2 - x^2b^2 = a^2(3x^2+1) - yx^2 \equiv 0 \pmod y$. Hence either $a - xb \equiv 0 \pmod y$ or $a + xb \equiv 0 \pmod y$. So either $(a, -b)$ or (a, b) is a such solution.

In general, we use induction on the factors of y. Suppose $y = y_1 y_2$, and (u_i, v_i) are solutions for y_i (for $i = 1, 2$), that is $y_i = 3u_i^2 + v_i^2$ and $u_i + xv_i \equiv 0 \pmod y$. Let

$$\begin{cases} u = u_1 v_2 + u_2 v_1, \\ v = v_1 v_2 - 3u_1 u_2. \end{cases}$$

Then $3u^2 + v^2 = y$ and

$$\begin{aligned} (u + xv)x &= (u_1v_2 + u_2v_1)x + (v_1v_2 - 3u_1u_2)x^2 \\ &\equiv xv_2(u_1 + xv_1) + u_2v_1x + u_1u_2 \pmod y \\ &= (u_1 + xv_1)(u_2 + xv_2) \equiv 0 \pmod y \end{aligned}$$

So $u + xv \equiv 0 \pmod y$ since $(x, y) = 1$. Therefore (u, v) is a solution for y.

Now we can complete the proof. Suppose $y = 3u^2 + v^2$ and $u + vx \equiv 0 \pmod y$. Then $v - 3xu \equiv v + 3x^2v = (3x^2+1)v \equiv 0 \pmod y$. Let

$$P = \begin{pmatrix} v & u & -u & v \\ \frac{u+xv}{y} & \frac{v-3xu}{y} & \frac{v-3xu}{y} & -\frac{u+xv}{y} \\ \frac{u+xv}{y} & \frac{3xu-v}{y} & 0 & \frac{2(u+xv)}{y} \\ -v & u & 2u & 0 \end{pmatrix}.$$

Then $P \in SP_4(\mathbb{Z})$ and $PV(0,1,1)P^{-1} = V(x, y, z)$. That is $V(0,1,1) \sim V(x, y, z)$.

The second part is similar. $\square$

Remark. The u, v in the proof are coprime. We see that there is a primitive solution of the Diophantine equation $3u^2 + v^2 = m$ if m is a product of a power of 4 and odd primes of form $6k + 1$.

Putting all the results from Lemmas 6.2, 6.3, 6.7, 6.8, 6.12, 6.13 and 6.16 together, we have

Proposition 6.6. *Any $X \in T_6$, is conjugate to one of following matrices*

$$-(W * W), \quad -(W' * W'), \quad -(W * W'); \tag{6.33}$$

$$I_2 * (-W), \quad I_2 * (-W'); \tag{6.34}$$

$$-(I_2 * W), \quad -(I_2 * W'); \tag{6.35}$$

$$(-I_2) * W, \quad (-I_2) * W'; \tag{6.36}$$

$$W * (-W), \quad W * (-W'), \quad W' * (-W), \quad W' * (-W');$$

$$I \circ W, \quad I \circ W', \quad V(0,1,1), \quad V(0,-1,-1). \tag{6.37}$$

with respect to characteristic polynomials (6.8), (6.9), (6.10), (6.11), (6.12).

6.4 Realizable Torsion

In this section we address the question of which classes of torsion in $SP_4(\mathbb{Z})$ can be realized by a cyclic action on some Riemann surface.

Proposition 6.7. *A complete list of realizable classes in $SP_4(\mathbb{Z})$ is as follows*

$$\text{Order 2,} \quad -I_4, \quad U \dotplus U'; \tag{6.38}$$

$$\text{Order 3,} \quad W * W'; \tag{6.39}$$

$$\text{Order 4,} \quad (-J_2) * J_2; \tag{6.40}$$

$$\text{Order 5,} \quad Y, \quad Y^2, \quad Y^3, \quad Y^4; \tag{6.41}$$

$$\text{Order 6,} \quad -(W * W'), \quad V(0,1,1), \quad V(0,-1,-1); \tag{6.42}$$

$$\text{Order 8,} \quad Z, \quad -Z; \tag{6.43}$$

$$\text{Order 10,} \quad -Y, \quad -Y^2, \quad -Y^3, \quad -Y^4 \tag{6.44}$$

where $U = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 \\ 1 & 1 & -1 & 0 \end{pmatrix}$, *and* $Z = \begin{pmatrix} 0 & -1 & 1 & 0 \\ -1 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$.

Consider the short exact sequence of groups

$$1 \to \Pi \to \Gamma \xrightarrow{\theta} G \to 1 \tag{6.45}$$

where $\Gamma = \Gamma(g_0; m_1, \ldots, m_t)$, G is a cyclic group and Π is torsion free. Recall the Riemann-Hurwitz formula

$$\frac{2(g-1)}{|G|} = 2(g_0 - 1) + \sum_{i=1}^{t} \left(1 - \frac{1}{m_i}\right),$$

where g is the genus of $\mathbb{U}/\Pi$. For $g = 2$ the Riemann-Hurwitz formula becomes

$$\sum_{i=1}^{t} \left(1 - \frac{1}{m_i}\right) = \frac{2}{|G|} + 2(1 - g_0). \tag{6.46}$$

Hence g_0 must be 0 or 1. For $g_0 = 0$ (resp. 1) we solve (6.46) for t and the m_i. Then for each solution we find a Fuchsian group Γ and an epimorphism $\theta : \Gamma \to G$ with torsion free kernel. To prove the realizability we choose a fundamental domain for Γ and use it to determine an intersection matrix. We illustrate this for the case of order 6; the other cases being similar.

Suppose $G = \mathbb{Z}_6$. If $g_0 = 1$, then (6.46) has no solution. We assume that $g_0 = 0$. We can find three solutions for (6.46).

(i) $t = 3$, $m_1 = 3$, $m_2 = m_3 = 6$,

(ii) $t = 4$, $m_1 = m_2 = 2$, $m_3 = m_4 = 3$,

(iii) $t = 4$, $m_1 = m_2 = m_3 = 2$, $m_4 = 6$.

If $t = 4$ and $\Gamma = \Gamma(0; 2, 2, 2, 6)$, then there is no epimorphism θ such that Π is torsion free. So we need only consider the first two cases.

Case I, $t = 3$, $m_1 = 3$, $m_2 = m_3 = 6$. That is

$$\Gamma = \Gamma(0; 3, 6, 6) = \left\langle A, B_1, B_2 | A^3 = B_1^6 = B_2^6 = AB_1B_2 = 1 \right\rangle.$$

There are two epimorphisms $\Gamma \to \mathbb{Z}_6$:

$$\theta_1 : \begin{cases} A \to T^4, \\ B_1 \to T, \\ B_2 \to T, \end{cases} \qquad \text{or} \qquad \theta_2 : \begin{cases} A \to T^2, \\ B_1 \to T^5, \\ B_2 \to T^5, \end{cases}$$

where T is a fixed generator of $\mathbb{Z}_6$.

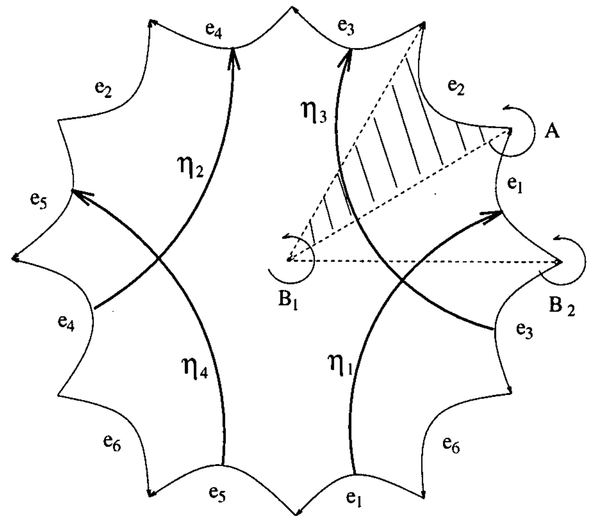

Figure 6.1: Fundamental Domain (order 6)

We first consider the case of the epimorphism θ_1. A particular fundamental domain of Π (see Figure 6.1) consists of 6 copies of the fundamental domain of Γ obtained by the 6 rotations B_1^k $(k = 0, \ldots, 5)$. The sides with the same label are identified in the Riemann surface $S = \mathbb{U}/\Pi$. It is easy to verify that $[\eta_1], [\eta_2], [\eta_3], [\eta_4]$ is a canonical basis of $H_1(S)$. θ_1 induces a homomorphism $T_* : H_1(S) \to H_1(S)$ given by

$$T_* : \begin{cases} \eta_1 \to \eta_3, \\ \eta_2 \to \eta_4, \\ \eta_3 \to -\eta_1 + \eta_4, \\ \eta_4 \to -\eta_2 + \eta_3. \end{cases}$$

Hence the matrix of T_* with respect to $[\eta_1], [\eta_2], [\eta_3], [\eta_4]$ is $V(0,1,1)$, and so $V(0,1,1)$ is realizable. Similarly, consideration of θ_2 proves that $V(0,-1,-1)$ is realizable.

Case II, $t = 4$, $m_1 = m_2 = 2$, $m_3 = m_4 = 3$. That is

$$\Gamma = \Gamma(0; 2, 2, 3, 3) = \left\langle A_1, A_2, B_1, B_2 | A_1^2 = A_2^2 = B_1^3 = B_2^3 = A_1 A_2 B_1 B_2 = 1 \right\rangle.$$

There are two epimorphisms $\theta : \Gamma \to \mathbb{Z}_6$

$$\theta : \begin{cases} A_1 \to T^3, \\ A_2 \to T^3, \\ B_1 \to T^2 \text{ (resp. } T^4), \\ B_2 \to T^4 \text{ (resp. } T^2). \end{cases}$$

Each θ induces an action, denoted by T, on some Riemann surface S. Consider that epimorphism θ such that $\theta(B_1) = T^2$. Let X be the symplectic matrix of T_* with respect to a canonical basis of $H_1(S)$. From a result of Macbeath[21], we see that T is fixed point free, and therefore $\mathrm{tr}(X) = 2$. Then X must be conjugate to one of the three matrices

$$-(W * W), \quad -(W' * W'), \quad -(W * W').$$

See Proposition 6.6. On the other hand, $X^2 \sim W * W'$. Hence $X \sim -(W * W')$, and so $-(W * W')$ is realizable. The other epimorphism leads to the same conjugate class. This completes the proof of the case of order 6.

Chapter 7

The Eichler Trace of $\mathbb{Z}_p$ Actions on Riemann Surfaces

7.1 The Eichler Trace

In this section we prove Theorem 9, 10 and 11. We begin by observing that the set A is not a subgroup of $\mathbb{Z}[\zeta]$. To see this suppose that $\chi \in A$, that is

$$\chi = 1 + \sum_{j=1}^{t} \frac{1}{\zeta^{k_j} - 1}$$

is the Eichler trace of some automorphism $T\colon S \to S$. The possible values for the number of fixed points are $t = 0,\ 2,\ 3, \ldots,$ and therefore the possible values of $\chi + \bar{\chi} = 2 - t$ are $2,\ 0,\ -1,\ -2, \ldots$ We also have $\bar{\chi} \in A$ since

$$\bar{\chi} = 1 + \sum_{j=1}^{t} \frac{1}{\zeta^{-k_j} - 1}$$

is the trace of $T^{-1}\colon S \to S$. Therefore, if A were a subgroup we would have $\chi + \bar{\chi} = 2 - t \in A$, and hence $\mathbb{Z}$ would be a subgroup of A. But if $n \in A$ is an integer, $n \geq 2$, then $n + \bar{n} = 2n \geq 4$ is not of the form $2 - t$ for an admissible t. Therefore A is not a subgroup.

Recall that $\widehat{A}$ is the set of realizable Eichler traces modulo $\mathbb{Z}$.

Proposition 7.1. *$\widehat{A}$ is a subgroup of $\widehat{\mathbb{Z}[\zeta]}$.*

Proof. Suppose χ_1 and χ_2 are in A, say

$$\chi_1 = 1 + \sum_{j=1}^{t} \frac{1}{\zeta^{k_j} - 1}, \quad \chi_2 = 1 + \sum_{j=1}^{u} \frac{1}{\zeta^{l_j} - 1}.$$

Therefore $\widehat{\chi_1} + \widehat{\chi_2} = \widehat{\chi}$, where $\chi = 1 + \sum_{j=1}^{t} \frac{1}{\zeta^{k_j}-1} + \sum_{j=1}^{u} \frac{1}{\zeta^{l_j}-1}$. If χ_1 and χ_2 are represented by $T_1\colon S_1 \to S_1$ and $T_2\colon S_2 \to S_2$ respectively, then χ can be represented by the equivariant connected sum of T_1 and T_2. Namely, for $j = 1, 2$ find discs D_j in S_j such that $D_j, T_j(D_j), \ldots, T_j^{p-1}(D_j)$ are mutually disjoint. Excise all discs $T^k(D_j)$, $k = 0, 1, \ldots, p-1$, from S_j, $j = 1, 2$, and then take the connected sum by matching $\partial(T^k(D_1))$ to $\partial(T^k(D_2))$ for $k = 0, 1, \ldots, p-1$. The resulting surface S has p tubes joining S_1 and S_2. The automorphisms T_1, T_2 can be extended to an automorphism $T\colon S \to S$ by permuting the tubes. The Eichler trace of T is χ. Thus $\widehat{A}$ is closed under sums.

If $\chi \in A$ then also $\bar{\chi} \in A$ and $\chi + \bar{\chi} = 2 - t$. Therefore $\bar{\chi}$ is the inverse of χ once we reduce modulo the integers. The identity element of $\widehat{A}$ is represented by any fixed point free action. □

To determine the index of $\widehat{A}$ in $\widehat{B}$ we need a basis for $\widehat{B}$, but first we find a basis for B. Let $m = (p-1)/2$.

Definition 7.1. Define elements $\theta_1, \theta_2, \ldots, \theta_m$ in $\mathbb{Z}[\zeta]$ by

$$\theta_1 = \zeta + \sum_{j=m+1}^{p-2} \zeta^j \quad \text{and} \quad \theta_k = \zeta^k - \zeta^{-k},\ 2 \le k \le m.$$

Proposition 7.2. *A basis of B is given by the $m+1$ elements $1, \theta_1, \theta_2, \ldots, \theta_m$.*

Proof. Suppose $\chi = \sum_{j=0}^{p-2} a_j \zeta^j \in \mathbb{Z}[\zeta]$. Then a short calculation gives

$$\chi + \bar{\chi} = 2a_0 - a_1 + \sum_{j=2}^{p-2} (a_j + a_{p-j} - a_1)\, \zeta^j,$$

and therefore $\chi \in B$ if, and only if, $a_j + a_{p-j} = a_1$, $2 \le j \le p-2$. Solving for $a_{m+1}, \ldots, a_{p-2}$ in terms of $a_1, \ldots, a_m$ and substituting into χ gives

$$\chi = a_0 + a_1\theta_1 + a_2\theta_2 + \cdots + a_m\theta_m.$$

Thus the elements $1, \theta_1, \theta_2, \ldots, \theta_m$ form a spanning set for B.

Now suppose some linear combination is zero, say $a_0 + a_1\theta_1 + a_2\theta_2 + \cdots + a_m\theta_m = 0$. It is easy to see that this is equivalent to

$$a_0 + a_1\zeta + \cdots + a_m\zeta^m + (a_1 - a_m)\zeta^{m+1} + \cdots + (a_1 - a_2)\zeta^{p-2} = 0.$$

Thus we get $a_0 = a_1 = a_2 = \cdots = a_m = 0$, that is the elements are linearly independent. $\square$

Remark. Every integer $n \in B$ since $\theta_1 + \overline{\theta}_1 = -1$. We also have $\zeta - \zeta^{-1} \in B$; in fact

$$\zeta - \zeta^{-1} = 1 + 2\theta_1 + \theta_2 + \cdots + \theta_m.$$

It follows that the elements $1,\ \zeta - \zeta^{-1},\ \zeta^2 - \zeta^{-2}, \ldots, \zeta^m - \zeta^{-m}$ form a basis for an index 2 subgroup of B.

An immediate corollary of Proposition 7.2 is

Corollary 7.1. *$\widehat{B}$ is a free abelian group of rank $(p-1)/2$. A basis is given by the elements*

$$\widehat{\theta_1},\ \widehat{\theta_2},\ \ldots,\ \widehat{\theta_m}.$$

Before completing the calculation of the index of $\widehat{A}$ in $\widehat{B}$ we first consider Question 4 from Chapter 1. Thus suppose two elements from A have the same Eichler trace, say

$$1 + \sum_{j=1}^{t} \frac{1}{\zeta^{k_j} - 1} = 1 + \sum_{j=1}^{u} \frac{1}{\zeta^{l_j} - 1}.$$

This leads us into consideration of when certain linear combinations of the elements $\frac{1}{\zeta^k - 1}$ are zero, that is we want to solve the equation $\sum_{k=1}^{p-1} \frac{x_k}{\zeta^k - 1} = 0$ for the integers x_k.

If s is any integer relatively prime to p then let $R(s)$ denote that integer q such that $1 \le q \le p-1$ and $q \equiv s \pmod p$, that is, $s = [s/p]p + R(s)$. In what follows $\sum_{jk\equiv n}$ denotes the sum over all ordered pairs (j,k) such that $jk \equiv n \pmod p$ and $1 \le j \le p-1$.

Lemma 7.1.

$$\sum_{k=1}^{p-1} \frac{x_k}{\zeta^k - 1} = -\frac{1}{p} \sum_{jk\equiv -1} jx_k + \frac{1}{p} \sum_{n=1}^{p-2} \left(\sum_{jk\equiv n} jx_k - \sum_{jk\equiv -1} jx_k \right) \zeta^n.$$

Proof. We use the identity $\frac{1}{\zeta^k-1} = \frac{1}{p}\sum_{j=1}^{p} j\zeta^{k(j-1)}$ and get

$$\begin{aligned}
\sum_{k=1}^{p-1}\frac{x_k}{\zeta^k-1} &= \frac{1}{p}\sum_{j=1}^{p}\sum_{k=1}^{p-1} jx_k\zeta^{k(j-1)} \\
&= \frac{1}{p}(x_1+\cdots+x_{p-1}) + \frac{1}{p}\sum_{j=2}^{p}\sum_{k=1}^{p-1} jx_k\zeta^{k(j-1)} \\
&= \frac{1}{p}(x_1+\cdots+x_{p-1}) + \frac{1}{p}\sum_{n=1}^{p-1}\left(\sum_{jk\equiv n}(j+1)x_k\right)\zeta^n \\
&= \frac{1}{p}(x_1+\cdots+x_{p-1}) + \frac{1}{p}\sum_{n=1}^{p-2}\left(\sum_{jk\equiv n}(j+1)x_k\right)\zeta^n + \frac{1}{p}\left(\sum_{jk\equiv -1}(j+1)x_k\right)\zeta^{p-1}.
\end{aligned}$$

Now substitute $\zeta^{p-1} = -1-\zeta-\cdots-\zeta^{p-2}$ into the last term to see that

$$\begin{aligned}
\sum_{k=1}^{p-1}\frac{x_k}{\zeta^k-1} &= \frac{1}{p}(x_1+\cdots+x_{p-1}) + \frac{1}{p}\sum_{n=1}^{p-2}\left(\sum_{jk\equiv n}(j+1)x_k - \sum_{jk\equiv -1}(j+1)x_k\right)\zeta^n \\
&- \frac{1}{p}\sum_{jk\equiv -1}(j+1)x_k \\
&= -\frac{1}{p}\sum_{jk\equiv -1} jx_k + \frac{1}{p}\sum_{n=1}^{p-2}\left(\sum_{jk\equiv n} jx_k - \sum_{jk\equiv -1} jx_k\right)\zeta^n.
\end{aligned}$$

□

As a corollary we get

Corollary 7.2. $\sum_{k=1}^{p-1}\frac{x_k}{\zeta^k-1} = 0$ *if, and only if,* $\sum_{jk\equiv n} jx_k = 0$, *for* $1 \le n \le p-1$.

Now it is convenient to change the variables $x_1,\ldots,x_{p-1}$ to new variables $y_1,\ldots,y_{p-1}$ according to the equation

$$y_l = x_k, \quad \text{where } kl \equiv 1 \pmod{p}. \tag{7.1}$$

Then Corollary 7.2 becomes

Corollary 7.3. $\sum_{k=1}^{p-1}\frac{x_k}{\zeta^k-1} = 0$ *if, and only if,* $\sum_{k=1}^{p-1} R(nk)y_k = 0$, *for* $1 \le n \le p-1$.

The coefficient matrix of this linear system is the $(p-1)\times(p-1)$ matrix M whose (i,j) entry is $M_{(i,j)} = R(ij)$. To solve this system of $p-1$ equations in $p-1$ unknowns y_k we apply a sequence of row and column operations to the matrix M. We use the fact that $R(ij) + R((p-i)j) = p$. Recall that $m = (p-1)/2$.

1. Adding the i^{th} row to the $(p-i)^{th}$ row, $1 \le i \le m$, yields the matrix

$$M_1 = \begin{pmatrix} 1 & 2 & \dots & m & m+1 & m+2 & \dots & p-1 \\ 2 & 4 & \dots & 2m & 1 & 3 & \dots & p-2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ i & R(2i) & \dots & R(mi) & R((m+1)i) & R((m+2)i) & \dots & R((p-1)i) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m & R(2m) & \dots & R(m^2) & R((m+1)m) & R((m+2)m) & \dots & R((p-1)m) \\ p & p & \dots & p & p & p & \dots & p \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p & p & \dots & p & p & p & \dots & p \end{pmatrix}$$

2. Adding the j^{th} column to the $(p-j)^{th}$ column, $1 \le j \le m$, yields the matrix

$$M_2 = \begin{pmatrix} 1 & 2 & \dots & m & p & p & \dots & p \\ 2 & 4 & \dots & 2m & p & p & \dots & p \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ i & R(2i) & \dots & R(mi) & p & p & \dots & p \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m & R(2m) & \dots & R(m^2) & p & p & \dots & p \\ p & p & \dots & p & 2p & 2p & \dots & 2p \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p & p & \dots & p & 2p & 2p & \dots & 2p \end{pmatrix}$$

3. Subtracting the $(m+1)^{st}$ row from rows $m+2, \dots, p-1$, and then subtracting the $(m+1)^{st}$ column from columns $m+2, \dots, p-1$ gives the new coefficient matrix

$$M_3 = \begin{pmatrix} 1 & 2 & \dots & m & p & 0 & \dots & 0 \\ 2 & 4 & \dots & 2m & p & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ i & R(2i) & \dots & R(mi) & p & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m & R(2m) & \dots & R(m^2) & p & 0 & \dots & 0 \\ p & p & \dots & p & 2p & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

The variables z_k for this coefficient matrix are related to the y_k by the equations

$$z_k = y_k - y_{p-k},\ 1 \leq k \leq m,\ z_{m+1} = y_{m+1} + \cdots + y_{p-1},\ z_{m+j} = y_{m+j},\ 2 \leq j \leq p-1.$$

Examination of the last $m-1$ columns of M_3 reveals that $z_{m+2}, \dots,\ z_{p-1}$ are completely independent; whereas, $z_1, \dots, z_{m+1}$ must satisfy the matrix equation

$$\begin{pmatrix} 1 & 2 & \dots & m & p \\ 2 & 4 & \dots & 2m & p \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ i & R(2i) & \dots & R(mi) & p \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ m & R(2m) & \dots & R(m^2) & p \\ p & p & \dots & p & 2p \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_i \\ \vdots \\ z_m \\ z_{m+1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$$

Now we apply another sequence of row and column operations to this last coefficient matrix.

1. Subtracting i times the first row from the i^{th} row, $2 \leq i \leq m$, yields the coefficient

matrix

$$\begin{pmatrix} 1 & 2 & \dots & j & \dots & m & p \\ 0 & 0 & \dots & 0 & \dots & 0 & -p \\ 0 & 0 & \dots & -[3j/p]p & \dots & -[3m/p]p & -2p \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -[ij/p]p & \dots & -[im/p]p & -(i-1)p \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -[mj/p]p & \dots & -[m^2/p]p & -(m-1)p \\ p & p & \dots & p & \dots & p & 2p \end{pmatrix}$$

2. Subtracting j times the first column from the j^{th} column, $2 \le j \le m$, yields the matrix

$$\begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 & p \\ 0 & 0 & \dots & 0 & \dots & 0 & -p \\ 0 & 0 & \dots & -[3j/p]p & \dots & -[3m/p]p & -2p \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -[ij/p]p & \dots & -[im/p]p & -(i-1)p \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -[mj/p]p & \dots & -[m^2/p]p & -(m-1)p \\ p & -p & \dots & -(j-1)p & \dots & -(m-1)p & 2p \end{pmatrix}$$

The new variables w_j, after these last column operations, are related to the z_j by the equations $w_1 = z_1 + 2z_2 + \cdots + mz_m$ and $w_j = z_j$, $2 \le j \le m+1$.

It follows that $w_1 = w_{m+1} = 0$ and $w_2, \ \dots, \ w_m$ are related by the equations

$$w_2 + 2w_3 + \cdots + (m-1)w_m = 0,$$

$$\begin{pmatrix} -[9/p]p & \dots & -[3j/p]p & \dots & -[3m/p]p \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ -[3i/p]p & \dots & -[ij/p]p & \dots & -[im/p]p \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ -[3m/p]p & \dots & -[mj/p]p & \dots & -[m^2/p]p \end{pmatrix} \begin{pmatrix} w_3 \\ \vdots \\ w_j \\ \vdots \\ w_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

The coefficient matrix of this system can be row reduced to the matrix whose (i,j) entry, $3 \leq i,j \leq m$, is $[ij/p]p - [(i-1)j/p]p$, by first subtracting row $m-3$ from row $m-2$, then row $m-4$ from row $m-3$, etc., and then changing all signs. The resulting matrix is invertible, in fact its determinant equals $\pm p^{m-2}h_1$, where h_1 is the first factor of the class number [28]. Thus $w_j = 0,\ 1 \leq j \leq m+1$.

This proves that $\sum_{k=1}^{p-1} \frac{x_k}{\zeta^k - 1} = 0$ if, and only if, $y_k = y_{p-k}$ for $1 \leq k \leq p-1$, and

$$y_m = -y_{m+2} - \cdots - y_{p-1},$$

where $y_{m+2}, \cdots, y_{p-1}$ are completely arbitrary. Translating back to the x_k variables we have:

Corollary 7.4. $\sum_{k=1}^{p-1} \frac{x_k}{\zeta^k - 1} = 0$ *if, and only if,* $x_k = x_{p-k}$ *for* $1 \leq k \leq p-1$, *and*

$$x_m = -x_{m+2} - \cdots - x_{p-1},$$

where $x_{m+2}, \cdots, x_{p-1}$ *are completely arbitrary.*

We can now complete the proof of Theorem 10.

Proof. Suppose $\chi_1 = \chi_2$ are the Eichler traces of two actions, say

$$\chi_1 = 1 + \sum_{j=1}^{t} \frac{1}{\zeta^{k_j} - 1} = 1 + \sum_{k=1}^{p-1} \frac{u_k}{\zeta^k - 1},$$

$$\chi_2 = 1 + \sum_{j=1}^{u} \frac{1}{\zeta^{l_j} - 1} = 1 + \sum_{k=1}^{p-1} \frac{v_k}{\zeta^k - 1},$$

where u_k is the number of times k appears as a rotation number in χ_1, and v_k is defined similarly. We immediately get $t = u$ since $\chi_1 + \overline{\chi}_1 = 2 - t$ and $\chi_2 + \overline{\chi}_2 = 2 - u$. The equation $\chi_1 - \chi_2 = 0$ gives the linear relation $\sum_{k=1}^{p-1} \frac{x_k}{\zeta^k - 1} = 0$, where $x_k = u_k - v_k$. It follows from Corollary 7.4 that the vector $\vec{x} = (x_1, \cdots, x_{p-1})$ is an integral linear combination of the vectors

$$\vec{e_j} = (\cdots, 1, \cdots, -1, -1, \cdots, 1, \cdots),\ 1 \leq j \leq m-1,$$

where the $1's$ are in positions $j,\ p-j$; the $-1's$ are in positions $m,\ m+1$; and the other entries are zero.

For argument's sake suppose $\vec{x} = \vec{e_j}$ for some j. This means we can move from the vector of rotation numbers $[u_1, \cdots, u_{p-1}]$ to the vector $[v_1, \cdots, v_{p-1}]$ by replacing a canceling pair $\{j, p-j\}$ by the canceling pair $\{m, m+1\}$. Taking linear combinations of the $\vec{e_j}$ corresponds to a sequence of such moves.

This completes the proof of Theorem 10. $\square$

The remainder of this section is concerned with the proof of Theorem 9. According to Proposition 2.3 and the Eichler Trace Formula (1.1) the set of Eichler traces is given by

$$A = \left\{ \chi \in \mathbb{Z}[\zeta] \;\middle|\; \chi = 1 + \sum_{j=1}^{t} \frac{1}{\zeta^{k_j} - 1} \right\},$$

where the only restriction on the rotation numbers k_j is that $\sum_{j=1}^{t} R(k_j^{-1}) \equiv 0 \pmod{p}$. If we define x_k to be the number of j, $1 \leq j \leq t$, such that $k_j = k$, then we can characterize A by

$$A = \left\{ \chi \in \mathbb{Z}[\zeta] \;\middle|\; \chi = 1 + \sum_{k=1}^{p-1} \frac{x_k}{\zeta^k - 1},\ x_k \geq 0 \textit{ and } \sum_{k=1}^{p-1} R(k^{-1}) x_k \equiv 0 \pmod{p} \right\}. \tag{7.2}$$

In the next lemma we show that by passing to $\widehat{A}$ we can remove the restriction that the x_k be non-negative integers.

Lemma 7.2. *The set of Eichler traces modulo $\mathbb{Z}$ is given by*

$$\widehat{A} = \left\{ \widehat{\chi} \in \widehat{\mathbb{Z}[\zeta]} \;\middle|\; \chi = \sum_{k=1}^{p-1} \frac{x_k}{\zeta^k - 1},\ \sum_{k=1}^{p-1} R(k^{-1}) x_k \equiv 0 \pmod{p} \right\}.$$

Proof. First note that by choosing all $x_k = 1$ in (7.2) we get an element $\chi \in A$. In fact a short calculation using Lemma 7.1 gives $\chi = 1 - (p-1)/2$, and thus this element represents 0 in $\widehat{A}$. By adding χ sufficiently many times to an element in A we can ensure that all the coefficients x_k become positive, and this does not change its value in $\widehat{A}$. $\square$

This description of $\widehat{A}$ contains a lot of redundancy. In fact we have the following characterization of $\widehat{A}$.

Lemma 7.3. *The set of Eichler traces modulo $\mathbb{Z}$ is given by*

$$\widehat{A} = \left\{ \widehat{\chi} \;\middle|\; \chi = \sum_{k=1}^{m} \frac{z_k}{\zeta^k - 1}, \; \sum_{k=1}^{m} R(k^{-1}) z_k \equiv 0 \pmod{p} \right\}.$$

Proof. According to Lemma 7.2 a typical element $\widehat{\chi} \in \widehat{A}$ can be represented by

$$\chi = \sum_{k=1}^{p-1} \frac{x_k}{\zeta^k - 1} = \sum_{k=1}^{m} \frac{x_k}{\zeta^k - 1} + \sum_{k=1}^{m} \frac{x_{p-k}}{\zeta^{-k} - 1},$$

where the x_k are integers satisfying $\sum_{k=1}^{p-1} R(k^{-1}) x_k \equiv 0 \pmod{p}$. Now we use the fact that

$$\frac{1}{\zeta^k - 1} + \frac{1}{\zeta^{-k} - 1} = -1$$

to see that $\widehat{\chi} = \widehat{\psi}$, where

$$\psi = \sum_{k=1}^{m} \frac{z_k}{\zeta^k - 1}, \; \textit{and } z_k = x_k - x_{p-k}.$$

The restriction on the integers z_k becomes $\sum_{k=1}^{m} R(k^{-1}) z_k \equiv 0 \pmod{p}$, since

$$\begin{aligned}
\sum_{k=1}^{p-1} R(k^{-1}) x_k &= \sum_{k=1}^{m} R(k^{-1}) x_k + \sum_{k=1}^{m} R((p-k)^{-1}) x_{p-k} \\
&= \sum_{k=1}^{m} R(k^{-1}) x_k + \sum_{k=1}^{m} (p - R(k^{-1})) x_{p-k} \\
&\equiv \sum_{k=1}^{m} R(k^{-1}) z_k \pmod{p}
\end{aligned}$$

and $\sum_{k=1}^{p-1} R(k^{-1}) x_k \equiv 0 \pmod{p}$. $\square$

In Definition 7.1 we introduced elements $\theta_1, \theta_2, \ldots, \theta_m$ and then in Corollary 7.1 we showed that the corresponding classes modulo $\mathbb{Z}$, that is $\widehat{\theta_1}, \widehat{\theta_2}, \ldots, \widehat{\theta_m}$, formed a basis of $\widehat{B}$. To determine the index of $\widehat{A}$ in $\widehat{B}$ we want to express a typical element of $\widehat{A}$ in terms of this basis. But first we need a definition.

Definition 7.2. For integers k, n define $C(k,n) = R(k^{-1}n) + R(k^{-1}) - p$.

The following properties of the coefficients $C(k,n)$ are easy to verify:

(i) $C(k,n) + C(p-k,n) = 0$ and $C(k,n) + C(k,p-n) = 2R(k^{-1}) - p$.

(ii) $C(1,n) = n+1-p$, $C(k,1) = 2R(k^{-1}) - p$, $C(p-1,n) = p-n-1$, and $C(k,p-1) = 0$.

Lemma 7.4. *The elements of $\widehat{A}$ are those elements $\widehat{\chi} \in \widehat{\mathbb{Z}[\zeta]}$ of the form*

$$\widehat{\chi} = \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\widehat{\theta_n},$$

where the only restriction on the integers z_k is $\sum_{k=1}^{m} R(k^{-1})z_k \equiv 0 \pmod{p}$.

Proof. By Lemma 7.3 a typical Eichler trace modulo $\mathbb{Z}$ is given by $\widehat{\chi}$, where $\chi = \sum_{k=1}^{m} \frac{z_k}{\zeta^k - 1}$, and $\sum_{k=1}^{m} R(k^{-1})z_k \equiv 0 \pmod{p}$. Using Lemma 7.1 we have

$$\chi = -\frac{1}{p}\sum_{jk\equiv -1} jz_k + \frac{1}{p}\sum_{n=1}^{p-2}\left(\sum_{jk\equiv n} jz_k - \sum_{jk\equiv -1} jz_k\right)\zeta^n.$$

The condition $\sum_{k=1}^{m} R(k^{-1})z_k \equiv 0 \pmod{p}$ can be written as $\sum_{jk\equiv 1} jz_k \equiv 0 \pmod{p}$, and so $\sum_{jk\equiv -1} jz_k = \sum_{jk\equiv 1}(p-j)z_k \equiv 0 \pmod{p}$. Therefore, modulo $\mathbb{Z}$ we have

$$\chi \equiv \frac{1}{p}\sum_{n=1}^{p-2}\left(\sum_{jk\equiv n} jz_k - \sum_{jk\equiv -1} jz_k\right)\zeta^n \equiv \frac{1}{p}\sum_{n=1}^{p-1}\left(\sum_{jk\equiv n} jz_k - \sum_{jk\equiv -1} jz_k\right)\zeta^n.$$

Note that the term corresponding to $n = p-1$ contributes 0 to the sum. Also note that $\sum_{jk\equiv n} jz_k - \sum_{jk\equiv -1} jz_k = \sum_{k=1}^{m} C(k,n)z_k$ and therefore $\chi \equiv \frac{1}{p}\sum_{n=1}^{p-1}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\zeta^n$.

Next we break the sum up into two pieces, one piece for $1 \le n \le m$, the other piece for the remaining values of n, and then use properties of the coefficients $C(k,n)$.

$$\begin{aligned}
\chi &\equiv \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\zeta^n + \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,p-n)z_k\right)\zeta^{p-n}\\
&\equiv \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\zeta^n + \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m}\left(2R(k^{-1}) - C(k,n) - p\right)z_k\right)\zeta^{-n}\\
&\equiv \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)(\zeta^n - \zeta^{-n}) + \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m}\left(2R(k^{-1}) - p\right)z_k\right)\zeta^{-n}\\
&\equiv \frac{1}{p}\sum_{n=2}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\theta_n + \left(\frac{1}{p}\sum_{k=1}^{m} C(k,1)z_k\right)(\zeta - \zeta^{-1})
\end{aligned}$$

$$
\begin{aligned}
+ & \quad \left(\frac{1}{p}\sum_{k=1}^{m} C(k,1)z_k\right)\left(\zeta^{m+1}+\cdots+\zeta^{p-1}\right) \\
\equiv & \quad \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\theta_n.
\end{aligned}
$$

The last equation follows from $\theta_1 = \zeta + \zeta^{m+1} + \cdots + \zeta^{p-2}$. $\square$

Any sequence $[a_1, \dots, a_t]$, as in Proposition 2.3, determines uniquely up to topological conjugacy, a compact connected Riemann surface S and an analytical automorphism $T\colon S \to S$ having order p, orbit genus 0, and whose Eichler trace is given by the equation

$$
\chi = 1 + \sum_{j=1}^{t} \frac{1}{\zeta^{k_j} - 1}, \text{ where } k_j a_j \equiv 1 \pmod{p}, \text{ for } 1 \le j \le t. \tag{7.3}
$$

Let $\chi[a_1, \dots, a_t]$ denote this Eichler trace. Then

(i) $\widehat{\chi}[a_1, \dots, a_t] + \widehat{\chi}[b_1, \dots, b_u] = \widehat{\chi}[a_1, \dots, a_t, b_1, \dots, b_u]$.

(ii) $\widehat{\chi}[\dots, a, \dots, p-a, \dots] = \widehat{\chi}[\dots, \widehat{a}, \dots, \widehat{p-a}, \dots]$.

If we define y_k to be the number of j, $1 \le j \le t$, such that $a_j = k$, then we obtain

$$
\widehat{\chi}[a_1, \dots, a_t] = \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k^{-1}, n)z_k\right)\widehat{\theta}_n \tag{7.4}
$$

where $z_k = y_k - y_{p-k}$. This is because that $y_k = x_{R(k^{-1})}$ and $\sum k y_k \equiv 0 \pmod{p}$.

Definition 7.3. Let K be the collection of m-tuples $\vec{v} = [z_1, \dots, z_m]$ satisfying the condition

$$
\sum_{k=1}^{m} k z_k \equiv 0 \pmod{p}.
$$

Thus K is a free abelian group of rank m. A basis of K is given by the vectors

$$
\begin{aligned}
\vec{v}_1 &= [2, -1, 0, \dots, 0], \\
\vec{v}_k &= [1, \dots, 1, -1, \dots], \quad 2 \le k \le m-1, \\
\vec{v}_m &= [1, 0, \dots, 0, 2],
\end{aligned}
$$

where for $2 \leq k \leq m-1$, the 1 is in the first and the k^{th} entries, the -1 is in the $(k+1)^{st}$ entry, and all other entries are zero. This is because the determinant of these m vectors is p.

Now consider the group homomorphism $L\colon K \to \widehat{A}$ defined by

$$L(\vec{v}) = \frac{1}{p}\sum_{n=1}^{m}(\sum_{k=1}^{m} C(k^{-1},n)z_k)\widehat{\theta_n}.$$

Lemma 7.4 implies that L is an epimorphism.

Proposition 7.3. *L is a group isomorphism.*

Proof. We first compute the images of the basis elements $\vec{v}_k$, $1 \leq k \leq m$, using properties of the coefficients $C(k,n)$:

$$\begin{aligned}
L(\vec{v}_1) &= \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\widehat{\theta_n} \\
&= \frac{1}{p}\sum_{n=1}^{m}\left(2C(1,n) - C(2^{-1},n)\right)\widehat{\theta_n} \\
&= \sum_{n=1}^{m} -\widehat{\theta_n}, \\
L(\vec{v}_k) &= \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\widehat{\theta_n} \\
&= \frac{1}{p}\sum_{n=1}^{m}\left(C(1,n) + C(k^{-1},n) - C((k+1)^{-1},n)\right)\widehat{\theta_n} \\
&= \frac{1}{p}\sum_{n=1}^{m}\left((n+1-p) + R(kn) + R(k) - p - R((k+1)n) - R(k+1) + p\right)\widehat{\theta_n} \\
&= \sum_{n=1}^{m}\left(\left[\frac{(k+1)n}{p}\right] - \left[\frac{kn}{p}\right] - 1\right)\widehat{\theta_n}, \\
L(\vec{v}_m) &= \frac{1}{p}\sum_{n=1}^{m}\left(\sum_{k=1}^{m} C(k,n)z_k\right)\widehat{\theta_n} \\
&= \frac{1}{p}\sum_{n=1}^{m}\left(C(1,n) + 2C(m^{-1},n)\right)\widehat{\theta_n} \\
&= \frac{1}{p}\sum_{n=1}^{m}\left(C(1,n) + C(m^{-1},n) - C((m+1)^{-1},n)\right)\widehat{\theta_n} \\
&= \sum_{n=1}^{m}\left(\left[\frac{(m+1)n}{p}\right] - \left[\frac{mn}{p}\right] - 1\right)\widehat{\theta_n},
\end{aligned}$$

where we have used the equation $kn = [\frac{kn}{p}]p + R(kn)$.

Now consider the $m \times m$ matrix M whose (k, n) entry is given by

$$M_{(k,n)} = \left[\frac{(m+1)n}{p}\right] - \left[\frac{mn}{p}\right] - 1$$

To complete the proof of the proposition we need only show that $\det(M) \neq 0$. In fact we will show that the determinant of this matrix is $\pm h_1$, thereby completing the proof of Theorem 9.

Note that all entries in the first row of M are -1. For each k, $2 \leq k \leq m$, we subtract the first row of M from the k^{th} row. The resulting entries of the new k^{th} row are

$$\left[\frac{(k+1)n}{p}\right] - \left[\frac{kn}{p}\right].$$

Clearly, the first column of these new entries is 0. This implies that

$$\det(M) = \pm \det \begin{pmatrix} & \vdots & \\ \cdots & [\frac{(k+1)n}{p}] - [\frac{kn}{p}] & \cdots \\ & \vdots & \end{pmatrix} \quad \text{where} \quad 2 \leq k, n \leq m.$$

The first column of this matrix is $0, \ldots, 0, 1$, hence

$$\det(M) = \pm \det \begin{pmatrix} & \vdots & \\ \cdots & [\frac{kn}{p}] - [\frac{(k-1)n}{p}] & \cdots \\ & \vdots & \end{pmatrix} \quad \text{where} \quad 3 \leq k, n \leq m.$$

According to [28] the determinant of this matrix is $\pm h_1$. This proves the proposition since the determinant of M has only changed by a $\pm$ sign in the course of the above elementary row and column operations. $\square$

The proof of Theorem 9 follows from the fact that $\det(M) = \pm h_1$ since the matrix M is the coefficient matrix for expressing the basis elements of $\widehat{A}$ in the basis elements of $\widehat{B}$.

Clearly, $\widehat{\chi}_{r,s} = L(\vec{v}_r)$, for $1 \leq r \leq m$ and $1 + r + s = p$. This complete the proof of Theorem 11.

As mentioned in the introduction, J. Ewing proves our Theorem 9, but in a different setting. See Theorem (3.2) in [6]. To Explain how Ewing's results relate to ours we need some notation.

Let W denote the Witt group of equivalence classes $[V, \beta, \rho]$, where V is a finitely generated free abelian group, β is a skew symmetric non-degenerate bilinear form on V, and ρ is a representation of $\mathbb{Z}_p$ into the group of β-isometries of V. To an automorphism of order p, $T\colon S \to S$, we assign the Witt class $[V, \beta, \rho]$, where V is the first cohomology group, β is the cup product form, and ρ is the induced representation on cohomology. This assignment is well defined up to cobordism and so defines a group homomorphism $ab\colon \Omega \to W$, the so-called Atiyah-Bott map.

The G-signature of Atiyah and Singer defines a group homomorphism from the group of Witt classes to the complex representation ring of $\mathbb{Z}_p$, $sig\colon W \to R(\mathbb{Z}_p)$. Let $e\colon R(\mathbb{Z}_p) \to \mathbb{Z}[\zeta]$ be the homomorphism that evaluates the character of a representation at the generator $T \in \mathbb{Z}_p$. Let $s\colon \Omega \to \mathbb{Z}[\zeta]$ denote the composite $e \circ sig \circ ab\colon \Omega \to \mathbb{Z}[\zeta]$.

Ewing proves that s is a monomorphism whose image has index h_1 in the subgroup R of $\mathbb{Z}[\zeta]$ spanned by the elements $\zeta^k - \zeta^{-k}, k = 1, \dots, m$. From the Remark earlier in this section it follows that $\widehat{R}$ has index 2 in $\widehat{B}$. If $< g \mid a_1, \dots, a_t >$ denotes the cobordism class of T, see Section 7.2 for the notation, then

$$\sigma = s < g \mid a_1, \dots, a_t > = \sum_{j=1}^{t} \frac{\zeta^{k_j} + 1}{\zeta^{k_j} - 1}$$

The relationship between the G-signature σ and the Eichler trace χ is given by $\sigma = 2\chi + t - 2$, and from this it is an easy matter to translate Ewing's results into ours.

7.2 Equivariant Cobordism

In this section we prove Theorem 12. To begin with suppose $T_1\colon S_1 \to S_1$ and $T_2\colon S_2 \to S_2$ are automorphisms of order p on compact connected Riemann surfaces. We do not assume that the orbit genus of either S_1 or S_2 is 0. We start with a standard definition.

Definition 7.4. We say that T_1 is equivariantly cobordant to T_2, written $T_1 \sim T_2$, if there exists a smooth, compact, connected 3-manifold W and a smooth $\mathbb{Z}_p$ action $T\colon W \to W$ such that

(i) The boundary of W is the disjoint union of S_1 and S_2, $\partial(W) = S_1 \sqcup S_2$.

(ii) T restricted to $\partial(W)$ agrees with $T_1 \sqcup T_2$.

The cobordism class of an automorphism $T\colon S \to S$ depends only upon its topological conjugacy class $[g \mid a_1, \dots, a_t]$. We denote this cobordism class by $< g \mid a_1, \dots, a_t >$, and if the orbit genus $g = 0$, we denote it by $< a_1, \dots, a_t >$.

The set of all cobordism classes of $\mathbb{Z}_p$ actions on compact connected Riemann surfaces is denoted by Ω. Addition of the cobordism classes of the automorphisms $T_1\colon S_1 \to S_1$, $T_2\colon S_2 \to S_2$ is defined by equivariant connected sum as follows. Find discs D_j in S_j such that $D_j,\ T_j(D_j), \dots, T_j^{p-1}(D_j)$ are mutually disjoint for $j = 1, 2$. Then excise all discs $T^k(D_j)$, $j = 1, 2,\ k = 0, 1, \dots, p-1$ from $S_1,\ S_2$ and take a connected sum by matching $\partial(T^k(D_1))$ to $\partial(T^k(D_2))$ for $k = 0, 1, \dots, p-1$. The resulting surface S has p tubes joining S_1 and S_2. The automorphisms $T_1,\ T_2$ can be extended to an automorphism $T\colon S \to S$ by permuting the tubes. The cobordism class of T does not depend on the choices made.

Thus addition in Ω is given by the formula

$$< g \mid a_1, \dots, a_t > + < h \mid b_1, \dots, b_u > = < g + h \mid a_1, \dots, a_t, b_1, \dots, b_u > . \tag{7.5}$$

The next two lemmas show that Ω is an abelian group generated by the cobordism classes $< a_1, \dots, a_t >$. The identity is represented by any fixed point free action, or by any cobordism class consisting entirely of canceling pairs, and the inverse of $< g \mid a_1, \dots, a_t >$ is represented by $< g \mid p - a_1, \dots, p - a_t >$. The proofs are not original, but are presented here to emphasize the relationship with $\widehat{A}$.

Lemma 7.5. $< g \mid a_1, \dots, a_t > = < a_1, \dots, a_t >$.

Proof. Let $T\colon S \to S$ represent the class $< a_1, \dots, a_t >$. First we take the product cobordism $W_1 = S \times [0,1]$, where T is extended over W_1 in the obvious way. Next we modify W_1 on the top end $S \times \{1\}$ as follows. Take a disc D in S such that D, $T(D), \dots, T^{p-1}(D)$ are mutually disjoint, and then to each disc $T^k(D)$ in $S \times \{1\}$, $k = 0, 1, \dots, p-1$, attach a copy of a handlebody H of genus g by identifying the disc $T^k(D)$ with some disc $D' \subset \partial(H)$. Let W_2 denote the resulting 3-manifold. See Figure 7.1. The action of $\mathbb{Z}_p$ can be extended to W_2 by permuting the handlebodies. The manifold W_2 provides the cobordism showing that $< g \mid a_1, \dots, a_t >=< a_1, \dots, a_t >$. □

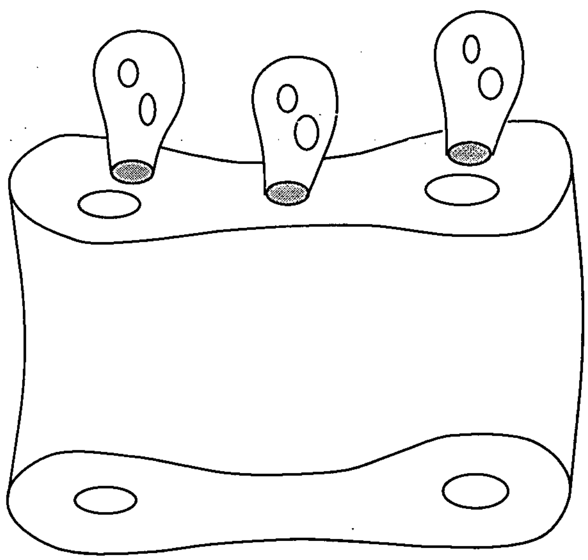

Figure 7.1: Cobordism of $g = 0$

Lemma 7.6. $< a, p-a, a_3, \dots, a_t >=< 1 \mid a_3, \dots, a_t >=< a_3, \dots, a_t >$.

Proof. The proof of this lemma is similar to the proof of the last one. Start with a product cobordism W_1. Suppose P_0, P_1 are the fixed points corresponding to the canceling pair $\{a, p - a\}$. Choose small invariant discs D_0, D_1 around P_0, P_1 respectively, and then modify the cobordism at the top end by adding a solid tube $D \times [0,1]$ so that $D \times \{0\} = D_0$ and $D \times \{1\} = D_1$. The automorphism T can be extended over this tube, and the resulting cobordism shows that

$$< a, p-a, a_3, \dots, a_t >=< 1 \mid a_3, \dots, a_t > .$$

See Figure 7.2. Lemma 7.5 completes the proof. □

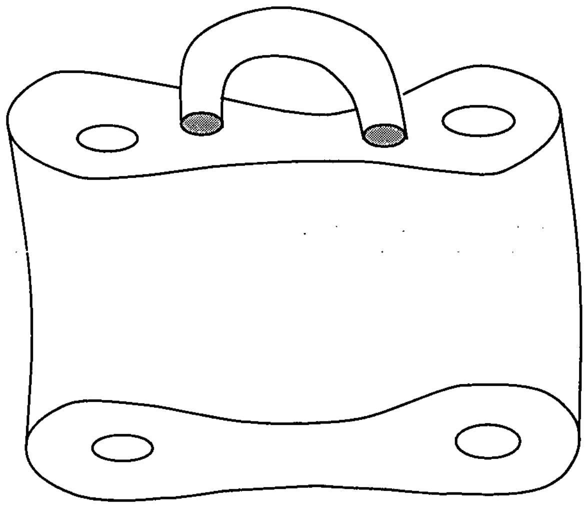

Figure 7.2: Cobordism with Canceling Pairs

Define the isomorphism of Theorem 12, $\phi\colon \widehat{A} \to \Omega$, by $\phi(\widehat{\chi}[a_1, \dots, a_t]) = < a_1, \dots, a_t >$. The same relations hold for cobordism classes, see Equation (7.5) and Lemma 7.6, and therefore the mapping ϕ is a well defined group homomorphism.

Now we complete the proof of Theorem 12. The argument is analogous to one used in [8].

Proof. From the remarks above we know that $\phi\colon \widehat{A} \to \Omega$ is a well defined group homomorphism. Lemma 7.5 implies that it is an epimorphism. It only remains to prove that ϕ is a monomorphism.

If there is an element in the kernel of ϕ we can assume it is a generator, say $\widehat{\chi}[a_1, \dots, a_t]$. Suppose $T\colon S \to S$ represents $[a_1, \dots, a_t]$. Then there is a compact, connected, smooth 3-manifold W such that $\partial(W) = S$, and an extension of T to a smooth homeomorphism $T\colon W \to W$ of order p, also denoted by T. The fixed point set of $T\colon W \to W$ must consist of disjoint, properly embedded arcs joining fixed points in S to fixed points in S. The fixed points at the end of each arc will form a canceling pair $\{a, p-a\}$. In this way we see that $[a_1, \dots, a_t]$ consists entirely of canceling pairs, and hence $\widehat{\chi}[a_1, \dots, a_t] = 0$ in $\widehat{A}$. □

7.3 Dihedral Groups of Automorphisms of Riemann Surfaces

We conclude this thesis by proving Theorem 13. The essential nature of its proof is the relation between group actions on compact connected Riemann surfaces and Fuchsian groups, as well as the Lefschetz Fixed Point Formula. Let D_{2p} be the dihedral group of $2p$ elements and T_p, $T_2 \in D_{2p}$ be two fixed generators of order p, 2 with the relations $T_p^p = T_2^2 = (T_pT_2)^2 = 1$. Suppose there is an embedding of D_{2p} in $\mathrm{Aut}\,(S)$. We have a faithful representation $R : D_{2p} \to GL_g(\mathbb{C})$, by passing to the space of holomorphic differentials on S, assuming $g > 1$.

We want to characterize such groups $R(D_{2p})$. We denote by $D_{2p}(A, B)$ any subgroup of $GL_g(\mathbb{C})$ generated by A, B with the relations $A^p = B^2 = (AB)^2 = I$. Let $G_i = D_{2p}(A_i, B_i)$ $(i = 1, 2)$. G_1 and G_2 are said to be conjugate, denoted by $G_1 \sim G_2$, if there is $Q \in GL_g(\mathbb{C})$ such that $Q^{-1}G_1Q = G_2$, and strongly conjugate, denoted by $G_1 \approx G_2$, if $Q^{-1}A_1Q = A_2$ and $Q^{-1}B_1Q = B_2$. A subgroup $D_{2p}(A, B)$ is said to be realizable if it is conjugate to some $R(D_{2p})$.

It is well known that the trace of an element of order 2 in $GL_g(\mathbb{C})$ is an integer, and the trace of an element of order p in $GL_g(\mathbb{C})$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta)$. A subgroup G in $GL_g(\mathbb{C})$ is called an I-group if all elements of G have integer traces.

Let $X \in D_{2p}(A, B)$ be of order p. Then $X \sim X^{-1}$, and hence $\mathrm{tr}\,(X) = \mathrm{tr}\,(X^{-1}) = \overline{\mathrm{tr}\,(X)}$. Therefore $\mathrm{tr}\,(X)$ is a real number. Furthermore if $\mathrm{tr}\,(X)$ is rational, then $\mathrm{tr}\,(X)$ is an integer.

Lemma 7.7. *If some element $X \in D_{2p}(A, B)$ of order p has rational trace, then $D_{2p}(A, B)$ is an I-group and all elements of order p in $D_{2p}(A, B)$ are conjugate.*

Proof. It is clear that $\mathrm{tr}\,(X) = k + k_1(\zeta + \zeta^{-1}) + \cdots + k_m(\zeta^m + \zeta^{-m})$ $(m = \frac{p-1}{2})$, for some non-negative integers k, k_1, $\ldots$, k_m with $k + 2(k_1 + \cdots + k_m) = g$. But $\zeta, \ldots \zeta^{p-1}$ are independent over the rational field $\mathbb{Q}$, so we have $k_1 = \cdots = k_m$, say l. Therefore $\mathrm{tr}\,(X) = k - l$ is an integer. □

Lemma 7.8. *Suppose $G_i = D_{2p}(A_i, B_i)$, $i = 1, 2$, are two I-groups. Then the following three conditions are equivalent.*

1. $G_1 \sim G_2$;

2. $G_1 \approx G_2$;

3. $\mathrm{tr}\,(A_1) = \mathrm{tr}\,(A_2)$ *and* $\mathrm{tr}\,(B_1) = \mathrm{tr}\,(B_2)$.

Proof. For a dihedral I-group we have the following canonical form $G = D_{2p}(A_l, B_{x,y})$, where

$$A_l = \begin{pmatrix} I_x & & & & \\ & I_y & & & \\ & & \zeta I_l & & \\ & & & \ddots & \\ & & & & \zeta^{p-1} I_l \end{pmatrix} \quad \text{and} \quad B_{x,y} = \begin{pmatrix} I_x & & & & \\ & -I_y & & & \\ & & & & I_l \\ & & & \iddots & \\ & & I_l & & \end{pmatrix}$$

where $x + y + (p-1)l = g$ and $\mathrm{tr}\,(A_l) = x + y - l$. Since the number of blocks of I_l's in $B_{x,y}$ is even, $\mathrm{tr}\,(B_{x,y}) = x - y$. □

If σ is an automorphism of S of finite order greater than 1, then we have the Lefschetz Fixed Point Formula, $\mathrm{tr}\,(\sigma) + \overline{\mathrm{tr}\,(\sigma)} = 2 - \mathrm{Fix}\,(\sigma)$, where $\mathrm{Fix}\,(\sigma)$ is the number of fixed points of σ, see [38]. It is easy to deduce

Lemma 7.9. *If $D_{2p}(A, B)$ is realizable, then $D_{2p}(A, B)$ is an I-group with* $\mathrm{tr}\,(A) \leq 1$ *and* $\mathrm{tr}\,(B) \leq 1$.

Thus we complete the proof of the necessity condition of Theorem 13.

To any action of D_{2p} on S we can associate a short exact sequence of groups

$$1 \to \Pi \to \Gamma(g_0; \overbrace{p, \ldots, p}^{t}, \overbrace{2, \ldots, 2}^{s}) \xrightarrow{\theta} D_{2p} \to 1$$

where Γ must has form

$$\Gamma(g_0; \overbrace{p, \ldots, p}^{t}, \overbrace{2, \ldots, 2}^{s}) = \langle X_1, \ldots, X_{g_0}, Y_1, \ldots, Y_{g_0}, A_1, \ldots, A_t, B_1, \ldots, B_s \rangle$$

with relations

$$A_1^p = \cdots = A_t^p = B_1^2 = \cdots = B_s^2 = [X_1, Y_1] \cdots [X_{g_0}, Y_{g_0}] A_1 \cdots A_t B_1 \cdots B_s = 1 \quad (7.6)$$

By the Riemann-Hurwitz formula (2.16) we see that s must be even. From the results of Macbeath[21], we obtain that $\mathrm{Fix}\,(T_p) = 2t$ and $\mathrm{Fix}\,(T_2) = s$. Hence if $D_{2p}(A, B)$ is realized by this action then $\mathrm{tr}(A) = 1 - t$ and $\mathrm{tr}(B) = \frac{2-s}{2}$.

To prove the sufficiency condition of Theorem 13, we need the following lemma. Assume that $D_{2p}(A, B)$ is an IR-group.

Lemma 7.10. *Then* $\frac{1}{2p}\left(g + (p-1)\,\mathrm{tr}\,(A) + p\,\mathrm{tr}\,(B)\right)$ *is a non-negative integer.*

Proof. This is an easy calculation. Let A, B be of forms A_l, $B_{x,y}$, as in the proof of Lemma 7.8.

$$\begin{aligned} & g + (p-1)\,\mathrm{tr}\,(A) + p\,\mathrm{tr}\,(B) \\ = \; & x + y + (p-1)l + (p-1)(x + y - l) + p(x - y) \\ = \; & p(x + y) + p(x - y) \\ = \; & 2px. \end{aligned}$$

Thus $\frac{1}{2p}\left(g + (p-1)\,\mathrm{tr}\,(A) + p\,\mathrm{tr}\,(B)\right) = x$ is a non-negative integer. $\square$

Now we can complete the proof of Theorem 13.

Proof of Theorem 13. Let $t = 1 - \mathrm{tr}\,(A)$, $s = 2 - 2\mathrm{tr}\,(B)$, and

$$g_0 = \frac{1}{2p}\left(g + (p-1)\,\mathrm{tr}\,(A) + p\,\mathrm{tr}\,(B)\right).$$

We define an epimorphism $\theta : \Gamma(g_0; \overbrace{p, \ldots, p}^{t}, \overbrace{2, \ldots, 2}^{s}) \to D_{2p}$ as follows:

Case 1: If $\mathrm{tr}\,(A) = 1$ and $\mathrm{tr}\,(B) = 1$, then $t = 0$, $s = 0$, and $g_0 \geq 2$. We set

$$\theta(X_1) = \theta(Y_1) = T_p \quad \text{and} \quad \theta(X_i) = \theta(Y_i) = T_2 \;\; (\text{for } i = 2, \ldots g_0).$$

Case 2: If $\operatorname{tr}(A) = 1$, $\operatorname{tr}(B) = 0$, then $t = 0$ and $s = 2$, and $g_0 \geq 1$. We define

$$\theta(B_1) = \theta(B_2) = T_2 \quad \text{and} \quad \theta(X_i) = \theta(Y_i) = T_p.$$

Case 3: If $\operatorname{tr}(A) = 1$ and $\operatorname{tr}(B) \leq -1$, then $t = 0$ and $s \geq 4$. We define

$$\theta(B_i) = T_p^{b_i} T_2 \quad \text{and} \quad \theta(X_j) = \theta(Y_j) = 1,$$

where b_i are integers (not all the same) with $0 \leq b_i \leq p-1$ and $\sum_{i=1}^{s} (-1)^i b_i \equiv 0 \pmod{p}$. Since s is even, θ preserves the group relations, and hence is an epimorphism.

Case 4: If $\operatorname{tr}(A) \leq 0$ and $\operatorname{tr}(B) = 1$, then $t \geq 1$, $s = 0$, and $g_0 \geq 1$. We define

$$\theta(A_i) = T_p^{a_i}, \quad \theta(X_j) = T_p^{c_j} \quad \text{and} \quad \theta(Y_j) = T_2,$$

where a_i, c_j are integers with $1 \leq a_i \leq p-1$ and $\sum_{i=1}^{t} a_i + 2\sum_{j=1}^{g_0} c_j \equiv 0 \pmod{p}$.

Case 5: If $\operatorname{tr}(A) \leq 0$ and $\operatorname{tr}(B) \leq 0$, then $t \geq 1$ and $s \geq 2$. We define

$$\theta(A_i) = T_p^{a_i}, \quad \theta(B_j) = T_p^{b_j} T_2 \quad \text{and} \quad \theta(X_k) = \theta(Y_k) = 1$$

where a_i, b_j are integers with $1 \leq a_i \leq p-1$ and $\sum_{i=1}^{t} a_i + \sum_{j=1}^{s} (-1)^{s+1} b_j \equiv 0 \pmod{p}$.

Let $\Pi = \operatorname{Ker}(\theta)$. We get a short exact sequence of Fuchsian groups

$$1 \to \Pi \to \Gamma(g_0; \overbrace{p, \ldots, p}^{t}, \overbrace{2, \ldots, 2}^{s}) \xrightarrow{\theta} D_{2p} \to 1.$$

It is easy to check that Π is torsion free. By Lemma 7.8, we get an action of D_{2p} on $S = \mathbb{U}/\Pi$ which realizes $D_{2p}(A, B)$. $\square$

Corollary 7.5. *The minimal genus of D_{2p} is $p - 1$.*

Bibliography

[1] E. Artin, *Geometric Algebra*, Interscience tracts in pure and applied mathematics, vol. 3, Interscience Publishers, New York, 1957.

[2] E. Bender, *Classes of Matrices over an Integral Domain*, Illinois J. Math. **11** (1957), 697–702.

[3] L. Bers, *Universal Teichmüller Space*, Conference of Complex Analysis Methods in Physics, University of Indiana, June 1968.

[4] C. J. Earle, *Reduced Teichmüller Space*, Trans. Amer. Math. Soc. **129** (1967), 54–63.

[5] A. L. Edmonds & J. H. Ewing, *Surface Symmetry and Homology*, Math. Proc. Camb. Phil. Soc. **99** (1986), 73–77.

[6] J. Ewing, *The Image of the Atiyah-Bott map*, Math. Z. **165** (1979), 53–71.

[7] ———, *Automorphisms of Surfaces and Class Number: An Illustration of the G-Index Theorem*, Topological Topics (I. M. James, ed.), London Math. Soc. Lecture Notes Series, vol. 86, Cambridge University Press, 1983.

[8] L. Edmonds & J. H. Ewing, *Remarks on the Cobordism Group of Surface Diffeomorphisms*, Math. Ann. **259** (1982), 497–504.

[9] D. Gabai, *Convergence Groups are Fuchsian Groups*, Ann. Math. **136** (1992), 447–510.

[10] W. Harvey, *Discrete Groups and Automorphic Functions*, Academic Press, New York, 1977.

[11] S. P. Kerckhoff, *The Nielsen Realization Problem*, Ann. Math. **117** (1983), 235–265.

[12] M. A. Knus, *Quadratic and Hermitian Forms over Rings*, Grundlehre der Mathematischen Wissenschaften, vol. 294, Springer Verlag, New York, 1991.

[13] H. M. Farkas & I. Kra, *Riemann Surfaces*, second edition ed., Graduate Texts in Mathematics, vol. 71, Springer Verlag, New York, 1992.

[14] I. Kuribayashi, *On Automorphisms of Prime Order of a Riemann Surface as Matrices*, Manuscripta Math. **44** (1983), 103–108.

[15] ———, *On an Algebraization of the Riemann-Hurwitz Relation*, Kodai Math. J. **7** (1984), 222–237.

[16] ———, *Classification of Automorphism Groups of Compact Riemann Surfaces of Genus Two*, Tsukuba (1986), 25–39.

[17] I. Kuribayashi & A. Kuribayashi, *Automorphism Groups of Compact Riemann Surfaces of Genera Three and Four*, J. of Pure and Applied Algebra **65** (1990), 277–292.

[18] A. Kuriyabashi, *Automorphism Groups of Compact Riemann Surfaces of Genus Five*, J. of Algebra **134** (1990), 80–103.

[19] S. Lang, *Algebraic Numbers*, Addison-Wesky, Reading, Mass., 1964.

[20] ———, *Cyclotomic Fields I and II*, Springer-Verlag, New York, 1990.

[21] A. M. Macbeath, *Action of Automorphisms of a Compact Riemann Surface on the First Homology Group*, Bull. London Math. Soc. **5** (1973), 103–108.

[22] C. G. Latimer & C. C. MacDuffee, *A Correspondence between Classes of Ideals and Classes of Matrices*, Ann. of Math. **34** (1933), 313–316.

[23] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[24] W. S. Massey, *Singular Homology Theory*, Graduate Texts in Mathematics, vol. 70, Spring-Verlag New York Inc., New York, 1980.

[25] B. Eckmann & H. Müller, *Plane Motion Groups and Virtual Poincaré Duality of dimension two*, Invent. Math. **69** (1982), 293–310.

[26] M. Newman, *Integral Matrices*, Academic Press, New York, 1972.

[27] J. Nielsen, *Abbildungklassen Endliche Ordung*, Acta Math. **75** (1943), 23–115.

[28] L. Carlitz & F. R. Olson, *Maillet's Determinant*, Proc. Amer. Math. Soc. **6** (1955), 265–269.

[29] I. Reiner, *Symplectic Modular Complements*, Trans. Amer. Math. Soc. **77** (1954), 498–505.

[30] ———, *Automorphisms of the Symplectic Modular Group*, Trans. Amer. Math. Soc. **80** (1955), 35–50.

[31] ———, *Integral Representations of Cyclic Groups of Prime Order*, Proc. Amer. Math. Soc. **8** (1957), 142–146.

[32] C. L. Siegel, *Symplectic Geometry*, Amer. J. Math. **65** (1943), 1–86.

[33] G. Jones & D. Singerman, *Complex Functions*, Cambridge Univ. Press, Cambridge, 1987.

[34] D. Sjerve, *Canonical Forms for Torsion Matrices*, Journal of Pure and Applied Algebra **22** (1981), 103–111.

[35] P. Symonds, *The Cohomology Representation of an Action C_p on a Surface*, Trans. Amer. Math. Soc. **306** (1988), 389–400.

[36] O. Taussky, *On a Theorem of Latimer and Macduffee*, Canadian J. Math. **1** (1949), 300–302.

[37] ———, *On Matrix Classes Corresponding to an Ideal and its Inverse*, Illinois J. Math. **1** (1957), 108–113.

[38] J. W. Vick, *Homology Theory*, Academic Press, 1973.

[39] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.