Conjugacy Classes of p-torsion in $SP_{p-1}(\mathbb{Z})$*

DENIS SJERVE AND QINGJIE YANG
Department of Mathematics
University of British Columbia
Vancouver, B.C., Canada V6T 1Z2

April 7, 2000

1 Motivation and Main Results

The main problem we consider in this paper is the conjugacy classification of p-torsion in $SP_{p-1}(\mathbb{Z})$, the symplectic group over the ring of integers $\mathbb{Z}$, where p is an odd prime. We also consider the related problem of the realizability of p-torsion in $SP_{p-1}(\mathbb{Z})$ by analytic automorphisms of compact connected Riemann surfaces of genus $\frac{p-1}{2}$.

Classification up to conjugacy plays an important role in group theory. The symplectic groups are of importance because they have numerous applications to number theory and the theory of modular functions of many variables, especially as developed by Siegel in [9] and in numerous other papers. But our original motivation for studying this problem came not from algebra but rather from Riemann surfaces.

Throughout the paper S will denote 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 automorphism 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 a basis for which the intersection matrix 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 $\{a, b\}$. Since T_* preserves intersection numbers, $X'JX = J$, where X' is the transpose of X.

Definition. The set of $2n \times 2n$ unimodular matrices X over $\mathbb{Z}$ such that

$$X'JX = J \tag{1.1}$$

[*] Research supported by NSERC grant A7218

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

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

Definition. 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 of genus g, such that X is the matrix of T_* with respect to some canonical basis of $H_1(S)$.

Two questions naturally arise.

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

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

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

The least genus of any surface S, other than the 2-sphere or torus, on which $\mathbb{Z}_p$ acts, is $\frac{p-1}{2}$. Thus $\mathbb{Z}_p$ actions on surfaces of genus $\frac{p-1}{2}$ are particularly interesting. If $p = 3$ then S is a torus, so to avoid this trivial case we will usually assume that $p \geq 5$.

If T is a preferred generator of $\mathbb{Z}_p$, and $\mathbb{Z}_p$ is acting on a surface S of genus $\frac{p-1}{2}$, then an easy consequence of the Riemann-Hurwitz formula is that T must have 3 fixed points, say P_1, P_2, P_3. If the action of T in a sufficiently small neighbourhood of the fixed point P_j is equivalent to a rotation through $\frac{2\pi k_j}{p}$, $1 \leq j \leq 3$, then the fixed point data of the action is by definition that set of integers modulo p, $\{a_1, a_2, a_3\}$, one for each fixed point, such that T^{a_j} is equivalent to a rotation by $\frac{2\pi}{p}$ near P_j, $1 \leq j \leq 3$. It is automatically true that $a_1 + a_2 + a_3 \equiv 0 \pmod{p}$. See Sjerve and Yang [14] for the details.

Suppose we have two such automorphisms of order p,

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

on surfaces of genus $\frac{p-1}{2}$. 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 $SP_{p-1}(\mathbb{Z})$ if and only if they have the same fixed point data, see A. Edmonds & J. Ewing [1], or P. Symonds [10]. This is true for all genera $g \geq 2$. By counting triples of fixed point data we see that there are only $\frac{p^2-1}{6}$ classes of p-torsion in $SP_{p-1}(\mathbb{Z})$ which can be realized. But we shall show that the number of conjugacy classes of p-torsion in $SP_{p-1}(\mathbb{Z})$ is $2^{\frac{p-1}{2}} h_1$, where h_1 is the first factor of class number of $\mathbb{Z}[\zeta]$ and $\zeta = e^{\frac{2\pi i}{p}}$. So in general most of the p-torsion in $SP_{p-1}(\mathbb{Z})$ is not realizable. However, we shall answer Question 2 in this case.

To explain our results we need to develop some notation.

Let $\mathcal{R} = \mathbb{Z}[\zeta]$ and $\mathcal{S} = \mathbb{Q}[\zeta]$. Then $\mathcal{S}$ is the quotient field of $\mathcal{R}$. An ideal (fractional ideal) in $\mathcal{S}$ is a non-zero finitely generated $\mathcal{R}$-submodule of $\mathcal{S}$ which is a free $\mathbb{Z}$-module of rank $p-1$. 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 λ, $\mu \in \mathcal{R}$ such that $\lambda\mathfrak{a} = \mu\mathfrak{b}$. We denote the equivalence class of $\mathfrak{a}$ by $\langle\mathfrak{a}\rangle$ and let $\mathcal{C}$ denote the collection of equivalence classes of ideals. $\mathcal{C}$ is an abelian group with respect to multiplication of ideals. The identity is $\langle\mathcal{R}\rangle$ and the inverse of $\langle\mathfrak{a}\rangle$ is $\langle\Delta\mathfrak{a}'\rangle$, where $\Delta = \frac{p\zeta^{(p+1)/2}}{\zeta-1}$ and $\mathfrak{a}'$ is the complementary ideal. See Section 2.1.

Let P be the set of pairs $(\mathfrak{a}, a)$ consisting of an integral ideal $\mathfrak{a}$ and an element $a \in \mathcal{R}$ such that $\mathfrak{a}\overline{\mathfrak{a}} = (a)$ and $a = \overline{a}$, where the bar denotes complex conjugation and $\overline{\mathfrak{a}} = \{\overline{\alpha} \mid \alpha \in \mathfrak{a}\}$. Two such pairs $(\mathfrak{a}, a)$ and $(\mathfrak{b}, b)$ are said to be equivalent if there are λ, $\mu \in \mathcal{R}^*$ such that $\lambda\mathfrak{a} = \mu\mathfrak{b}$ and $\lambda\overline{\lambda}a = \mu\overline{\mu}b$. We denote by $\langle\mathfrak{a}, a\rangle$ the equivalence class of $(\mathfrak{a}, a)$. Let $\mathcal{P}$ denote the set of all classes of P.

Suppose $X \in M_p$. There is an eigenvector $\alpha = (\alpha_1, \ldots, \alpha_{p-1})' \in \mathcal{R}^{p-1}$ corresponding to ζ, that is $X\alpha = \zeta\alpha$. Let $\mathfrak{a}$ be the $\mathbb{Z}$-module generated by $\alpha_1, \ldots, \alpha_{p-1}$, $\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_{p-1}$, and let $a = \Delta^{-1}\alpha' J\overline{\alpha}$. It is easy to check that $\mathfrak{a}$ is an integral ideal in $\mathcal{R}$ and $a = \overline{a}$. Thus $\alpha_1, \ldots, \alpha_{p-1}$ are independent over $\mathbb{Z}$. Furthermore we will prove that $(\mathfrak{a}, a) \in P$ and that the mapping $\Psi : \mathcal{M}_p \to \mathcal{P}$, $\Psi : \langle X\rangle \to \langle\mathfrak{a}, a\rangle$ is well defined.

Theorem 1. *Ψ is a bijection.*

Thus we can count conjugacy classes of p-torsion in $SP_{p-1}(\mathbb{Z})$ by enumerating the elements of $\mathcal{P}$. This is a problem in algebraic number theory. $\mathcal{P}$ turns out to be an abelian group where multiplication is given by $\langle\mathfrak{a}, a\rangle\langle\mathfrak{b}, b\rangle = \langle\mathfrak{a}\mathfrak{b}, ab\rangle$. Let $\mathcal{C}_0$ denote the subgroup of integral ideal classes defined by

$$\mathcal{C}_0 = \big\{\mathfrak{a} \in \mathcal{C} \mid \mathfrak{a}\overline{\mathfrak{a}} = (a), a = \overline{a} \text{ for some } a \in \mathcal{R}\big\} \tag{1.2}$$

Let U be the group of units in $\mathcal{R}$, $U^+ = \big\{u \in U \mid u = \overline{u}\big\}$ and $C = \big\{u\overline{u} \mid u \in U\big\}$. Clearly $C \subset U^+$ and both are subgroups of U. We shall show

Theorem 2. *There is a short exact sequence of abelian groups*

$$1 \to U^+/C \xrightarrow{\phi} \mathcal{P} \xrightarrow{\psi} \mathcal{C}_0 \to 1 \tag{1.3}$$

where $\phi\langle u\rangle = \langle\mathbb{Z}[\zeta], u\rangle$ and $\psi\langle\mathfrak{a}, a\rangle = \langle\mathfrak{a}\rangle$.

Consequently we have

Theorem 3. *The number of elements in $\mathcal{M}_p$ is $q_p = 2^{\frac{p-1}{2}}h_1$.*

Let

$$u_k = \frac{\sin\frac{k\pi}{p}}{\sin\frac{\pi}{p}}, \quad \text{for } (k,p) = 1, \tag{1.4}$$

be the cyclotomic units of $\mathbb{Z}[\zeta]$. If the fixed point data of T is $\{a,b,c\}$, where $1 \leq a,b,c \leq p-1$ and $a+b+c \equiv 0 \pmod{p}$ then we let $M(a,b,c)$ denote the symplectic matrix represented by T_*. Theorem 4 is similar to a result of P. Symonds [10], but our approach is new.

Theorem 4. $\Psi(M(a,b,c)) = \langle \mathbb{Z}[\zeta], u_a u_b u_{a+b} \rangle$

Corollary. *Let $X \in SP_{p-1}(\mathbb{Z})$ have 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 $1 \leq a,b \leq p-1$ and $a+b \neq p$.

2 The Conjugacy Classes

Assume $f(x)$ is a monic irreducible polynomial of degree n over $\mathbb{Z}$. Then it is well known that there is an one-to-one correspondence between the conjugacy classes of matrices of rational integers with characteristic polynomial $f(x)$ and the classes of ideals in $\mathbb{Z}[x]/(f(x))$, see Latimer and MacDuffee [5], or Taussky [11]. The equivalence relation between ideals is given by fractional equivalence.

Let A be any $n \times n$ matrix over $\mathbb{Z}$ such that $f(A) = 0$ and let ζ be a root of $f(x)$. Then the correspondence may be described as follows: If $(\alpha_1, \ldots, \alpha_n)'$, $\alpha_i \in \mathbb{Z}[\zeta]$, is an eigenvector of A with respect to ζ, and $\mathfrak{a}$ is the ideal generated by $\alpha_1, \ldots, \alpha_n$, then the ideal class determined by $\mathfrak{a}$ corresponds to the matrix class determined by A. It is also known that under some conditions, the matrix class generated by the transpose of X corresponds to the inverse ideal class, see Taussky [12]. In Section 2.1 we shall review some results of ideal theory, see Lang [3], [6] or any book on ideal theory. In Section 2.2 we introduce S-pairs and prove Theorem 1. In Section 2.3 we shall prove Theorem 2 and Theorem 3.

If $f(x) = 1 + x + \cdots + x^{p-1}$ then we get a one-to-one correspondence between the conjugacy classes of p-torsion in $SL_{p-1}(\mathbb{Z})$ and $\mathcal{C}$, the group of ideal classes. It is worthwhile repeating how this correspondence works. If $A \in SL_{p-1}(\mathbb{Z})$ has order p then $\zeta = e^{\frac{2\pi i}{p}}$ is an eigenvalue with a one dimensional eigenspace. Thus there exists an eigenvector $\alpha = (\alpha_1, \ldots, \alpha_{p-1})'$, unique up to multiples, and so the ideal $\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_{p-1}$ is well defined up to fractional equivalence. If $B = QAQ^{-1}$, where $Q \in GL_{p-1}(\mathbb{Z})$ then $\beta = Q\alpha$ is an eigenvector for B and the corresponding ideal is also $\mathfrak{a}$. Thus the mapping $\langle A \rangle \to \langle \mathfrak{a} \rangle$ is a well defined mapping from the conjugacy classes of p-torsion in $SL_{p-1}(\mathbb{Z})$ to the classes of ideals in $\mathbb{Z}[\zeta]$. This mapping is a bijection.

2.1 S-pairs

We denote the set of non-zero elements of $\mathcal{R}$ by $\mathcal{R}^*$. The trace of an element α in $\mathcal{S}$ is

$$\mathrm{Tr}\,(\alpha) = \sum_{i=1}^{p-1} \alpha^{(i)} \quad \in \mathbb{Q}, \tag{2.1}$$

where $\alpha^{(i)}$ is that conjugate of α defined by $\zeta^{(i)} = \zeta^i$. It is clear that if $\alpha \in \mathcal{R}$, then $\mathrm{Tr}\,(\alpha) \in \mathbb{Z}$.

Suppose $\alpha_1, \ldots, \alpha_{p-1} \in \mathcal{S}$. The discriminant of $\alpha_1, \ldots, \alpha_{p-1}$ is

$$\Delta(\alpha_1, \ldots, \alpha_{p-1}) = \det \begin{pmatrix} \alpha_1^{(1)} & \alpha_1^{(2)} & \cdots & \alpha_1^{(p-1)} \\ \alpha_2^{(1)} & \alpha_2^{(2)} & \cdots & \alpha_2^{(p-1)} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{p-1}^{(1)} & \alpha_{p-1}^{(2)} & \cdots & \alpha_{p-1}^{(p-1)} \end{pmatrix}. \tag{2.2}$$

Lemma 2.1. *$\alpha_1, \ldots, \alpha_{p-1}$ are independent over $\mathbb{Q}$ if, and only if $\Delta(\alpha_1, \ldots, \alpha_{p-1}) \neq 0$.*

For a proof see Lang [3].

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

$$\mathfrak{a}' = \left\{ \alpha \in \mathcal{S} \;\middle|\; \mathrm{Tr}\,(\alpha\mathfrak{a}) \subset \mathbb{Z} \right\}. \tag{2.3}$$

Let $\alpha_1, \ldots, \alpha_{p-1}$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Then there is a dual basis $\alpha'_1, \ldots, \alpha'_{p-1}$ 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

$$\sum_k {\alpha'}_i^{(k)} \alpha_j^{(k)} = \delta_{ij} \qquad \text{or} \qquad \sum_k \alpha_k^{(i)} {\alpha'}_k^{(j)} = \delta_{ij}. \tag{2.4}$$

We also have $\mathfrak{a}\mathfrak{a}' = \mathcal{R}/\Delta$, where $\Delta = \frac{p\zeta^{(p+1)/2}}{\zeta - 1}$, $\overline{\Delta} = -\Delta$ and

$$\mathfrak{a}' = \mathbb{Z}\alpha'_1 + \cdots + \mathbb{Z}\alpha'_{p-1}. \tag{2.5}$$

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

$$\overline{A} = (\overline{\alpha}_{ij}) \quad \text{and} \quad A^{(k)} = \left(\alpha_{ij}^{(k)}\right) \tag{2.6}$$

if $A = (\alpha_{ij})$ is a matrix with entries in $\mathcal{S}$. The following lemma is very useful.

Lemma 2.2. *Let M, N be two $(p-1)\times(p-1)$ matrices over $\mathbb{Z}$ and $\alpha = (\alpha_1, \ldots, \alpha_{p-1})' \in \mathcal{S}^{p-1}$, where $\alpha_1, \ldots, \alpha_{p-1}$ are independent over $\mathbb{Z}$. Suppose $\alpha' M \overline{\alpha}^{(i)} = \alpha' N \overline{\alpha}^{(i)}$ (for $i = 1, \ldots, p-1$). Then $M = N$.*

Proof. We only prove the special case $N = 0$. Let $a_i = \alpha' M \overline{\alpha}^{(i)}$. Then $a_i^{(k)} = \alpha'^{(k)} M (\overline{\alpha}^{(i)})^{(k)} = 0$. For any $1 \le k, l \le p-1$, let $1 \le i \le p-1$ be such that $ki \equiv l \pmod p$. Then $\left(\overline{\alpha}^{(i)}\right)^{(k)} = \overline{\alpha}^{(l)}$ and hence $\alpha'^{(k)} M \overline{\alpha}^{(l)} = 0$ (for $k, l = 1, \ldots, p-1$), that is $A'MB = 0$, where $A = \left(\alpha_i^{(j)}\right)$ and $B = \left(\overline{\alpha}_i^{(j)}\right)$ are $(p-1)\times(p-1)$ matrices. By Lemma 2.1, $\det A \neq 0$ and $\det B \neq 0$, since $\alpha_1, \ldots, \alpha_{p-1}$ are independent over $\mathbb{Z}$, and therefore $M = 0$. □

Definition. A pair $(\mathfrak{a}, a)$ consisting of an integral ideal $\mathfrak{a}$ and an element a in $\mathcal{R}$ is said to be an S-pair, if there is a basis $\alpha_1, \ldots, \alpha_{p-1}$ of $\mathfrak{a}$, such that

$$\alpha' J \overline{\alpha}^{(i)} = \delta_{1i}\, a\Delta, 1 \leq i \leq p-1, \tag{2.7}$$

where $\alpha = (\alpha_1, \ldots, \alpha_{p-1})'$. The basis $\alpha_1, \ldots, \alpha_{p-1}$ 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 $(\mathfrak{a}, a)$.

The bilinear form defined on column vectors $\alpha = (\alpha_1, \ldots, \alpha_{p-1})'$ and $\beta = (\beta_1, \ldots, \beta_{p-1})'$ by $\langle \alpha, \beta \rangle = \alpha' J \overline{\beta}$ is a non-degenerate skew-hermitian form. In particular, if $\lambda = \alpha' J \overline{\alpha}$ then $\overline{\lambda} = -\lambda$. Since $\overline{\Delta} = -\Delta$ it follows that if $(\mathfrak{a}, a)$ is an S-pair, then $a = \overline{a}$.

Remark. Equation 2.7 is equivalent to

$$\alpha'^{(i)} J \overline{\alpha}^{(j)} = \delta_{ij}\, a^{(i)} \Delta^{(i)}, 1 \leq i, j \leq p-1.$$

Remark. Since $\mathfrak{a}\mathfrak{a}' = \mathcal{R}/\Delta$ for any ideal $\mathfrak{a}$, we have $\mathfrak{a}\overline{\mathfrak{a}} = (a)$ if and only if $\overline{\mathfrak{a}} = a\Delta\mathfrak{a}'$.

Lemma 2.3. *A pair $(\mathfrak{a}, a)$ is an S-pair if, and only if $(\mathfrak{a}, a) \in P$.*

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

For the converse, suppose $(\mathfrak{a}, a) \in P$. If $\beta_1, \ldots, \beta_{p-1}$ is a basis of $\mathfrak{a}$ then $\overline{\beta}_1, \ldots, \overline{\beta}_{p-1}$ is a basis of $\overline{\mathfrak{a}}$. Let $\gamma_1, \ldots, \gamma_{p-1}$ be the dual basis of $\beta_1, \ldots, \beta_{p-1}$. Then $\mathrm{Tr}\,(\beta_i \gamma_j) = \delta_{ij}$, and we have $\beta'^{(i)} \gamma^{(j)} = \delta_{ij}$, where $\beta = (\beta_1, \ldots, \beta_{p-1})'$ and $\gamma = (\gamma_1, \ldots, \gamma_{p-1})'$. Since $\overline{\mathfrak{a}} = a\Delta\mathfrak{a}'$, there is $M \in GL_{p-1}(\mathbb{Z})$ such that $M\overline{\beta} = a\Delta\gamma$. Then

$$\beta' M \overline{\beta}^{(i)} = a^{(i)} \Delta^{(i)} \beta' \gamma^{(i)} = \delta_{1i}\, a\Delta, \tag{2.8}$$

but also

$$\beta' M' \overline{\beta}^{(i)} = \overline{a}\overline{\Delta}\overline{\gamma}'\overline{\beta}^{(i)} = -a\Delta\overline{\gamma'\beta}^{(i)} = -\delta_{1i}\, a\Delta, \tag{2.9}$$

Thus $\beta' M \overline{\beta}^{(i)} = -\beta' M' \overline{\beta}^{(i)}$ (for $i = 1, \ldots, p-1$), and so $M' = -M$ (by Lemma 2.2). According to Newman [8] there is $Q \in GL_{p-1}(\mathbb{Z})$ such that $M = Q' J Q$. If $\alpha = Q\beta$, then

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

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

Remark. From the Remark above we see that $(\mathfrak{a}, a)$ is an S-pair if and only if $\overline{\mathfrak{a}} = a\Delta\mathfrak{a}'$ and $a = \overline{a}$.

Example. From this lemma it follows that $(\mathcal{R}, u)$, for any $u \in U^+$, is an S-pair.

2.2 The Correspondence Ψ

Suppose $X \in M_p$. There is an eigenvector $\alpha = (\alpha_1, \dots, \alpha_{p-1})' \in \mathcal{R}^{p-1}$ corresponding to ζ, that is $X\alpha = \zeta\alpha$. Let $\mathfrak{a}$ be the $\mathbb{Z}$-module generated by $\alpha_1, \dots, \alpha_{p-1}$, $\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_{p-1}$, and let $a = \Delta^{-1}\alpha' J\overline{\alpha}$. It is easy to check that $\mathfrak{a}$ is an integral ideal in $\mathcal{R}$ and $a = \overline{a}$. Thus $\alpha_1, \dots, \alpha_{p-1}$ are independent over $\mathbb{Z}$. Furthermore we have

Lemma 2.4. *The pair $(\mathfrak{a}, a)$ is an S-pair.*

Proof. We only need to prove that $\alpha' J\overline{\alpha}^{(i)} = 0$ (for $i = 2, \dots, p-1$). Assume $2 \le i \le p-1$. From $X\alpha = \zeta\alpha$ we have $X\alpha^{(i)} = \zeta^i\alpha^{(i)}$ and $X\overline{\alpha}^{(i)} = \frac{1}{\zeta^i}\overline{\alpha}^{(i)}$. Hence

$$\alpha' J\overline{\alpha}^{(i)} = \frac{\zeta^i}{\zeta}\alpha' X' J X\overline{\alpha}^{(i)} = \frac{\zeta^i}{\zeta}\alpha' J\overline{\alpha}^{(i)}. \tag{2.10}$$

The last equality follows from the fact that $X \in SP_{p-1}(\mathbb{Z})$. Since $\zeta \neq \zeta^i$, we get $\alpha' J\overline{\alpha}^{(i)} = 0$. □

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

Lemma 2.5. *$X \sim Y$ if, and only if $\langle \mathfrak{a}, a\rangle = \langle \mathfrak{b}, b\rangle$.*

Proof. Necessity. Suppose there is $Q \in SP_{p-1}(\mathbb{Z})$ 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

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

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 $\lambda\overline{\lambda}a = \mu\overline{\mu}b$. Then there is $Q \in GL_{p-1}(\mathbb{Z})$ 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 $QY\beta = XQ\beta$, and therefore $QY = XQ$, i.e. $Y = Q^{-1}XQ$.

It remains to prove that $Q \in SP_{p-1}(\mathbb{Z})$. If $i = 2, \dots, p-1$, then

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

If $i = 1$, then

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

Hence $Q' JQ = J$ (see Lemma 2.2). □

Let Ψ denote the correspondence from $\mathcal{M}_p$ to $\mathcal{P}$ defined as above, that is $\Psi\langle X\rangle = \langle \mathfrak{a}, a\rangle$. Lemma 2.5 guarantees Ψ is well defined and injective. The proof of Theorem 1 is completed by following lemma.

Lemma 2.6. *Ψ is surjective.*

Proof. Let $\alpha = (\alpha_1, \ldots, \alpha_{p-1})'$ be a J-vector with respect to $(\mathfrak{a}, a)$. Then $\zeta\alpha_1, \ldots, \zeta\alpha_{p-1}$ is another basis of $\mathfrak{a}$, and so there is $X \in GL_{p-1}(\mathbb{Z})$ such that $X\alpha = \zeta\alpha$. It is clear that X has order p. We only need to prove that $X \in SP_{p-1}(\mathbb{Z})$. We have

$$\alpha' X' J X \overline{\alpha}^{(i)} = \tfrac{\zeta}{\zeta^i} \alpha' J \overline{\alpha}^{(i)} = \delta_{1i}\, \alpha' J \overline{\alpha}.$$

Hence $\alpha' X' J X \overline{\alpha}^{(i)} = \alpha' J \overline{\alpha}^{(i)}$. By Lemma 2.2, $X'JX = J$, that is $X \in SP_{p-1}(\mathbb{Z})$. This completes the proof. □

Proposition 2.1. *For any $X \in M_p$, we have $X \not\sim X^{-1}$.*

Proof. Let $\alpha \in \mathcal{R}^{p-1}$ 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 $\alpha' J \overline{\alpha} = -\overline{\alpha}' J \alpha$. □

2.3 Class Number of $\mathcal{P}$

In this section we prove Theorem 2 and Theorem 3. The set $\mathcal{C}$ of ideal classes is an abelian group and we easily see that $\mathcal{P}$ is an abelian group if we define multiplication in $\mathcal{P}$ 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 $\langle \overline{\mathfrak{a}}, a\rangle$.

For the proof of Theorem 2 we will need the following lemmas.

Lemma 2.7. *Suppose $(\mathfrak{a}, a) \in P$, $\lambda \in \mathcal{R}^*$. Then*

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

The proof is trivial.

Lemma 2.8. *Suppose $(\mathfrak{a}, a)$, $(\mathfrak{a}, b) \in P$. Then $\langle \mathfrak{a}, a\rangle = \langle \mathfrak{a}, b\rangle$ if and only if $\frac{a}{b} \in C$.*

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

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

Lemma 2.9. *Let* $(\mathfrak{a}, a), (\mathfrak{b}, b) \in P$, *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 $\overline{\lambda}\overline{\mathfrak{a}} = \overline{\mu}\overline{\mathfrak{b}}$. Hence $(\lambda\overline{\lambda}a) = \lambda\mathfrak{a}\overline{\lambda}\overline{\mathfrak{a}} = \mu\mathfrak{b}\overline{\mu}\overline{\mathfrak{b}} = (\mu\overline{\mu}b)$. There is a unit $u \in U^+$ such that $\lambda\overline{\lambda}a = \mu\overline{\mu}ub$. Therefore $\langle \mathfrak{a}, a\rangle = \langle \lambda\mathfrak{a}, \lambda\overline{\lambda}a\rangle = \langle \mu\mathfrak{b}, \mu\overline{\mu}ub\rangle = \langle \mathfrak{b}, ub\rangle$. □

Now we can prove Theorem 2; namely there is a short exact sequence

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

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

Proof of Theorem 2. Clearly ϕ is well defined and a group monomorphism (by Lemma 2.8). ψ is also well defined and a group epimorphism. $\psi\phi[u] = \psi\langle \mathcal{R}, u\rangle = \langle \mathcal{R}\rangle$ (by definition) and Ker ψ = Im ϕ (by Lemma 2.9). This completes the proof. □

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

$$\mathcal{C}_1 = \big\{\mathfrak{a} \in \mathcal{C} \mid \mathfrak{a}\overline{\mathfrak{a}} = (a) \text{ for some } a \in \mathcal{R}\big\}. \tag{2.11}$$

$\mathcal{C}_1$ is a subgroup of $\mathcal{C}$, the set of ideal classes 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 2.10. $(1 - \zeta)$ *is a prime ideal of* $\mathcal{R}$.

See Washington [13].

Lemma 2.11. $\mathcal{C}_0 = \mathcal{C}_1$.

Proof. Suppose $\mathfrak{a}\overline{\mathfrak{a}} = (a_0)$ where $a_0 \in \mathcal{R}^*$. 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 Washington [13] $u_0 = \pm\zeta^k$, 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. We then have $u_0 = -\zeta^k$ for some integer k because if $u_0 = \zeta^{2k-1}$ then $u_0 = \zeta^{2k-1+p}$, where $2k - 1 + p$ is even. We want to show that this leads to a contradiction. Note that

$$a \equiv \overline{a} \pmod{1 - \zeta^2} \tag{2.12}$$

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

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 $\overline{\mathfrak{a}} \subset (1 - \zeta)$, by Lemma 2.10. 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 $a_1 \in \mathcal{R}^*$ and $u_0 = \frac{\overline{a}_1}{a_1}$. Continuing this procedure, there is $a \in \mathcal{R}^*$ with $a \notin (1 - \zeta)$ such that $u_0 = \frac{\overline{a}}{a}$.

Now suppose $u_0 = -\zeta^k$. Then, by (2.12), $a \equiv \overline{a} = -\zeta^k a \equiv -a \pmod{1 - \zeta}$, hence $2a$ is equivalent to 0 modulo $(1 - \zeta)$. Since (2) is a prime ideal different from $(1 - \zeta)$ we have a is equivalent to 0 modulo $(1 - \zeta)$, that is $a \in (1 - \zeta)$. Contradiction. □

Lemma 2.12 (Dirichlet). *The unit group U of $\mathcal{R}$ is the direct product $W \times V$, where $V \subset U^+$ is a free abelian group of rank $\frac{p-3}{2}$ and $W = \left\{\pm\zeta^l\right\}$.*

From this lemma we have

Lemma 2.13. $[U^+ : C] = 2^{\frac{p-1}{2}}$.

This completes the proof of Theorem 3 (by applying Theorem 2).

2.4 An Example

Theorem 1 gives us a way to find representatives for M_p. Suppose we have an S-pair $(\mathfrak{a}, a)$ and a basis $\beta_1, \dots, \beta_{p-1}$ of $\mathfrak{a}$, which is not necessarily J-orthogonal. Then the following steps will find a symplectic matrix $X \in M_p$ such that $\Psi(X) = \langle \mathfrak{a}, a\rangle$.

1. Find the dual basis $\gamma_1, \dots, \gamma_{p-1}$ of $\beta_1, \dots, \beta_{p-1}$ by solving the linear system
$$\gamma' \beta^{(i)} = \delta_{1i} \tag{2.13}$$
where $\beta = (\beta_1, \dots, \beta_{p-1})'$ and $\gamma = (\gamma_1, \dots, \gamma_{p-1})'$;
2. Find the integral matrix $Y \in GL_{p-1}(\mathbb{Z})$ such that $Y\beta = \zeta\beta$;
3. Let $M \in GL_{p-1}(\mathbb{Z})$ be such that $M\overline{\beta} = a\Delta\gamma$. Then M is a skew symmetric matrix;
4. Find a matrix $Q \in GL_{p-1}(\mathbb{Z})$ such that $M = Q'JQ$, see Newman [8];
5. Let $X = QYQ^{-1}$ and $\alpha = Q\beta$. Then α is a J-orthogonal basis and Lemma 2.6 shows that $X \in SP_{p-1}(\mathbb{Z})$ and $\Psi(X) = \langle \mathfrak{a}, a\rangle$.

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 $1, \zeta, \dots, \zeta^{p-2}$ is a basis of $\mathcal{R}$. The dual basis of $1, \zeta, \dots, \zeta^{p-2}$ is $\gamma_1, \dots, \gamma_{p-1}$, where
$$\gamma_i = \frac{(\zeta - 1)\zeta}{p}\left(1 + \cdots + \zeta^{p-1-i}\right), \quad i = 1, \dots, p-1. \tag{2.14}$$

Let $\beta = \left(1, \zeta, \dots, \zeta^{p-2}\right)'$ and $\gamma = (\gamma_1, \dots, \gamma_{p-1})'$. Then Y is the companion matrix
$$C_{p-1} = \begin{pmatrix} 0 & 1 & & \\ & & \ddots & \\ & & & 1 \\ -1 & -1 & \dots & -1 \end{pmatrix}.$$

After a routine calculation we see that $\Delta\gamma = M\overline{\beta}$, where $M = \begin{pmatrix} & L_{\frac{p-1}{2}} \\ -L'_{\frac{p-1}{2}} & \end{pmatrix}$, and L_n is the $n \times n$ matrix whose entries above the diagonal are 0 and the others are -1. M is a skew symmetric matrix and we easily see that $M = Q'JQ$, where $Q = \begin{pmatrix} I & \\ & L_{\frac{p-1}{2}} \end{pmatrix} \in GL_{p-1}(\mathbb{Z})$. Therefore we have shown

Proposition 2.2. *Let*

$$X = QCQ^{-1} = \left(\begin{array}{cccc|cccc} 0 & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & 0 & -1 & & & \\ \hline & & & & -1 & 1 & & \\ & & & & -1 & & \ddots & \\ & & & & \vdots & & & 1 \\ 1 & 1 & \dots & 1 & -1 & & & 0 \end{array}\right) \tag{2.15}$$

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

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 3.2 we shall see that all X are realizable if $p \geq 5$.

3 Realizable p-Torsion

3.1 Cyclotomic Units

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

$$u_k = \frac{\sin \frac{k\pi}{p}}{\sin \frac{\pi}{p}}, \quad \text{for } (k,p) = 1. \tag{3.1}$$

Since

$$\frac{1-\zeta^k}{1-\zeta} = \lambda^{k-1} u_k, \quad \text{where } \lambda = -\zeta^{\frac{p+1}{2}}, \tag{3.2}$$

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:

$$u_1 = 1 \quad \text{and} \quad u_{mp+k} = -u_{mp-k} = (-1)^m u_k \tag{3.3}$$

$$\begin{cases} u_k > 0, & 1 \leq k \leq p-1, \\ u_k < 0, & p+1 \leq k \leq 2p-1. \end{cases} \tag{3.4}$$

Lemma 3.1. $\sum_{j=1}^{k} u_{2j+l} = u_k u_{k+l+1}$.

This follows from some standard trigonometric formulas.

Lemma 3.2. $u_k^{(i)} = (-1)^{(k-1)(i+1)} u_{ik} u_i^{-1}$.

Proof. Using (3.2), we see that

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

□

Lemma 3.3. $\Delta^{(k)} = (-1)^{k-1} u_k^{-1} \Delta$.

Proof. Recall that $\Delta = \frac{p\zeta^{\frac{p+1}{2}}}{\zeta - 1}$. The proof is easy. □

Lemma 3.4. *Suppose $X \in M_p$ and $\Psi(X) = \langle \mathfrak{a}, a\rangle$. Then $\Psi(X^k) = \langle \mathfrak{a}^{(k')}, (-1)^{k'-1}u_{k'}^{-1}a^{(k')}\rangle$, where $1 \le k \le p-1$, k' is the inverse of k modulo p, and $\mathfrak{a}^{(k')} = \{\alpha^{(k')} \mid \alpha \in \mathfrak{a}\}$.*

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 $\Psi(X^k) = \langle \mathfrak{a}^{(k')}, a_k\rangle$, 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 3.3). This completes the proof. □

Lemma 3.5. *$u_k \notin C$, 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 $1 \le l \le p-1$ such that $p+1 \le lk \le 2p-1$. Then $u_k^{(l)} = u_{lk}u_l^{-1} < 0$, hence $u_k \notin C$. □

Lemma 3.6. *$u_k u_l^{-1}$, $u_k u_l \notin C$, for $1 \le k, l \le \frac{p-1}{2}$ and $k \ne l$.*

Proof. There is $2 \le i \le p-2$, such that $il \equiv k \pmod p$. Then $u_k u_l^{-1} = \pm u_{il}u_l^{-1} = \pm u_i^{(l)} \notin C$, and $u_k u_l = (u_k u_l^{-1})u_l^2 \notin C$ (since $u_l^2 \in C$). □

By Lemma 3.5 and Lemma 3.6, the following corollary is easy to prove.

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

Proposition 3.1. *Let X be the matrix given by Equation* (2.15)*. Then $X, X^2, \dots, X^{p-1}$ are not similar to each other.*

Proof. $\Psi(X) = \langle \mathcal{R}, 1 \rangle$ and so by Lemma 3.4 we have $\Psi(X^k) = \langle \mathcal{R}, (-1)^{k'-1} u_{k'}^{-1} \rangle$. According to Lemma 2.8 we need only show that the elements $u_1^{-1}, -u_2^{-1}, \cdots, -u_{p-1}^{-1}$ are distinct modulo $\mathcal{C}$. But modulo $\mathcal{C}$ this set of elements is the same as $\pm u_1, \pm u_2, \cdots, \pm u_{\frac{p-1}{2}}$.

□

Example. Let $p = 5$. Then $h_1 = 1$, and hence $q_5 = 4$. There are 4 classes in M_5. Here is a list of canonical matrices of M_5:

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

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

Proposition 3.2. *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 $X, \dots, X^{p-1}$.*

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 $a = \Delta^{-1}\alpha' J \overline{\alpha}$. From Lemma 3.4 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

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

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

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

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

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 3.3. *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 $p \equiv 1 \pmod 3$, $x^2 + x + 1 \equiv 0 \pmod p$ 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 we have $\Psi(X^k) = \langle \mathcal{R}, u\rangle$, 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 $X \sim X^k$. □

To finish this section we give a proposition:

Proposition 3.4. *There are integers $k_1, \ldots, k_n$, such that $2 \leq k_1 < \cdots < k_n \leq \frac{p-1}{2}$, 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 Lang [4]. 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 $u^2 = u_{l_1}^{r_1} \cdots u_{l_t}^{r_t}$ where not all of r_j are even. Thus $u^2 = u_{k_1} \cdots u_{k_n} v^2$ for some distinct integers $2 \leq k_j \leq \frac{p-1}{2}$ and some $v \in C_1$. It follows that $u_{k_1} \cdots u_{k_n} \in C$. □

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

3.2 Realizable p-Torsion

In Sjerve and Yang [14] it was shown that there is a one-to-one correspondence between analytic conjugacy classes of $\mathbb{Z}_p$ actions on compact connected Riemann surfaces of genus $\frac{p-1}{2}$ and short exact sequences $1 \to \Pi \to \Gamma \xrightarrow{\theta} \mathbb{Z}_p \to 1$, where Γ is a Fuchsian group of signature $(0; p, p, p)$ and the Kernel Π is torsion free. The short exact sequence corresponds to the induced action of $\mathbb{Z}_p$ on $S = \mathbb{U}/\Pi$, where $\mathbb{U}$ denotes the upper half plane.

As an abstract group Γ has the presentation:

$$\Gamma(0;p,p,p) = \langle A_1, A_2, A_3 \mid A_1A_2A_3 = A_1^p = A_2^p = A_3^p = 1\rangle.$$

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 $\mathbb{Z}_p$, $1 \leq a,b,c \leq p-1$ and $a+b+c \equiv 0 \pmod p$. We use $M(a,b,c)$ to denote the matrix class which is induced by T.

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

The remainder of this section is concerned with the proof of Theorem 4.

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

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

then Theorem 4 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 3.4, we would then get

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

and by Lemma 3.2, we would then have

$$\begin{aligned} u &= (-1)^{a-1}u_a(u_{b_1}u_{b_1+1})^{(a)} \\ &= (-1)^{a-1}u_a(-1)^{(b_1-1)(a+1)}u_{b_1a}u_a^{-1}(-1)^{b_1(a+1)}u_{(b_1+1)a}u_a^{-1} \\ &= u_a^{-1}u_{mp+b}u_{mp+a+b} \\ &= u_a^{-1}(-1)^m u_b(-1)^m u_{a+b} = u_a^{-1}u_b u_{a+b} \end{aligned}$$

where m satisfies $b_1a = mp + b$. We see that $u/u_au_bu_{a+b} = u_a^{-2} \in C$.

Thus we assume $a = 1$ and $1 \leq b \leq \frac{p-1}{2}$. Then $\frac{p-1}{2} \leq c \leq p-2$ since $1+b+c = p$. We choose a particular embedding of Γ in $\mathrm{Aut}\,(\mathbb{U})$, 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 (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 $(k = 0, \dots, p-1)$, see Figure (2). Let $e_1, \dots, e_{2p}$ be the $2p$ sides of D, and $\eta_i = e_{2i-1} + e_{2i}$ (for $i = 1.\dots,p$). Then

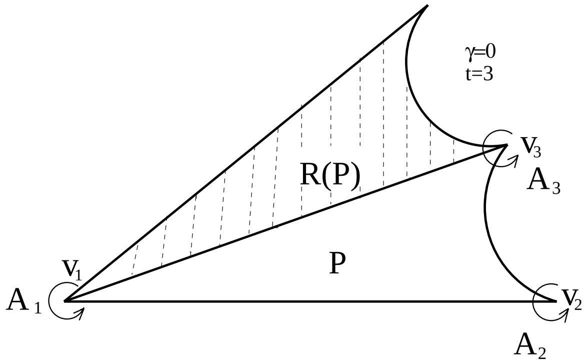

Figure 1: Fundamental Domain of Γ

$\eta_1, \ldots, \eta_p$ are closed paths on S and $[\eta_1], \ldots, [\eta_{p-1}]$ forms a basis of $H_1(S)$, see Massey [7]. 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 $[e_{2i-1}]_\Pi = [-e_{2c+2i}]_\Pi$. Here we are using the notation $[\ ]_\Pi$ to denote equivalence classes under the action of Π on $\mathbb{U}$. 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 $H_1(S)$. Hence the transform matrix from $[\eta]$'s to $[\xi]$'s is the $(p-1) \times (p-1)$ matrix

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

where the entries x_{ij} are given by

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

The determinant of this matrix is ± 1. Hence $[\xi_1], \ldots, [\xi_{p-1}]$ is a basis of $H_1(S)$.

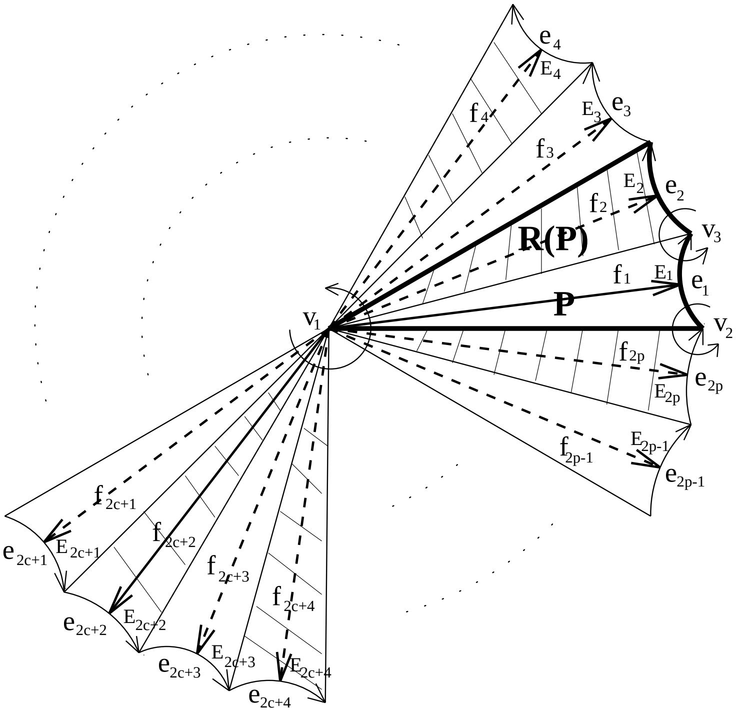

Figure 2: Fundamental Domain of Π

Lemma 3.7. *The matrix of T_* with respect to $[\xi_1], \ldots, [\xi_{p-1}]$ 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 $i = 1, \ldots, 2p$. 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 $k = 1, \ldots, p$. Therefore $T_*([\xi_k]) = [\xi_{k+1}]$, for $k = 1, \ldots, p-1$. 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 3.8. *For any $1 \leq i, j \leq p-1$, $m_{i,j} = m_{i+1,j+1}$ and $m_{1,j+1} = -m_{1,p-j+1}$.*

Proof. T_* preserves the intersection number of closed chains. By Lemma 3.7,

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

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

$$M_j = \left(\begin{array}{ccccccc} 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & \ddots & & \vdots \\ 0 & & & & & \ddots & 0 \\ -1 & & & & & & 1 \\ 0 & \ddots & & & & & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \dots & 0 & -1 & 0 & \dots & 0 \end{array} \right),$$

whose entries $x_{kl}^{(j)}$ are given by

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

By Lemma 3.8, we see that $k_j = m_{1,j+1} = -m_{1,p-j+1} = k_{p-j}$ 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 3.9.

$$k_j = \begin{cases} 1 & 1 \leq j \leq p-c-1 \\ 0 & p-c \leq j \leq \frac{p-1}{2} \end{cases} \tag{3.5}$$

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 (3.5) is straightforward by referring to Figure 3 and Figure 4. □

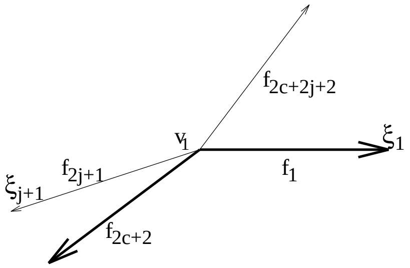

Figure 3: $p - c \leq j \leq (p-1)/2$

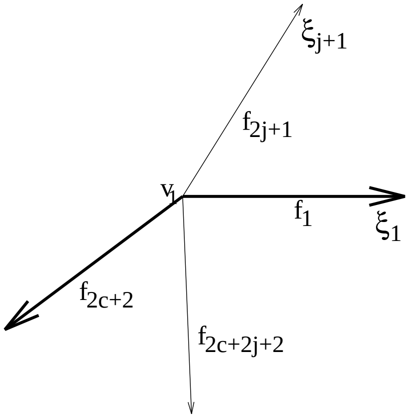

Figure 4: $1 \leq j \leq p - c - 1$

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 3.10. *Let*

$$y_k = \begin{cases} \Delta^{-1}\alpha' M_1 \overline{\alpha}, & k = 1, \\ \Delta^{-1}\alpha'(M_k - M_{p-k})\overline{\alpha}, & k = 2, \ldots, \frac{p-1}{2}. \end{cases}$$

Then $y_k = u_{2k}$.

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

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

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

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 4. 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 3.1 and Lemma 3.10, we obtain $\Delta^{-1}\alpha' M \overline{\alpha} = u_b u_{b+1}$. This completes the proof of Theorem 4. □

References

[1] A. L. Edmonds & J. H. Ewing, *Surface Symmetry and Homology*, Math. Proc. Camb. Phil. Soc. **99** (1986), 73–77.

[2] H. M. Farkas & I. Kra, *Riemann Surfaces*, second edition ed., Graduate Texts in Mathematics, vol. 71, Springer Verlag, New York, 1992.

[3] S. Lang, *Algebraic Numbers*, Addison-Wesky, Reading, Mass., 1964.

[4] ———, *Cyclotomic Fields I and II*, Springer-Verlag, New York, 1990.

[5] C. G. Latimer & C. C. MacDuffee, *A Correspondence between Classes of Ideals and Classes of Matrices*, Ann. of Math. **34** (1933), 313–316.

[6] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[7] W. S. Massey, *Singular Homology Theory*, Graduate Texts in Mathematics, vol. 70, Spring-Verlag New York Inc., New York, 1980.

[8] M. Newman, *Integral Matrices*, Academic Press, New York, 1972.

[9] C. L. Siegel, *Symplectic Geometry*, Amer. J. Math. **65** (1943), 1–86.

[10] P. Symonds, *The Cohomology Representation of an Action C_p on a Surface*, Trans. Amer. Math. Soc. **306** (1988), 389–400.

[11] O. Taussky, *On a Theorem of Latimer and Macduffee*, Canadian J. Math. **1** (1949), 300–302.

[12] ———, *On Matrix Classes Corresponding to an Ideal and its Inverse*, Illinois J. Math. **1** (1957), 108–113.

[13] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

[14] D. Sjerve & Q. Yang, *Eichler Trace of $\mathbb{Z}_p$ Actions on Riemann Surfaces*, submitted (1996).