Involutions in Arithmetic Geometry

by

Anbo Chen

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2013

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirements for the degree of Doctor of Philosophy.

(required signature)

Bruce Jordan

Date

Chair of Examining Committee

(required signature)

Linda Keen

Date

Executive Officer

Bruce Jordan

Carlos Moreno

Kenneth Kramer

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

Involutions in Arithmetic Geometry

by

Anbo Chen

Advisor: Professor Bruce Jordan

We first study the integral representation L of $G = \langle\sigma\rangle$, where σ is an involution. When $L = H_1(X, \mathbb{Z})$ for some algebraic curve X, we determine the structure L completely by the the intersection of J_+ and J_-, where $J_\pm$ are the subvarieties of the Jabocian J of X. Then, we study the structure of $L = H_1(X, \mathbb{Z})$ as the integral representation of Klein 4 group $G = \langle\sigma, \tau\rangle$, where σ and τ are two commuting involutions. Computations are also included in our work.

Acknowledgements

I would express my deepest gratitue to my advisor Bruce Jordan, for his guidence and help during my study. Bruce introduced me into the field of Shimura curves and modular curves, explained the idea and techinique, help me find the topic of my thesis. During the time I writing my thesis, Bruce shared his idea and insight in mathematics, and always enouraged me when I met problems. He also helped me to revise my thesis, even in language. He is also a reliable friend: I know every member in his family. I enjoyed discussing mathematics in his lovely backyard.

I also indebted to the professors in number theory and algebraic geometry in (or was in) Graduate Center of CUNY: Carlos Moreno, Kenneth Krammer, Raymond Hoobler, Yiannis Petridis, Lucien Szpiro, Victor Kolyvagin, and others. They taught me many courses and seminars such as Galois theory, elliptic curves, algebraic K-theory, modular forms, algebraic geometry and dynamics. Thanks to Professor Yunping Jiang and Jun Hu for their help.

Thanks to Professor Jozef Dodziuk, Linda Keen and Mr. Robert Landsman. Thanks to Professor Robert Thompson helping me in Hunter College. Thanks to the mathematicians in number theory in New York: we have good experience to meet every Thursday evening, discuss mathematics, and have dinner (as a student, I only pay $5, I indebted to those senior mathematicians). Thanks to Professor Shouwu Zhang, who introduced me to Bruce and taught algebraic number theory and automorphic forms.

Special thanks to my classmate and friend in GC and New York area: Kwang Hyun Kim, Yimao Chen, Tao Chen, Zhe Wang, Yunchun Hu, Mingmin Shen, Yanhong Yang, Zhengyu Xiang, Terence Swaine, Marriana Bonanome, Anupan Bhatnagar, Subir, Hongzhong Zhang, Andrew Stout, Liang Zhao, Heng Yang, Hengyu Zhou, Daniel Garbin, Yelena Baishanski, Michael Beck, Ni Lu, Sunil Philip, Jenne, Shenglan Yuan, and others. Thanks to Ying Zong in Toronto University, who always give me answers in algebraic geometry and number theory.

Finaly, I would thank to my wife, Yiping, for her love and support over years. To my daughters, Youran, Yiran, and Anran. To my parents, Zhigen Chen and Xianjiao Ren, for their understanding and support for so many years.

Contents

Chapter 1

Introduction

Let $N \geq 1$ be a square-free integer and $J_0(N)_{/\mathbb{Q}}$ be the Jacobian of the classical elliptic modular curve $X_0(N)$. The abelian varieties $J_0(N)$ are some of the most important objects in number theory since they simultaneously contain information on modular forms, Galois extensions of $\mathbb{Q}$ (= representations of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$), and elliptic curves defined over $\mathbb{Q}$. It is important to understand how information on these three fundamental objects is encoded in $J_0(N)$. The richness of the subject comes from the Hecke algebra

$$\mathbb{T} = \mathrm{End}_{\mathbb{Q}}(J_0(N)) = \mathrm{End}_{\mathbb{C}}(J_0(N)) \ , \tag{1.0.1}$$

the last equality being a theorem of Ribet [Ribet75]. The Hecke algebra will play the central role in understanding how these objects are aspects of $J_0(N)$. We are especially interested in certain involutions in $\mathbb{T}$, the Atkin-

Lehner involutions w_n for $n|N$.

Cusp forms of weight 2 for the congruence subgroup $\Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ are the differential 1-forms on the curve $X_0(N)$, and hence are also the cotangent space to its Jacobian $J_0(N)$. The Langlands correspondence (here a theorem of Eichler and Shimura) shows that to every weight-2 cusp form $f \in S_2(\Gamma_0(N)$ which is an eigenfunction of $\mathbb{T}$ there is associated an ℓ-adic Galois representation ρ_f of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This ρ_f is constructed by taking the action of Galois on the torsion points of the abelian subvariety $A_f \subseteq J_0(N)$ whose cotangent space is f together with its Galois conjugates. Finally the Shimura-Taniyama Conjecture (proved by Wiles[Wiles95] and Taylor-Wiles[TaylorWiles95]) shows that if E is an elliptic curve defined over $\mathbb{Q}$ of conductor N, then E is a factor of $J_0(N)$.

The abelian variety $J_0(N)$ breaks up into simple factors (up to isogeny) the same way $\mathbb{T} \otimes \mathbb{Q}$ breaks up into products of fields. This fundamental decomposition is not at all understood. The only place we know the dimensions of the factors is when we decompose $J_0(N)$ under the action of the modular involutions w_n, $n|N$. So it makes sense to start here and ask what this decomposition means for cusp forms, Galois representations, and elliptic curves over $\mathbb{Q}$. To simplify exposition, let's consider the case of $J := J_0(N)$ where N is prime. Then we have $J_+ \subseteq J$ whose cotangent space consists of all

modular forms of weight 2 where w_N acts as $+1$ and similarly $J_- \subseteq J$ where w_N acts as -1. Up to an isogeny whose kernel is killed by 2, $J \cong J_+ \times J_-$. But how big is the fusion at 2 between J_+ and J_-? It is well-known that

Theorem 1.0.1. *Suppose N is prime and set $J = J_0(N)$. Then $J_+ \cap J_- = J_+[2]$.*

This is interesting because there is remarkably different behavior in the Mordell-Weil groups of J_+ and J_-: The Mordell-Weil group of J_+ is a torsion-free abelian group of positive rank, while J_- contains the Eisenstein quotient $\tilde{J}$ which is rank 0. [Mazur77]

I prove Theorem 1.0.1 by proving a more general theorem on algebraic curves:

Theorem 1.0.2. *Suppose J is the Jacobian variety of an algebraic curve X, and σ is an involution of X. Then,*

a. $J_+ \cap J_- = J_+[2]$ if σ has fixed points on X;

b. $J_+ \cap J_- = J_-[2]$ if σ has no fixed point on X.

Ogg [Ogg83] counted the numbers of fixed points of Atkin-Lehner involutions w_n when $n|N$ of $X_0(N)$ and of Shimura curves $X_0^D(N)$, for square-free N . So we can explicitly describe $J_+ \cap J_-$ for modular curves and Shimura curves with Atkin-Lehner involutions.

Another formulation of this problem is to consider $L = H_1(X, \mathbb{Z})$ as an integral representation of group $G = \langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$. L has the form $A_+^a \oplus A_-^b \oplus R_2^c$ where a, b, c are nonnegative integers. $A_\pm$ is the line with $\sigma|_{A_\pm} = \pm 1$, and R_2 is the 2-dimensional regular representation of G [CurtisReiner81]. We determine the value of a, b and c in the following theorem:

Theorem 1.0.3. *Let $X/\mathbb{C}$ be an algebraic curve of genus g, $L = H_1(X, \mathbb{Z})$, and σ be an involution on X. Denote $J_\pm = (1 \pm \sigma)\mathrm{Jac}X$ and $g_\pm = \dim J_\pm$.*

a. If σ has fixed points on X, then $L \cong A_-^{2g_- - 2g_+} \oplus R_2^{2g_+}$;

b. If σ has no fixed point on X, then $L \cong A_+^{2g_+ - 2g_-} \oplus R_2^{2g_-}$.

Theorem 1.0.2 and Theorem 1.0.3 are equivalent.

As another application of an involution acting of the integral homology of an algebraic curve, assume $X = X/\mathbb{R}$ is defined over $\mathbb{R}$, we have a similar theorem for the action of $G = \langle\tau\rangle$ with τ complex conjugation, on $L = H_1(X, \mathbb{Z})$ ([GrossHarris81], [Mazur], or [Jaffee80]). We have specialize it to the case of $X = X_0(N)$:

Theorem 1.0.4. *For the modular curve $X = X_0(N)$ of genus g, where N is a product of n distinct primes, consider τ as the complex conjugation τ acting on $L = H_1(X, \mathbb{Z})$. Then*

$$L \cong A_+^{r-1} \oplus A_-^{r-1} \oplus R_2^{1+g-r}$$

where

$$r = \begin{cases} 2^{n-1} & \text{if } 2 \nmid N, \\ 2^{n-2} & \text{if } 2 \mid N. \end{cases}$$

This theorem, is proved by combining results of [GrossHarris81], [Mazur] or [Jaffee80], and [Ogg83].

In my thesis, I also study the case of two commuting involutions σ and τ acting on$X$. We can similarly define J_{++}, J_{+-}, J_{-+}, J_{--}, and compute their intersections. Denote $g_{\pm\pm} = \dim J_{\pm\pm}$. Now, $L = H_1(X, \mathbb{Z})$ is an integral representation of the Klein 4-group $G = \langle \sigma, \tau \rangle$. Integral representations of the Klein 4-group have been classified by [GelfandPonomarev70], [Brenner74] and [Butler73]. In the two-involution case, the theorems of intersections and integral representation are much more complicated. We use the theorem for one involution to determine some intersections of $J_{\pm\pm}$, and use these results to determine the integral representation. Finally, knowing the integral representation determine all intersections.

Theorem 1.0.5. *Using the notation as above and assuming $\sigma\tau$ has fixed points, suppose the defect of the 4-subspace system corresponding to the integral representation of Klein-4 group $G = \langle \sigma, \tau \rangle$ is 0, and let $v(\sigma)$, $v(\tau)$, $v(\sigma\tau)$ be the number of the fixed points of σ, τ, $\sigma\tau$ acting on X respectively.*
a. If both σ and τ have fixed points on X, then $J_{++} \cap J_{+-} = J_{++} \cap$

$J_{-+} = J_{++} \cap J_{--} = J_{++}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$, $J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\sigma\tau)/2-1}$, $J_{+-} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\tau)/2-1}$, *and* $J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\sigma)/2-1}$;

b. If σ *has fixed points on* X *but* τ *has no fixed points on* X*, then* $J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$, $J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\sigma\tau)/2-2}$, $J_{+-} \cap J_{--} = J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$, *and* $J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\sigma)/2-2}$;

c. If both σ *and* τ *have no fixed points on* X*, then* $J_{--} \cap J_{++} = J_{--} \cap J_{+-} = J_{--} \cap J_{-+} = J_{--}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}$, $J_{++} \cap J_{+-} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}+1}$, $J_{++} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}+1}$, *and* $J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{v(\sigma\tau)/2} - 1$.

The defect, which will be defined later, equals 0 is a techinical assumption. All our computations in case of modular curves with Atkin-Lehner involution show the assumption hold. We hope we can remove this assumption later.

As part of my thesis, I computed examples of $J_+ \cap J_-$ and intersections of J_{++}, J_{+-}, J_{-+} and J_{--} for modular curves using modular symbols. I used the packages MAGMA and Sage for my computations. Also, I computed the 4-subspace system associated to $L = H_1(X, \mathbb{Z})$, which helps us determine the integral representation of the Klein 4-group $G = \langle w_{n_1}, w_{n_1} \rangle$ where $w_{n_{1,2}}$ are Atkin-Lehner involutions of modular curve $X_0(N)$, $N = n_1 n_2$ and n_1, n_2 coprime. These results are the first step of my thesis which leads to the

theorems above.

As mentioned in Mazur's paper [Mazur77], the 2-torsion part is the most complicated part of the problem in determining the structure of torsion points of $J_0(N)(\mathbb{Q})$. In my thesis, I establish new results about the 2-torsion parts of J in extensions of $\mathbb{Q}$. For future work, I will focus on the arithmetic problems related to my theorems for modular curves. For example, as we know from the Theorem 1.0.1, we have $J_+ \cap J_- = J_+[2]$, so we can find modular forms f and g of weight 2 and level N to associated to J_+ and J_- such that $f \equiv g \pmod 2$. This theorem has implications for the Birch and Swinnerton-Dyer conjecture 2-adically.

Chapter 2

The Case of One Involution

Let's first list some notation which we will use in this chapter:

Let X be an algebraic curve and $X^+ := X/\langle\sigma\rangle$, where σ is an involution on X.

Let $\mathrm{Div}^0 X$ and $\mathrm{Prin}X$ be the set of degree zero divisors on X and the set of principal divisors on X. Similarly, we can replace X by X^+ to define the corresponding sets $\mathrm{Div}^0 X^+$ and $\mathrm{Prin}X^+$ for X^+.

Let $J := \mathrm{Jac}X$ be the Jacobian of X. As an abelian scheme, the set of all its closed points is isomorphic to of $\mathrm{Div}^0 X/\mathrm{Prin}X$. We also define $J_\pm := (1 \pm \sigma)J$.

Assume $K = \bar{K}$ is an algebraic closed field with $\mathrm{char}K \neq 2$. Let $K(X)$ be the function field of X over K and $K(X)^*$ be the set of nonzero elements in $K(X)$. Similarly, we can define $K(X^+)$ and $K(X^+)^*$. We can write $K(X) = K(X^+)(\sqrt{h})$ as an extension of the function field $K(X^+)$, for some

$h \in K(X^+)$. Let B be the set consisting of the points on X^+ where the cover $X \to X^+$ is ramified. (B can be an empty set.)

If $f \in K(X)^*$ or $K(X^+)^*$, we denote by (f) the corresponding principal divisor. If $D \in \mathrm{Div}^0(X)$ or $\mathrm{Div}^0(X^+)$, we write $[D]$ for the equivalence class containing D in $\mathrm{Jac}X$ or $\mathrm{Jac}X^+$. Let g be the genus of X, which is also the dimension of $\mathrm{Jac}X \cong \mathbb{C}^g/H_1(X,\mathbb{Z})$. Let $g_\pm := \dim J_\pm$ and we have $g = g_+ + g_-$.

In this chapter, we will first discuss the problem of $J_+ \cap J_-$. Our main theorem is:

Theorem 2.0.6. *Suppose J is the Jacobian variety of an algebraic curve X, and σ is an involution of X. Then σ indues an action on J. Let $J_\pm = (1 \pm \sigma)J$ and $g_\pm = \dim J_\pm$. Then,*

(a) $J_+ \cap J_- = J_+[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_+}$, *if σ has fixed points on X;*

(b) $J_+ \cap J_- = J_-[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_-}$, *if σ has no fixed point on X.*

Then, we will state the theorems of Ogg [Ogg83] and Kenku [Kenku77] about the numbers of the fixed points of Atkin-Lehner involutions on the modular curves $X_0(N)$ and Shimura curves $X_0^D(N)$, where N is a squarefree integer. We can apply Theorem 2.0.6 to these cases. In the last part of this chapter, we give an equivalent formulation of our problem: the explicit decomposition

of the integral representation $H_1(X,\mathbb{Z})$ of the group $G=\langle\sigma\rangle$. We have

Theorem 2.0.7. *Consider $L=H_1(X,\mathbb{Z})$ as an integral representation of the cyclic 2-group $G=\langle\sigma\rangle$, where X is an algebraic curve and σ is an involution on X. Let $g_\pm=\dim J_\pm$. As a $\mathbb{Z}[\sigma]$-module, we have that:*

(a) *if σ has fixed points, $L\cong A_-^{2g_--2g_+}\oplus R_2^{2g_+}$;*

(b) *if σ has no fixed point, $L\cong A_+^2\oplus R_2^{2g_-}$,*

where $\sigma|_{A_\pm}=\pm 1$, and $\sigma|_{R_2}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.

We also discuss the decomposition of integral representation $L=H_1(X_0(N),\mathbb{Z})$ as a representation of $G=\langle\tau\rangle$, where τ is the complex conjugation on L. The symplectic pairing on L induced by oriented intersection is also treated.

In order to the get the formula for $J_+\cap J_-$, we also need the following lemma (the proof of the first part can be found on Page 97 of [Mazur77]):

Lemma 2.0.8. (a) *If σ has fixed points on X, $J_+=\mathrm{Jac}X^+=\mathrm{Jac}(X/\langle\sigma\rangle)$.*

(b) *If σ has no fixed point on X, $J_+=\mathrm{Jac}X^+/P$, where P is a cyclic group of order 2.*

To prove Lemma 2.0.8, we need the following lemmas:

Lemma 2.0.9. *For any algebraic curve X, and any point $P\in X$, there exists $f\in K(X)$ such that f has a simple zero at P.*

Proof. For any algebraic curve X, let $D \in \mathrm{Div}X$, and $f \in K(X)$. Let g be the genus of X. Define

$$\mathscr{L}(D) := \{f \in K(X) | (f) + D \geq 0\} \cong H^0(X, \theta(D)). \tag{2.0.1}$$

Set $h^0(D) = \dim_K \mathscr{L}(D) = \dim_K H^0(X, \theta(D))$, and let K be the canonical divisor of X. We have the following results (See, for example §4.1 in [Hartshorne77]):

$$h^0(D) = 0 \text{ if } \deg D < 0; \tag{2.0.2}$$

the Riemann-Roch Theorem:

$$h^0(D) - h^0(K - D) = \deg D - g + 1; \tag{2.0.3}$$

and its corollary

$$\deg K = 2g - 2. \tag{2.0.4}$$

We can always find a divisor $D_1 \in \mathrm{Div}X$, such that $P \notin \mathrm{Supp}D_1$ and $\deg D_1 > 2g + 1$. Consider the divisor $D = -P + D_1 \in \mathrm{Div}X$,

$$\deg D = -1 + \deg D_1 > -1 + 2g + 1 = 2g, \tag{2.0.5}$$

$$\deg(K - D) = \deg K - \deg D = 2g - 2 - \deg D < 2g - 2 - 2g = -2 < 0. \tag{2.0.6}$$

So $h^0(K-D)=0$ since $\deg(K-D)<0$, and $h^0(D)=\deg D-g+1$ by the Riemann-Roch Theorem. Since

$$h^0(D)=\deg D-g+1>2g-g+1=g+1\geq 1, \tag{2.0.7}$$

We have $h^0(D)=\dim_K \mathscr{L}(D)\geq 1$, As a result, there exists $f\in K(X)$ such that $(f)+D=(f)-P+D_1\geq 0$, which means that f has a zero at P.

Furthermore, we can prove the rank of the zero can be chosen to be 1. Let $D_2=-P+D=-2P+D_1$,

$$\deg D_2=\deg D-1\geq 2g-1>2g-2, \tag{2.0.8}$$

$$\deg(K-D_2)=\deg K-\deg D_2<(2g-2)-(2g-2)=0. \tag{2.0.9}$$

Hence $h^0(K-D_2)=0$, and

$$h^0(D_2)=\deg D_2-g+1=(\deg D-1)-g+1=\deg D-g=h^0(D)-1\geq x0. \tag{2.0.10}$$

So $\mathscr{L}(D_2)\subsetneq\mathscr{L}(D)$, There exists $f\in\mathscr{L}(D)$ but $f\notin\mathscr{L}(D_2)$. We have $(f)+(-P+D_1)\geq 0$ but $(f)+(-2P+D_1)\ngeq 0$, where $P\notin \mathrm{Supp}D_1$. So f has a simple zero at P. □

Lemma 2.0.10. *Suppose $h\in K(X^+)$ is a function with $K(X)=K(X^+)(\sqrt{h})$, and let B be the set consisting of the points on X^+ where the cover $X\to X^+$ is ramified. If $(h)=\sum_{x_i\in B}m_ix_i+\sum_{y_j\notin B}n_jy_j$, then all m_i's are odd, and all n_j's are even.*

Proof. The points where the cover $X \to X^+$ is ramified are exactly the primes ramified in the extension $K(X^+)(\sqrt{h})/K(X^+)$. So any prime ramified in $X \to X^+$ is in the support of (h).

First, we prove all m_i's are odd. Suppose one of m_i's, say $m_1 = 2a$, is even. By Lemma 2.0.9, we can find a function $f \in K(X^+)$ such that f has a simple zero at the point x_1. $K(X) = K(X^+)(\sqrt{h}) = K(X^+)(\sqrt{hf^{-2a}})$, hence we can replace h by hf^{-2a}. Then $x_1 \notin \mathrm{Supp}(hf^{-2a})$, and so $X \to X^+$ cannot be ramified at x_1, which contradicts that fact that the extension $K(X)$ over $K(X^+)$ has ramification a point x_1. So all m_i's are odd.

Then, we prove all n_j's are even. Say $\pi^*(h) = g^2$ for some $g \in K(X)$, and $(g) \in \mathrm{Div}X$. Suppose one of n_j's, say n_1, is odd. Then $(h) = n_1 y_1 + D'$ for some $D' \in \mathrm{Div}X^+$ and $y_1 \notin \mathrm{Supp}D'$. So

$$(g) = \frac{1}{2}\pi^*(h) = \frac{1}{2}(n_1\pi^* y_1 + \pi^* D') = \frac{n_1}{2}(\bar{y}_{11} + \bar{y}_{12}) + \frac{1}{2}\pi^* D', \qquad (2.0.11)$$

where $\pi(\bar{y}_{11}) = \pi(\bar{y}_{12}) = y_1$ and $\bar{y}_{11},\ \bar{y}_{12} \notin \mathrm{Supp}\pi^* D'$. $\bar{y}_{11}$ and $\bar{y}_{12}$ have non-integer coefficients since n_1 is odd, which contradicts the fact that $(g) \in \mathrm{Div}X$. So, all n_j's are even. □

From Lemma 2.0.10, we can easily get the following lemma.

Lemma 2.0.11. *Suppose $h \in K(X^+)$ is a function with $K(X) = K(X^+)(\sqrt{h})$. Then $\pi : X \to X^+$ is unramified if and only if $(h) = 2D$, for $D \in \mathrm{Div}^0 X^+$.*

Lemma 2.0.12. (a)*If π is ramified, then $\pi^* : \mathrm{Pic}^0 X^+ \to \mathrm{Pic}^0 X$ is injective;* (b)*If π is unramified, then $\pi^* : \mathrm{Pic}^0 X^+ \to \mathrm{Pic}^0 X$ has a kernel isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

Proof. (a) Suppose $0 \neq P \in \ker(\pi^*)$. $(\pi_* \circ \pi^*)(P) = 2P = 0$. Let $D \in \mathrm{Div}^0(X^+)$ satisfies $P = [D]$ and fix $h \in K(X^+)$ with $(h) = 2D$, $D \neq (g)$ for any $g \in K(X^+)$. $\pi^*(P) = 0$ implies $\pi^*(D) = (f)$ for $f \in K(X)$. We get $(f^2) = (\pi^* h)$ which means $f^2 = ch$ for some $c \in K$. Hence $\sqrt{h} = \frac{1}{\sqrt{c}} f \in K(X)$. But $\sqrt{h} \notin K(X^+)$ (since $D \neq (g)$ for any $g \in K(X^+)$). Hence $K(X) = K(X^+)(\sqrt{h})$, $(h) = 2D$, which implies $\pi : X \to X^+$ is unramified by Lemma 2.0.11. This proves (a).

(b) Assume π is unramified, $K(X) = K(X^+)(\sqrt{h})$. By Lemma 2.0.11, $(h) = 2D$ for some $D \in \mathrm{Div}^0 X^+$. Since $\sqrt{h} \notin K(X^+)$, $0 \neq [D] \in \mathrm{Pic}^0 X^+$. $\pi^* D = (\sqrt{h}) \in K(X)$, implying $0 \neq D \in \ker\pi^*$. Suppose $0 \neq D' \in \ker\pi^*$, we have $2D' = \pi_* \circ \pi^* D' = 0$, and $2D' = (h')$ for some $h' \in K(X^+)$ but $\sqrt{h'} \notin K(X^+)$. So we have $K(X) = K(X^+)(\sqrt{h}) = K(X^+)(\sqrt{h'})$. Hence $h' = hg^2$ for some $g \in K(X^+)$. We get $(h') = (h) + 2(g)$, or $D' = D + (g)$, so we get $D \sim D'$. As a result, we have $\ker\pi^* = \langle D \rangle \cong \mathbb{Z}/2\mathbb{Z}$. □

Now, we can prove Lemma 2.0.8.

Proof. $\mathrm{Jac}X = \mathrm{Pic}^0 X$ and $\mathrm{Jac}X^+ = \mathrm{Pic}^0 X^+$. Consider $\pi^* : \mathrm{Jac}X^+ \to \mathrm{Jac}X$,

the image of π^* identifies the connected component of the identity in the +-eigenspace of σ in Jac$X$, which is exact $J_+ := (1+\sigma)\text{Jac}X$. Together with Lemma 2.0.12, we prove the lemma. □

By definition, $J_+ = (1+\sigma)J$ and $J_- = (1-\sigma)J$, where σ is an involution with $\sigma^2 = Id$. For any $x \in J_+ \cap J_-$, $x = (1+\sigma)y$ for some $y \in J$ and $\sigma x = (\sigma + \sigma^2) = (1+\sigma)y = x$ since $x \in J_+$. Similarly, $x = (1-\sigma)z$ for some $z \in J$ and $\sigma x = (\sigma - \sigma^2)z = (\sigma - 1)z = -x$. We have $x = -x$, $2x = 0$, consequently, $J_+ \cap J_- \cong (\mathbb{Z}/2\mathbb{Z})^r$ for some integer r. The proof of the main theorem (Theorem 2.0.6) of this chapter is to determine the integer r.

2.1 Intersection of J_+ and J_-: the Case σ Has Fixed Points

In this section, we consider the case that the involution σ has fixed points, and prove the first part of Theorem 2.0.6.

We have the canonical projection π:

$$\begin{array}{c} X \\ \downarrow_\pi \\ X^+, \end{array} \tag{2.1.1}$$

where $X^+ := X/\langle\sigma\rangle$, and an extension of the function field:

$$\begin{array}{c} K(X) \\ | \\ K(X^+), \end{array} \tag{2.1.2}$$

where $K(X) = K(X^+)(\sqrt{h})$, $K = \bar{K}$, $K(X)$ and $K(X^+)$ are function fields of X and X^+ respectively. Let $B \neq \emptyset$ be the set of the σ fixed points, which are also the ramification points of $K(X^+)$ under $K(X)$. Here $K(X)$ is a quadratic extension of $K(X^+)$ by a function $\sqrt{h}$, where $h \in K(X^+)$, and the principal divisor (h) has odd coefficients on the points in B and even outside.

To prove the first part of the Theorem 2.0.6, we will construct the following diagram step by step.

$$\begin{array}{ccc} & 0 & \\ & \downarrow & \\ \{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}/(K(X^+)^*)^2 & \overset{\psi}{\underset{\cong}{\longrightarrow}} & J_+[2] \\ & \downarrow i & \downarrow j \\ \{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}/h^{\mathbb{Z}}(K(X^+)^*)^2 & \overset{\phi}{\underset{\cong}{\longrightarrow}} & J[2]^\sigma \\ & \downarrow & \\ & (\mathbb{Z}/2\mathbb{Z})^{|B|}_{\mathrm{Deg}0}/\langle(1,1,...,1)\rangle & \\ & \downarrow & \\ & 0. & \end{array} \tag{2.1.3}$$

From the above Lemma 2.0.8, we know that $J_+ := (1+\sigma)J = \mathrm{Jac}X^+$ when σ has fixed points. So we have

$$\begin{aligned} J_+[2] &= \mathrm{Jac}X^+[2] \\ &\cong \frac{\{D \in \mathrm{Div}^0 X^+ | 2D = (f) \text{ for some } f \in K(X^+)^*\}}{\{D \in \mathrm{Div}^0 X^+ | D = (g) \text{ for some } g \in K(X^+)^*\}} \\ &\cong \frac{\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}}{(K(X^+)^*)^2}. \end{aligned} \tag{2.1.4}$$

So we have constructed

$$\frac{\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}}{(K(X^+)^*)^2} \xrightarrow{\psi}_{\cong} J_+[2]. \tag{2.1.5}$$

In the following part, we will construct

$$\frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2} \xrightarrow{\phi}_{\cong} J[2]^\sigma. \tag{2.1.6}$$

We can define the map $\mathrm{Div}X^+ \xrightarrow{\pi^*} \mathrm{Div}X$ induced by the projection $X \xrightarrow{\pi} X^+$. It coincides with the embedding $K(X^+) \hookrightarrow K(X)$. By abusing the notation, we can also use π^* to denote the embedding. Using the map π^* we can define

$$\begin{aligned} \{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\} &\xrightarrow{\tilde{\phi}} J \\ f &\mapsto [\frac{1}{2}(\pi^* f)]. \end{aligned} \tag{2.1.7}$$

Lemma 2.1.1. $\mathrm{Im}\tilde{\phi} \subseteq J[2]^\sigma$.

Proof. For any $f \in \{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}$, $2[\frac{1}{2}(\pi^* f)] = [(\pi^* f)]$, which is a principal, we have $\mathrm{Im}\tilde{\phi} \subseteq J[2]$.

Moreover, (f) has the form

$$(f) = \sum_{x_i \in B} n_i x_i + 2 \sum_{y_j \notin B} m_j y_j. \tag{2.1.8}$$

We have

$$(\pi^* f) = 2 \sum_{\pi(\bar{x}_i) = x_i \in B} n_i \bar{x}_i + 2 \sum_{\pi(\bar{y}_{jk}) = y_j \notin B,\ k=1,2} m_j (\bar{y}_{j1} + \bar{y}_{j2}). \tag{2.1.9}$$

The coefficient 2 of the first term comes from the ramification index 2 of the points in B. $\bar{x}_i$ is the unique pre-image of x_i under π, $\bar{y}_{j1}$ and $\bar{y}_{j2}$ are the pre-images of y_j under π, and x_i's are σ-invariant while σ exchange $\bar{y}_{j1}$ and $\bar{y}_{j2}$ to each other. Consequently we get $\frac{1}{2}(\pi^* f) = \sum n_i \bar{x}_i + \sum m_j(\bar{y}_{j1} + \bar{y}_{j2})$ is σ-invariant. So we get $\mathrm{Im}\tilde{\phi} \subseteq J[2]^\sigma$. □

From the above lemma, we can define the map

$$\begin{aligned} \{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\} &\xrightarrow{\tilde{\phi}} J[2]^\sigma \\ f &\mapsto [\frac{1}{2}(\pi^* f)]. \end{aligned} \tag{2.1.10}$$

Let us consider the kernel of $\tilde{\phi}$, we have:

Lemma 2.1.2. $\ker\tilde{\phi} = h^{\mathbb{Z}}(K(X^+)^*)^2$.

Proof. If $f \in h^{\mathbb{Z}}(K(X^+)^*)^2$, we can always write f as $h^a g^2$, for some $g \in K(X^+)^*$ and a is 0 or 1. We consider π^* as an embedding $K(X^+) \hookrightarrow K(X) = K(X^+)(\sqrt{h})$. When a=0, $f = g^2$, $\tilde{\phi}(f) = [\frac{1}{2}(\pi^* f)] = [\frac{1}{2}(g^2)] = [(g)] = 0$, we get $f \in \ker\tilde{\phi}$. When a=1, $f = hg^2$, $\tilde{\phi}(f) = [\frac{1}{2}(\pi^* f)] = [\frac{1}{2}(hg^2)] = [(\sqrt{h}g)] = 0$, since $\sqrt{h} \in K(X)^*$, we get $f \in \ker\tilde{\phi}$. So $\ker\tilde{\phi} \supseteq h^{\mathbb{Z}}(K(X^+)^*)^2$.

For the other direction, assume $f \in \ker\tilde{\phi}$, $[\frac{1}{2}(\pi^* f)] = [(g)]$ for some $g \in K(X)^*$. Since $K(X) = K(X^+)(\sqrt{h})$, we can always write $g \in K(X)^*$ as $g = s\sqrt{h} + r$, where $s, r \in K(X^+)$. Since $[(\pi^* f)] = [2(g)] = [(g^2)]$, and $g^2 =$

$(s\sqrt{h}+r)^2 = (s^2h+r^2)+2sr\sqrt{h}$, we have $sr = 0$. In fact, for $a,\ b \in K(X^+)^*$, if $(a+b\sqrt{h}) = (a-b\sqrt{h})$, we have $(a+b\sqrt{h}) = c(a-b\sqrt{h})$ for some constant c. Either $c = 1$ and $b = 0$, or $c = -1$ and $a = 0$. For $g^2 = (s^2h+r^2)+2sr\sqrt{h}$, if $s^2h + r^2 = 0$, we have $(h) = (-r^2/s^2) = 2(r/s)$, contradict to the fact that (h) has odd coefficients on B. So, we have $2st = 0$. We either have $s \equiv 0$ or $r \equiv 0$. If $s \equiv 0$, we have $g = r \in K(X^+)^*$, and $f = cg^2$ for some constant c. We can modify g by $\sqrt{c}g$. Since K is algebraic closed, we always have $\sqrt{c} \in K$. then we get $f = g^2$, so $f \in h^{\mathbb{Z}}(K(X^+)^*)^2$. If $r \equiv 0$, we have $g = s\sqrt{h}$, and $f = cs^2h$ for some constant c. we can modify g by $\sqrt{c}s$, we get $f = g^2h$, so $f \in h^{\mathbb{Z}}(K(X^+)^*)^2$. So we get $\ker\tilde{\phi} \subseteq h^{\mathbb{Z}}(K(X^+)^*)^2$.

We proved $\ker\tilde{\phi} = h^{\mathbb{Z}}(K(X^+)^*)^2$. □

By Lemma 2.1.2, we can define the injection ϕ:

$$\frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2} \overset{\phi}{\hookrightarrow} J[2]^\sigma. \tag{2.1.11}$$

In fact, we will show that ϕ is an isomorphism in the following lemma:

Lemma 2.1.3. *ϕ is surjective.*

Proof. To prove this lemma, we need the following result first:

Lemma 2.1.4. *If $[D] \in J[2]^\sigma$, then there is a σ-invariant representative $D \in \mathrm{Div}^0X$, i.e., $\sigma D = D$, in this class.*

Proof. The proof of this lemma relies on some technique of group cohomology (See, for example, [Olson70]).

There is a canonical projection $\mathrm{Div}^0 X \to J$. Let M be the pre-image of the $J[2]$ under this map. So we have the short exact sequence:

$$0 \to \mathrm{Prin}X \to M \to J[2] \to 0, \tag{2.1.12}$$

where $\mathrm{Prin}X = K(X)^*/K^*$ is the principal divisor. This short exact sequence will induce a long exact sequence of group cohomology:

$$... \to M^\sigma \to J[2]^\sigma \to H^1(G, \mathrm{Prin}X) \to ..., \tag{2.1.13}$$

where $G = \langle\sigma\rangle$. If we prove $H^1(G, \mathrm{Prin}X) = 0$, then we know that $M^\sigma \to J[2]^\sigma$ is a surjection, and there exist an element $D \in M^\sigma$, i.e., $\sigma D = D$.

To prove $H^1(G, \mathrm{Prin}X) = 0$, we need the short exact sequence:

$$1 \to K^* \to K(X)^* \to \mathrm{Prin}X \to 1. \tag{2.1.14}$$

which induce a long exact sequence:

$$... \to H^1(G, K(X)^*) \to H^1(G, \mathrm{Prin}X) \to H^2(G, K^*) \to .... \tag{2.1.15}$$

$H^1(G, K(X)^*) = 0$ by Hilbert 90. $H^2(G, K^*) = \hat{H}^2(G, K^*)$, where $\hat{H}$ is Tate cohomology. From the knowledge of Tate cohomology, we know that $\hat{H}^2(G, K^*) = \hat{H}^0(G, K^*)$ since G is a cyclic group of order 2, and

$\hat{H}^0(G, K^*) = (K^*)^G/N(K^*)$. Each element in K^* is σ-invariant, hence we have $(K^*)^G = K^*$. $N(K^*) = K^* \cdot K^{*G} = (K^*)^2$, while $K = \bar{K}$, we have $(K^*)^2 = K^*$, so we get $H^0(G, K^*) = K^*/(K^*)^2 = 0$. Then from the above exact sequence 2.1.15 we know that $H^1(G, \mathrm{Prin}X) = 0$. □

Now we can prove the surjectivity.

If $[D] \in J[2]^\sigma$, we can find a σ-invariant element $D \in \mathrm{Div}^0 X$ such that $\sigma D = D$ by the above lemma. We can write

$$D = \sum_{\pi(\bar{x}_i)=x_i \in B} n_i \bar{x}_i + \sum_{\pi(\bar{y}_{jk})=y_j \notin B,\ k=1,2} m_j(\bar{y}_{j1} + \bar{y}_{j2}), \tag{2.1.16}$$

where $\bar{x}_i$ is fixed by σ, σ exchanges $\bar{y}_{j1}$ and $\bar{y}_{j2}$, and $\pi(\bar{x}_i) = x_i$, $\pi(\bar{y}_{j1}) = \pi(\bar{y}_{j2}) = y_j$. The coefficients of $\bar{y}_{j1}$ and $\bar{y}_{j2}$ are equal since D is σ-invariant, and we also have $\sum_i n_i + 2\sum_j m_j = 0$ since $D \in \mathrm{Div}^0 X$. We have $2D = 2\sum_i n_i \bar{x}_i + 2\sum_j m_j(\bar{y}_{j1} + \bar{y}_{j2})$, and we can find that $\pi^* E = 2D$, where $E = \sum_{x_i \in B} n_i x_i + 2\sum_{y_j \notin B} m_j y_j \in \mathbb{Z}B + 2\mathrm{Div}X^+$. To prove that ϕ is surjective, we only need to prove $E = (f)$ for some $f \in K(X^+)^*$.

Since $2D = (g)$ for some $g \in K(X)^*$, we have (g) is σ-invariant. From $\sigma(g) = (g)$ we have $\sigma g = cg$ for some constant c. Since $\sigma^2 = 1$, $c^2 g = c\sigma g = \sigma^2 g = g$, we have $c^2 = 1$. So we have $\sigma g = g$ or $\sigma g = -g$.

When $\sigma g = g$, we know that $g \in (K(X)^*)^\sigma = K(X^+)^*$, so we can think π^* as an embedding of $K(X^+) \overset{\pi^*}{\hookrightarrow} K(X)$ by $f \mapsto g$ and $(f) = \sum_{x_i \in B} n_i x_i +$

$2\sum_{y_i\notin B} m_i y_i = E \in \mathbb{Z}B + 2\mathrm{Div}X^+$.

When $\sigma g = -g$, we will show that this case never happens: If such g exists, since $g \in K(X)^* = (K(X^+)(\sqrt{h}))^*$, we can always write g in form of $a + b\sqrt{h}$ where $a, b \in K(X^+)^*$. Since σ fixed the points on X^+ and $\sigma\sqrt{h} = -\sqrt{h}$, we get $g = b\sqrt{h}$ in this case, hence $(g) = (b) + \frac{1}{2}(h)$. If we consider b and h as functions in $K(X^+)$ by abusing the notations. We have $(g) = \pi^*(b) + \frac{1}{2}\pi^*(h)$, where $b = \sum_{x_{bi}\in B} n_{bi}x_{bi} + \sum_{y_j\notin B} m_{bj}y_{bj}$, and $h = \sum_{x_{hi}\in B} n_{hi}x_{hi} + \sum_{y_{hj}\notin B} m_{hj}y_{hj}$, and all n_{hi}'s are odd as we assumed before. Then, we get $\pi^*(b) = 2\sum_{x_{bi}\in B} n_{bi}\bar{x}_{bi} + \sum_{y_{bj}\notin B} m_{bj}(\bar{y}_{bj1} + \bar{y}_{bj2})$, and $\frac{1}{2}\pi^*(h) = \sum_{x_{hi}\in B} n_{hi}\bar{x}_{hi} + \frac{1}{2}\sum_{y_{hj}\notin B} m_{hj}(\bar{y}_{hj1} + \bar{y}_{hj2})$, so we get odd coefficients on the points $\bar{x}_{hi}$, which contradict to $(g) = 2D$.

So for every $[D] \in J[2]^\sigma$, we can find $(f) \in \mathbb{Z}B + 2\mathrm{Div}X^+$, such that $\phi(f) = [\frac{1}{2}(\pi^* f)] = [D]$, and we prove the surjectivity. □

So, we have:

$$\frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2} \xrightarrow{\phi}_{\cong} J[2]^\sigma. \tag{2.1.17}$$

Lemma 2.1.5. *The following diagram is commutative:*

$$\begin{array}{ccc} \{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}/(K(X^+)^*)^2 & \xrightarrow{\psi}_{\cong} & J_+[2] \\ \downarrow i & \circlearrowleft & \downarrow j \\ \{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}/h^{\mathbb{Z}}(K(X^+)^*)^2 & \xrightarrow{\phi}_{\cong} & J[2]^\sigma. \end{array} \tag{2.1.18}$$

Proof. We have constructed the maps ϕ and ψ in (2.1.5) and (2.1.17). Now we will construct the maps i and j in Diagram (2.1.18). The map j is just the restriction of $\mathrm{Jac}X^+ \to \mathrm{Jac}X$ to $J_+[2]$ induced by the projection $\pi : X \to X^+$. Since σ has fixed points, the induced map j is injection. For any $x \in J_+[2]$ we have $\sigma j(x) = \sigma x = x = j(x)$, and $2j(x) = 2x = 0$, so $\mathrm{Im}j \subseteq J[2]^\sigma$. We can construct map i from the injection $\tilde{i} : \{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\} \to \{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}$, and it is easy to see that $\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\} \cap h^{\mathbb{Z}}(K(X^+)^*)^2 = (K(X^+)^*)^2$ which induced the injection i.

For any $f \in \{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}$, $j \circ \psi(f) = j(\frac{1}{2}[(f)]) = \frac{1}{2}[(f)]$, and $\phi \circ i(f) = \phi(f) = \frac{1}{2}[(f)]$, and Diagram (2.1.18) is commutative. □

Theorem 2.1.6. *If X has σ-fixed points, then* $\mathrm{rank}_{\mathbb{F}_2} J[2]^\sigma = 2g_-$.

Proof. By (2.1.17)

$$\frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2} \cong J[2]^\sigma, \tag{2.1.19}$$

we only need to prove that

$$\mathrm{rank}_{\mathbb{F}_2} \frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2} = 2g_-. \tag{2.1.20}$$

Let's look at the cokernel of the map

$$\frac{\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}}{(K(X^+)^*)^2} \xrightarrow{i} \frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2}. \tag{2.1.21}$$

It is not hard to see that

$$\text{coker } i \cong \frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\text{Div}X^+\}}{h^{\mathbb{Z}} \cdot \{f \in K(X^+)^* | (f) \in 2\text{Div}^0 X^+\}}. \tag{2.1.22}$$

We can further get the following identity:

$$\text{coker } i \cong (\mathbb{Z}/2\mathbb{Z})^{|B|}_{\text{Deg0}}/\langle(1, 1, ..., 1)\rangle, \tag{2.1.23}$$

where $|B|$ is the number of σ-fixed points. Since for every element in $\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\text{Div}X^+\}$, the corresponding principal divisor (f) has even coefficients on the points outside B, while every element in $\{f \in K(X^+)^* | (f) \in 2\text{Div}^0 X^+\}$ has even coefficients on all points. So their quotient should be $|B|$ copies of $\mathbb{Z}/2\mathbb{Z}$. But we need add one additional restriction: the degree (the sum of the coefficients of all the points) of a principal divisor is 0, while the sum of all the coefficients of the points outside B is even, so the sum of all the coefficients of the points on B should also even, which we add a subscript Deg0, meaning that the sum of all components of $|B|$ copies of $\mathbb{Z}/2\mathbb{Z}$ is 0 (mod 2). Then, we can consider the affection of function h: h is equivalent to $\langle(1, 1, ..., 1)\rangle$ in $(\mathbb{Z}/2\mathbb{Z})^{|B|}$, so we should quotient $\langle(1, 1, ..., 1)\rangle$ at last.

As a result, we have

$$0 \to \frac{\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}}{(K(X^+)^*)^2} \xrightarrow{i} \frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2}$$
$$\to (\mathbb{Z}/2\mathbb{Z})^{|B|}_{\mathrm{Deg}0}/\langle (1,1,...,1)\rangle \to 0. \tag{2.1.24}$$

We finished the construction of Diagram 2.1.3.

We have

$$\mathrm{rank}_{\mathbb{F}_2}(\mathrm{coker}\ i) = \mathrm{rank}_{\mathbb{F}_2}\frac{(\mathbb{Z}/2\mathbb{Z})^{|B|}_{\mathrm{Deg}0}}{\langle (1,1,...,1)\rangle} = |B| - 2, \tag{2.1.25}$$

and

$$\begin{aligned}
&\mathrm{rank}_{\mathbb{F}_2}\frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2} \\
&= \mathrm{rank}_{\mathbb{F}_2}\frac{\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}}{(K(X^+)^*)^2} + \mathrm{rank}_{\mathbb{F}_2}\mathrm{coker}i \\
&= 2g_+ + |B| - 2.
\end{aligned} \tag{2.1.26}$$

From the Riemann-Hurwitz theorem, for the projection $X \to X^+$, we know that $2-2g = 2(2-2g_+) - |B|$. By $g = g_+ + g_-$, we have $2-2g_+-g_- = 4-4g_+-|B|$, and then $2g_- = 2g_+ - 2 + |B|$. We finally get

$$\begin{aligned}
\mathrm{rank}_{\mathbb{F}_2}J[2]^\sigma &= \mathrm{rank}_{\mathbb{F}_2}\frac{\{f \in K(X^+)^* | (f) \in \mathbb{Z}B + 2\mathrm{Div}X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2} \\
&= 2g_+ + |B| - 2 \\
&= 2g_-.
\end{aligned} \tag{2.1.27}$$

□

Corollary 2.1.7. *If X has σ-fixed points, then $J_+ \cap J_- = J_+[2]$.*

Proof. We know that $J_+ \cap J_- \subseteq J_+[2]$. We need to prove that $J_+ \cap J_- \supseteq J_+[2]$, and in fact we only need to prove $J_- \supseteq J_+[2]$, i.e., we need to prove $J_+[2] \subseteq (1-\sigma)J$.

In fact, we prove a stronger statement:

$$J_+[2] \subseteq (1-\sigma)(J[2]). \tag{2.1.28}$$

Consider the map $J[2] \stackrel{1-\sigma}{\to} J[2]$, we have

$$\dim_{\mathbb{F}_2}\ker(1-\sigma) + \operatorname{rank}_{\mathbb{F}_2}(1-\sigma)(J[2]) = \dim_{\mathbb{F}_2} J[2]. \tag{2.1.29}$$

We know that $(1-\sigma)(J[2]) = (1+\sigma)(J[2]) \subseteq J_+[2]$. So, to prove $J_+[2] \subseteq (1-\sigma)(J[2])$ is equivalent to proving $J_+[2] = (1-\sigma)(J[2])$. This reduces to prove

$$\operatorname{rank}_{\mathbb{F}_2}(1-\sigma)(J[2]) = \operatorname{rank}_{\mathbb{F}_2} J_+[2] = 2g_+. \tag{2.1.30}$$

From Theorem 2.1.6, we know that $\operatorname{rank}_{\mathbb{F}_2} J[2]^\sigma = 2g_-$, together with the facts $\ker(1-\sigma) = J[2]^\sigma$, and $g = g_+ + g_-$, we finally get

$$\operatorname{rank}_{\mathbb{F}_2}(1-\sigma)(J[2]) = \dim_{\mathbb{F}_2} J[2] - \dim_{\mathbb{F}_2}\ker(1-\sigma) = 2g - 2g_- = 2g_+. \tag{2.1.31}$$

□

In proof of Corollary 2.1.7, we have the following important results:

Corollary 2.1.8. *Let M be the matrix corresponding σ acting on the lattice $H_1(X, \mathbb{Z})$. If X has σ-fixed points, then* $\mathrm{rank}_{\mathbb{F}_2}(Id - M) = \mathrm{rank}_{\mathbb{F}_2}(1 - \sigma)(J[2]) = 2g_+$.

Corollary 2.1.9. *If X has σ-fixed points, then $J_+[2] \subseteq J_-[2]$.*

Proof. Since $2x = 0$ for all $x \in J_+ \cap J_-$, we have $J_+ \cap J_- \subseteq J_-[2]$, combining with Corollary 2.1.7 $J_+ \cap J_- = J_+[2]$, we can easily get $J_+[2] \subseteq J_-[2]$. □

2.2 Intersection of J_+ and J_-: the Case σ Has No Fixed Point

In this section, we will discuss the case σ has no fixed point.

Let $K(X) = K(X^+)(\sqrt{h})$, $(h) = 2D_0$, and $(\pi^* h) = 2\pi^* D_0 = 2(\sqrt{h})$. As a result, $D_0 \in \mathrm{Div}^0 X^+$ is not principal, but $\pi^* D_0 \in \mathrm{Div}^0 X$ is principal.

we will construct the following diagram to prove the main theorem:

$$\begin{array}{ccccc}
0 & & 0 & & \\
\downarrow & & \downarrow & & \\
(h)/(h^2) = (h)/2(h) \cong \mathbb{Z}/2\mathbb{Z} & & \xrightarrow{\iota} \langle [D_0] \rangle \cong \mathbb{Z}/2\mathbb{Z} & & \\
\downarrow & & \downarrow & & \\
\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}/(K(X^+)^*)^2 & & \xrightarrow{\psi}_{\cong} \mathrm{Jac}X^+[2] & & \\
\downarrow i & & \downarrow j & & \\
0 \to \{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}/h^{\mathbb{Z}}(K(X^+)^*)^2 & & \xrightarrow{\phi} J[2]^\sigma & \xrightarrow{\chi} & \{\pm 1\} \to 0 \\
\downarrow & & & & \\
0 & & & &
\end{array} \tag{2.2.1}$$

Comparing to Diagram 2.1.3, in Diagram 2.2.1, map ϕ is no longer an isomorphism, but an injection with cokernal $\{\pm 1\}$ (isomorphic to $\mathbb{Z}/2\mathbb{Z}$) and the map i has no cokernel but a kernel isomorphic to $\mathbb{Z}/2\mathbb{Z}$ for the absence of the σ-fixed points.

We define the map ι by:

$$\begin{aligned}
\iota : (h)/(h^2) &\to \langle [D_0] \rangle \\
h &\mapsto [\frac{1}{2}(h)] = [D_0],
\end{aligned} \tag{2.2.2}$$

and, as in the first section, we can also define the isomorphism ψ by:

$$\begin{aligned}
\psi : \frac{\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}}{(K(X^+)^*)^2} &\xrightarrow{\cong} \mathrm{Jac}X^+[2] \\
f &\mapsto [\frac{1}{2}(f)].
\end{aligned} \tag{2.2.3}$$

Now, we define the map ϕ by:

$$\phi : \frac{\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}}{h^{\mathbb{Z}}(K(X^+)^*)^2} \to J[2]^\sigma$$
$$f \mapsto [\pi^* D], \tag{2.2.4}$$

where $(f) = 2D$.

Lemma 2.2.1. $\mathrm{Im}\phi \in J[2]^\sigma$.

Proof. We have $2\phi(f) = 2\pi^* D = \pi^*(2D) = \pi^*(f) \in K(X)^*$. Furthermore, $D \in \mathrm{Div}^0 X^+$ implies $D^\sigma = D$, $(\pi^* D)^\sigma = \pi^* D$, and $[\pi^* D] \in J^\sigma$. So, we proved $\phi(f) = [\pi^* D] \in J[2]^\sigma$. □

Lemma 2.2.2. *ϕ is well-defined.*

Proof. Let $g \in K(X^+)^*$, $[\phi(fhg^2)] = [\pi^*(D) + \pi^*(D_0) + \pi^*(g)] = [\pi^*(D) + (\sqrt{h}g)] = [\pi^*(D)] = [\phi(f)]$. □

Lemma 2.2.3. *ϕ is injective.*

Proof. Let's denote

$$\tilde{\phi} : \{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\} \to J[2]^\sigma$$
$$(f) = 2D \mapsto [\pi^* D]. \tag{2.2.5}$$

The injectivity of ϕ is equivalent to $\ker\tilde{\phi} = h^{\mathbb{Z}}(K(X^+)^*)^2$.

Suppose $(f) = 2D \in \ker\tilde{\phi}$, and $\tilde{\phi}(f) = [\pi^* D] = 0$, we have $\pi^* D = (g)$ for some $g \in K(X)$. Since $D \in \mathrm{Div}^0 X^+$, $\pi^* D$ is σ-invariant, which also implies $(g)^\sigma = (g)$, or $(g^\sigma) = (g)$. We have $g^\sigma = cg$. Since $g^{\sigma^2} = c^2 g = g$, $c^2 = 1$, we either have $g^\sigma = g$ or $g^\sigma = -g$. If $g^\sigma = g$, it implies $g \in (K(X)^\sigma)^* = K(X^+)^*$, and $(g) = D \in \mathrm{Div}^0(X^+)^*$, hence we can find f with $(f) = 2D$, such that $f = g^2 \in (K(X^+)^*)^2$. $g^\sigma = -g$ implies $g = \sqrt{h}k$ for some $k \in K(X^+)^*$, hence $f = hk^2$. In either case, we have $f \in h^{\mathbb{Z}}(K(X^+)^*)^2$. So $\ker\tilde{\phi} \subseteq h^{\mathbb{Z}}(K(X^+)^*)^2$.

For the other direction, if $f \in h^{\mathbb{Z}}(K(X^+)^*)^2$, we can write $f = h^a g^2$ for some $g \in K(X^+)^*$ and $a = 0$ or 1, By $(f) = a(h) + 2(g) = 2aD_0 + 2(g)$, we get $D = (g)$, $\tilde{\phi}((f)) = \pi^* D = \pi^*(g) \in \mathrm{Prin} X$, so we have $\tilde{\phi}((f)) = 0 \in J[2]^\sigma$, which means $\ker\tilde{\phi} \supseteq h^{\mathbb{Z}}(K(X^+)^*)^2$.

So, we have $\ker\tilde{\phi} = h^{\mathbb{Z}}(K(X^+)^*)^2$, or equivalently, ϕ is injective. □

Lemma 2.2.4. *If σ has no fixed point, we have the exact sequence:*

$$0 \to \{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}/h^{\mathbb{Z}}(K(X^+)^*)^2 \xrightarrow{\phi} J[2]^\sigma \xrightarrow{\chi} \{\pm 1\} \to 0, \tag{2.2.6}$$

where $\phi((f)) = [\phi^* D]$ for $(f) = 2D$, and $\chi(D) = g^\sigma/g$ for $(g) = 2D$.

Proof. We have proved the injectivity in Lemma 2.2.3.

Then, we will prove the sequence is exact at $J[2]^\sigma$. For any $D_1 = \pi^* D = \phi((f))$, where $2D = (f)$ for $f \in K(X^+)$, let $(g) = 2D_1$, we can easily get $g = f \in K(X^+)$. So $g^\sigma = g$, and $g^\sigma/g = 1$. We get $\chi \circ \phi((f)) = 1$, which

means $\mathrm{Im}\phi \subseteq \ker\chi$. On the other hand, if $D \in \ker\chi$, we have $(g) = 2D$ where $g \in K(X)^*$. such that $g^\sigma = g$, we have $g \in (K(X)^*)^\sigma = K(X^+)^*$. So we can find $g \in K(X^+)^*$ such that $D \in \phi((g))$.

Finally, the surjectivity of χ is obvious. □

Theorem 2.2.5. *If σ has no fixed point, then* $\mathrm{rank}_{\mathbb{F}_2} J[2]^\sigma = 2g_+$.

Proof. We get this result by simply counting the rank. From Diagram 2.2.1, we can get:

$$\begin{aligned}
\mathrm{rank}_{\mathbb{F}_2} J[2]^\sigma &= \mathrm{rank}_{\mathbb{F}_2}\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}/h^{\mathbb{Z}}(K(X^+)^*)^2 + 1 \\
&= \mathrm{rank}_{\mathbb{F}_2}\{f \in K(X^+)^* | (f) \in 2\mathrm{Div}^0 X^+\}/(K(X^+)^*)^2 + 1 - 1 \\
&= \mathrm{rank}_{\mathbb{F}_2}\mathrm{Jac}X^+[2] + 1 - 1 \\
&= 2g_+. \qquad (2.2.7)
\end{aligned}$$

□

We can get the following corollaries:

Corollary 2.2.6. *If X has no σ-fixed point, then $J_+ \cap J_- = J_-[2]$.*

Proof. The proof is quite similar to the proof of Corollary 2.1.7. We know that $J_+ \cap J_- \subseteq J_-[2]$. We need to prove that $J_+ \cap J_- \supseteq J_-[2]$, and in fact we only need to prove $J_+ \supseteq J_-[2]$, i.e., we need to prove $J_-[2] \subseteq (1+\sigma)J$.

In fact, we can prove a stronger statement:

$$J_-[2] \subseteq (1+\sigma)(J[2]). \tag{2.2.8}$$

Consider the map $J[2] \overset{1-\sigma}{\to} J[2]$, we have

$$\dim_{\mathbb{F}_2}\ker(1-\sigma) + \operatorname{rank}_{\mathbb{F}_2}(1-\sigma)(J[2]) = \dim_{\mathbb{F}_2} J[2]. \tag{2.2.9}$$

We know that $(1-\sigma)(J[2]) = (1+\sigma)(J[2]) \subseteq J_-[2]$. So, to prove $J_-[2] \subseteq (1-\sigma)(J[2])$ is equivalent to prove $J_-[2] = (1-\sigma)(J[2])$. This reduces to prove

$$\operatorname{rank}_{\mathbb{F}_2}(1-\sigma)(J[2]) = \operatorname{rank}_{\mathbb{F}_2} J_-[2] = 2g_- \tag{2.2.10}$$

From Theorem 2.2.5, we know that $\operatorname{rank}_{\mathbb{F}_2} J[2]^\sigma = 2g_+$, together with $\ker(1-\sigma) = J[2]^\sigma$, and $g = g_+ + g_-$, we finally get $\operatorname{rank}_{\mathbb{F}_2}(1-\sigma)(J[2]) = \dim_{\mathbb{F}_2} J[2] - \dim_{\mathbb{F}_2}\ker(1-\sigma) = 2g - 2g_+ = 2g_-$.

So, we get $J_+ \cap J_- = J_-[2]$. □

We have also proved the following important corollaries:

Corollary 2.2.7. *Let M be the matrix corresponding to σ acting on the lattice $H_1(X,\mathbb{Z})$. If X has no σ-fixed point, then* $\operatorname{rank}_{\mathbb{F}_2}(Id-M) = \operatorname{rank}_{\mathbb{F}_2}(1-\sigma)(J[2]) = 2g_-$.

Corollary 2.2.8. *If X has no σ-fixed point, $J_-[2] \subseteq J_+[2]$.*

Proof. Since $2x = 0$ for all $x \in J_+ \cap J_-$, we have $J_+ \cap J_- \subseteq J_+[2]$, combining Corollary 2.2.7, we can easily get $J_+[2] \subseteq J_-[2]$. □

Corollary 2.2.9. *If X has no σ-fixed point, $J_+[2] = J[2]^\sigma$.*

Proof. We know that $J_+[2] \subseteq J[2]^\sigma$, and $\text{rank}_{\mathbb{F}_2} J_+[2] = 2g_+$. Since $\text{rank}_{\mathbb{F}_2} J[2]^\sigma = 2g_+$, we get $J_+[2] = J[2]^\sigma$. □

2.3 Applications: Modular Curves, Shimura Curves and Atkin-Lehner Involutions

As we proved in the first two sections, the explicit expression of $J_+ \cap J_-$ depends on the number of the involution-fixed points. In this section, we will discuss examples of modular curves $X_0(N)$ and Shimura curves $X_0^D(N)$ with Atkin-Lehner involutions. Thank to Ogg and other mathematicians, now we know the numbers of fixed points of Atkin-Lehner involutions for these two examples.

2.3.1 Modular Curves $X_0(N)$ with Atkin-Lehner Involutions

Ogg ([Ogg74]) and Kenku ([Kenku77]) had given us the complete solution for the numbers of fixed points of modular curves $X_0(N)$ under Atkin-Lehner involutions.

Theorem 2.3.1. *(Ogg and Kenku) Let w_m be the Atkin-Lehner involution of level m of $X_0(N)$, where $m|N$, and m is coprime to $n = N/m$. Let $F(m)$ be the number of fixed points of w_m.*

(a) *If $m > 3$, n odd, then*

$$F(m) = v(m)\prod_{p|n}(1 + (\frac{-4m}{p})), \tag{2.3.1}$$

where

$$v(m) = \begin{cases} h(-m) + h(-4m) & \text{if } m \equiv 3(4), \\ h(-4m) & \text{otherwise.} \end{cases} \tag{2.3.2}$$

and $h(-m) \neq 0$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-m})$.

(i) *If $m \equiv 1(4)$, n even, then*

$$F(m) = h(-4m)\begin{cases} \prod_{p|n,\ p\ odd}(1 + (\frac{-4m}{p})) & \text{if } 4 \nmid m, \\ 0 & \text{if } 4|m. \end{cases} \tag{2.3.3}$$

(ii) *If $m \equiv 3(8)$, n even, then*

$$F(m) = 6h(-m)\begin{cases} \prod_{p|n,\ p\ odd}(1 + (\frac{-4m}{p})) & \text{if } 8 \nmid m, \\ 0 & \text{otherwise.} \end{cases} \tag{2.3.4}$$

(iii) *If $m \equiv 7(8)$, n even, then*

$$F(m) = h(-m)\begin{cases} 4\prod_{p|n,\ p\ odd}(1 + (\frac{-4m}{p})) & \text{if } 2 \parallel m, \\ 6\prod_{p|n,\ p\ odd}(1 + (\frac{-4m}{p})) & \text{if } 4|m,\ p \text{ odd.} \end{cases} \tag{2.3.5}$$

(b)

$$F(3) = \begin{cases} 2\prod_{p|m,\ p\ odd}(1+(\frac{-4m}{p})) & \text{if } 8 \nmid m, \\ 0 & \text{otherwise.} \end{cases} \tag{2.3.6}$$

(c)

$$F(2) = \prod_{p|m}(1+(\frac{-8}{p})) + \prod_{p|m}(1+(\frac{-4}{p})). \tag{2.3.7}$$

Corollary 2.3.2. *w_N has fixed points on $X_0(N)$ for $N > 3$.*

Proof. By Theorem 2.3.1, the number of the fixed points $F(N) = v(N)$, where

$$v(N) = \begin{cases} h(-N) + h(-4N) & \text{if } N \equiv 3(4), \\ h(-4N) & \text{otherwise,} \end{cases} \tag{2.3.8}$$

which is non-zero. □

Corollary 2.3.3. *If the algebraic curve is $X_0(N)$, and the involution is w_N, then the intersection $J_+ \cap J_- = (\mathbb{Z}/2\mathbb{Z})^{2g_+}$, where g_+ is the genus of $X^+(N) = X_0(N)/w_N$ and the dimension of $J_+(N) = (1+w_N)J(N) = \mathrm{Jac}(X_0(N)/w_N)$.*

2.3.2 Shimura Curves $X_0^D(N)$ with Atkin-Lehner Involutions

In [Ogg83], also see [Clark03], we can find the formula for the numbers of fixed points of Atkin-Lehner involutions on Shimura curves $X_0^D(N)$, where

D is the discriminant of the Shimura curve, and square free number N is the level of the Shimura curve. (We can consider the cases of the modular curve $X_0(N)$ as a special case of Shimura curve with $D = 1$). For any $m \parallel DN$, we have the formula for the number of fixed points for Atkin-Lehner involution w_m.

Theorem 2.3.4. *Let $F(m)$ be the number of the fixed points of the Shimura curve $X_0^D(N)$, under Atkin-Lehner involution w_m, where $m \parallel DN$. Then we have*

$$F(m) = \sum_{\mathcal{S}} h(\mathcal{S}) \prod_{p|DN} \nu_p(\mathcal{S}, \mathcal{O}) = \sum_{\mathcal{S}} h(\mathcal{S}) \prod_{p|D} (1 - (\frac{\mathcal{S}}{p})) \prod_{p|N} (1 + (\frac{\mathcal{S}}{p})), \tag{2.3.9}$$

where we sum over certain imaginary quadratic orders in $\mathcal{S}$ as follows:

(a) *If $m = 2$, we sum over $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$;*

(b) *If $m > 2$ and $m \equiv 1$ or $2 \pmod 4$, then $\mathcal{S} = \mathbb{Z}[\sqrt{-m}]$;*

(c) *If $m \equiv -1 \pmod 4$, we sum over $\mathbb{Z}[\frac{1+\sqrt{-m}}{2}]$ and $\mathbb{Z}[\sqrt{-m}]$,*

where $\mathcal{O}$ is the fixed Eichler order of level N in the quaternion algebra $\mathcal{B}$ with discriminant D. $\nu_p(\mathcal{S}, \mathcal{O})$ is the number of inequivalent optimal embeddings of $\mathcal{S}_p$ into $\mathcal{O}$.

2.4 Intersection $J_+ \cap J_-$ and Integral Representations of $G = \langle\sigma\rangle$

In this section, we will discuss the relation between the intersection $J_+ \cap J_-$ and integral representations of the cyclic 2-group $G = \langle\sigma\rangle$.

Consider J_+ and J_- as subabelian varieties of $J/\mathbb{C}$, then the problem of $J_+ \cap J_-$ is a special case of the following proposition (see, for example [Stein00] Proposition 3.20):

Proposition 2.4.1. *Suppose a complex abelian variety $J = V/\Lambda$ and its subvarieties $A = V_A/\Lambda_A$, $B = V_B/\Lambda_B$, then*

$$A \cap B \cong \left(\frac{\Lambda}{\Lambda_A + \Lambda_B}\right)_{torsion}. \tag{2.4.1}$$

In our case, $J = (\mathbb{C})^g/L$ where $L = H_1(X, \mathbb{Z})$. $J_+ = (1+\sigma)J = (\frac{(1+\sigma)\mathbb{C}^g}{L\cap(1+\sigma)\mathbb{C}^g})$, and $J_- = (1-\sigma)J = (\frac{(1-\sigma)\mathbb{C}^g}{L\cap(1-\sigma)\mathbb{C}^g})$.

We define $L_\pm := \{\sigma x = \pm x | x \in L\}$, or equivalently, $\sigma|_{L_\pm} = \pm Id$ for sublattices $L_\pm \subseteq L$.

Lemma 2.4.2. *$L_\pm = (1 \pm \sigma)\mathbb{C}^g \cap L$, where $g = \frac{1}{2}\text{rank}_\mathbb{Z} L$.*

Proof. $\text{rank}_\mathbb{Z} L = 2g$ implies $L \otimes \mathbb{C} = \mathbb{C}^g$. For any $x \in L_\pm \subseteq L$, $x = \frac{x+\sigma x}{2} + \frac{x-\sigma x}{2} = \frac{x\pm\sigma x}{2} = (1 \pm \sigma)\frac{x}{2} \in (1 \pm \sigma)\mathbb{C}^g$. The second equality is true because $x = \pm\sigma x$. So we have "$\subseteq$". On the other hand, for any $x \in (1\pm\sigma)\mathbb{C}^g \cap L \subseteq L$,

$x = (1 \pm \sigma)y$ for some $y \in \mathbb{C}^g$, and $\sigma x = \sigma(1 \pm \sigma)y = (\sigma \pm 1)y = \pm x$, which means $x \in L_{\pm}$. □

Lemma 2.4.3.

$$L \otimes \mathbb{Z}[1/2] = (L_+ + L_-) \otimes \mathbb{Z}[1/2]. \tag{2.4.2}$$

Proof. Obviously, $L_+ + L_- \subseteq L$, so we have $(L_+ + L_-) \otimes \mathbb{Z}[1/2] \subseteq L \otimes \mathbb{Z}[1/2]$. For any $x \in L$, $x = (1+\sigma)x/2 + (1-\sigma)x/2$. $(1+\sigma)\sigma \in L_+$ and $(1-\sigma)x \in L_-$. we have $L \otimes \mathbb{Z}[1/2] \subseteq (L_+ + L_-) \otimes \mathbb{Z}[1/2]$. □

Remark 2.4.4. (2.4.2) *tell us*

$$L \otimes \mathbb{Q} = (L_+ + L_-) \otimes \mathbb{Q}. \tag{2.4.3}$$

As a result,

$$\frac{L}{L_+ + L_-} = \left(\frac{L}{L_+ + L_-}\right)_{torsion}. \tag{2.4.4}$$

By (2.4.2), we have

Proposition 2.4.5.

$$\begin{aligned} J_+ \cap J_- &\cong \left(\frac{L}{L_+ + L_-}\right) \\ &\cong (\mathbb{Z}/2\mathbb{Z})^r, \quad \textit{for some integer } r. \end{aligned} \tag{2.4.5}$$

In fact there exists a deep relation between the intersection of J_+ and J_- and integral representations of $G = \langle\sigma\rangle$.

Let's first review the results of integral representations of the cyclic 2-group. It satifies Krull-Schmidt theorem, see [Benson]. More precise, it is a special case of Reiner's more general theorem for integral representations of cyclic p-groups. We can find it in Theorem 34.31 (Page 729) of [CurtisReiner81].

Theorem 2.4.6. *Let $G = C_p$ be the cyclic group of order p, where p is prime. Let h be the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$ and let $b_1, ..., b_h$ be representatives of the ideal class group of $\mathbb{Q}(\zeta_p)$. Then,*

(a) *Every $\mathbb{Z}[G]$ module is a direct sum indecomposable $\mathbb{Z}[G]$-modules.*

(b) *There are 2h+1 indecomposable $\mathbb{Z}[G]$-modules: one of dimension 1, h of dimension (p-1), and h of dimension p.*

(c) *The h of dimension $p-1$ over $\mathbb{Z}$ are the ideals $b_1, ..., b_h$. Up to isomorphism, there is only 1 extension of b_i by $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module, denoted $(b_i,\ \mathbb{Z};\ 1)$. The h of dimension p over $\mathbb{Z}$ are the $(b_i,\ \mathbb{Z};\ 1)$.*

For the notation $(b_i,\ \mathbb{Z};\ 1)$, see [CurtisReiner81] near Page 729.

In our case, $p = 2$, we have our special form of the above theorem as follows:

Theorem 2.4.7. *The integral representation L of cyclic 2-group $G = \langle\sigma\rangle$ can be decomposed as a direct sum of indecomposable subrepresentations*

$$L \cong A_+^a \oplus A_-^b \oplus R_2^c \tag{2.4.6}$$

where $\sigma|_{A_\pm} = \pm 1$, and $\sigma|_{R_2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, if we choose a suitable basis.

In our special case, considering $L = H_1(X, \mathbb{Z})$ as an integral represestion of $G = \langle\sigma\rangle$, where σ is an involution on L (induced by the involution on the algebraic curve X), we can find the relation between $J_+ \cap J_-$ and the integral representations.

Theorem 2.4.8. *Using the same notation as before, we consider $L = H_1(X, \mathbb{Z})$ as an integral representation of $G = \langle\sigma\rangle$. We can decompose the integral representation $L \cong A_+^a \oplus A_-^b \oplus R_2^c$, where $\sigma|_{A_\pm} = \pm 1$ and $\sigma|_{R_2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then $\frac{L}{L_+ + L_-} \cong (\mathbb{Z}/2\mathbb{Z})^c$.*

Proof. We will prove this result by direct computation. The eigenspace of the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has a basis $\mathbf{v}_+ = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ with eigenvalue $\lambda = 1$, and $\mathbf{v}_- = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ with eigenvalue $\lambda = -1$.

For the simplicity our proof, we need introduce some simple notations for vector space. Let $\mathbf{e}_i$ be the i-th vector in the standard basis of vector. ($\mathbf{e}_i = (0, ..., 0, 1, 0, ..., 0)^\dagger$, where the non-zero element 1 lies on the i-th entry.)

If we write

$$L \cong A_+^a \oplus A_-^b \oplus R_2^c = \langle \mathbf{e}_1, ..., \mathbf{e}_{a+b+2c} \rangle, \tag{2.4.7}$$

as disucssed before, we can write

$$L_+ = \langle \mathbf{e}_1, ..., \mathbf{e}_a, \mathbf{e}_{a+b+1} + \mathbf{e}_{a+b+2}, ..., \mathbf{e}_{a+b+2c-1} + \mathbf{e}_{a+b+2c} \rangle, \tag{2.4.8}$$

$$L_- = \langle \mathbf{e}_{a+1}, ..., \mathbf{e}_{a+b}, \mathbf{e}_{a+b+1} - \mathbf{e}_{a+b+2}, ..., \mathbf{e}_{a+b+2c-1} - \mathbf{e}_{a+b+2c} \rangle. \tag{2.4.9}$$

So, we have

$$\begin{aligned}
&\frac{L}{L_+ + L_-} \\
=&\langle \mathbf{e}_1, ..., \mathbf{e}_{a+b+2c} \rangle / \langle \mathbf{e}_1, ..., \mathbf{e}_{a+b}, \mathbf{e}_{a+b+1} + \mathbf{e}_{a+b+2}, \mathbf{e}_{a+b+1} - \mathbf{e}_{a+b+2}, ..., \\
&\mathbf{e}_{a+b+2c-1} + \mathbf{e}_{a+b+2c}, \mathbf{e}_{a+b+2c-1} - \mathbf{e}_{a+b+2c} \rangle \\
=&\langle \mathbf{e}_{a+b+1}, ..., \mathbf{e}_{a+b+2c} \rangle / \langle \mathbf{e}_{a+b+1} + \mathbf{e}_{a+b+2}, \mathbf{e}_{a+b+1} - \mathbf{e}_{a+b+2}, ..., \\
&\mathbf{e}_{a+b+2c-1} + \mathbf{e}_{a+b+2c}, \mathbf{e}_{a+b+2c-1} - \mathbf{e}_{a+b+2c} \rangle \\
=&\bigoplus_{i=1}^{c} \frac{\langle \mathbf{e}_{a+b+2i-1}, \mathbf{e}_{a+b+2i} \rangle}{\langle \mathbf{e}_{a+b+2i-1} + \mathbf{e}_{a+b+2i}, \mathbf{e}_{a+b+2i-1} - \mathbf{e}_{a+b+2i} \rangle} \\
=&(\mathbb{Z}/2\mathbb{Z})^c
\end{aligned} \tag{2.4.10}$$

The last equality holds because

$$\frac{\langle \mathbf{e}_i, \mathbf{e}_{i+1} \rangle}{\langle \mathbf{e}_i + \mathbf{e}_{i+1}, \mathbf{e}_i - \mathbf{e}_{i+1} \rangle} = \frac{\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle}{\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle} = \frac{\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle}{\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\rangle} = \mathbb{Z}/2\mathbb{Z} \tag{2.4.11}$$

So, we have

$$\frac{L}{L_+ + L_-} \cong (\mathbb{Z}/2\mathbb{Z})^c, \qquad \text{where } L = H_1(X,\ \mathbb{Z}) \cong A_+^a \oplus A_-^b \oplus R_2^c. \quad (2.4.12)$$

□

From this theorem and Proposition 2.4.5, we can easily get:

Corollary 2.4.9. *$J_+ \cap J_- \cong (\mathbb{Z}/2\mathbb{Z})^c$, if $L = H_1(X,\ \mathbb{Z}) \cong A_+^a \oplus A_-^b \oplus R_2^c$.*

Theorem 2.4.10. *Under the same notation as above, let $g_\pm = \dim J_\pm$,*

(a) *If σ has fixed points, $a = 0$, $b = 2g_- - 2g_+$, and $c = 2g_+$, hence $L \cong A_-^{2g_- - 2g_+} \oplus R_2^{2g_+}$;*

(b) *If σ has no fixed point, $a = 2g_+ - 2g_- = 2$, $b = 0$, and $c = 2g_-$, hence $L \cong A_+^2 \oplus R_2^{2g_-}$.*

Proof. Let $L \cong A_+^a \oplus A_-^b \oplus R_2^c$, and M be the matrix associate to σ, the characteristic polynomial of the M is $(\lambda-1)^{2g_+}(\lambda+1)^{2g_-} = (\lambda-1)^a(\lambda+1)^b[(\lambda-1)(\lambda+1)]^c$, we have $a + c = 2g_+$ and $b + c = 2g_-$. Also, we have $\mathrm{rank}_{\mathbb{F}_2}(Id - M) = c$.

If σ has fixed points, $\mathrm{rank}_{\mathbb{F}_2}(Id - M) = 2g_+$ (Corollary 2.1.8), we have $c = 2g_+$, consequently $a = 0$ and $b = 2g_- - 2g_+$.

If σ has no fixed point, $\text{rank}_{\mathbb{F}_2}(Id - M) = 2g_-$ (Corollary 2.2.7), we have $c = 2g_-$, consequently $b = 0$ and $a = 2g_+ - 2g_-$. Furthermore, by Riemann-Hurwitz theorem, $g_+ - g_- = 1$, we get $a = 2$. □

Remark 2.4.11. *Theorem* 2.4.10 *and Theorem* 2.0.6 *are equivalent.*

In fact, we proved Theorem 2.4.10 by two corollaries (Corollary 2.1.8 and 2.2.7) of Theorem 2.0.6. On the other hand, if we know Theorem 2.4.10, using Corollary 2.4.9, we can easily get Theorem 2.0.6.

Remark 2.4.12. *From Theorem* 2.4.10*, we have the following properties for the integral representations of a cyclic* 2*-group* $G = \langle\sigma\rangle$ *appearing in* L*:*

(a) A_+ *and* A_- *cannot appear at the same time;*

(b) *The multiple of* A_+ *is two, appears only when* σ *has no fixed point on* X*;*

(c) *The multiple of* A_- *is even, appears only when* σ *has fixed points on* X*.*

2.5 Integral Representations and Sympletic Pairings

For the general discussion of symplectic pairing, see §11 of [Bourbaki59]. For our convenience, all the discussion is over $\mathbb{Z}$. Here, we list some results we need.

Definition 2.5.1. *Let* V *be a* $\mathbb{Z}$*-module. A symplectic pairing* $\langle\cdot,\cdot\rangle$ *on* V *is*

a nondegenerate antisymmetric bilinear form on V. A bilinear from $\langle \cdot, \cdot \rangle$ is called nondegenerate if $\langle u, v \rangle = 0$ for every $v \in V$ implies that $u = 0$.

Proposition 2.5.2. *For any symplectic pairing $\langle \cdot, \cdot \rangle$, there is a basis of V such that $\langle \cdot, \cdot \rangle$ is represented by the matrix*

$$M = \begin{pmatrix} & & & & & & c_1 & & \\ & & & & & & & c_2 & \\ & & & & & & & & \ddots \\ & & & & & & & & & c_g \\ -c_1 & & & & & & & & & \\ & -c_2 & & & & & & & & \\ & & \ddots & & & & & & & \\ & & & -c_g & & & & & & \end{pmatrix} \tag{2.5.1}$$

with $c_1|c_2|...|c_g$.

Proof. See §11 of [Bourbaki59]. □

A lattice is a free abelian group of finite rank with integral symplectic form $\langle \cdot, \cdot \rangle$. The discriminant of a lattice is the discriminant of matrix corresponding to the symplectic pairing. The lattice is unimodular if the discriminant is ± 1.

For $L = H_1(X, \mathbb{Z})$, $\text{rank}_{\mathbb{Z}} L = 2g$ if the genus of X is g. As a $\mathbb{Z}$-lattice of even rank we can associate (L, σ) a σ-equivariant non-degenerated symplectic pairing $\langle \cdot, \cdot \rangle$. In fact, this pairing is exactly the cup product defined

on homology $L = H_1(X, \mathbb{Z})$ (See §0.4 [GriffithsHarris78]), and $(L, \langle \cdot, \cdot \rangle)$ is unimodular.

Definition 2.5.3. *Lattice $M \subseteq L$. L is saturated in M if $mn \in L$ for $m \in M$ implies $m \in L$.*

Lemma 2.5.4. *If L and M have the same rank, M saturated in L, then $M = L$.*

Lemma 2.5.5. *$\langle \cdot, \cdot \rangle$ nondegenerate on L, then $L^* \subseteq \mathrm{Hom}(L, \mathbb{Z})$ is saturated, so $L^* \cong \mathrm{Hom}(L, \mathbb{Z})$.*

Lemma 2.5.6. *Let $(L, \langle \cdot, \cdot \rangle)$ unimodular, $M \subseteq L$ saturated, then we have the surjection $L^* \twoheadrightarrow M^*$.*

Proof. From the exact sequence $0 \to M \to L \to L/M \to O$, we have $\mathrm{Hom}(L, \mathbb{Z}) \to \mathrm{Hom}(M, \mathbb{Z}) \xrightarrow{\partial} \mathrm{Ext}^1(L/M, \mathbb{Z})$. (Theorem 7.5 of [Rotman]) But M is saturated $\Leftrightarrow$ L/M is torsion-free $\Leftrightarrow$ L/M is free, hence is projective $\Rightarrow$ $\mathrm{Ext}^1(L/M, \mathbb{Z}) = 0$ (Theorem 7.7 of [Rotman]). We also have $L^* \cong \mathrm{Hom}(L, \mathbb{Z})$ and $M^* \cong \mathrm{Hom}(M, \mathbb{Z})$. So we get the surjection. □

Proposition 2.5.7. *Suppose $(L, \langle \cdot, \cdot \rangle)$ unimodular. Let $M, N \subseteq L$ be saturated sublattices of L which are orthogonal complements: $L \oplus \mathbb{Q} \cong (M \otimes \mathbb{Q}) \oplus (N \otimes \mathbb{Q})$ and $\langle m, n \rangle = 0$ for all $m \in M \otimes \mathbb{Q}$, $n \in N \otimes \mathbb{Q}$. Then $M^* \cong L/N$.*

Proof. By Lemma 2.5.6, $L^* \twoheadrightarrow M^*$. But since L is unimodular, the map $L \to L^*$ by $l \mapsto \langle l, \cdot \rangle$ is an isomorphism. Hence the composition $\phi : L \to L^* \to M^*$ by $l \mapsto \langle l, \cdot \rangle : M \to \mathbb{Z}$, is surjective. $N \subseteq \ker\phi$ since M and N are orthogonal. So $L/N \twoheadrightarrow M^*$. Since L/N is free (N is saturated) and so L/N, M^* are $\mathbb{Z}$-modules of the same finite rank, $L/N \twoheadrightarrow M^*$ surjective implies it is an isomorphism. □

Let $M = L_+$ and $N = L_-$, we can easily get the following theorem.

Theorem 2.5.8. *Let $(L, \langle , \rangle)$ be a unimodular symplectic lattice, σ be an involution acting on $(L, \langle \cdot, \cdot \rangle)$. Then $L_+^* \cong L/L_-$ and $L_-^* \cong L/L_+$.*

Corollary 2.5.9.

$$\frac{L}{L_+ + L_-} \cong \frac{L_+^*}{L_+} \cong \frac{L_-^*}{L_-}. \tag{2.5.2}$$

$(L, \langle \cdot, \cdot \rangle)$ be symplectic lattice. For $v \in L$, $I_L(v) := (\langle v, w \rangle | w \in L) \subseteq \mathbb{Z}$ is an ideal in $\mathbb{Z}$, hence it has a positive generator $d_L(v)$, such that $I_L(v) = (d_L(v))$.

A vector $v \in L$ is primitive if $\frac{1}{d}v \in L$ implies $d = \pm 1$.

Lemma 2.5.10. *Suppose $v \in L$ is primitive and $\langle \cdot, \cdot \rangle|_L$ is unimodular. Then $d_L(v) = 1$.*

Proof. Let $\{v_1, ..., v_g : w_1, ..., w_g\}$ be a Frobenius normal basis for L, i.e., $\langle v_i, v_j\rangle = \langle w_i, w_j\rangle = 0$, $\langle v_i, w_j\rangle = \delta_{ij}$, for $1 \leq i, j \leq g$. Let $v = a_1v_1 + ... + a_gv_g + b_1w_1 + ... + b_gw_g$ be primitive. Then $\gcd(a_1, ..., a_g, b_1, ..., b_g) = 1$. Hence by Chinese Remainder Theorem, there exist $c_1, ..., c_g, d_1, ..., d_g \in \mathbb{Z}$ so that $a_1c_1 + ... + a_gc_g + b_1d_1 + ... + b_gd_g = 1$. Let $v' = c_1w_1 + ... + c_gw_g - d_1v_1 - ... - d_gv_g$. Then $\langle v, v'\rangle = a_1c_1 + ...a_gc_g + b_1d_1 + ... + b_gd_g = 1$ implying that $d_L(v) = 1$. □

If $(M, \langle\cdot,\cdot\rangle)$ is a lattice, where $\langle\cdot,\cdot\rangle$ is nondegenerate ($\langle\cdot,\cdot\rangle$ can be symmetric or alternative), the Discriminant $\mathrm{Disc}(M, \langle\cdot,\cdot\rangle)$ is the determinant of the matrix representing $\langle\cdot,\cdot\rangle$ with respect to a basis of M. The following is well-known:

Lemma 2.5.11. *Suppose $M' \subseteq M$ is a sublattice of index d, and $(M, \langle\cdot,\cdot\rangle)$ is nondegenerate. Then $(M', \langle\cdot,\cdot\rangle|_{M'})$ is nondegenerate, and* $\mathrm{Disc}(M', \langle\cdot,\cdot\rangle|_{M'}) = d^2\mathrm{Disc}(M, \langle\cdot,\cdot\rangle)$.

Now return to the situation that $(L, \langle\cdot,\cdot\rangle)$ is a unimodular symplectic lattice. Then $L_+^* = (\frac{1+\sigma}{2})L \subseteq L_+ \otimes \mathbb{Q}$, $L_-^* = (\frac{1-\sigma}{2})L \subseteq L_- \otimes \mathbb{Q}$.

Lemma 2.5.12. *$(L_+, \langle\cdot,\cdot\rangle|_{L_+})$ and $(L_-, \langle\cdot,\cdot\rangle|_{L-})$ are nondegenerate lattices.*

Proof. $L \otimes \mathbb{Q} = (L_+ \otimes \mathbb{Q}) \oplus (L_- \otimes \mathbb{Q})$ and $L_+ \otimes \mathbb{Q}$, $L_- \otimes \mathbb{Q}$ are orthogonal. Hence $(L, \langle\cdot,\cdot\rangle)$ nondegenerate implies $(L_+, \langle\cdot,\cdot\rangle|_{L_+})$ and $(L_-, \langle\cdot,\cdot\rangle|_{L-})$ are nondegenerate. □

Lemma 2.5.13. *Suppose $v \in L_+$ is primitive. Then $d_{L_+} = 1$ or 2. Similarly, if $v \in L_-$ is primitive, then $d_{L_-} = 1$ or 2.*

Proof. If v is primitive in L_+, then v is primitive in L. $(L, \langle \cdot, \cdot \rangle)$ is unimodular implies that there exists $w \in L$, such that $\langle v, w \rangle = 1$. But then $(1+\sigma)w = w+\sigma w \in L_+$ and $\langle v, (1+\sigma)w \rangle = \langle v, w \rangle + \langle v, \sigma w \rangle = 1 + \langle \sigma v, w \rangle = 1 + \langle v, w \rangle = 2$. So $d_{L_+}(v)|2$ implies $d_{L_+}(v) = 1$ or 2. A similar argument applies to L_-. □

By Lemma 2.5.13, $\langle \cdot, \cdot \rangle$ has a Frobenius normal form:

$$\langle\cdot,\cdot\rangle|_{L_+} = \begin{pmatrix} & & & & & & & & 1 & & & & \\ & & & & & & & \alpha\Big\{ & & \ddots & & & \\ & & & & & & & & & & 1 & & \\ & & & & & & & & & & & 2 & \\ & & & & & & & & \beta\Big\{ & & & & \ddots \\ & & & & & & & & & & & & & 2 \\ -1 & & & & & & & & & & & & & \\ & \ddots & & & & & & & & & & & & \\ & & -1 & & & & & & & & & & & \\ & & & -2 & & & & & & & & & & \\ & & & & \ddots & & & & & & & & & \\ & & & & & -2 & & & & & & & & \end{pmatrix} \tag{2.5.3}$$

$$\text{with } \mathrm{Disc}(\langle\cdot,\cdot\rangle|_{L_+}) = \det \begin{pmatrix} & & & & & & & & 1 & & & & \\ & & & & & & & \alpha\Big\{ & & \ddots & & & \\ & & & & & & & & & & 1 & & \\ & & & & & & & & & & & 2 & \\ & & & & & & & & \beta\Big\{ & & & & \ddots \\ & & & & & & & & & & & & & 2 \\ -1 & & & & & & & & & & & & & \\ & \ddots & & & & & & & & & & & & \\ & & -1 & & & & & & & & & & & \\ & & & -2 & & & & & & & & & & \\ & & & & \ddots & & & & & & & & & \\ & & & & & -2 & & & & & & & & \end{pmatrix} = 2^{2\beta}. \tag{2.5.4}$$

Now $L_+^* = (\frac{1+\sigma}{2})L$ and $(L_+^*, \langle\cdot,\cdot\rangle)$ is unimodular. If $L \cong A_+^a \oplus A_-^b \oplus R_2^c$, then $L_+^* = (\frac{1+\sigma}{2})L \cong [(\frac{1+\sigma}{2})A_+]^a \oplus [(\frac{1+\sigma}{2})A_-]^b \oplus [(\frac{1+\sigma}{2})R_2]^c = A_+^a \oplus 0 \oplus [(\frac{1+\sigma}{2})R_2]^c$ and $L_+ = A_+^a \oplus [(1+\sigma)R_2]^c$. So, $\mathrm{rank}L_+^* = \mathrm{rank}L_+ = 2g_+ = a+c$, and the index of L_+ in L_+^* is 2^c.

Hence by Lemma 2.5.11:

$$\mathrm{Disc}(L_+, \langle\cdot,\cdot\rangle|_{L_+}) = (2^c)^2 \mathrm{Disc}(L_+^*, \langle\cdot,\cdot\rangle|_{L_+^*}). \tag{2.5.5}$$

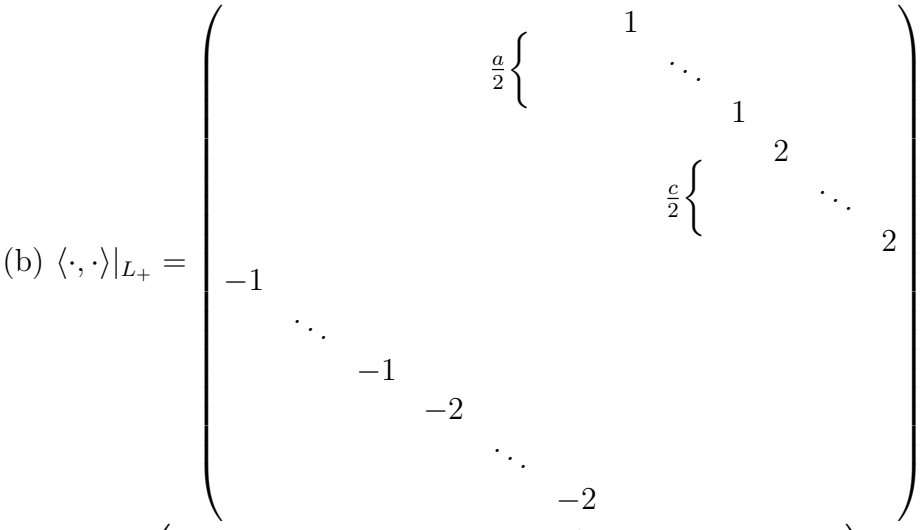
If $\langle\cdot,\cdot\rangle|_{L_+} =$ $\begin{pmatrix} & & & & & & & & & & \\ & & & & \alpha\Big\{ & & 1 & & & & \\ & & & & & & \ddots & & & & \\ & & & & & & & 1 & & & \\ & & & & & & & & 2 & & \\ & & & & & & \beta\Big\{ & & & \ddots & \\ & & & & & & & & & & 2 \\ -1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & -1 & & & & & & & & \\ & & & -2 & & & & & & & \\ & & & & \ddots & & & & & & \\ & & & & & -2 & & & & & \end{pmatrix}$ as in (2.5.3),

with Frobenius normal basis $v_1, ..., v_\alpha, v'_1, ..., v'_\beta, w_1, ..., w_\alpha, w'_1, ..., w'_\beta$, such that $\langle v_i, w_j\rangle = \delta_{ij}$, for $1 \le i, j \le \alpha$, and $\langle v'_i, w'_j\rangle = 2\delta_{ij}$, for $1 \le i, j \le \beta$. Then L_+^* has basis $v_1, ..., v_\alpha, \frac{1}{2}v'_1, ..., \frac{1}{2}v_\beta, w_1, ..., w_\alpha, \frac{1}{2}w'_1, ..., \frac{1}{2}w'_\beta$, and $\mathrm{Disc}L_+^* = (\frac{1}{2})^{2\beta}$. Hence from (2.5.11) we get $2^{2\beta} = 2^{2c}(\frac{1}{2})^{2\beta}$, then $2^{4\beta} = 2^{2c}$, which implies $\beta = c/2$ and hence $\alpha = a/2$. The case of L_- is done similarly.

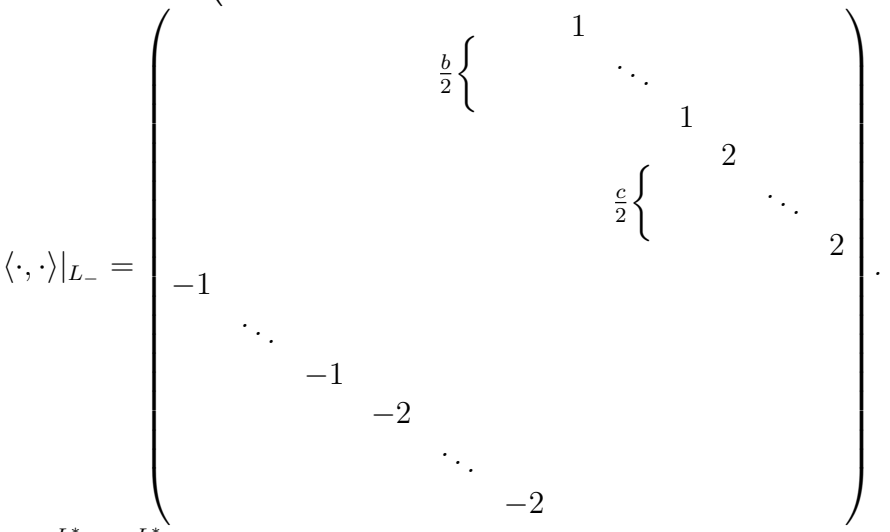
So we have

Theorem 2.5.14. *Suppose $(L, \langle\cdot,\cdot\rangle)$ is a unimodular symplectic lattice, and σ is an involution of $(L, \langle\cdot,\cdot\rangle)$. Suppose $L \cong A_+^a \oplus A_-^b \oplus R_2^c$, $\mathrm{rank}_{\mathbb{Z}} L = 2g$, $\mathrm{rank}_{\mathbb{Z}} L_\pm = 2g_\pm$.*

(a) *a, b, c are all even.*

(b) $\langle\cdot,\cdot\rangle|_{L_+} =$ 

,

$\langle\cdot,\cdot\rangle|_{L_-} =$ 

.

(c) $\frac{L_+^*}{L_+} \cong \frac{L_-^*}{L_-} \cong \frac{L}{L_+ + L_-} \cong (\mathbb{Z}/2\mathbb{Z})^c$.

(d) $\langle\cdot,\cdot\rangle$ *induces a unimodular symplectic pairing on* $\frac{L_+^*}{L_+} \cong \frac{L_-^*}{L_-} \cong \mathbb{F}_2^c$ *as an* $\mathbb{F}_2$*-vector space.*

In the following part, we will introduce the 2-subspace system $(V; V_1, V_2)$ associate to a integral representation A of the cyclic 2-group G. It is quite similar to the 4-subspace system associate to a integral representation of

Klein 4-group in the next chapter.

Definition 2.5.15. *For any cyclic 2-group $G = \langle\sigma\rangle$, and any integral representation L of G, we define the 2-subspace system $\mathcal{V}(L) := (V; V_1, V_2)$ over $\mathbb{F}_2$ as follows:*

$$V_1 = V_+ = (e_1L + L)/L,\ V_2 = V_- = (e_2L + L)/L,\ V = V_1 + V_2, \quad (2.5.6)$$

where $e_1 = e_+ = (1 + \sigma)/2,\ e_2 = e_- = (1 - \sigma)/2$.

Combining with the theorem of integral representations of cyclic 2-group (Theorem 2.4.7), we have the following theorem of the corresponding 2-subspace system:

Theorem 2.5.16. *For the cyclic 2-group $G = \langle\sigma\rangle$, let $L \cong A_+^a \oplus A_-^b \oplus R_2^c$ be the integral representation of G. Then, $V_1 \cong V_2 \cong (\mathbb{F}_2)^c$, hence $\mathcal{V}(L) = (V;\ V_1,\ V_2) \cong ((\mathbb{F}_2)^c;\ (\mathbb{F}_2)^c,\ (\mathbb{F}_2)^c)$.*

Proof. For $L \cong A_+^a \oplus A_-^b \oplus R_2^c$, by directly computation, we have

$$\begin{aligned}\mathcal{V}(L) =& (V(L); V_1(L), V_2(L))\\ =& (V(A_+); V_1(A_+), V_2(A_+))^a \oplus (V(A_-); V_1(A_-), v_2(A_-))^b\\ &\oplus (V(R_2); V_1(R_2), V_2(R_2))^c. \end{aligned} \quad (2.5.7)$$

For the $\mathbb{Z}$-module A_+, we have $\sigma|_{A_+} = +1$, hence $V_1(A_+) = (\frac{1+\sigma}{2}A_+ + A_+)/A_+ = (A_+ + A_+)/A_+ = A_+/A_+ = 0$, $V_2(A_+) = (\frac{1-\sigma}{2}A_+ + A_+)/A_+ = (0 + A_+)/A_+ = A_+/A_+ = 0$, and $V = V_1 + V_2 = 0$.

So,

$$(V(A_+);\ V_1(A_+),\ V_2(A_+)) = (0;\ 0,\ 0). \tag{2.5.8}$$

Similarly,

$$(V(A_-);\ V_1(A_-),\ V_2(A_-)) = (0;\ 0,\ 0). \tag{2.5.9}$$

For the $\mathbb{Z}$-module R_2, considering $R \cong \mathbb{Z}^2$ and $\sigma R_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} R_2$, $V_1(R_2) = (\frac{1+\sigma}{2}R_2 + R_2)/R_2 = ((1+\sigma)R_2 + 2R_2)/2R_2 = (\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + 2R_2)/2R_2 = \frac{\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\rangle}{\left\langle \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\rangle} = \mathbb{F}_2$, $V_2(R_2) = (\frac{1-\sigma}{2}R_2 + R_2)/R_2 = ((1-\sigma)R_2 + 2R_2)/2R_2 = (\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} + 2R_2)/2R_2 = \frac{\left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\rangle}{\left\langle \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\rangle} = \mathbb{F}_2$, and we have $V(R_2) = V_1(R_2) + V_2(R_2) = \mathbb{F}_2$.

So, $V_1 = V_2 = (\mathbb{F}_2)^c$ and $(V;\ V_1,\ V_2) \cong ((\mathbb{F}_2)^c;\ (\mathbb{F}_2)^c,\ (\mathbb{F}_2)^c)$. □

Corollary 2.5.17.

$$J_+ \cap J_- = V_+ \cap V_-. \tag{2.5.10}$$

Proof. Theorem 2.5.16 shows $V_+ = V_- = \mathbb{F}_2^c$, which means $V_+ \cap V_- = \mathbb{F}_2^c$, combining with Corollary 2.4.9, we can get $J_+ \cap J_- = V_+ \cap V_-$. □

2.6 Complex conjugate τ and Integral Representations of $G = \langle\tau\rangle$

We can also consider the action of complex conjugate τ on $L = H_1(X, \mathbb{Z})$. Let group $G = \langle\tau\rangle$ be the cyclic 2-group generated by complex conjugation τ. Considering L as a G-module, from Theorem 2.4.7, L can be decomposed in forms of $A_+^a \oplus A_-^b \oplus R_2^c$, where $\tau|_{A_\pm} = \pm 1$, and $\tau|_{R_2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, by choosing a suitable basis.

Similar to the case of involution, we can determine the multiples a, b, and c by the following theorem ([Jaffee80], also see [Mazur] and [GrossHarris81]):

Theorem 2.6.1. *Let $X = X/\mathbb{R}$ be a closed, connected complex algebraic curve defined over $\mathbb{R}$ with genus g. Let r be the number of the connected components of $X(\mathbb{R})$.*

(a) *If $X(\mathbb{R}) \neq \emptyset$, $r > 0$, then $L \cong A_+^{r-1} \oplus A_-^{r-1} \oplus R_2^{1+g-r}$;*

(b) *If $X(\mathbb{R}) = \emptyset$ and g odd, then $L \cong A_+ \oplus A_- \oplus R_2^{g-1}$;*

(c) *If $X(\mathbb{R}) = \emptyset$ and g even, then $L \cong R_2^g$.*

For the modular curve $X_0(N)$ where N is square free, Oggs had given the number of connected components [Ogg83]:

Theorem 2.6.2. *If $X = X_0(N)$ with N is the product of n distinct primes, then the number of components r of $X(\mathbb{R})$ is*

$$r = \begin{cases} 2^{n-1} & \text{if } 2 \nmid N, \\ 2^{n-2} & \text{if } 2 \mid N. \end{cases}$$

So, we have

Corollary 2.6.3. *For the modular curve $X = X_0(N)$ of genus g, where N is a product of n distinct primes, then*

$$L \cong A_+^{r-1} \oplus A_-^{r-1} \oplus R_2^{1+g-r}, \tag{2.6.1}$$

where

$$r = \begin{cases} 2^{n-1} & \text{if } 2 \nmid N, \\ 2^{n-2} & \text{if } 2 \mid N. \end{cases}$$

For the Shimura curve $X_0^D(N)$ of discriminant D and level N, where D is a product of even number of distinct primes. The following theorem due to Shimura is well-known:

Theorem 2.6.4. *(Shimura) $X_0^D(N)(\mathbb{R}) = \emptyset$.*

As a corollary, we have

Corollary 2.6.5. *For the Shimura curve $X = X_0^D(N)$ with discriminant $D > 1$ and level N, then*

$$L \cong \begin{cases} A_+ \oplus A_- \oplus R_2^{g-1}, & \text{if } g \text{ odd}, \\ R_2^g, & \text{if } g \text{ even}, \end{cases}$$

where g is the genus of the X.

Chapter 3

The Case of Two Commuting Involutions

In this chapter, we discuss the problem of two commuting involutions acting on an algebraic curve X. They also induce actions on $L = H_1(X, \mathbb{Z})$. Let σ and τ be two commuting involutions. We say an involution σ is ramified if there exit fixed points under the involution σ on X. Otherwise, we say the involution is unramified. For some technical reasons, in this chapter, we only discuss the cases that the involution of $\sigma\tau$ has fixed points. In many interesting cases this assumption holds: for example, in the problem of the Atkin-Lehner involutions w_{N_1}, w_{N_2} acting on the modular curve $X_0(N)$, where $N = N_1N_2$, and N_1, N_2 are coprime and square free, the Atkin-Lehner involution $w_N = w_{N_1}w_{N_2}$ always has fixed points on $X_0(N)$ (See Corollary 2.3.2).

Some notations:

$J = \mathrm{Jac}X,$

$J_{\pm,\sigma} = (1 \pm \sigma)J,\ J_{\pm,\tau} = (1 \pm \tau)J,\ J_{\pm,\sigma\tau} = (1 \pm \sigma\tau)J,$

$J_{++} = (1+\sigma)(1+\tau)J,\ J_{+-} = (1+\sigma)(1-\tau)J,$

$J_{-+} = (1-\sigma)(1+\tau)J,\ J_{--} = (1-\sigma)(1-\tau)J.$

$g = \dim X = \mathrm{genus}J,$

$g_{\pm,\sigma} = \dim J_{\pm,\sigma},\ g_{\pm,\tau} = \dim J_{\pm,\tau},\ g_{\pm,\sigma\tau} = \dim J_{\pm,\sigma\tau},$

$g_{++} = \dim J_{++},\ g_{+-} = \dim J_{+-},\ g_{-+} = \dim J_{-+},\ g_{--} = \dim J_{--}.$

And, we have the following identities:

$g_{\pm,\sigma} = g_{\pm+} + g_{\pm-},\ g_{\pm,\tau} = g_{+\pm} + g_{-\pm},\ g_{+,\sigma\tau} = g_{++} + g_{--},\ g_{-,\sigma\tau} = g_{+-} + g_{-+},$

$g = g_{+,\sigma} + g_{-,\sigma} = g_{+,\tau} + g_{-,\tau} = g_{+,\sigma\tau} + g_{-,\sigma\tau} = g_{++} + g_{+-} + g_{-+} + g_{--}.$

3.1 Ramification of the Case of Two Involutions and Some Intersections of $J_{\pm\pm}$: Easy Part

Assume $\sigma\tau$ has fixed points. Let X be an algebraic curve.

$$\begin{array}{ccccc} & & X & & \\ & \swarrow p_1 & \downarrow p_2 & \searrow p_3 & \\ X/\langle\sigma\rangle & & X/\langle\sigma\tau\rangle & & X/\langle\tau\rangle \\ & \searrow p_4 & \downarrow p_5 & \swarrow p_6 & \\ & & X/\langle\sigma,\tau\rangle & & \end{array} \tag{3.1.1}$$

p_2 is ramifed since $\sigma\tau$ has fixed points by our assumption. We will discuss the ramification problem in three different cases.

Lemma 3.1.1. *Let X be an algebraic curve, σ and τ be two commuting involutions. Assume $\sigma\tau$ has fixed points. We have the following three different situations:*

(Case I) *If both σ and τ are ramified, then all six projections are ramified;*

(Case II) *If only one of σ and τ is ramified, say, σ is ramified, τ is unramified, then all but p_3 are ramified;*

(Case III) *If σ and τ are unramified, then only p_2, p_4 and p_6 are ramified.*

Proof.

$$\begin{array}{ccccc} & & X & & \\ & \swarrow^{r_\sigma} & \downarrow{\scriptstyle r_{\sigma\tau}} & \searrow^{r_\tau} & \\ X/\langle\sigma\rangle & & X/\langle\sigma\tau\rangle & & X/\langle\tau\rangle \\ & \searrow & \downarrow & \swarrow & \\ & & X/\langle\sigma,\tau\rangle & & \end{array} \tag{3.1.2}$$

Let r_σ, $r_{\sigma\tau}$, and r_τ be the numbers of the fixed points of the corresponding projections shown on the upper part of Diagram 3.1.1 and Diagram 3.1.2. By our assumption, $r_{\sigma\tau} \neq 0$, while r_σ and r_τ can be zero or nonzero. In the following, we will show that the numbers of fixed points of projections p_i, $i = 4, 5, 6$ depend only on r_σ, r_τ, and $r_{\sigma\tau}$.

Consider the projection $p_4 : X/\langle\sigma\rangle \twoheadrightarrow X/\langle\sigma,\tau\rangle$. For any $x \in X$, denote its

image on $X/\langle\sigma\rangle$ by $\bar{x} = \{x, \sigma x\}$. If $\bar{x} = \{x, \sigma x\}$ is fixed under the projection p_4, $\tau\{x, \sigma x\} = \{\tau x, \tau\sigma x\} = \{x, \sigma x\}$, then either $\tau x = x$ or $\sigma\tau x = x$. On the other hand, if either $\tau x = x$ or $\sigma\tau x = x$ is true, $\tau\{x, \sigma x\} = \{x, \sigma x\}$, which means $\bar{x} = \{x, \sigma x\}$ is fixed under the projection p_4. So, p_4 is ramified if and only if either r_τ or $r_{\sigma\tau}$ is nonzero. Similarly, p_5 is ramified if and only if either r_σ or r_τ is nonzero, and p_6 is ramified if and only if either r_σ or $r_{\sigma\tau}$ is nonzero.

By the assumption, $r_{\sigma\tau}$ is nonzero, p_2 is always ramified, so p_4 and p_6 are ramified for all three cases. In Case I, p_1 and p_3 are ramified, hence p_5 is also ramified. So, all six projections are ramified. In Case II, p_1 is ramified, hence p_5 is also ramified. So, all but p_3 are ramified. In Case III, p_1 and p_3 are unramified, hence p_5 is unramified. So, only p_2, p_4 and p_6 are ramified. □

Theorem 3.1.2. (Case I) *If σ and τ are ramified, then $g_{++} \leq g_{+-}, g_{-+}, g_{--}$, and $J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$.*

Proof. Denote the number of the fixed points of p_4, p_5, and p_6 by r_4, r_5, and r_6 respectively. For Case I, by Lemma 3.1.1, p_4, p_5, and p_6 are all ramified, which means $r_4 > 0$, $r_5 > 0$, and $r_6 > 0$. By Riemann-Hurwitz formula, $2 - 2g_{+,\sigma} = 2(2 - 2g_{++}) - r_4$, or

$$g_{+-} - g_{++} = r_4/2 - 1 \geq 0, \tag{3.1.3}$$

and similarly,

$$g_{--} - g_{++} = r_5/2 - 1 \geq 0,\ g_{-+} - g_{++} = r_6/2 - 1 \geq 0. \tag{3.1.4}$$

Hence $g_{++} \leq g_{+-}, g_{-+}, g_{--}$, if both σ and τ have fixed points.

For the second part of the theorem, we need to use Corollary 2.0.8 in the first chapter. Here, $J_{++} = (1+\sigma)(1+\tau)J = (1+\tau)[(1+\sigma)J] = (1+\tau)\mathrm{Jac}(X/\langle\sigma\rangle)$, where the second equality holds since σ and τ commute, and the third equality holds due to Corollary 2.0.8. Similarly, $J_{+-} = (1-\tau)\mathrm{Jac}(X/\langle\sigma\rangle)$. By Lemma 3.1.1 (Case I), $X/\langle\sigma\rangle$ has fixed points under the projection $X/\langle\sigma\rangle \twoheadrightarrow X/\langle\sigma,\tau\rangle$, we have $(1+\tau)\mathrm{Jac}(X/\langle\sigma\rangle) = \mathrm{Jac}(X/\langle\sigma,\tau\rangle)$. Again, by Corollary 2.0.8, $J_{++} \cap J_{+-} = (1+\tau)\mathrm{Jac}(X/\langle\sigma\rangle) \cap (1-\tau)\mathrm{Jac}(X/\langle\sigma\rangle) = \mathrm{Jac}(X/\langle\sigma,\tau\rangle)[2] = J_{++}[2]$. Using the same method, we have $J_{++} \cap J_{-+} = J_{++}[2]$ and $J_{++} \cap J_{--} = J_{++}[2]$. And, J_{++} is a connected abelian variety of dimension g_{++}, hence $J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$. □

Corollary 3.1.3. *In Case I,* $J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{++}[2]$.

Theorem 3.1.4. (Case II) *If* σ *is ramified and* τ *is not, then* $g_{++} \leq g_{+-}, g_{-+}, g_{--}$, *and* $J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$.

Proof. The proof of the first part of the theorem for Case II is exactly the same as that for Case I, since in Case II, all of p_4, p_5 and p_6 are ramified as

in Case I. We can prove that g_{++} is the smallest if only one of σ and τ, say σ has fixed points.

Using the same method in Case I, we can prove $J_{++} \cap J_{+-} = J_{++}[2]$ and $J_{++} \cap J_{--} = J_{++}[2]$, since both σ and $\sigma\tau$ have fixed points and all of p_4, p_5 and Corollary 2.0.8.

Now we begin to prove $J_{++} \cap J_{-+} = J_{++}[2]$. It is easy to see $J_{++} \cap J_{-+} \subseteq J_{++}[2]$ since all the points in $J_{++} \cap J_{-+}$ are 2-torsion points and belong to J_{++}. To prove $J_{++} \cap J_{-+} = J_{++}[2]$, we only need to show that $J_{++}[2] \subseteq J_{-+}[2] \subseteq J_{-+}$. $J_{++}[2] = [(1+\sigma)(1+\tau)J][2] = [(1+\tau)\mathrm{Jac}(X/\langle\sigma\rangle)][2]$ since σ has fixed points on X Consider the exact sequence:

$$0 \to (\mathrm{Jac}(X/\langle\sigma\rangle)[2])^{\tau} \to \mathrm{Jac}(X/\langle\sigma\rangle)[2] \to (1-\tau)(\mathrm{Jac}(X/\langle\sigma\rangle)[2]) \to 0, \tag{3.1.5}$$

$\mathrm{rank}_{\mathbb{F}_2}(\mathrm{Jac}(X/\langle\sigma\rangle)[2])^{\tau} = 2g_{+-}$ due to Theorem 2.1.6 and the fact that τ has fixed points under the projection $p_6 : X/\langle\sigma\rangle \twoheadrightarrow X/\langle\sigma,\tau\rangle$. Considering $\mathrm{rank}_{\mathbb{F}_2}\mathrm{Jac}(X/\langle\sigma\rangle)[2] = 2g_{+,\sigma}$, $\mathrm{rank}_{\mathbb{F}_2}(1-\tau)(\mathrm{Jac}(X/\langle\sigma\rangle)[2]) = 2g_{+,\sigma} - 2g_{+-} = 2g_{++}$. Since $(1-\tau)(\mathrm{Jac}(X/\langle\sigma\rangle)[2]) = (1+\tau)(\mathrm{Jac}(X/\langle\sigma\rangle)[2]) \subseteq ((1+\tau)\mathrm{Jac}(X/\langle\sigma\rangle))[2]$ and $\mathrm{rank}_{\mathbb{F}_2}((1+\tau)\mathrm{Jac}(X/\langle\sigma\rangle))[2] = 2g_{++}$, we have

$$(1+\tau)(\mathrm{Jac}(X/\langle\sigma\rangle)[2]) = [(1+\tau)\mathrm{Jac}(X/\langle\sigma\rangle)][2]$$

Also, $J_{+,\sigma} \subseteq J_{-,\sigma}$, since σ has fixed points for X and Corollary 2.1.9. So,

$$\begin{aligned} J_{++}[2] &= [(1+\sigma)(1+\tau)J][2] = [(1+\tau)\mathrm{Jac}(X/\langle\sigma\rangle)][2] = (1+\tau)[\mathrm{Jac}(X/\langle\sigma\rangle)][2] \\ &= (1+\tau)[(1+\sigma)J][2] = (1+\tau)J_{+,\sigma}[2] \\ &\subseteq (1+\tau)J_{-,\sigma}[2] = (1+\tau)([(1-\sigma)J][2]) = [(1+\tau)(1-\sigma)J][2] \\ &= J_{-+}[2]. \end{aligned}$$

As we discussed before, $J_{++}[2] \subseteq J_{-+}[2]$ implies $J_{++} \cap J_{-+} = J_{++}[2]$.

So, we proved

$$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}. \qquad (3.1.6)$$

The last isomorphism is true because J_{++} is a connected abelian variety of dimension g_{++}. □

Corollary 3.1.5. *In Case II,* $J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{++}[2]$.

Theorem 3.1.6. (Case III) *If* σ *and* τ *are unramified, then* $g_{--} = g_{++} - 1 < g_{++} \leq g_{+-}$, g_{-+}, *and* $J_{--} \cap J_{+-} = J_{--} \cap J_{-+} = J_{++} \cap J_{--} = J_{--}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}$.

Proof. Since the projection p_4 and p_6 are ramified ($r_4 \neq 0$ and $r_6 \neq 0$), p_5 is

unramified ($r_5 = 0$), we have

$$g_{+-} - g_{++} = r_4/2 - 1 \geq 0,$$

$$g_{-+} - g_{++} = r_6/2 - 1 \geq 0,$$

$$g_{--} - g_{++} = -1.$$

We have $g_{--} = g_{++} - 1 < g_{++}$, $g_{++} \leq g_{+-}$, and $g_{++} \leq g_{-+}$, so $g_{--} \leq g_{++},\ g_{+-},\ g_{-+}$ if both σ and τ have no fixed points.

Since $p_2 : X \twoheadrightarrow X/\langle\sigma\tau\rangle$ is ramified, we have $(1+\sigma\tau)J = \mathrm{Jac}(X/\langle\sigma\tau\rangle)$. So, we have $J_{++} = (1+\sigma)(1+\tau)J = (1+\sigma)(1+\sigma\tau)J = (1+\sigma)\mathrm{Jac}(X/\langle\sigma\tau\rangle)$ and $J_{--} = (1-\sigma)(1-\tau)J = (1-\sigma)(1+\sigma\tau)J = (1-\sigma)\mathrm{Jac}(X/\langle\sigma\tau\rangle)$.

Since $p_5 : X/\langle\sigma\tau\rangle \twoheadrightarrow X/\langle\sigma,\tau\rangle$ is unramified, by the Corollary 2.2.6, we have $(1+\sigma)\mathrm{Jac}(X/\langle\sigma\tau\rangle) \cap (1-\sigma)\mathrm{Jac}(X/\langle\sigma\tau\rangle) = [(1-\sigma)\mathrm{Jac}(X/\langle\sigma\tau\rangle)][2]$, or $J_{++} \cap J_{--} = J_{--}[2]$

To prove $J_{--} \cap J_{+-} = J_{--}[2]$, we only need to prove $J_{--} \subseteq J_{+-}[2] \subseteq J_{+-}$. We have $J_{--} = [(1-\sigma)(1-\tau)J][2] = [(1+\sigma\tau)(1-\tau)J][2] = [(1-\tau)\mathrm{Jac}(X/\langle\sigma\tau\rangle)][2]$, and

$$0 \to (\mathrm{Jac}(X/\langle\sigma\tau\rangle)[2])^\tau \to \mathrm{Jac}(X/\langle\sigma\tau\rangle)[2] \to (1-\tau)(\mathrm{Jac}(X/\langle\sigma\tau\rangle)[2]) \to 0$$

Since $p_5 : X/\langle\sigma\tau\rangle \twoheadrightarrow X/\langle\sigma,\tau\rangle$ are unramified, by Lemma 3.1.1, we have $\mathrm{rank}_{\mathbb{F}_2}(\mathrm{Jac}(X/\langle\sigma\tau\rangle)[2])^\tau = 2g_{++}$. Since $\mathrm{rank}_{\mathbb{F}_2}\mathrm{Jac}(X/\langle\sigma\tau\rangle)[2] = 2g_{+,\sigma\tau}$, we

have $\text{rank}_{\mathbb{F}_2}(1-\tau)(\text{Jac}(X/\langle\sigma\tau\rangle)[2]) = 2g_{+,\sigma\tau} - 2g_{++} = 2g_{--}$. Together with the fact $(1-\tau)((\text{Jac}(X/\langle\sigma\tau\rangle)[2]) \subseteq ((1-\tau)(\text{Jac}(X/\langle\sigma\tau\rangle))[2]$ and $\text{rank}_{\mathbb{F}_2}((1-\tau)(\text{Jac}(X/\langle\sigma\tau\rangle)))[2] = \text{rank}_{\mathbb{F}_2} J_{--}[2] = 2g_{--}$, we have $(1-\tau)((\text{Jac}(X/\langle\sigma\tau\rangle)[2]) = ((1-\tau)(\text{Jac}(X/\langle\sigma\tau\rangle)))[2]$. Since X has $\sigma\tau$-fixed points, by (2.1.9), we have $([(1+\sigma\tau)J][2]) \subseteq ([(1-\sigma\tau)J][2])$.

Finally, we have

$$\begin{aligned} J_{--}[2] &= [(1-\sigma)(1-\tau)J][2] = [(1+\sigma\tau)(1-\tau)J][2] = [(1-\tau)\text{Jac}(X/\langle\sigma\tau\rangle)][2] \\ &= (1-\tau)[\text{Jac}(X/\langle\sigma\tau\rangle)][2] = (1-\tau)([(1+\sigma\tau)J][2]) \\ &\subseteq (1-\tau)([(1-\sigma\tau)J][2]) \\ &\subseteq [(1-\tau)(1-\sigma\tau)J][2]) = [(1-\tau)(1+\sigma)J][2]) \\ &= J_{+-}[2] \end{aligned}$$

So, we have $J_{--}[2] \subseteq J_{+-}[2]$, implying $J_{--} \cap J_{+-} = J_{--}[2]$. By the same argument, $J_{--} \cap J_{-+} = J_{--}[2]$.

So, we have

$$J_{--} \cap J_{+-} = J_{--} \cap J_{-+} = J_{++} \cap J_{--} = J_{--}[2] = (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}. \quad (3.1.7)$$

The last identity comes from the fact that J_{--} is a connected abelian variety of dimension g_{--}. □

Corollary 3.1.7. *In Case III,* $J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{--}[2]$

For each of the three cases, we determine the three intersections by directly or indirectly using the results of the first chapter, especially part (a) of Lemma 2.0.8 and Corollary 2.1.7. To determine the other three intersections, we need to consider the integral representations of the Klein 4-group $G = \langle \sigma, \tau \rangle$.

3.2 Integral Representations of the Klein 4-Group and 4-Subspace Systems

In this section, we summarize the the theory of integral representations of the Klein 4-group. The 4-subspace system is an important concept in the theory of integral representations of the Klein 4-group. We introduce the 4-subspace system first, and then discuss the indecomposible components of the Klein 4-group G (by Krull-Schmidt theorem ([Benson]), the representation is unique as a direct sum of indecomposible components):

(a) $\mathbb{Z}G$-free and rank 4 regular representation R_4;

(b) Rank 1 repersentations A_{++}, A_{+-},A_{-+} and A_{--};

(c) Reduced representations.

We also calculate the 4-subspace system for each of them.

3.2.1 4-Subspace System

Let $G = \langle \sigma, \tau \rangle$ be the Klein 4-group, σ and τ be the two generators, and M be a $\mathbb{Z}G$-lattice. Similar to the 2-subspace system we discussed in the last chapter, let

$$\begin{aligned} e_{++} = e_1 &= \frac{1+\sigma}{2} \cdot \frac{1+\tau}{2}, & e_{+-} = e_2 &= \frac{1+\sigma}{2} \cdot \frac{1-\tau}{2}, \\ e_{-+} = e_3 &= \frac{1-\sigma}{2} \cdot \frac{1+\tau}{2}, & e_{--} = e_4 &= \frac{1-\sigma}{2} \cdot \frac{1-\tau}{2}, \\ e_* &= e_1 + e_2 + e_3 + e_4. \end{aligned} \tag{3.2.1}$$

Define the 4-subspace system $(V; V_{++}, V_{+-}, V_{-+}, V_{--}) = (V; V_1, V_2, V_3, V_4)$ by

$$V = e_* M/M,\ V_i = (e_i M + M)/M, \text{ for i=1, 2, 3, 4.} \tag{3.2.2}$$

3.2.2 Regular Representation R_4

For Klein 4-group $G = \langle \sigma, \tau \rangle$, let R_4 be the regular representation, a free $\mathbb{Z}$-module of rank 4.

$$R_4 = \mathbb{Z}[G] = \mathbb{Z}1 + \mathbb{Z}\sigma + \mathbb{Z}\tau + \mathbb{Z}\sigma\tau \tag{3.2.3}$$

So

$$e_i R_4 = e_i \mathbb{Z}, i = 1, 2, 3, 4. \tag{3.2.4}$$

Let $M = R_4$, we have

$$\begin{aligned} M_* =& e_* M = e_1 M + e_2 M + e_3 M + e_4 M = e_1\mathbb{Z} + e_2\mathbb{Z} + e_3\mathbb{Z} + e_4\mathbb{Z} \\ =& \frac{1+\sigma+\tau+\sigma\tau}{4}\mathbb{Z} + \frac{1+\sigma-\tau-\sigma\tau}{4}\mathbb{Z} + \frac{1-\sigma+\tau-\sigma\tau}{4}\mathbb{Z} + \frac{1-\sigma-\tau+\sigma\tau}{4}\mathbb{Z}. \end{aligned} \tag{3.2.5}$$

If we choose $1\mathbb{Z}$,$\sigma\mathbb{Z}$,$\tau\mathbb{Z}$ and $\sigma\tau\mathbb{Z}$ as a basis, M_* can be written as

$$M_* = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \tag{3.2.6}$$

and $M = Id_{4\times 4}$. We can easily get (see the appendix for the detail computations)

$$V = M_*/M = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \tag{3.2.7}$$

By the same basis, we can associate σ an operator S_σ as

$$S_\sigma = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{3.2.8}$$

since $S_\sigma \cdot 1\mathbb{Z} = \sigma\mathbb{Z}$, $S_\sigma \cdot \sigma\mathbb{Z} = 1\mathbb{Z}$, $S_\sigma \cdot \tau\mathbb{Z} = \sigma\tau\mathbb{Z}$, and $S_\sigma \cdot \sigma\tau\mathbb{Z} = \tau\mathbb{Z}$. Similarly, we can associate τ an operator S_τ as

$$S_\tau = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \tag{3.2.9}$$

and associate $\sigma\tau$ an operator $S_{\sigma\tau}$ as

$$S_{\sigma\tau} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{3.2.10}$$

They satisfy $S_\sigma^2 = S_\tau^2 = S_{\sigma\tau}^2 = Id$ and $S_{\sigma\tau} = S_\sigma S_\tau = S_\tau S_\sigma$.

$$V_1 = \frac{e_1 M + M}{M} = \frac{(1+\sigma+\tau+\sigma\tau)M + 4M}{4M} = \mathbb{Z}/4\mathbb{Z}. \tag{3.2.11}$$

(See the appendix for detail computations.)

Similarly,

$$V_i = \mathbb{Z}/4\mathbb{Z}, \text{ for } i = 1, 2, 3, 4 \tag{3.2.12}$$

So, we have

Theorem 3.2.1. *For the regular representation R_4,*

$$(V; V_1, V_2, V_3, V_4) = (\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2; \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}). \tag{3.2.13}$$

Lemma 3.2.2. *For the regular representation R_4, $V_i \cap V_j \cong \mathbb{Z}/2\mathbb{Z}$, for $1 \leq i < j \leq 4$.*

Proof. See the appendix. □

Lemma 3.2.3. *For the regular representation R_4, $V_1 \cap V_2 \cap V_3 \cap V_4 \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. Direct conclusion by Lemma 3.2.2. □

3.2.3 Rank 1 Representations A_{++}, A_{+-}, A_{-+}, and A_{--}

Let A_{++} be the rank 1 representation of $G = \langle \sigma, \tau \rangle$ such that $\sigma|_{A_{++}} = 1$ and $\tau|_{A_{++}} = 1$. Similar, we can define A_{+-}, A_{-+}, and A_{--}.

Theorem 3.2.4. *For the representation $A_{\pm\pm}$,*

$$(V; V_1, V_2, V_3, V_4) = (0; 0, 0, 0, 0). \tag{3.2.14}$$

The proof of the above theorem is quite similar with the proof for 2-subspace system for $A_{\pm}$ case (Theorem 2.5.16) in Chapter 1.

3.2.4 Reduced Representations

In this subsection, we state the classification of reduced integral representations of the Klein 4-group, the representations neither R_4 nor $A_{\pm\pm}$. They don't appear in the integral representations of the cyclic 2-group.

The problem of the classification of reduced integral representations is equivalent to the classification of reduced 4-subspace systems, which was known in late 1960s'. The classification is first done by L. A. Nazarova [Nazarova67] then by M. C. R. Butler [Butler73]. Both of these appoaches is based on the classification of the 4-subspace systems solved by Gel'fand and Ponomarev [GelfandPonomarev70]

Here, we state the theorem of the classification of the 4-subspace systems

following the paper of S. Brenner [Brenner74]. Let V be a finite dimensional vector space over a field K, and (V_1, V_2, V_3, V_4) be an ordered set of subspaces of V. Define the defect of $(V; V_i)_{1\leq i\leq 4}$ by $\rho(V; V_i) = \sum_i \dim V_i - 2\dim V$. Let π be a permutation of (1,2,3,4), $V_* = (V; V_i) = (V; V_1, V_2, V_3, V_4)$, We have the following notations in the next theorem:

Q and X be the vector space over K of dimension m and 1;

μ_1, μ_2, μ_3 are monomorphisms from X to V;

ζ_1, ζ_2 are monomorphisam from Q to V;

J is an indecomposable nilpotent endomorphism of Q;

$c \in \mathrm{Hom}(X, Q)$ satisfies that cX generates Q as a J-module;

$b \in \mathrm{Hom}(Q, V)$ satisfies $b\ker J = X$;

ι is the identity permutation of $(1, 2, 3, 4)$.

Theorem 3.2.5. *Any indecomposable 4-subspace system is isomorphic to one the 4-space in the following list up to permutation.*

(1) $\rho = 0$, $\dim V = 2m \geq 2$, *A a nonsingular indecomposable endomorphism of Q for which neither 0 nor 1 is an eigenvalue.*

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q; \zeta_1 Q, \zeta_2 Q, (\zeta_1 + \zeta_2)Q, (\zeta_1 + \zeta_2 A)Q)$,

$\Pi = \{\iota, (12), (13), (14), (34)(13), (34)(14)\}$.

(2) $\rho = 0$, $\dim V = 2m \geq 2$.

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q; \zeta_1 Q, \zeta_2 Q, (\zeta_1 + \zeta_2)Q, (\zeta_1 + \zeta_2 J)Q)$,

$\Pi = \{\iota, (12), (13), (24), (34), (12)(34)\}$.

(3) $\rho = 0$, $\dim V = 2m + 1 \geq 1$.

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q \oplus \mu_3 X; \zeta_1 Q \oplus \mu_3 X, \zeta_2 Q \oplus \mu_3 X, (\zeta_1 + \zeta_2)Q, (\zeta_1 + \zeta_2(J + 1) + \mu_3 b)Q)$,

$\Pi = \{\iota, (23), (24), (13), (14), (13)(24)\}$.

(4) $\rho = -1$, $\dim V = 2m + 2 \geq 2$.

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q \oplus \mu_1 X \oplus \mu_2 X; \zeta_1 Q \oplus \mu_1 X, \zeta_2 Q \oplus \mu_2 X, (\zeta_1 + \zeta_2)Q, (\zeta_1 + \zeta_2 J + \mu_2 b)Q \oplus (\mu_1 + \zeta_2 c)X)$, *(for $m = 0$, $\zeta_2 c = \mu_2$).*

$\Pi = \{\iota, (13), (23), (24), (34)\}$.

(5) $\rho = 1$, $\dim V = 2m \geq 2$.

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q; \zeta_1 Q, \zeta_2 Q, (\zeta_1 + \zeta_2)Q, (\zeta_1 + \zeta_2 J)Q \oplus \zeta_2 cX)$,

$\Pi = \{\iota, (14), (24), (34)\}$.

(6) $\rho = -1$, $\dim V = 2m + 1 \geq 3$ [1].

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q \oplus \mu_1 X; \zeta_1 Q \oplus \mu_1 X, \zeta_2 Q, (\zeta_1 + \zeta_2)Q, (\zeta_1 J + \zeta_2 + \mu_1 b)Q)$,

$\Pi = \{\iota, (12), (13), (14)\}$.

(7) $\rho = 1$, $\dim V = 2m + 1 \geq 1$.

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q \oplus \mu_1 X; \zeta_1 Q \oplus \mu_1 X, \zeta_2 Q, (\zeta_1 + \zeta_2)Q \oplus \mu_1 X, (\zeta_1 J + \zeta_2 J + \mu_1 b)Q \oplus \zeta_1 cX)$, *(for $m = 0$, $\zeta_1 c = \mu_1$).*

[1] In the Brenner's original paper, $\dim V = 2m+1 \geq 1$. It is a typo since when $\dim V = 1$, $(V; V_i) = (V; V, 0, 0, 0)$. It contradicts to $V_2 \cup V_3 \cup V_4 = V$.

$\Pi = \{\iota, (12), (23), (24)\}$.

(8) $\rho = -2$, $\dim V = 2m + 1 \geq 1$.

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q \oplus \mu_1 X; \zeta_1 Q, \zeta_2 Q, (\zeta_1 J + \zeta_2 + \mu_1 b)Q, (\zeta_1 + \zeta_2 J + \mu_1 b)Q)$,

$\Pi = \{\iota\}$.

(9) $\rho = 2$, $\dim V = 2m + 1 \geq 1$.

$(V; V_i) = (\zeta_1 Q \oplus \zeta_2 Q \oplus \mu_1 X; \zeta_1 Q \oplus \mu_1 X, \zeta_2 Q \oplus \mu_1 X, (\zeta_1 J + \zeta_2 + \mu_1 b)Q \oplus$

$\zeta_1 cX, (\zeta_1 + \zeta_2 J + \mu_1 b)Q \oplus \zeta_2 cX)$, *(for* $m = 0$, $\zeta_1 c = \zeta_2 c = \mu_1$*).*

$\Pi = \{\iota\}$.

3.3 An Important Lemma: Relation Between Integral Representations of the Klein 4-Group and Intersections of J_{++}, J_{+-}, J_{-+}, J_{--}

In this section, we will prove an important lemma, relating the intersections of V_{++}, V_{+-}, V_{-+}, V_{--} and the intersections of J_{++}, J_{+-}, J_{-+}, J_{--}.

Lemma 3.3.1.

$$V_{++} \cap V_{+-} = J_{++} \cap J_{+-},\ V_{++} \cap V_{-+} = J_{++} \cap J_{-+},\ V_{++} \cap V_{--} = J_{++} \cap J_{--},$$
$$V_{+-} \cap V_{-+} = J_{+-} \cap J_{-+},\ V_{+-} \cap V_{--} = J_{+-} \cap J_{--},\ V_{-+} \cap V_{--} = J_{-+} \cap J_{--}. \tag{3.3.1}$$

Proof. The proof of these six identities are similar. Here we just prove the

first one. We can get the other five identities by simply changing the subscripts.

Let X be an algebraic curve. Since $J = \mathrm{Jac}X \cong \mathbb{C}^g/L$, where $L = H_1(X,\mathbb{Z})$ and $g = \dim J$ =genus of X, we have $J_{tor} \cong L\otimes\mathbb{Q}/L$, where J_{tor} denote the torsion points of J. And we have the projection $\pi : L\otimes\mathbb{Q} \twoheadrightarrow J_{tor} \subseteq J$.

Let $e_{++} := \frac{(1+\sigma)(1+\tau)}{4}$ and $e_{+-} := \frac{(1+\sigma)(1-\tau)}{4}$. $e_{++}^2 = e_{++}$ and e_{++} is a projection of: $L\otimes\mathbb{Q} \twoheadrightarrow A_{++}\otimes\mathbb{Q}$. We have similar formulas for e_{+-}.

$V_{++} = \frac{e_{++}L+L}{L} \subseteq \frac{L\otimes\mathbb{Q}}{L} = J_{tor}$. Also, we have $V_{++} = \frac{e_{++}L+L}{L} = \frac{(1+\sigma)(1+\tau)(L/4)+L}{L} \subseteq J_{++}$. So we have $V_{++} \subseteq J_{tor}\cap J_{++} := (J_{++})_{tor}$. Similarly, we have $V_{+-} \subseteq (J_{+-})_{tor}$. Hence we have $V_{++}\cap V_{+-} \subseteq J_{++}\cap J_{+-}$.

On the other direction, we need to prove $V_{++}\cap V_{+-} \supseteq J_{++}\cap J_{+-}$

We define $L_{++} := \{v\in L|\sigma v = \tau v = v\}$ and $L_{+-} := \{v\in L|\sigma v = v, \tau v = -v\}$, $\widetilde{J_{++}} := \{v\in L\otimes\mathbb{Q}|\pi v \in J_{++}\subseteq J\}$ and $\widetilde{J_{+-}} := \{v\in L\otimes\mathbb{Q}|\pi v \in J_{+-}\subseteq J\}$. It is easy to see that $\widetilde{J_{++}}/L = (J_{++})_{tor}$ and $\widetilde{J_{+-}}/L = (J_{+-})_{tor}$. If $v\in\widetilde{J_{++}}$, we have $\sigma\pi v = \pi v$ and $\tau\pi v = \pi v$, it follows $\sigma v = v + L$ and $\tau v = v + L$. As a result, we have $\widetilde{J_{++}} = L_{++}\otimes\mathbb{Q} + L$. We can get $\widetilde{J_{+-}} = L_{+-}\otimes\mathbb{Q} + L$ similarly.

Let $\alpha\in J_{++}\cap J_{+-}$. We can always lift α to $\tilde{\alpha}\in\widetilde{J_{++}}\cap\widetilde{J_{+-}}$, such that $\tilde{\alpha}\in L_{++}\otimes\mathbb{Q}$ and $\tilde{\alpha}\in L_{+-}\otimes\mathbb{Q}+L$ by carefully choosing the representative

of $\tilde{\alpha}$ in $L \otimes \mathbb{Q}$.

So we can write

$$\tilde{\alpha} = \tilde{\alpha}' + w \tag{3.3.2}$$

where $\tilde{\alpha} \in L_{++} \otimes \mathbb{Q}$, $\tilde{\alpha}' \in L_{+-} \otimes \mathbb{Q}$ and $w \in L$. And, $L_{++} \otimes \mathbb{Q} \cap L_{+-} \otimes \mathbb{Q} = 0 \in L \otimes \mathbb{Q}$.

We have $e_{++}\tilde{\alpha} = \tilde{\alpha}$ since $\tilde{\alpha} \in L_{++} \otimes \mathbb{Q}$, and $e_{++}\tilde{\alpha}' = 0$ since $\tilde{\alpha}' \in L_{+-} \otimes \mathbb{Q}$, then we have $\tilde{\alpha} = e_{++}w$. It implies $\alpha \in \frac{e_{++}L+L}{L}$. Similarly we have $\tilde{\alpha}' = e_{++}(-w)$, and $\alpha \in \frac{e_{+-}L+L}{L}$. So we have $V_{++} \cap V_{+-} \supseteq J_{++} \cap J_{+-}$. $\square$

From this lemma, we know that the integral representations of $G = \langle \sigma, \tau \rangle$ determine the intersections of $J_{\pm\pm}$. To determine the remainder intersetions, our hope lies on understanding the integral representations appear in $L = H_1(X, \mathbb{Z})$. Not all integral representations will appear in $L = H_1(X, \mathbb{Z})$, just like not all integral representations of cyclic 2-group will appear in $L = H_1(X, \mathbb{Z})$ when we discuss the problem of intersection $J_+ \cap J_-$, as Remark 2.4.12 states. In fact, we will use the fact in Remark 2.4.12 on the integral representations of cyclic 2-group in $L = H_1(X, \mathbb{Z})$ on the problem of intersection $J_+ \cap J_-$ to determine the integral representations of the Klein 4-group appears in $L = H_1(X, \mathbb{Z})$ on the problem of intersection of $J_{\pm\pm}$'s. The bridge is that the restriction of integral representation of the Klein 4-group

appears in L to its cyclic 2-subgroup is the the integral representations of cyclic 2-subgroup appear in L. In the next section and the appendix at the end of this chapter, we will give the explicit computation of restriction of integral representations.

3.4 Reduction of Integral Representation of the Klein 4-Group $\langle\sigma,\tau\rangle$ to Integral Representation of Group $\langle\sigma\rangle$, $\langle\tau\rangle$ and $\langle\sigma\tau\rangle$

The Lemma 3.3.1 shows that, if we know the structure of 4-subspace system $(V; V_1, V_2, V_3, V_4)$ associate to $L = H_1(X, \mathbb{Z})$, we know all the intersections of J_{++}, J_{+-}, J_{-+} and J_{--}. And, the structure of 4-subspace systems is equivalent to integral representations of Klein 4-group (the only exception is the rank 1 representation $A_{\pm\pm}$ has no contribution to 4-subspace system $(V; V_1, V_2, V_3, V_4)$). In the remainder part of this chapter, will determine the irreducible integral sub-representations of Klein 4-group $G = \langle\sigma,\tau\rangle$ appearing in $L = H_1(X, \mathbb{Z})$. Not all integral representations listed in Section 3.2 can appear in L. An direct result is the integral representations of Klein 4-group $\langle\sigma,\tau\rangle$ restrict to integral representation of group $\langle\sigma\rangle$, $\langle\tau\rangle$ and $\langle\sigma\tau\rangle$ should satisfy Theorem 2.4.10. In this section, we will repeatedly using this theorem to rule out some representations not appearing in L.

All the lemmas we discussed in this section are technical. We are not discussing reduction of all possible integral representations of Klein 4-group. We only discuss the results we will use in next three sections.

3.4.1 The Regular Representation R_4

Lemma 3.4.1. *For the regular representations R_4 of $G = \langle \sigma, \tau \rangle$, we have the following identities when they are restricted to their cylic 2-subgroups $\langle \sigma \rangle$, $\langle \tau \rangle$ and $\langle \sigma\tau \rangle$:*

$$R_4|_{\langle \sigma \rangle} = R_2^2;\ R_4|_{\langle \tau \rangle} = R_2^2;\ R_4|_{\langle \sigma\tau \rangle} = R_2^2. \tag{3.4.1}$$

Proof. From the definition of the regular representation, $R_4 = 1\mathbb{Z} \oplus \sigma\mathbb{Z} \oplus \tau\mathbb{Z} \oplus \sigma\tau\mathbb{Z} = 1\mathbb{Z} \oplus \sigma\mathbb{Z} \oplus 1(\tau\mathbb{Z}) \oplus \sigma(\tau\mathbb{Z})$, and $\sigma R_4 = \sigma\mathbb{Z} \oplus 1\mathbb{Z} \oplus \sigma(\tau\mathbb{Z}) \oplus 1(\tau\mathbb{Z}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (\sigma\mathbb{Z} \oplus 1\mathbb{Z}) \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (1(\tau\mathbb{Z}) \oplus \sigma(\tau\mathbb{Z}))$, which imply $R_4|_{\langle \sigma \rangle} = R_2^2$ since $\sigma R_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} R_2$.

Similarly, we can prove $R_4|_{\langle \tau \rangle} = R_2^2$ and $R_4|_{\langle \sigma\tau \rangle} = R_2^2$. □

3.4.2 Rank 1 Representations A_{++}, A_{+-}, A_{-+} and A_{--}

From the definition of A_{++}, A_{+-}, A_{-+} and A_{--}, we can easily get the following lemma:

Lemma 3.4.2. *For the* rank 1 *integral representations A_{++}, A_{+-}, A_{-+} and A_{--} of $G = \langle \sigma, \tau \rangle$, we have the following identities when they are restricted*

to their cylic 2*-subgroups* $\langle\sigma\rangle$, $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$A_{++}|_{\langle\sigma\rangle} = A_+,\ A_{++}|_{\langle\tau\rangle} = A_+,\ A_{++}|_{\langle\sigma\tau\rangle} = A_+; \tag{3.4.2}$$

$$A_{+-}|_{\langle\sigma\rangle} = A_+,\ A_{+-}|_{\langle\tau\rangle} = A_-,\ A_{+-}|_{\langle\sigma\tau\rangle} = A_-; \tag{3.4.3}$$

$$A_{-+}|_{\langle\sigma\rangle} = A_-,\ A_{-+}|_{\langle\tau\rangle} = A_+,\ A_{-+}|_{\langle\sigma\tau\rangle} = A_-; \tag{3.4.4}$$

$$A_{--}|_{\langle\sigma\rangle} = A_-,\ A_{--}|_{\langle\tau\rangle} = A_-,\ A_{--}|_{\langle\sigma\tau\rangle} = A_+. \tag{3.4.5}$$

Corollary 3.4.3. *A_{++} and A_{--} do not appear in L in all three cases.*

Proof. Since $\sigma\tau$ always has fixed points as we assumed, $L|_{\langle\sigma\tau\rangle}$ does not have A_+ by Theorem 2.4.10. As subrepresentations of L, both A_{++} and A_{--} will contribute A_+ when they are restrict on the subgroup $\langle\sigma\tau\rangle$, so they cannot appear in L in all cases. □

Corollary 3.4.4. *A_{-+} do not appear in L in Case I and Case III.*

Proof. For Case I, $L|_{\langle\tau\rangle}$ do not have A_+ by Theorem 2.4.10. But $A_{-+}|_{\langle\tau\rangle} = A_+$. So, A_{-+} do not appear in L in Case I.

For Case III, $L|_{\langle\sigma\rangle}$ do not have A_- by Theorem 2.4.10. But $A_{-+}|_{\langle\sigma\rangle} = A_-$. So, A_{-+} do not appear in L in Case III. □

Corollary 3.4.5. *A_{+-} do not appear in L in all three cases.*

Proof. For Case I and Case II, $L|_{\langle\sigma\rangle}$ do not have A_+ by Theorem 2.4.10. But $A_{+-}|_{\langle\sigma\rangle} = A_+$. So, A_{+-} do not appear in L in Case I.

For Case III, $L|_{\langle\tau\rangle}$ do not have A_- by Theorem 2.4.10. But $A_{+-}|_{\langle\tau\rangle} = A_-$. So, A_{+-} do not appear in L in Case III. □

3.4.3 Some Reduced Representations

We will discuss some reduced representations we will meet in the next three sections. The proves rely on the concrete computation, we just give the results in this subsection and leave the proves to the appendix in this chapter.

We need some notations: Type (3) with $\dim V = 1$: Considering the permutation, we use the following notation:

$$M_{12} := (\mathbb{Z}/2\mathbb{Z}; \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0, 0);\ M_{13} := (\mathbb{Z}/2\mathbb{Z}; \mathbb{Z}/2\mathbb{Z}, 0, \mathbb{Z}/2\mathbb{Z}, 0); \quad (3.4.6)$$

$$M_{14} := (\mathbb{Z}/2\mathbb{Z}; \mathbb{Z}/2\mathbb{Z}, 0, 0, \mathbb{Z}/2\mathbb{Z});\ M_{23} := (\mathbb{Z}/2\mathbb{Z}; 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0); \quad (3.4.7)$$

$$M_{24} := (\mathbb{Z}/2\mathbb{Z}; 0, \mathbb{Z}/2\mathbb{Z}, 0, \mathbb{Z}/2\mathbb{Z});\ M_{34} := (\mathbb{Z}/2\mathbb{Z}; 0, 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}). \quad (3.4.8)$$

Lemma 3.4.6. *For the regular representations of Type* (3) *with* $\dim V = 1$ M_{ij} *where* $1 \leq i < j \leq 4$ *of* $G = \langle\sigma, \tau\rangle$*, we have the following identities when*

they are restricted to their cyclic 2*-subgroups* $\langle\sigma\rangle$, $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$M_{12}|_{\langle\sigma\rangle} = A_+^2,\ M_{12}|_{\langle\tau\rangle} = R_2,\ M_{12}|_{\langle\sigma\tau\rangle} = R_2; \tag{3.4.9}$$

$$M_{13}|_{\langle\sigma\rangle} = R_2,\ M_{13}|_{\langle\tau\rangle} = A_+^2,\ M_{13}|_{\langle\sigma\tau\rangle} = R_2; \tag{3.4.10}$$

$$M_{14}|_{\langle\sigma\rangle} = R_2,\ M_{14}|_{\langle\tau\rangle} = R_2,\ M_{14}|_{\langle\sigma\tau\rangle} = A_+^2; \tag{3.4.11}$$

$$M_{23}|_{\langle\sigma\rangle} = R_2,\ M_{23}|_{\langle\tau\rangle} = -R_2,\ M_{23}|_{\langle\sigma\tau\rangle} = A_-^2; \tag{3.4.12}$$

$$M_{24}|_{\langle\sigma\rangle} = R_2,\ M_{24}|_{\langle\tau\rangle} = A_-^2,\ M_{24}|_{\langle\sigma\tau\rangle} = -R_2; \tag{3.4.13}$$

$$M_{34}|_{\langle\sigma\rangle} = A_-^2,\ M_{34}|_{\langle\tau\rangle} = R_2,\ M_{34}|_{\langle\sigma\tau\rangle} = -R_2. \tag{3.4.14}$$

Lemma 3.4.7. *For the reduced representation of Type* (9) *with* $\dim V = 1$*, denoted by* M_{1234}*, of* $G = \langle\sigma, \tau\rangle$*, we have the following identity when it is restricted to its cyclic* 2*-subgroups* $\langle\sigma\rangle$, $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$M_{1234}|_{\langle\sigma\rangle} = R_2 \oplus A_+ \oplus A_-. \tag{3.4.15}$$

Corollary 3.4.8. *The reduced representation with Type* (9) *with* $\dim V = 1$ *does not appear in* L*.*

Proof. As we find in last lemma, A_+ and A_- appear at the same time when we restrict the reduced representation of Type (9) with $\dim V = 1$ M_{1234} to subgroup $\langle\sigma\rangle$, which is contradict to Remark 3.2.3. So, M_{1234} does not appear. □

Type (4) with $\dim V = 2$: Considering the permutation, we use the following notation:

$$M_{123} := ((\mathbb{Z}/2\mathbb{Z})^2; \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0); \tag{3.4.16}$$

$$M_{124} := ((\mathbb{Z}/2\mathbb{Z})^2; \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0, \mathbb{Z}/2\mathbb{Z}); \tag{3.4.17}$$

$$M_{134} := ((\mathbb{Z}/2\mathbb{Z})^2; \mathbb{Z}/2\mathbb{Z}, 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}); \tag{3.4.18}$$

$$M_{234} := ((\mathbb{Z}/2\mathbb{Z})^2; 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}). \tag{3.4.19}$$

And, Type (7) with $\dim V = 1$: Considering the permutation, we use the following notation:

$$\bar{M}_{123} := (\mathbb{Z}/2\mathbb{Z}; \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0); \tag{3.4.20}$$

$$\bar{M}_{124} := (\mathbb{Z}/2\mathbb{Z}; \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0, \mathbb{Z}/2\mathbb{Z}); \tag{3.4.21}$$

$$\bar{M}_{134} := (\mathbb{Z}/2\mathbb{Z}; \mathbb{Z}/2\mathbb{Z}, 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}); \tag{3.4.22}$$

$$\bar{M}_{234} := (\mathbb{Z}/2\mathbb{Z}; 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}). \tag{3.4.23}$$

Lemma 3.4.9. *For the reduced representation of Type* (4) *with* $\dim V = 2$*, denoted by* M_{123}*,* M_{124}*,* M_{134} *and* M_{234} *of* $G = \langle \sigma, \tau \rangle$*, we have the following*

identity when it is restricted to its cyclic 2*-subgroups* $\langle\sigma\rangle$, $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$M_{123}|_{\langle\sigma\rangle} = A_+ \oplus R_2,\ M_{123}|_{\langle\tau\rangle} = A_+ \oplus R_2,\ M_{123}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2; \quad (3.4.24)$$

$$M_{124}|_{\langle\sigma\rangle} = A_+ \oplus R_2,\ M_{124}|_{\langle\tau\rangle} = A_- \oplus R_2,\ M_{124}|_{\langle\sigma\tau\rangle} = A_+ \oplus R_2; \quad (3.4.25)$$

$$M_{134}|_{\langle\sigma\rangle} = A_- \oplus R_2,\ M_{134}|_{\langle\tau\rangle} = A_+ \oplus R_2,\ M_{134}|_{\langle\sigma\tau\rangle} = A_+ \oplus R_2; \quad (3.4.26)$$

$$M_{234}|_{\langle\sigma\rangle} = A_- \oplus R_2,\ M_{234}|_{\langle\tau\rangle} = A_- \oplus R_2,\ M_{234}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2. \quad (3.4.27)$$

Lemma 3.4.10. *For the reduced representation of Type* (7) *with* $\dim V = 1$*, denoted by* $\bar{M}_{123}$*,* $\bar{M}_{124}$*,* $\bar{M}_{134}$ *and* $\bar{M}_{234}$ *of* $G = \langle\sigma, \tau\rangle$*, we have the following identity when it is restricted to its cyclic* 2*-subgroups* $\langle\sigma\rangle$, $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$\bar{M}_{123}|_{\langle\sigma\rangle} = A_+ \oplus R_2,\ \bar{M}_{123}|_{\langle\tau\rangle} = A_+ \oplus R_2,\ \bar{M}_{123}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2; \quad (3.4.28)$$

$$\bar{M}_{124}|_{\langle\sigma\rangle} = A_+ \oplus R_2,\ \bar{M}_{124}|_{\langle\tau\rangle} = A_- \oplus R_2,\ \bar{M}_{124}|_{\langle\sigma\tau\rangle} = A_+ \oplus R_2; \quad (3.4.29)$$

$$\bar{M}_{134}|_{\langle\sigma\rangle} = A_- \oplus R_2,\ \bar{M}_{134}|_{\langle\tau\rangle} = A_+ \oplus R_2,\ \bar{M}_{134}|_{\langle\sigma\tau\rangle} = A_+ \oplus R_2; \quad (3.4.30)$$

$$\bar{M}_{234}|_{\langle\sigma\rangle} = A_- \oplus R_2,\ \bar{M}_{234}|_{\langle\tau\rangle} = A_- \oplus R_2,\ \bar{M}_{234}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2. \quad (3.4.31)$$

3.5 Intersections of J_{++}, J_{+-}, J_{-+} and J_{--}: Case I

For Case I, each of σ, τ and $\sigma\tau$ has fixed points on X, by Theorem 3.1.2 and Corollary 3.1.3,

$$g_{++} \leq g_{+-}, g_{-+}, g_{--}; \tag{3.5.1}$$

$$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}; \tag{3.5.2}$$

$$J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}. \tag{3.5.3}$$

By the Lemma 3.3.1, we can reformulate (3.5.2) and (3.5.3) above to

$$V_{++} \cap V_{+-} = V_{++} \cap V_{-+} = V_{++} \cap V_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}; \tag{3.5.4}$$

$$V_{++} \cap V_{+-} \cap V_{-+} \cap V_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}. \tag{3.5.5}$$

By (3.5.4) and (3.5.5), combining the knowledge of integral representations and 4-subspace systems in Section 3.2, we can almost determine the representations appearing in L, from which we can derive the other intersections.

Lemma 3.5.1. *In Case I, only the regular representation R_4 contributes to $V_{++} \cap V_{+-} \cap V_{-+} \cap V_{--}$.*

Proof. Since there is no rank 1 representations $L_{\pm\pm}$'s in Case I (Corollary 3.4.3, Corollary 3.4.4 and Corollary 3.4.5), we only need to exclude

the reduced presentations.

After carefully investigating Theorem 3.2.5, we find the only possible reduced representation with non-zero contribution of $V_{++} \cap V_{+-} \cap V_{-+} \cap V_{--}$ is the reduced representation of Type (9) in the list with $\dim V = 1$. But, we had excluded it in Corollary 3.4.8. □

Since every regular representation, associated with $\mathcal{V}(R_4) = (V; V_1, V_2, V_3, V_4) = (\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2; \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z})$ (See (3.2.14)), with intersection $V_1 \cap V_2 \cap V_3 \cap V_4 = \mathbb{Z}/2\mathbb{Z}$ (See (3.2.3)), contribute an intersection of the form $J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})$ by Lemma 3.3.1, we introduce the following notation:

$$\begin{aligned} &\mathcal{V}(L) = (V; V_1, V_2, V_3, V_4) = \mathcal{V}(R_4)^{2g_{++}} \oplus \tilde{\mathcal{V}}(L), \\ &\tilde{\mathcal{V}}(L) = (\tilde{V}; \tilde{V}_1, \tilde{V}_2, \tilde{V}_3, \tilde{V}_4);\ V_i = (\mathbb{Z}/4\mathbb{Z})^{2g_{++}} \oplus \tilde{V}_i \end{aligned} \tag{3.5.6}$$

Lemma 3.5.2. *In Case I, $V_1 \cong (\mathbb{Z}/4\mathbb{Z})^{2g_{++}}$, and $\tilde{V}_1 = 0$.*

Proof. By definition (See 3.2.2), $V_1 = \frac{e_1 L + L}{L}$, where $e_1 = \frac{(1+\sigma)}{2}\frac{(1+\tau)}{2}$, we have $\mathrm{rank}_{\mathbb{Z}}(1+\sigma)(1+\tau)L = \dim J_{++} = 2g_{++}$, hence the cardinality of V_1, $\mathrm{Card} V_1 = \mathrm{Card}\frac{e_1 L + L}{L} \leq \mathrm{Card}\frac{e_1 L}{L} = \mathrm{Card}(\mathbb{Z}/4\mathbb{Z})^{2g_{++}} = 4^{2g_{++}}$. We also have $V_1 = (\mathbb{Z}/4\mathbb{Z})^{2g_{++}} \oplus \tilde{V}_1$, so we have $\tilde{V}_1 = 0$ and $V_1 = (\mathbb{Z}/4\mathbb{Z})^{2g_{++}}$. □

Now we need to further investigate the structure of $\tilde{\mathcal{V}}(L) = (\tilde{V}; 0, \tilde{V}_2, \tilde{V}_3, \tilde{V}_4)$. Since $\tilde{V}_1 = 0$, $\tilde{\mathcal{V}}(L)$ comes from reduced representations. Also using the fact

of $\tilde{V}_1 = 0$, we can derive that only limited representations in list of Theorem 3.2.5 contribute to $\tilde{\mathcal{V}}(L)$:

Lemma 3.5.3. *In Case I, only the following Type of the reduced representations in Theorem 3.2.5 can possibly contribute to L:*

a. Type (3) *with* $\dim V = 1$*:* $M_{23} = (\mathbb{Z}/2\mathbb{Z}; 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0)$*,* $M_{24} = (\mathbb{Z}/2\mathbb{Z}; 0, \mathbb{Z}/2\mathbb{Z}, 0, \mathbb{Z}/2\mathbb{Z})$*, and* $M_{34} = (\mathbb{Z}/2\mathbb{Z}; 0, 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$*;*

b. Type (4) *with* $\dim V = 2$*:* $M_{234} = ((\mathbb{Z}/2\mathbb{Z})^2; 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$*;*

c. Type (7) *with* $\dim V = 1$*:* $\bar{M}_{234} = (\mathbb{Z}/2\mathbb{Z}; 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$*.*

Theorem 3.5.4. *In Case I, if only Type* (3) *reduced representations appears in L,*

$$L \cong R_4^{2g_{++}} \oplus M_{23}^{v(\sigma\tau)/2-1} \oplus M_{24}^{v(\tau)/2-1} \oplus M_{34}^{v(\sigma)/2-1} \tag{3.5.7}$$

where $v(*)$ *is the number of fixed points in* X *under the involution* $*$*.*

Proof. By the assumption, we have

$$L \cong R_4^{2g_{++}} \oplus M_{23}^{r_{23}} \oplus M_{24}^{r_{24}} \oplus M_{34}^{r_{34}}, \tag{3.5.8}$$

and we will determine the multiples r_{23}, r_{24}, and r_{34} in the rest of the proof.

By Lemma 3.4.1 and Lemma 3.4.6, we have

$$L|_{\langle\sigma\rangle} = R_2^{4g_{++}+r_{23}+r_{24}} \oplus A_-^{2r_{34}}; \tag{3.5.9}$$

$$L|_{\langle\tau\rangle} = R_2^{4g_{++}+r_{23}+r_{34}} \oplus A_-^{2r_{24}}; \tag{3.5.10}$$

$$L|_{\langle\sigma\tau\rangle} = R_2^{4g_{++}+r_{24}+r_{34}} \oplus A_-^{2r_{23}}. \tag{3.5.11}$$

while all involutions have fixed points on X, from Theorem 2.4.10, we have

$$L|_{\langle\sigma\rangle} = R_2^{2g_{+,\sigma}} \oplus A_-^{2g_{-,\sigma}-2g_{+,\sigma}} = R_2^{2g_{+,\sigma}} \oplus A_-^{v(\sigma)-2}; \tag{3.5.12}$$

$$L|_{\langle\tau\rangle} = R_2^{2g_{+,\tau}} \oplus A_-^{2g_{-,\tau}-2g_{+,\tau}} = R_2^{2g_{+,\tau}} \oplus A_-^{v(\tau)-2}; \tag{3.5.13}$$

$$L|_{\langle\sigma\tau\rangle} = R_2^{2g_{+,\sigma\tau}} \oplus A_-^{2g_{-,\sigma\tau}-2g_{+,\sigma\tau}} = R_2^{2g_{+,\sigma\tau}} \oplus A_-^{v(\sigma\tau)-2}. \tag{3.5.14}$$

where $v(*)$ is the number of fixed points on X under involution $*$, and the last equality of each equation comes from Riemann-Hurwitz formula.

Comparing the two sets of identities, we have:

$$r_{23} = g_{-,\sigma\tau} - g_{+,\sigma\tau} = v(\sigma\tau)/2 - 1 = g_{+-} + g_{-+} - g_{--} - g_{++}; \tag{3.5.15}$$

$$r_{24} = g_{-,\tau} - g_{+,\tau} = v(\tau)/2 - 1 = g_{+-} + g_{--} - g_{-+} - g_{++}; \tag{3.5.16}$$

$$r_{34} = g_{-,\sigma} - g_{+,\sigma} = v(\sigma)/2 - 1 = g_{-+} + g_{--} - g_{+-} - g_{++}. \tag{3.5.17}$$

So, we have

$$L \cong R_4^{2g_{++}} \oplus M_{23}^{v(\sigma\tau)/2-1} \oplus M_{24}^{v(\tau)/2-1} \oplus M_{34}^{v(\sigma)/2-1}. \tag{3.5.18}$$

□

Write in terms of 4-subspace system, we have

$$\mathcal{V}(L) = \mathcal{V}(R_4)^{2g_{++}} \oplus \tilde{\mathcal{V}}(L); \tag{3.5.19}$$

$$\tilde{\mathcal{V}}(L) = ((\mathbb{Z})^{g-4g_{++}}; 0, (\mathbb{Z}/2\mathbb{Z})^{2g_{+-}-2g_{++}}, (\mathbb{Z}/2\mathbb{Z})^{2g_{-+}-2g_{++}}, (\mathbb{Z}/2\mathbb{Z})^{2g_{--}-2g_{++}}). \tag{3.5.20}$$

Remark 3.5.5. *In Theorem 3.5.4, we add a restriction that only Type* (3) *reduced representation appears in L. We can release this restriction to a weaker condition: the defect of the 4-subspace system $\rho = 0$, which implies that if one of Type* (4) *(M_{234}) or Type* (7) *($\bar{M}_{234}$) representation appears, the other one also appears. What's more, their multiple should be the same, otherwise the total defect is non-zero (Type* (3) *has defect* 0*).*

Lemma 3.5.6. *$M_{23} \oplus M_{24} \oplus M_{34}$ and $M_{234} \oplus \bar{M}_{234}$ contribute the same intersections of $J_{+-} \cap J_{-+}$, $J_{+-} \cap J_{--}$ and $J_{-+} \cap J_{--}$. Or, equivalently, we cannot distinguish $M_{23} \oplus M_{24} \oplus M_{34}$ and $M_{234} \oplus \bar{M}_{234}$ by the information of $J_{+-} \cap J_{-+}$, $J_{+-} \cap J_{--}$ and $J_{-+} \cap J_{--}$.*

Proof. From Theorem 3.2.5, we can find both $M_{23} \oplus M_{24} \oplus M_{34}$ and $M_{234} \oplus \bar{M}_{234}$ contribute the intersections of $V_{+-} \cap V_{-+} = V_{+-} \cap V_{--} = V_{-+} \cap V_{--} = \mathbb{Z}/2\mathbb{Z}$. By Theorem 3.3.1, it implies both two Type contribute $J_{+-} \cap J_{-+} = J_{+-} \cap J_{--} = J_{-+} \cap J_{--} = \mathbb{Z}/2\mathbb{Z}$. □

Remark 3.5.7. *Under the assumption the defect $\rho = 0$, from Lemma 3.5.7, if we are only interested in 2-intersections such as$J_{+-} \cap J_{-+}$, we can equivalently*

think the "only" reduced representation appears in L is the Type (3) *reduced representation in Theorem 3.2.5. More precisely, in our case, are the reduced representations* M_{23}, M_{24} *and* M_{34}.

To distinguish Type (4) *and Type* (7) *from Type* (3), *or* $M_{234} \oplus \bar{M}_{234}$ *from* $M_{23} \oplus M_{24} \oplus M_{34}$, *we need to investigate* 3*-intersection* $J_{+-} \cap J_{-+} \cap J_{--}$.

So, we can restate Theorem 3.5.4 as following by changing to a weaker restriction:

Theorem 3.5.8. *In Case I, if the reduced representations appears in L has a total defect 0, then*

$$L \cong R_4^{2g_{++}} \oplus M_{23}^{v(\sigma\tau)/2-1} \oplus M_{24}^{v(\tau)/2-1} \oplus M_{34}^{v(\sigma)/2-1} \tag{3.5.21}$$

where $v(*)$ *is the number of fixed points in* X *under the involution* $*$.

Finally, we have the theorem of intersections for Case I under a techinque assumption:

Theorem 3.5.9. *Let* X *be any algebraic curve, and* σ *and* τ *are commuting involutions, assuming* σ, τ *and* $\sigma\tau$ *have fixed points, and assuming that the reduced subrepresentations* $L = H_1(X, \mathbb{Z})$ *of Klein 4-group* $G = \langle \sigma, \tau \rangle$ *has a total defect 0 for the corresponding 4-subspace system (or, equivalently* $2\dim\tilde{V} = \sum_{i=1}^{4} \dim\tilde{V}_i$ *in the 4-subspace system), then we have:*

$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$,

$J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\sigma\tau)/2-1}$, $J_{+-} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\tau)/2-1}$, *and* $J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\sigma)/2-1}$.

where $v(*)$ *is the number of the fixed points in* X *under the involution* $*$.

Proof. By Theorem 3.5.8, the facts that,

a. each regular representation R_4 contributes a $J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})$, and

b. each M_{23} contributes an intersection $J_{+-} \cap J_{-+}$, each M_{24} contributes an intersection $J_{+-} \cap J_{--}$, and each M_{34} contributes an intersection $J_{-+} \cap J_{--}$,

we can easily get. □

Remark 3.5.10. *The computation in Chapter 3 shows that the intersections in Theorem 3.5.9 hold, which suggests the defect condition is hold.*

3.6 Intersections of J_{++}, J_{+-}, J_{-+} and J_{--}: Case II

For case II, all σ and $\sigma\tau$ have fixed points on X, but τ have not, from Theorem 3.1.4 and Corollary 3.1.5 we know that

$$g_{++} \leq g_{+-}, g_{-+}, g_{--}; \tag{3.6.1}$$

$$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}; \tag{3.6.2}$$

$$J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{++}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}. \tag{3.6.3}$$

By the Lemma 3.3.1, we can reformulate the identities (3.6.2) and (3.6.3) to

$$V_{++} \cap V_{+-} = V_{++} \cap V_{-+} = V_{++} \cap V_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}; \tag{3.6.4}$$

$$V_{++} \cap V_{+-} \cap V_{-+} \cap V_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}. \tag{3.6.5}$$

By the identities (3.6.4), (3.6.5), and combining the knowledge of representations and 4-subspace systems in Section 3.2, we can determine the representations appearing in L, from which we can derive the other intersections.

Similar to the Case I, after rule out other integral representations, we can write the integral representation as:

$$L \cong R_4^{2g_{++}} \oplus A_{-+}^{a} \oplus M_{23}^{r_{23}} \oplus M_{24}^{r_{24}} \oplus M_{34}^{r_{34}} \oplus M_{234}^{r_{234}} \oplus \bar{M}_{234}^{\bar{r}_{234}}$$

The exclusion of the other possible representations are exactly the same as we do in Case I, except that we cannot exclude rank 1 representation A_{-+} in Case II.

Lemma 3.6.1. *In Case II, M_{234} and $\bar{M}_{234}$ do not appear.*

Proof. By Lemma 3.4.9, A_- appears in $M_{234}|_{\langle\tau\rangle}$ and $\bar{M}_{234}|_{\langle\tau\rangle}$. But, in Case II, τ has no fixed points on X, $L|_{\langle\tau\rangle}$ do not has the component A_- (see Remark 2.4.12 (c)). So, M_{234} and $\bar{M}_{234}$ do not appear in Case II. □

Finally, we have

$$L \cong R_4^{2g_{++}} \oplus A_{-+}^a \oplus M_{23}^{r_{23}} \oplus M_{24}^{r_{24}} \oplus M_{34}^{r_{34}}$$

We can determine all the coefficients in formula above:

Theorem 3.6.2. *In Case II, we have*

$$L \cong R_4^{2g_{++}} \oplus A_{-+}^2 \oplus M_{23}^{v(\sigma\tau)/2-2} \oplus M_{34}^{v(\sigma)/2-2} \tag{3.6.6}$$

where $v(*)$ is the number of fixed points on X under the involution $*$.

Proof. By Lemmas 3.4.1, 3.4.2 and 3.4.6, we have

$$L|_{\langle\sigma\rangle} = R_2^{4g_{++}+r_{23}+r_{24}} \oplus A_-^{a+2r_{34}}; \tag{3.6.7}$$

$$L|_{\langle\tau\rangle} = R_2^{4g_{++}+r_{23}+r_{34}} \oplus A_-^{2r_{24}} \oplus A_+^a; \tag{3.6.8}$$

$$L|_{\langle\sigma\tau\rangle} = R_2^{4g_{++}+r_{24}+r_{34}} \oplus A_-^{a+2r_{23}}. \tag{3.6.9}$$

σ and $\sigma\tau$ have but τ do not have fixed points on X, from Theorem 2.4.10, we have

$$L|_{\langle\sigma\rangle} = R_2^{2g_{+,\sigma}} \oplus A_-^{2g_{-,\sigma}-2g_{+,\sigma}} = R_2^{2g_{+,\sigma}} \oplus A_-^{v(\sigma)-2}; \tag{3.6.10}$$

$$L|_{\langle\tau\rangle} = R_2^{2g_{-,\tau}} \oplus A_+^{2g_{+,\tau}-2g_{-,\tau}} = R_2^{2g_{+,\tau}} \oplus A_+^2; \tag{3.6.11}$$

$$L|_{\langle\sigma\tau\rangle} = R_2^{2g_{+,\sigma\tau}} \oplus A_-^{2g_{-,\sigma\tau}-2g_{+,\sigma\tau}} = R_2^{2g_{+,\sigma\tau}} \oplus A_-^{v(\sigma\tau)-2}. \tag{3.6.12}$$

where $v(*)$ is the number of fixed points on X under the involution $*$, and the last equality in each identity comes from Riemann-Hurwitz formula.

Comparing the two sets of identities, we have:

$$a = 2; \tag{3.6.13}$$

$$r_{23} = g_{-,\sigma\tau} - g_{+,\sigma\tau} - 1 = v(\sigma\tau)/2 - 2 = g_{+-} + g_{-+} - g_{--} - g_{++} - 1; \tag{3.6.14}$$

$$r_{24} = 0; \tag{3.6.15}$$

$$r_{34} = g_{-,\sigma} - g_{+,\sigma} - 1 = v(\sigma)/2 - 2 = g_{-+} + g_{--} - g_{+-} - g_{++} - 1. \tag{3.6.16}$$

As a result, we have

$$L \cong R_4^{2g_{++}} \oplus A_{-+}^2 \oplus M_{23}^{v(\sigma\tau)/2-2} \oplus M_{34}^{v(\sigma)/2-2} \tag{3.6.17}$$

□

Finally, we have the theorem of intersections for Case II:

Theorem 3.6.3. *Let X be any algebraic curve, and σ and τ are commuting involutions, assuming σ and $\sigma\tau$ have but τ does not have fixed points, then we have:*

$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$,

$J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\sigma\tau)/2-2}$, $J_{+-} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$, *and* $J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(\sigma)/2-2}$.

where $v(*)$ is the number of fixed points on X under the involution $*$.

Proof. By Theorem 3.5.4, and the facts that,

a. each regular representation R_4 contributes a $J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})$, and

b. each M_{23} contributes an intersection $J_{+-} \cap J_{-+}$, each M_{24} contributes an intersection $J_{+-} \cap J_{--}$, and each M_{34} contributes an intersection $J_{-+} \cap J_{--}$;

c. A_{-+} has no contribution to intersections,

we can easily get the results. □

3.7 Intersections of J_{++}, J_{+-}, J_{-+} and J_{--}: Case III

For case III, all σ and τ have no but $\sigma\tau$ have fixed points on X, from Theorem 3.1.6 and Corollary 3.1.7 we know that

$$g_{--} \leq g_{++}, g_{+-}, g_{-+}; \tag{3.7.1}$$

$$J_{--} \cap J_{++} = J_{--} \cap J_{-+} = J_{++} \cap J_{-+} = J_{--}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}; \tag{3.7.2}$$

$$J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{--}[2] \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}. \tag{3.7.3}$$

By the Lemma 3.3.1, we can reformulate the identities (3.7.2) and (3.7.3) to

$$V_{++} \cap V_{+-} = V_{++} \cap V_{-+} = V_{++} \cap V_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}; \tag{3.7.4}$$

$$V_{++} \cap V_{+-} \cap V_{-+} \cap V_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}. \tag{3.7.5}$$

By the identities (3.7.4) and (3.7.5), and combining the knowledge of representations and 4-subspace systems in Section 3.2, we can determine the representations appearing in L, from which we can derive the other intersections.

Lemma 3.7.1. *In Case III, only the regular representation contribute to* $V_{++} \cap V_{+-} \cap V_{-+} \cap V_{--}$.

Proof. Since there is no rank 1 representations in Case III, we only need to exclude the reduced presentations. After carefully investigating Theorem 3.2.5, we find the only possible reduced representation with non-zero contribution of $V_{++} \cap V_{+-} \cap V_{-+} \cap V_{--}$ is the reduced representation of Type (9) in the list with $\dim V = 1$. But, we had excluded it in Corollary 3.4.8. □

Since every regular representation, associated with $\mathcal{V}(R_4) = (V; V_1, V_2, V_3, V_4) = (\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2; \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z})$ (See 3.2.14), with intersection $V_1 \cap V_2 \cap V_3 \cap V_4 = \mathbb{Z}/2\mathbb{Z}$ (See 3.2.3), contribute a intersections of the form $J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})$ by Lemma 3.3.1, we have

$$\mathcal{V}(L) = (V; V_1, V_2, V_3, V_4) = \mathcal{V}(R_4)^{2g_{--}} \oplus \tilde{\mathcal{V}}(L)$$

$$\tilde{\mathcal{V}}(L) = (\tilde{V}; \tilde{V}_1, \tilde{V}_2, \tilde{V}_3, \tilde{V}_4);$$

$$V_i = (\mathbb{Z}/4\mathbb{Z})^{2g_{--}} \oplus \tilde{V}_i$$

Lemma 3.7.2. *In Case III, $V_4 \cong (\mathbb{Z}/4\mathbb{Z})^{2g_{--}}$, and $\tilde{V}_4 = 0$.*

Proof. By definition (See 3.2.2), $V_4 = \frac{e_4 L + L}{L}$, where $e_4 = \frac{(1-\sigma)}{2}\frac{(1-\tau)}{2}$, we have $\mathrm{rank}_{\mathbb{Z}}(1-\sigma)(1-\tau)L = \dim J_{--} = 2g_{--}$, hence the cardinality of V_4, $\mathrm{Card} V_4 = \mathrm{Card}\frac{e_4 L + L}{L} \leq \mathrm{Card}\frac{e_4 L}{L} = \mathrm{Card}(\mathbb{Z}/4\mathbb{Z})^{2g_{--}} = 4^{2g_{--}}$. We also have $V_4 = (\mathbb{Z}/4\mathbb{Z})^{2g_{--}} \oplus \tilde{V}_4$, so we have $\tilde{V}_4 = 0$ and $V_4 = (\mathbb{Z}/4\mathbb{Z})^{2g_{--}}$. □

Now we need to further investigate the structure of $\tilde{\mathcal{V}}(L) = (\tilde{V}; \tilde{V}_1, \tilde{V}_2, \tilde{V}_3, 0)$.

Since $\tilde{V}_4 = 0$, $\tilde{\mathcal{V}}(L)$ comes from reduced representations. Also using the fact of $\tilde{V}_4 = 0$, we can derive that only limited representations in list of Theorem 3.2.5 contribute to $\tilde{\mathcal{V}}(L)$:

Lemma 3.7.3. *In Case III, only the following Type in Theorem 3.2.5 can possibly contribute the reduced part of representation of L:*

a. Type (3) *with* $\dim V = 1$*: M_{12}, M_{13}, and M_{23};*

b. Type (4) *with* $\dim V = 2$*: M_{123};*

c. Type (7) *with* $\dim V = 1$*: $\bar{M}_{123}$.*

So, we can write:

$$L \cong R_4^{2g--} \oplus M_{12}^{r_{12}} \oplus M_{13}^{r_{13}} \oplus M_{23}^{r_{23}} \oplus M_{123}^{r_{123}} \oplus \bar{M}_{123}^{\bar{r}_{123}}. \tag{3.7.6}$$

Theorem 3.7.4. *In Case III, if only Type* (3) *reduced representations appear in L, then*

$$L \cong R_4^{2g--} \oplus M_{12} \oplus M_{13} \oplus M_{23}^{v(\sigma\tau)/2-1} \tag{3.7.7}$$

where $v(*)$ is the number of fixed points on X under the involution $*$.

Proof. By assumption, we can write $L \cong R_4^{2g--} \oplus M_{12}^{r_{12}} \oplus M_{13}^{r_{13}} \oplus M_{23}^{r_{23}}$. By

Lemmas 3.4.1 and 3.4.6, we have

$$L|_{\langle\sigma\rangle} = R_2^{4g_{--}+r_{13}+r_{23}} \oplus A_+^{2r_{12}}; \tag{3.7.8}$$

$$L|_{\langle\tau\rangle} = R_2^{4g_{--}+r_{12}+r_{23}} \oplus A_+^{2r_{13}}; \tag{3.7.9}$$

$$L|_{\langle\sigma\tau\rangle} = R_2^{4g_{--}+r_{12}+r_{13}} \oplus A_-^{2r_{23}}. \tag{3.7.10}$$

while σ and τ have no but $\sigma\tau$ has fixed points on X, from Theorem 2.4.10, we have

$$L|_{\langle\sigma\rangle} = R_2^{2g_{-,\sigma}} \oplus A_+^{2g_{+,\sigma}-2g_{-,\sigma}} = R_2^{2g_{-,\sigma}} \oplus A_+^2; \tag{3.7.11}$$

$$L|_{\langle\tau\rangle} = R_2^{2g_{-,\tau}} \oplus A_+^{2g_{+,\tau}-2g_{-,\tau}} = R_2^{2g_{-,\tau}} \oplus A_+^2; \tag{3.7.12}$$

$$L|_{\langle\sigma\tau\rangle} = R_2^{2g_{+,\sigma\tau}} \oplus A_-^{2g_{-,\sigma\tau}-2g_{+,\sigma\tau}} = R_2^{2g_{+,\sigma\tau}} \oplus A_-^{v(\sigma\tau)-2}. \tag{3.7.13}$$

where $v(*)$ is the number of fixed points on X under the involution $*$, and the last equality of each identity comes from Riemann-Hurwitz formula.

Comparing the two sets of equations, we have:

$$r_{12} = 1;\ r_{13} = 1;\ r_{23} = v(\sigma\tau)/2 - 1. \tag{3.7.14}$$

As a result, we have

$$L \cong R_4^{2g_{--}} \oplus M_{12} \oplus M_{13} \oplus M_{23}^{v(\sigma\tau)/2-1} \tag{3.7.15}$$

□

Lemma 3.7.5. *In Case III, if Type* (4) (M_{123}) *or Type* (7) ($\bar{M}_{123}$)*, appears in L, then:*

$$L \cong R_4^{2g--} \oplus M_{23}^{v(\sigma\tau)/2-2} \oplus M_{123}^{r_{123}} \oplus \bar{M}_{123}^{\bar{r}_{123}}, \tag{3.7.16}$$

where $v(\sigma\tau)$ is the number of the fixed points on X of under the involution $\sigma\tau$ and $r_{123} + \bar{r}_{123} = 2$.

Proof. By (3.7.6), we have $L \cong R_4^{2g--} \oplus M_{12}^{r_{12}} \oplus M_{13}^{r_{13}} \oplus M_{23}^{r_{23}} \oplus M_{123}^{r_{123}} \oplus \bar{M}_{123}^{\bar{r}_{123}}$. Since X has no fixed point under involution σ and τ, $L|_{\langle\sigma\rangle} = L|_{\langle\tau\rangle} = A_+^2$ (Remark 2.4.12). Let's consider the restriction of each components. $M_{123}|_{\langle\sigma\rangle} = \bar{M}_{123}|_{\langle\tau\rangle} = A_+ \oplus R_4$, who contribute odd multiples of A_+. However, $M_{12}|_{\langle\sigma\rangle} = M_{13}|_{\langle\tau\rangle} = A_+^2$, $M_{13}|_{\langle\sigma\rangle} = M_{12}|_{\langle\tau\rangle} = M_{23}|_{\langle\sigma\rangle} = M_{23}|_{\langle\tau\rangle} = R_2$: all of them contribute multiples of A_+. So $r_{123} + \bar{r}_{123} = 2$ and $r_{12} = r_{13} = 0$. We can further get the multiple $r_{23} = v(\sigma\tau)/2 - 2$ by comparing the multiple of R_2 in $M_{123}|_{\langle\sigma\tau\rangle}$, $\bar{M}_{123}|_{\langle\sigma\tau\rangle}$, $M_{23}|_{\langle\sigma\tau\rangle}$ and $L|_{\langle\sigma\tau\rangle}$. □

Finally, we have the theorem of intersections for Case III:

Theorem 3.7.6. *Let X be any algebraic curve, and σ and τ are commuting involutions, assuming σ and τ have no fixed points but $\sigma\tau$ on X, and assuming the total defect of reduced representation is 0, i.e., either*

a. only contains Type (3)*, or*

b. both contain Type (4) *and Type* (7) *reduced representation,*

then we have:

$J_{++} \cap J_{--} = J_{+-} \cap J_{--} = J_{-+} \cap J_{--} = J_{--}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}$,

$J_{++} \cap J_{+-} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}+1}$, $J_{++} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}+1}$,

and

$J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}+v(\sigma\tau)/2-1}$.

where $v(\sigma\tau)$ *is the number fixed points on* X *under the involution* $\sigma\tau$.

Proof. If L contains Type (4) and Type (7) representation, by Lemma 3.7.5, they both have the multiplicity one. For $M_{123} \oplus \bar{M}_{123}$, the 2-intersections are exact the same as $M_{12} \oplus M_{13} \oplus M_{23}$. (See the discussion in Case I.) Hence, we only need to discuss the case L only contains Type (3) representations. By Theorem 3.7.4, and the facts that,

a. each regular representation R_4 contributes a $J_{++} \cap J_{--} = J_{+-} \cap J_{--} = J_{-+} \cap J_{--} = J_{--}[2] = J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})$, and

b. each M_{12} contributes an intersection $J_{++} \cap J_{+-}$, each M_{13} contributes an intersection $J_{++} \cap J_{-+}$, and each M_{23} contributes an intersection $J_{+-} \cap J_{-+}$,

we can get our results. □

Remark 3.7.7. *The computations in Chapter 3 shows the intersection of*

$J_{\pm\pm}$ satisfies the conclusion of Theorem 3.7.6, which suggests the assumption of the theorem is true.

.1 Appendix: Some Computation for Regular Represnetations

Lemma .1.1. *(Lemma 3.2.1) For regular representation R_4, the 4-subspace system*

$$(V; V_1, V_2, V_3, V_4) = (\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2; \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}). \quad (.1.1)$$

Proof. By (3.2.6), we know

$$M_* = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad (.1.2)$$

and $M = Id_{4\times 4}$. So $V = M_*/M = \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2$. We can easily get this result by direct computation, or using MAGMA to calculate it:

```
M_star := LatticeWithBasis(4, [1,1,1,1,  1,-1,1,-1, 1,1,-1,-1, 1,-1,-1,1]);
M:=4*StandardLattice(4);
quo<M_star|M>
```

For V_i, we can also calculate using MAGMA. For example, we calculate V_1. $V_1 = (e_1M + M)/M = ((1 + \sigma + \tau + \sigma\tau)M + 4M)/4M$. We can write

$(1+\sigma+\tau+\sigma\tau)M$ by the matrix $Id_{4\times4}+S_\sigma+S_\tau+S_{\sigma\tau}$. By (3.2.8), (3.2.9), and (3.2.10), we have

$$Id_{4\times4}+S_\sigma+S_\tau+S_{\sigma\tau}=\begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix} \tag{.1.3}$$

So, $(1+\sigma+\tau+\sigma\tau)M$ is generated by $(1,1,1,1)$. Using MAGMA code:

```
M_1 := LatticeWithBasis(4, [1,1,1,1]);

M:=4*StandardLattice(4);

V_1:=quo<M_1+M|M>;

V_1;
```

We get $V_1=\mathbb{Z}/4\mathbb{Z}$.

For V_2, $(1+\sigma-\tau-\sigma\tau)M$ is generated by $(1,1,-1,-1)$. Using MAGMA code:

```
M_2 := LatticeWithBasis(4, [1,1,-1,-1]);

M:=4*StandardLattice(4);

V_2:=quo<M_2+M|M>;

V_2;
```

We get $V_2=\mathbb{Z}/4\mathbb{Z}$.

For V_3, $(1-\sigma+\tau-\sigma\tau)M$ is generated by $(1,-1,1,-1)$. Using MAGMA code:

```
M_3 := LatticeWithBasis(4, [1,-1,1,-1]);

M:=4*StandardLattice(4);

V_3:=quo<M_3+M|M>;

V_3;
```

We get $V_3 = \mathbb{Z}/4\mathbb{Z}$.

For V_4, $(1-\sigma-\tau+\sigma\tau)M$ is generated by $(1,-1,-1,1)$. Using MAGMA code:

```
M_4 := LatticeWithBasis(4, [1,-1,-1,1]);

M:=4*StandardLattice(4);

V_4:=quo<M_4+M|M>;

V_4;
```

We get $V_4 = \mathbb{Z}/4\mathbb{Z}$. Similarly, we have $V_i = \mathbb{Z}/4\mathbb{Z}$, for $i = 1, 2, 3, 4$ □

Lemma .1.2. *(Lemma 3.2.2) For the regular representation R_4, $V_i \cap V_j \cong \mathbb{Z}/2\mathbb{Z}$, for $1 \leq i < j \leq 4$.*

Proof. We can calculate all the intersections $V_i \cap V_j$, $1 \leq i < j \leq 4$, by MAGMA:

```
M_12:=(M_1+M) meet (M_2+M);

V_12:=quo<M_12+M|M>;
```

```
V_12;

M_13:=(M_1+M) meet (M_3+M);

V_13:=quo<M_13+M|M>;

V_13;

M_14:=(M_1+M) meet (M_4+M);

V_14:=quo<M_14+M|M>;

V_14;

M_23:=(M_2+M) meet (M_3+M);

V_23:=quo<M_23+M|M>;

V_23;

M_24:=(M_2+M) meet (M_4+M);

V_24:=quo<M_24+M|M>;

V_24;

M_34:=(M_3+M) meet (M_4+M);

V_34:=quo<M_34+M|M>;

V_34;
```

We get $V_i \cap V_j \cong \mathbb{Z}/2\mathbb{Z}$, for $1 \leq i < j \leq 4$. □

.2 Appendix: Reduction of Some Representations

In this appendix, we will do some computation for reduction of reduced integral representation of Klein 4-group to integral representation of its cyclic 2-subgroup. The computation depends on the explicit construction of 4-subspace system corresponding reduced integral representation of Klein 4-group. By the construction of the 4-subspace system (also see [Butler73]), we have

$$0 \to M \to e_*M \xrightarrow{\pi} V \to 0 \tag{.2.1}$$

where M is the $\mathbb{Z}$-free $\mathbb{Z}G$-module, $G = \langle \sigma, \tau \rangle$, $e_*M = e_1M + e_2M + e_3M + e_4M$, $e_1 = e_{++} = \frac{1+\sigma}{2}\frac{1+\tau}{2}$, $e_2 = e_{+-} = \frac{1+\sigma}{2}\frac{1-\tau}{2}$, $e_3 = e_{-+} = \frac{1-\sigma}{2}\frac{1+\tau}{2}$, $e_4 = e_{--} = \frac{1-\sigma}{2}\frac{1-\tau}{2}$, and $V_i = (e_iM + M)/M$.

Lemma .2.1. *(Lemma 3.4.6)*

For the regular representations of Type (3) *with* $\dim V = 1$ M_{ij} *where* $1 \leq i < j \leq 4$ *of* $G = \langle \sigma, \tau \rangle$*, we have the following identities when they are restricted*

to their cyclic 2*-subgroups* $\langle\sigma\rangle$, $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$M_{12}|_{\langle\sigma\rangle} = A^2_+,\ M_{12}|_{\langle\tau\rangle} = R_2,\ M_{12}|_{\langle\sigma\tau\rangle} = R_2; \tag{.2.2}$$

$$M_{13}|_{\langle\sigma\rangle} = R_2,\ M_{13}|_{\langle\tau\rangle} = A^2_+,\ M_{13}|_{\langle\sigma\tau\rangle} = R_2; \tag{.2.3}$$

$$M_{14}|_{\langle\sigma\rangle} = R_2,\ M_{14}|_{\langle\tau\rangle} = R_2,\ M_{14}|_{\langle\sigma\tau\rangle} = A^2_+; \tag{.2.4}$$

$$M_{23}|_{\langle\sigma\rangle} = R_2,\ M_{23}|_{\langle\tau\rangle} = -R_2,\ M_{23}|_{\langle\sigma\tau\rangle} = A^2_-; \tag{.2.5}$$

$$M_{24}|_{\langle\sigma\rangle} = R_2,\ M_{24}|_{\langle\tau\rangle} = A^2_-,\ M_{24}|_{\langle\sigma\tau\rangle} = -R_2; \tag{.2.6}$$

$$M_{34}|_{\langle\sigma\rangle} = A^2_-,\ M_{34}|_{\langle\tau\rangle} = R_2,\ M_{34}|_{\langle\sigma\tau\rangle} = -R_2. \tag{.2.7}$$

Proof. We only need to prove one case, say M_{23}, for example. In our notation M_{23} means the 4-subspace system of type of type (3) in the List 3.2.5 with $\dim V = 1$. It has the form $(V; V_1, V_2, V_3, V_4) = (\mathbb{Z}/2\mathbb{Z}; 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0)$.

For the exact sequence .2.1 in our case, $V = \mathbb{Z}/2\mathbb{Z}$, $V_2 = V_3 = \mathbb{Z}/2\mathbb{Z}$, and $V_1 = V_4 = 0$. So we know that $e_1M \subseteq M$ and $e_2M \subseteq M$. We write $M_{+-} = e_{+-}M + M$, $M_{-+} = e_{-+}M + M$ and $e_*M = M_{+-} \oplus M_{-+}$.

$$0 \to M \to M_{+-} \oplus M_{-+} \xrightarrow{\pi} V \to 0$$

$$(a, b) \mapsto a + b$$

and we have $\pi(a, b) = a + b$ by theorem 3.2.5, so $M = \ker\pi = \{(a, b) | a \equiv b($ mod 2$)\}$. Let $v_1 = (1, 1)$, $v_2 = (1, -1)$ be a basis of M,

For σ, we have $\sigma v_1 = (1, -1) = v_2$, and $\sigma v_2 = (1, 1) = v_1$. So σ acts on M

as matrix multiplication from the left by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which means $M_{23}|_{\langle\sigma\rangle} = R_2$.

For τ, we have $\tau v_1 = (-1, 1) = -v_2$, and $\tau v_2 = (-1, -1) = -v_1$. So τ acts on M as matrix multiplication from the left by $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, which means $M_{23}|_{\langle\tau\rangle} = -R_2$.

For $\sigma\tau$, we have $\sigma\tau v_1 = (-1, -1) = -v_1$, and $\sigma\tau v_2 = (-1, 1) = -v_2$. So $\sigma\tau$ acts on M as matrix multiplication from the left by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, which means $M_{23}|_{\langle\tau\rangle} = A^2_-$.

So we have $M_{23}|_{\langle\sigma\rangle} = R_2,\ M_{23}|_{\langle\tau\rangle} = -R_2,\ M_{23}|_{\langle\sigma\tau\rangle} = A^2_-$.

Similarly, we can get other reduction of this type of representation. □

Lemma .2.2. *(Lemma 3.4.7)*

For the reduced representation of Type (9) *with* $\dim V = 1$*, denoted by* M_{1234}*, of* $G = \langle\sigma, \tau\rangle$*, we have the following identity when it is restricted to its cyclic* 2*-subgroups* $\langle\sigma\rangle$*,* $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$M_{1234}|_{\langle\sigma\rangle} = R_2 \oplus A_+ \oplus A_-. \tag{.2.8}$$

Proof. In our notation M_{1234} means the 4-subspace system of type of type (9) in the List 3.2.5 with $\dim V = 1$. It has the form $(V; V_1, V_2, V_3, V_4) = (\mathbb{Z}/2\mathbb{Z}; \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$.

For the exact sequence .2.1 in our case, $V = \mathbb{Z}/2\mathbb{Z}$, $V_1 = V_2 = V_3 = V_4 = \mathbb{Z}/2\mathbb{Z}$. So we know that $e_i M \subseteq M$ for $i = 1, 2, 3, 4$. We write $M_{++} =$

$e_{++}M + M$ $M_{+-} = e_{+-}M + M$, $M_{-+} = e_{-+}M + M$, $M_{--} = e_{--}M + M$, and $e_*M = M_{+-} \oplus M_{+-} \oplus M_{-+} \oplus M_{--}$.

$$0 \to M \to M_{+-} \oplus M_{+-} \oplus M_{-+} \oplus M_{--} \xrightarrow{\pi} V \to 0$$

$$(a, b, c, d) \mapsto a + b + c + d$$

and we have $\pi(a, b, c, d) = a + b + c + d$ by Theorem 3.2.5, so $M = \ker\pi = \{(a, b, c, d) | a+b+c+d \equiv 0(\mod 2)\}$. Let $v_1 = (1, 0, 1, 0)$, $v_2 = (1, 0, -1, 0)$, $v_3 = (1, 1, 0, 0)$, $v_4 = (0, 0, 1, 1)$ be a basis of M,

For σ, we have $\sigma v_1 = (1, 0, -1, 0) = v_2$, $\sigma v_2 = (1, 0, 1, 0) = v_1$, $\sigma v_3 = (1, 1, 0, 0) = v_3$, $\sigma v_4 = (0, 0, -1, -1) = -v_4$. So σ acts on M as matrix multiplication from the left by $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$, which means $M_{1234}|_{\langle\sigma\rangle} = R_2 \oplus A_+ \oplus A_-$. □

Lemma .2.3. *(Lemma 3.4.9)*

For the reduced representation of Type (4) *with* $\dim V = 2$*, denoted by* M_{123}*,* M_{124}*,* M_{134} *and* M_{234} *of* $G = \langle\sigma, \tau\rangle$*, we have the following identity when it is*

restricted to its cyclic 2*-subgroups* $\langle\sigma\rangle$, $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$M_{123}|_{\langle\sigma\rangle} = A_+ \oplus R_2,\ M_{123}|_{\langle\tau\rangle} = A_+ \oplus R_2,\ M_{123}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2; \quad (.2.9)$$

$$M_{124}|_{\langle\sigma\rangle} = A_+ \oplus R_2,\ M_{124}|_{\langle\tau\rangle} = A_- \oplus R_2,\ M_{124}|_{\langle\sigma\tau\rangle} = A_+ \oplus R_2; \quad (.2.10)$$

$$M_{134}|_{\langle\sigma\rangle} = A_- \oplus R_2,\ M_{134}|_{\langle\tau\rangle} = A_+ \oplus R_2,\ M_{134}|_{\langle\sigma\tau\rangle} = A_+ \oplus R_2; \quad (.2.11)$$

$$M_{234}|_{\langle\sigma\rangle} = A_- \oplus R_2,\ M_{234}|_{\langle\tau\rangle} = A_- \oplus R_2,\ M_{234}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2. \quad (.2.12)$$

Proof. We only need to prove one case, say M_{123}, for example. In our notation M_{123} means the 4-subspace system of type of type (4) in the List 3.2.5 with $\dim V = 2$. It has the form $(V; V_1, V_2, V_3, V_4) = ((\mathbb{Z}/2\mathbb{Z})^2; \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0)$.

For the exact sequence .2.1 in our case, $V = (\mathbb{Z}/2\mathbb{Z})^2$, $V_1 = V_2 = V_3 = \mathbb{Z}/2\mathbb{Z}$, and $V_4 = 0$. So we know that $e_i M \subseteq M$ for $i = 1, 2, 3$. We write $M_{++} = e_{++}M + M$, $M_{+-} = e_{+-}M + M$, $M_{-+} = e_{-+}M + M$, and $e_*M = M_{++} \oplus M_{+-} \oplus M_{-+}$.

$$0 \to M \to M_{++} \oplus M_{+-} \oplus M_{-+} \xrightarrow{\pi} V \to 0$$

$$(a, b, c) \mapsto (a + b, b + c)$$

and we have $\pi(a, b, c) = (a + b, b + c)$ by Theorem 3.2.5, so $M = \ker\pi = \{(a, b, c) | a + b \equiv b + c \equiv 0(\mod 2)\}$.

For σ, we choose $v_1 = (1, 1, 0)$, $v_2 = (0, 1, 1)$, and $v_3 = (0, -1, 1)$ be a basis of M. we have $\sigma v_1 = (1, 1, 0) = v_1$, $\sigma v_2 = (0, -1, 1) = v_3$, and

$\sigma v_3 = (0,1,1) = v_2$. So σ acts on M as matrix multiplication from the left by $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, which means $M_{123}|_{\langle\sigma\rangle} = A_+ \oplus R_2$.

For τ, we choose $u_1 = (1,0,1)$, $u_2 = (1,1,0)$, and $u_3 = (1,-1,0)$ be a basis of M. we have $\tau u_1 = (1,0,1) = u_2$, $\tau u_2 = (1,-1,0) = u_3$, and $\tau u_3 = (1,1,0) = u_2$. So τ acts on M as matrix multiplication from the left by $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, which means $M_{123}|_{\langle\tau\rangle} = A_+ \oplus R_2$.

For $\sigma\tau$, we choose $w_1 = (1,1,0)$, $w_2 = (1,-1,0)$, and $w_3 = (0,1,1)$ be a basis of M. we have $\sigma\tau w_1 = (1,-1,0) = w_2$, $\sigma\tau w_2 = (1,1,0) = w_1$, and $\sigma\tau w_3 = (0,-1,-1) = -w_3$. So $\sigma\tau$ acts on M as matrix multiplication from the left by $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, which means $M_{123}|_{\langle\sigma\tau\rangle} = R_2 \oplus A_-$.

So we have $M_{123}|_{\langle\sigma\rangle} = A_+ \oplus R_2$, $M_{123}|_{\langle\tau\rangle} = A_+ \oplus R_2$, $M_{123}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2$.

Similarly, we can get other reduction of this type of representation by permutations of the index.

□

Lemma .2.4. *(Lemma 3.4.10)*

For the reduced representation of Type (7) *with* $\dim V = 1$*, denoted by* $\bar{M}_{123}$*,* $\bar{M}_{124}$*,* $\bar{M}_{134}$ *and* $\bar{M}_{234}$ *of* $G = \langle\sigma,\tau\rangle$*, we have the following identity when it is*

restricted to its cyclic 2*-subgroups* $\langle\sigma\rangle$, $\langle\tau\rangle$ *and* $\langle\sigma\tau\rangle$*:*

$$\bar{M}_{123}|_{\langle\sigma\rangle} = A_+ \oplus R_2,\ \bar{M}_{123}|_{\langle\tau\rangle} = A_+ \oplus R_2,\ \bar{M}_{123}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2; \quad (.2.13)$$

$$\bar{M}_{124}|_{\langle\sigma\rangle} = A_+ \oplus R_2,\ \bar{M}_{124}|_{\langle\tau\rangle} = A_- \oplus R_2,\ \bar{M}_{124}|_{\langle\sigma\tau\rangle} = A_+ \oplus R_2; \quad (.2.14)$$

$$\bar{M}_{134}|_{\langle\sigma\rangle} = A_- \oplus R_2,\ \bar{M}_{134}|_{\langle\tau\rangle} = A_+ \oplus R_2,\ \bar{M}_{134}|_{\langle\sigma\tau\rangle} = A_+ \oplus R_2; \quad (.2.15)$$

$$\bar{M}_{234}|_{\langle\sigma\rangle} = A_- \oplus R_2,\ \bar{M}_{234}|_{\langle\tau\rangle} = A_- \oplus R_2,\ \bar{M}_{234}|_{\langle\sigma\tau\rangle} = A_- \oplus R_2. \quad (.2.16)$$

Proof. We only need to prove one case, say $\bar{M}_{123}$, for example. In our notation $\bar{M}_{123}$ means the 4-subspace system of type of type (7) in the List 3.2.5 with $\dim V = 1$. It has the form $(V; V_1, V_2, V_3, V_4) = (\mathbb{Z}/2\mathbb{Z}; \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, 0)$.

For the exact sequence .2.1 in our case, $V = \mathbb{Z}/2\mathbb{Z}$, $V_1 = V_2 = V_3 = \mathbb{Z}/2\mathbb{Z}$, and $V_4 = 0$. So we know that $e_i M \subseteq M$ for $i = 1, 2, 3$. We write $M_{++} = e_{++}M + M$, $M_{+-} = e_{+-}M + M$, $M_{-+} = e_{-+}M + M$, and $e_*M = M_{++} \oplus M_{+-} \oplus M_{-+}$.

$$0 \to M \to M_{++} \oplus M_{+-} \oplus M_{-+} \xrightarrow{\pi} V \to 0$$

$$(a, b, c) \mapsto a + b + c$$

and we have $\pi(a, b, c) = a + b + c$ by Theorem 3.2.5, so $M = \ker\pi = \{(a, b, c) | a + b + c \equiv 0(\mod 2)\}$.

For σ, we choose $v_1 = (1, 0, 1)$, $v_2 = (1, 0, -1)$, and $v_3 = (1, 1, 0)$ be a basis of M. we have $\sigma v_1 = (1, 0, -1) = v_2$, $\sigma v_2 = (1, 0, 1) = v_1$, and

$\sigma v_3 = (1,1,0) = v_3$. So σ acts on M as matrix multiplication from the left by $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, which means $\bar{M}_{123}|_{\langle\sigma\rangle} = R_2 \oplus A_+$.

For τ, we choose $u_1 = (1,1,0)$, $u_2 = (1,-1,0)$, and $u_3 = (1,0,1)$ be a basis of M. we have $\tau u_1 = (1,-1,0) = u_2$, $\tau u_2 = (1,1,0) = u_1$, and $\tau u_3 = (1,0,1) = u_3$. So τ acts on M as matrix multiplication from the left by $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, which means $\bar{M}_{123}|_{\langle\tau\rangle} = R_2 \oplus A_+$.

For $\sigma\tau$, we choose $w_1 = (1,1,0)$, $w_2 = (1,-1,0)$, and $w_3 = (0,1,1)$ be a basis of M. we have $\sigma\tau w_1 = (1,-1,0) = w_2$, $\sigma\tau w_2 = (1,1,0) = w_1$, and $\sigma\tau w_3 = (0,-1,-1) = -w_3$. So $\sigma\tau$ acts on M as matrix multiplication from the left by $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, which means $\bar{M}_{123}|_{\langle\sigma\tau\rangle} = R_2 \oplus A_-$.

So we have $\bar{M}_{123}|_{\langle\sigma\rangle} = R_2 \oplus A_+$, $\bar{M}_{123}|_{\langle\tau\rangle} = R_2 \oplus A_+$, $\bar{M}_{123}|_{\langle\sigma\tau\rangle} = R_2 \oplus A_-$.

Similarly, we can get other reduction of this type of representation by permutations of the index. $\square$

Chapter 4

Computational Aspect

In this chapter, we will do some computation which is my starting point leading to the results in the first two chapters. In this chapter, we will consider the case of modular curve under Atkin-Lehner involutions. In this case, we can compute explicitly using modular symbols. Some mathematical program package, such as MAGMA, Sage, can help us to compute this problems.

Let $X = X_0(N)$ where N is a square free integer, and $N = st$, $(s,t) = 1$. w_s, w_t and w_N are Atkin-Lehner involutions. And, we will omit the subscript if it will not cause confusion.

4.1 Computation of One Involution Case

By Proposition 2.3, we can compute $J_+ \cap J_-$ explicitly.

$$J_+ \cap J_- \cong \frac{L}{L_+ + L_-},$$

where $L = H_1(X, \mathbb{Z})$ and $L_\pm = \{v \in L | wL = \pm L\}$.

4.1.1 MAGMA code

a. MAGMA code for compute $J_+ \cap J_-$ when involution is w_N.

```
N:=37;    //imput an integer N

J:=JZero(N);  // J=J_0(N)

L:=StandardLattice(2*Dimension(J));

M:=MatrixAlgebra(Integers(),2*Dimension(J));

id:=M!1;

wN:=M!Matrix(AtkinLehnerOperator(J,N));

L_N_plus:=Lattice(Kernel(id-wN));

L_N_minus:=Lattice(Kernel(id+wN));

L_N_plus_minus:=L_N_plus + L_N_minus;

G_N_plus_minus:=quo<L|L_N_plus_minus>;


Dimension(L_N_plus);   //dim A_+ =2g_+
```

```
Dimension(L_N_minus);  //dim A_- =2g_-


G_N_plus_minus;   //$J_+ \cap J_-$
```

b. MAGMA code for compute $J_+ \cap J_-$ when involution is w_s, $s||N$.

```
s:=5; t:=41;  //input s and t

N:=s*t;    // N=st

J:=JZero(N);  // J=J_0(N)

L:=StandardLattice(2*Dimension(J));

M:=MatrixAlgebra(Integers(),2*Dimension(J));

id:=M!1;

ws:=M!Matrix(AtkinLehnerOperator(J,s));  //w_s

wt:=M!Matrix(AtkinLehnerOperator(J,t));  //w_t

wN:=M!Matrix(AtkinLehnerOperator(J,N));  //w_N

L_s_plus:=Lattice(Kernel(id-ws));    //L_{+,s}

L_s_minus:=Lattice(Kernel(id+ws));

L_s_plus_minus:=L_s_plus + L_s_minus;

G_s_plus_minus:=quo<L|L_s_plus_minus>;

L_t_plus:=Lattice(Kernel(id-wt));

L_t_minus:=Lattice(Kernel(id+wt));
```

```
L_t_plus_minus:=L_t_plus + L_t_minus;

G_t_plus_minus:=quo<L|L_t_plus_minus>;

L_N_plus:=Lattice(Kernel(id-wN));

L_N_minus:=Lattice(Kernel(id+wN));

L_N_plus_minus:=L_N_plus + L_N_minus;

G_N_plus_minus:=quo<L|L_N_plus_minus>;


Dimension(L_s_plus);  // dim L_{+,s}=2g_{+,s}

Dimension(L_s_minus);  // dim L_{-,s}=2g_{-,s}

Dimension(L_t_plus);  // dim L_{+,t}=2g_{+,t}

Dimension(L_t_minus);  // dim L_{-,t}=2g_{-,t}

Dimension(L_N_plus);  // dim L_{+,st}=2g_{+,st}

Dimension(L_N_minus);  // dim L_{-,st}=2g_{-,st}


G_s_plus_minus;   // $J_{+,s}\cap J_{-,s}$

G_t_plus_minus;   // $J_{+,t}\cap J_{-,t}$

G_N_plus_minus;   // $J_{+,st}\cap J_{-,st}$
```

4.1.2 Results

Example 4.1.1.

$$N = 37,\ 2g_+ = 2,\ 2g_- = 2,\ J_+ \cap J_- \cong \mathbb{Z}^2.$$

$$N = 61,\ 2g_+ = 2,\ 2g_- = 6,\ J_+ \cap J_- \cong \mathbb{Z}^2.$$

$$N = 1093,\ 2g_+ = 86,\ 2g_- = 941,\ J_+ \cap J_- \cong \mathbb{Z}^{86}.$$

$$N = 74,\ 2g_+ = 4,\ 2g_- = 12,\ J_+ \cap J_- \cong \mathbb{Z}^4.$$

$$N = 77,\ 2g_+ = 4,\ 2g_- = 10,\ J_+ \cap J_- \cong \mathbb{Z}^4.$$

$$N = 221,\ 2g_+ = 12,\ 2g_- = 16,\ J_+ \cap J_- \cong \mathbb{Z}^{12}.$$

From Example 4.1.1, we can get the following conjecture:

Conjecture 4.1.2. *For $J_0(N)$, let $J_\pm = (1 \pm w_N)J$, then*

$J_+ \cap J_- \cong \mathbb{Z}^{2g_+}$ where $g_+ = \dim J_+$, which implies $J_+ \cap J_- = J_+[2]$.

The Conjecture 4.1.2 is proved as Corollary 2.3.3 in the first chapter as a special case of a more general theorem, [Theorem 2.4.5]. Here w_N always has fixed points as a consequence of Ogg and Kenku's theorem in Section 2.3.

More general, we can compute $J_+ \cap J_-$ when involution is w_s for $s||N$.

From Ogg and Kenku's theorem in Section 2.3, we know that if $N = st$, where s and t are prime, we can find that w_s has fixed points iff $(\frac{-s}{t}) = 1$,

and w_s has fixed points iff $(\frac{-s}{t}) = -1$. In MAGMA, we can use

```
LegendreSymbol(-s, t) //substitute the value of s and t
```

to value the Legendre symbol $(\frac{-s}{t})$.

Example 4.1.3.

$N = 5 \cdot 41,\ s = 5,\ t = 41,$ *all of* w_s, w_t, w_st *have fixed points,*

$2g_{+,s} = 18,\ 2g_{-,s} = 20,\ J_{+,s} \cap J_{-,s} = (\mathbb{Z}/2\mathbb{Z})^{18}$;

$2g_{+,t} = 12,\ 2g_{-,t} = 26,\ J_{+,t} \cap J_{-,t} = (\mathbb{Z}/2\mathbb{Z})^{12}$;

$2g_{+,st} = 16,\ 2g_{-,st} = 22,\ J_{+,st} \cap J_{-,st} = (\mathbb{Z}/2\mathbb{Z})^{16}$.

$N = 23 \cdot 3,\ s = 23,\ t = 3,$ w_s *and* w_st *have fixed points but* w_t *do not has,*

$2g_{+,s} = 2,\ 2g_{-,s} = 12,\ J_{+,s} \cap J_{-,s} = (\mathbb{Z}/2\mathbb{Z})^{2}$;

$2g_{+,t} = 8,\ 2g_{-,t} = 6,\ J_{+,t} \cap J_{-,t} = (\mathbb{Z}/2\mathbb{Z})^{6}$;

$2g_{+,st} = 4,\ 2g_{-,st} = 10,\ J_{+,st} \cap J_{-,st} = (\mathbb{Z}/2\mathbb{Z})^{4}$.

$N = 5 \cdot 37,\ s = 5,\ t = 37,$ w_st *has fixed points but* w_s *and* w_t *do not have,*

$2g_{+,s} = 18,\ 2g_{-,s} = 16,\ J_{+,s} \cap J_{-,s} = (\mathbb{Z}/2\mathbb{Z})^{16}$;

$2g_{+,t} = 18,\ 2g_{-,t} = 16,\ J_{+,t} \cap J_{-,t} = (\mathbb{Z}/2\mathbb{Z})^{16}$;

$2g_{+,st} = 10,\ 2g_{-,st} = 24,\ J_{+,st} \cap J_{-,st} = (\mathbb{Z}/2\mathbb{Z})^{10}$.

From Example 4.1.3, we can get the following conjecture:

Conjecture 4.1.4. *For $J_0(N)$, let $J_\pm = (1 \pm w_s)J$, where $s||N$, then*

a. if w_s has fixed points, $J_+ \cap J_- \cong \mathbb{Z}^{2g_+}$ where $g_+ = \dim J_+$, which implies $J_+ \cap J_- = J_+[2]$;

b. if w_s has no fixed points, $J_+ \cap J_- \cong \mathbb{Z}^{2g_-}$ where $g_- = \dim J_-$, which implies $J_+ \cap J_- = J_-[2]$.

We finally prove this conjecture by prove a more general case. In Theorem 2.0.6, we prove not only for modular curves $X_0(N)$ with Atkin-Lehner involutions, but for all algebraic curve with all involutions.

4.2 Computation of Two Involution Case

In this section we will continue to compute the intersections of $J_{\pm\pm}$ for modular curves with Atkin-Lehner involutions. For two involution case, we have

4 $J_{\pm\pm}$s: J_{++}, J_{+-}, J_{-+} and J_{--},

6 intersections: $J_{++} \cap J_{+-}$, $J_{++} \cap J_{-+}$, $J_{++} \cap J_{--}$, $J_{+-} \cap J_{-+}$, $J_{+-} \cap J_{--}$, $J_{-+} \cap J_{++}$.

And, we need to discuss the problem with 3 different cases:

Case I. both w_s and w_t have fixed points;

Case II. one of w_s and w_t, say w_s has fixed points;

Case III. both w_s and w_t have no fixed points.

For computation of the intersections, we use the similar formulas as we do in the one involution case. For example,

$$J_{++} \cap J_{+-} \cong \frac{L_{+,s}}{L_{++} + L_{+-}}$$

where $L_{++} = L_{+,s} \cap L_{+,t}$, and $L_{+-} = L_{+,s} \cap L_{-,t}$.

We also need to compute the 4-subspace system $(V; V_1, V_2, V_3, V_4)$. And compare the intersections and the 4-subspace system to get our conjectures for the two involutions case.

$$e_1 = \frac{1+\sigma}{2} \cdot \frac{1+\tau}{2},\ e_2 = \frac{1+\sigma}{2} \cdot \frac{1-\tau}{2},$$
$$e_3 = \frac{1-\sigma}{2} \cdot \frac{1+\tau}{2},\ e_4 = \frac{1-\sigma}{2} \cdot \frac{1-\tau}{2},$$
$$e_* = e_1 + e_2 + e_3 + e_4.$$
$$V = e_* L/L,$$
$$V_i = (e_i L + L)/L, \quad \text{for i=1, 2, 3, 4}$$

where $L = H_1(X_0(N), \mathbb{Z})$.

4.2.1 MAGMA codes

a. MAGMA code for intersections.

```
s:=23;t:=29;    //we need to input different s and q each time.

J:=JZero(s*t);    //J:=$J_0(st)$ where s=23 and t=29

L:=StandardLattice(2*Dimension(J)); //L:=H_1(X_0(st),\mathbb{Z})

M:=MatrixAlgebra(Integers(),2*Dimension(J));

id:=M!1;

ws:=M!Matrix(AtkinLehnerOperator(J,s));

wt:=M!Matrix(AtkinLehnerOperator(J,t));

wst:=M!Matrix(AtkinLehnerOperator(J,s*t));

L_s_plus:=Lattice(Kernel(id-ws));

L_s_minus:=Lattice(Kernel(id+ws));

L_s_plus_minus:=L_s_plus + L_s_minus;

G_s_plus_minus:=quo<L|L_s_plus_minus>;

L_t_plus:=Lattice(Kernel(id-wt));

L_t_minus:=Lattice(Kernel(id+wt));

L_t_plus_minus:=L_t_plus + L_t_minus;

G_t_plus_minus:=quo<L|L_t_plus_minus>;

L_st_plus:=Lattice(Kernel(id-wst));

L_st_minus:=Lattice(Kernel(id+wst));

L_st_plus_minus:=L_st_plus + L_st_minus;

G_st_plus_minus:=quo<L|L_st_plus_minus>;
```

```
L_s_plus_t_plus:=L_s_plus meet L_t_plus;

L_s_plus_t_minus:=L_s_plus meet L_t_minus;

L_plusplus_plusminus:=L_s_plus_t_plus+L_s_plus_t_minus;

G_plusplus_plusminus:=quo<L_s_plus|L_plusplus_plusminus>;

L_s_minus_t_plus:=L_s_minus meet L_t_plus;

L_s_minus_t_minus:=L_s_minus meet L_t_minus;

L_plusplus_minusminus:=L_s_plus_t_plus + L_s_minus_t_minus;

G_plusplus_minusminus:=quo<L_st_plus|L_plusplus_minusminus>;

L_plusminus_minusminus:=L_s_plus_t_minus + L_s_minus_t_minus;

G_plusminus_minusminus:=quo<L_t_minus|L_plusminus_minusminus>;

L_plusminus_minusplus:=L_s_plus_t_minus + L_s_minus_t_plus;

G_plusminus_minusplus:=quo<L_st_minus|L_plusminus_minusplus>;

L_plusplus_minusplus:=L_s_plus_t_plus + L_s_minus_t_plus;

G_plusplus_minusplus:=quo<L_t_plus|L_plusplus_minusplus>;

L_minusplus_minusminus:=L_s_minus_t_plus + L_s_minus_t_minus;

G_minusplus_minusminus:=quo<L_s_minus|L_minusplus_minusminus>;


Dimension(L_s_plus_t_plus);

Dimension(L_s_plus_t_minus);

Dimension(L_s_minus_t_plus);
```

```
Dimension(L_s_minus_t_minus);


G_plusplus_plusminus;

G_plusplus_minusplus;

G_plusplus_minusminus;

G_plusminus_minusplus;

G_plusminus_minusminus;

G_minusplus_minusminus;
```

b. MAGMA code for computation of 4-subspace system.

```
s:=23;t:=29;    //we need to input different s and q each time.

J:=JZero(s*t);    //J:=$J_0(st)$ where s=23 and t=29

L:=StandardLattice(2*Dimension(J)); //L:=H_1(X_0(st),\mathbb{Z})

M:=MatrixAlgebra(Integers(),2*Dimension(J));

id:=M!1;

ws:=M!Matrix(AtkinLehnerOperator(J,s));

wt:=M!Matrix(AtkinLehnerOperator(J,t));

wst:=M!Matrix(AtkinLehnerOperator(J,s*t));


e1:=1+ws+wt+wst;
```

```
e2:=1+ws-wt-wst;

e3:=1-ws+wt-wst;

e4:=1-ws-wt+wst;


M:=StandardLattice(2*Dimension(J));

V1:=quo<(e1*M+4*M)|4*M>;V1;

V2:=quo<(e2*M+4*M)|4*M>;V2;

V3:=quo<(e3*M+4*M)|4*M>;V3;

V4:=quo<(e4*M+4*M)|4*M>;V4;

V:=quo<(e1*M+e2*M+e3*M+e4*M)|4*M>;V
```

We can use the formulas in Section 2.3, or using the Riemann-Hurwitz formula to compute the numbers of the fixed points of Atkin-Lehner involutions on modular curves $X_0(N)$. The Riemann-Hurwitz formula for our case is:

$$v(w_s) = 2g_{-,s} - 2g_{+,s} + 2 = 2g_{-+} + 2g_{--} - 2g_{++} - 2g_{+-} + 2;$$

$$v(w_t) = 2g_{-,t} - 2g_{+,t} + 2 = 2g_{+-} + 2g_{--} - 2g_{++} - 2g_{-+} + 2;$$

$$v(w_s t) = 2g_{-,st} - 2g_{+,st} + 2 = 2g_{+-} + 2g_{-+} - 2g_{++} - 2g_{--} + 2.$$

4.2.2 Results for Case I

Case I: both w_s and w_t have fixed points.

Example 4.2.1.

$N = 13 \cdot 29,\ s = 13,\ t = 27.$

$2g_{++} = 10,\ 2g_{+-} = 22,\ 2g_{-+} = 18,\ 2g_{--} = 16,$

$v(s) = 4, v(t) = 12, v(st) = 16.$

$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = (\mathbb{Z}/2\mathbb{Z})^{10},\ 2g_{++} = 10;$

$J_{+-} \cap J_{-+} = (\mathbb{Z}/2\mathbb{Z})^{17},\ 2g_{++} + v(st)/2 - 1 = 17;$

$J_{+-} \cap J_{--} = (\mathbb{Z}/2\mathbb{Z})^{15},\ 2g_{++} + v(t)/2 - 1 = 15;$

$J_{-+} \cap J_{--} = (\mathbb{Z}/2\mathbb{Z})^{11},\ 2g_{++} + v(s)/2 - 1 = 11.$

$(V; V_1, V_2, V_3, V_4)$

$= ((\mathbb{Z}/4\mathbb{Z})^{10} \oplus (\mathbb{Z}/2\mathbb{Z})^{33};$

$(\mathbb{Z}/4\mathbb{Z})^{10}, (\mathbb{Z}/4\mathbb{Z})^{10} \oplus (\mathbb{Z}/2\mathbb{Z})^{12}, (\mathbb{Z}/4\mathbb{Z})^{10} \oplus (\mathbb{Z}/2\mathbb{Z})^{8}, (\mathbb{Z}/4\mathbb{Z})^{10} \oplus (\mathbb{Z}/2\mathbb{Z})^{6})$

$= R_4^{10} \oplus ((\mathbb{Z}/2\mathbb{Z})^{13}; 0, (\mathbb{Z}/2\mathbb{Z})^{12}, (\mathbb{Z}/2\mathbb{Z})^{8}, (\mathbb{Z}/2\mathbb{Z})^{6})$

$= R_4^{10} \oplus M_{23}^7 \oplus M_{24}^5 \oplus M_{34}^1.$

$g - 4g_{++} = 13,\ 2g_{+-} - 2g_{++} = 12,\ 2g_{-+} - 2g_{++} = 8,\ 2g_{--} - 2g_{++} = 6;$

$v(st)/2 - 1 = 7,\ v(t)/2 - 1 = 5,\ v(s)/2 - 1 = 1.$

From the Example 4.2.1 and other computations which are not listed above, we can conclude:

Conjecture 4.2.2. *In Case I, all of the involutions w_s, w_t and w_{st} have*

fixed points.

For intersections, we have:

a. $J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$, *which implies*

$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2]$ *and*

$J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{++}[2]$;

b. $J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(st)/2-1}$,

$J_{+-} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(t)/2-1}$,

$J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(s)/2-1}$.

For 4*-subspace systems, we have:*

$\mathcal{V} = R_4^{2g_{++}} \oplus \widetilde{\mathcal{V}}$,

where $\widetilde{\mathcal{V}} = ((\mathbb{Z}/2\mathbb{Z})^{g-4g_{++}}; 0, (\mathbb{Z}/2\mathbb{Z})^{2g_{+-}-2g_{++}}, (\mathbb{Z}/2\mathbb{Z})^{2g_{-+}-2g_{++}}, (\mathbb{Z}/2\mathbb{Z})^{2g_{--}-2g_{++}})$

$= M_{23}^{v(st)/2-1} \oplus M_{24}^{v(t)/2-1} \oplus M_{34}^{v(s)/2-1}$;

and $\rho(\widetilde{\mathcal{V}}) := 2\dim\widetilde{V} - 2\sum_{i=1}^{4} \dim\widetilde{V}_i = 0$.

4.2.3 Results for Case II

Case II: one of w_s and w_t, say w_s has fixed points.

Example 4.2.3.

$N = 43 \cdot 47,\ s = 43,\ t = 47.$

$2g_{++} = 70,\ 2g_{+-} = 102,\ 2g_{-+} = 106,\ 2g_{--} = 72,$

$v(s) = 8, v(t) = 0, v(st) = 68.$

$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = (\mathbb{Z}/2\mathbb{Z})^{70},\ 2g_{++} = 70;$

$J_{+-} \cap J_{-+} = (\mathbb{Z}/2\mathbb{Z})^{102},\ 2g_{++} + v(st)/2 - 2 = 102;$

$J_{+-} \cap J_{--} = (\mathbb{Z}/2\mathbb{Z})^{70},\ 2g_{++} = 70;$

$J_{-+} \cap J_{--} = (\mathbb{Z}/2\mathbb{Z})^{72},\ 2g_{++} + v(s)/2 - 2 = 72.$

$(V; V_1, V_2, V_3, V_4)$

$= ((\mathbb{Z}/4\mathbb{Z})^{70} \oplus (\mathbb{Z}/2\mathbb{Z})^{174};$

$$(\mathbb{Z}/4\mathbb{Z})^{70}, (\mathbb{Z}/4\mathbb{Z})^{70} \oplus (\mathbb{Z}/2\mathbb{Z})^{32}, (\mathbb{Z}/4\mathbb{Z})^{70} \oplus (\mathbb{Z}/2\mathbb{Z})^{34}, (\mathbb{Z}/4\mathbb{Z})^{70} \oplus (\mathbb{Z}/2\mathbb{Z})^{2})$$

$= R_4^{70} \oplus ((\mathbb{Z}/2\mathbb{Z})^{34}; 0, (\mathbb{Z}/2\mathbb{Z})^{32}, (\mathbb{Z}/2\mathbb{Z})^{34}, (\mathbb{Z}/2\mathbb{Z})^{2})$

$= R_4^{70} \oplus M_{23}^{32} \oplus M_{34}^{2}.$

$g - 4g_{++} - 1 = 34,\ 2g_{+-} - 2g_{++} = 32,\ 2g_{-+} - 2g_{++} - 2 = 34,\ 2g_{--} - 2g_{++} = 2;$

$v(st)/2 - 2 = 32,\ v(s)/2 - 2 = 2.$

From the Example 4.2.3 and other computations which are not listed above, we can conclude:

Conjecture 4.2.4. *In Case II, all but w_t have fixed points.*

For intersections, we have:

a. $J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$, *which implies*

$J_{++} \cap J_{+-} = J_{++} \cap J_{-+} = J_{++} \cap J_{--} = J_{++}[2]$ *and*

$J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{++}[2]$;

b. $J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(st)/2-2}$,

$J_{+-} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}}$,

$J_{-+} \cap J_{--} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{++}+v(s)/2-2}$.

For 4*-subspace systems, we have:*

$\mathcal{V} = R_4^{2g_{++}} \oplus \widetilde{\mathcal{V}}$,

where $\widetilde{\mathcal{V}} = ((\mathbb{Z}/2\mathbb{Z})^{g-4g_{++}}; 0, (\mathbb{Z}/2\mathbb{Z})^{2g_{+-}-2g_{++}}, (\mathbb{Z}/2\mathbb{Z})^{2g_{-+}-2g_{++}-2}, (\mathbb{Z}/2\mathbb{Z})^2)$

$= M_{23}^{v(st)/2-2} \oplus M_{34}^{v(s)/2-2}$;

and $\rho(\widetilde{\mathcal{V}}) := 2\mathrm{dim}\widetilde{V} - 2\sum_{i=1}^{4} \mathrm{dim}\widetilde{V}_i = 0$.

4.2.4 Results for Case III

Case III. both w_s and w_t has no fixed points.

Example 4.2.5.

$N = 5 \cdot 77,\ s = 5,\ t = 77.$

$2g_{++} = 22,\ 2g_{+-} = 24,\ 2g_{-+} = 24,\ 2g_{--} = 20,$

$v(s) = 0, v(t) = 0, v(st) = 8.$

$J_{--} \cap J_{++} = J_{--} \cap J_{+-} = J_{--} \cap J_{-+} = (\mathbb{Z}/2\mathbb{Z})^{20},\ 2g_{--} = 20;$

$J_{++} \cap J_{+-} = (\mathbb{Z}/2\mathbb{Z})^{21},\ 2g_{--} + 1 = 21;$

$J_{++} \cap J_{-+} = (\mathbb{Z}/2\mathbb{Z})^{21},\ 2g_{--} + 1 = 21;$

$J_{+-} \cap J_{-+} = (\mathbb{Z}/2\mathbb{Z})^{23},\ 2g_{--} + v(st)/2 - 1 = 23.$

$(V; V_1, V_2, V_3, V_4)$

$= ((\mathbb{Z}/4\mathbb{Z})^{20} \oplus (\mathbb{Z}/2\mathbb{Z})^{45};$

$\qquad (\mathbb{Z}/4\mathbb{Z})^{20} \oplus (\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/4\mathbb{Z})^{20} \oplus (\mathbb{Z}/2\mathbb{Z})^4, (\mathbb{Z}/4\mathbb{Z})^{20} \oplus (\mathbb{Z}/2\mathbb{Z})^4, (\mathbb{Z}/4\mathbb{Z})^{20})$

$= R_4^{20} \oplus ((\mathbb{Z}/2\mathbb{Z})^5; (\mathbb{Z}/2\mathbb{Z})^2, (\mathbb{Z}/2\mathbb{Z})^4, (\mathbb{Z}/2\mathbb{Z})^4, 0)$

$= R_4^{20} \oplus M_{12} \oplus M_{13} \oplus M_{23}^3.$

$g - 4g_{--} = 5,\ 2g_{++} - 2g_{--} = 2,\ 2g_{+-} - 2g_{--} = 2g_{-+} - 2g_{--} = 4;$

$v(st)/2 - 1 = 3.$

From the Example 4.2.5 and other computations which are not listed above, we can conclude:

Conjecture 4.2.6. *In Case III, w_s and w_t have no but w_{st} have fixed points.*

For intersections, we have:

a. $J_{--} \cap J_{++} = J_{--} \cap J_{+-} = J_{--} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}}$, *which implies*

$J_{--} \cap J_{++} = J_{--} \cap J_{+-} = J_{--} \cap J_{-+} = J_{--}[2]$ *and*

$J_{++} \cap J_{+-} \cap J_{-+} \cap J_{--} = J_{--}[2]$;

b. $J_{++} \cap J_{+-} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}+1}$,

$J_{++} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}+1}$,

$J_{+-} \cap J_{-+} \cong (\mathbb{Z}/2\mathbb{Z})^{2g_{--}+v(st)/2-1}$.

For 4*-subspace systems, we have:*

$\mathcal{V} = R_4^{2g_{--}} \oplus \widetilde{\mathcal{V}}$,

where $\widetilde{\mathcal{V}} = ((\mathbb{Z}/2\mathbb{Z})^{g-4g_{--}}; (\mathbb{Z}/2\mathbb{Z})^{2g_{++}-2g_{--}}, (\mathbb{Z}/2\mathbb{Z})^{2g_{+-}-2g_{--}}, (\mathbb{Z}/2\mathbb{Z})^{2g_{-+}-2g_{--}}, 0)$

$= M_{12} \oplus M_{13} \oplus M_{23}^{v(st)/2-1}$;

and $\rho(\widetilde{\mathcal{V}}) := 2\mathrm{dim}\widetilde{V} - 2\sum_{i=1}^{4} \mathrm{dim}\widetilde{V}_i = 0$.

Bibliography

Bibliography

[Benson] Benson, D, *Representations and Colomology*. Cambridge, 1998.

[Bourbaki59] Bourbaki, N, *Algèbre: Chapitre 9*. Hermann Paris, 1959.

[Brenner74] Brenner, Sheila, *On four subspaces of a vector space*. J. Algebra 29 (1974), 587-599.

[Butler73] Butler, M. C. R. *The 2-adic representations of Klein's four group*. Proceedings of the Second International Conference on the Theory of Groups (Australian Nat. Univ., Canberra, 1973), pp. 197-203. Lecture Notes in Math., Vol. 372, Springer, Berlin, 1974.

[Clark03] Pete Clark, *Rational points on Atkin-Lehner quotients of Shimura curves*. Ph.D. thesis, 2003.

[CurtisReiner81] C Curtis; I Reiner, *Methods of representation theory. Vol. I. With applications to finite groups and orders*, Pure and Applied Mathematics. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1981.

[GelfandPonomarev70] Gelfand, I. M.; Ponomarev, V. A. *Problems of linear algebra and classification of quadruples of subspaces in a finite-dimensional vector space*. Hilbert space operators and operator algebras (Proc. Internat. Conf., Tihany, 1970), pp. 163-237. Colloq. Math. Soc. Janos Bolyai, 5, North-Holland, Amsterdam, 1972.

[GriffithsHarris78] Griffiths, Philip; Harris, Joe. *Principles of Algebraic Geometry*. Wiley and Sons, 1978.

[GrossHarris81] Gross, Benedict H.; Harris, Joe. *Real algebraic curves*. Ann. Sci. cole Norm. Sup. (4) 14 (1981), no. 2, 157-182.

[Hartshorne77] Hartshorne, Robin. *Algebraic Geometry*. Springer-Verlag New York, 1977.

[Kenku77] M.Kenku, *Atkin-Lehner involutions and class number residuality*, Acta Arith. 33 (1977), no. 1, 19.

[Jaffee80] H.Jaffee, *Real algebraic curves*. Topology 19 (1980), no. 1, 81-87.

[Mazur] B.Mazur, *Complex conjugate on* $X_0(N)$. Unpublished.

[Mazur77] B.Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33-186 (1978).

[Mumford70] David Mumford, *Abelian Varieties*, Oxford University Press, 1st edition 1970.

[Nazarova67] L.A.Nazarova, *Representations of a tetrad*. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 31 1967 1361-1378.

[Ogg74] A.Ogg, *Hyperelliptic modular curves* Bulletin de la Socit Mathmatique de France, 102 (1974), p. 449-462

[Ogg83] A.Ogg, *Real points on Shimura curves. Arithmetic and geometry*, Vol. I, 277307, Progr. Math., 35, Birkhuser Boston, Boston, MA, 1983.

[Olson70] Loren D.Olson, *Galois Cohomology of Cycles and Applicaton to Elliptic Curves*, American Journal of Mathematics, Vol.92.No.1, p.75-85.

[Ribet75] K.Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*. Ann. Math. (2) 101 (1975), 555-562.

[Ribet83] K.Ribet, *Congruence relations between modular forms*. Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), 503-514, PWN, Warsaw, 1984.

[Rotman] J.Rotman, *An Introduction to Homological Algebra*. Springer, 2008.

[Stein00] W.Stein, *Explicit approaches to modular abelian varieties*, (UC Berkeley Ph.D. thesis) (2000)

[TaylorWiles95] R.Taylor, A.Wiles, *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. (2) 141 (1995), no. 3, 553-572.

[Wiles95] A.Wiles, *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) 141 (1995), no. 3, 443-551.