DISSERTATION

CONJUGACY CLASSES OF MATRIX GROUPS OVER LOCAL RINGS AND AN APPLICATION TO THE ENUMERATION OF ABELIAN VARIETIES

Submitted by

Cassandra L Williams

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2012

Doctoral Committee:

Advisor: Jeffrey Achter

Richard Eykholt
Alexander Hulpke
Tim Penttila

ABSTRACT

CONJUGACY CLASSES OF MATRIX GROUPS OVER LOCAL RINGS AND AN APPLICATION TO THE ENUMERATION OF ABELIAN VARIETIES

The Frobenius endomorphism of an abelian variety over a finite field $\mathbb{F}_q$ of dimension g can be considered as an element of the finite matrix group $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r)$. The characteristic polynomial of such a matrix defines a union of conjugacy classes in the group, as well as a totally imaginary number field K of degree $2g$ over $\mathbb{Q}$. Suppose $g = 1$ or 2. We compute the proportion of matrices with a fixed characteristic polynomial by first computing the sizes of conjugacy classes in $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ and $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$. Then we use an equidistribution assumption to show that this proportion is related to the number of abelian varieties over a finite field with complex multiplication by the maximal order of K via a theorem of Everett Howe.

ACKNOWLEDGEMENTS

I would like to thank Jeff Achter for all of his guidance, and Hilary Smallwood for her help in completing Appendix B.

TABLE OF CONTENTS

1. INTRODUCTION

Abelian varieties are geometric objects defined as projective zero sets of polynomials which have a (commutative) group structure on their points. For example, elliptic curves are abelian varieties of genus one. An isogeny between two such objects is a particular type of map, and it induces an equivalence relation on the set of all abelian varieties of a particular dimension.

Over fields of characteristic zero, isogeny classes of abelian varieties with complex multiplication can be represented by the totally imaginary field in which the complex multiplication lies. While these classes may be infinite, the number of abelian varieties with complex multiplication by the maximal order in an imaginary field (i.e., the ring of integers) is finite. In fact, the number of such varieties is closely related to the class number of the imaginary field.

Alternatively, over finite fields Tate's theorem [22] says that isogeny classes of abelian varieties are determined by the characteristic polynomial of the Frobenius endomorphism. These Frobenius maps are naturally elements of $\mathrm{GL}_{2g}(\mathbb{Z}/n)$ for $n \in \mathbb{N}$, and since every abelian variety admits a polarization we can instead represent them in $\mathrm{GSp}_{2g}(\mathbb{Z}/n)$. In this group, we can compute the size of the conjugacy class of such a matrix.

An interesting question one could ask is how likely is it that a random abelian variety over a finite field $\mathbb{F}_q$ has a Frobenius endomorphism with a given characteristic polynomial f. Gekeler formulated this question for elliptic curves [9] and, after assuming the Frobenius elements are equidistributed in the matrix group, he showed that the answer has to do with the local factors in the Euler product expansion of an

L-series. Note that this equidistribution assumption cannot possibly be true, since there are only finitely many abelian varieties of a given dimension over $\mathbb{F}_q$.

In this paper, we have two main goals. First, we use number theory, algebraic geometry, and group theory to determine representatives for and sizes of conjugacy classes of the matrix groups $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ and $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$. In particular, we prove a smoothness result (Theorem 4.3.9) on centralizers in to find a formula for the centralizer order of any $\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$. We use this conjugacy class data to efficiently reproduce Gekeler's result for $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$.

Gekeler noted that the probability he computed was equal to an Euler factor of an L-series. We interpret this relationship slightly differently; consider this L-series as one that occurs in the Dedekind zeta function of a certain totally imaginary field. Then the L-series is (up to a real constant) related to the class number of the field, and a theorem of Howe (as communicated in [10]) gives a formula for the size of the set of abelian varieties over a finite field with complex multiplication by the maximal order of the field in terms of the class number. Our second goal is to use this theorem to interpret Gekeler's result in terms of the size of an isogeny class of elliptic curves, and extend the computation to abelian surfaces using our results about the conjugacy classes of $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$.

Let $\mathcal{C}(\gamma)$ denote the conjugacy class of γ. Our main result is the following theorem.

Theorem 1.0.1 (Main Theorem)**.** *Suppose $f(T) \in \mathbb{Z}[T]$ is such that $K = \mathrm{Split}(f)$ is a totally imaginary quartic field. Let $\mathcal{I}_K$ be the set of isomorphism classes of principally polarized abelian surfaces over a finite field with complex multiplication by the maximal order of K. Then for an explicit real constant ξ,*

$$\#\mathcal{I}_K = \frac{1}{\xi} \prod_{\ell \in \mathbb{Z} \ \textit{prime}} \frac{\#\left\{\textit{cyclic } \gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell) | \mathcal{C}(\gamma) \leftrightarrow f \ \textit{mod } \ell\right\}}{\ell^{-2}\ \#\,\mathrm{Sp}_4(\mathbb{F}_\ell)}.$$

2. BACKGROUND: NUMBER THEORY AND ALGEBRAIC GEOMETRY

We will make use of many standard results from algebraic number theory and algebraic geometry, and for the sake of convenience we collect them here. In addition, we will set some notation.

2.1 Splitting of primes in Galois extensions of $\mathbb{Q}$

Although many results are cited with specific references, much of the material in this section comes from classic graduate texts in number theory, perhaps most frequently from Marcus [16], Neukirch [18], and Serre [19].

Recall that a *Dedekind domain* is an integral domain such that every ideal is finitely generated, every nonzero prime ideal is maximal, and such that it is integrally closed. An important attribute of Dedekind domains is that they have unique factorization of ideals.

Let A be a Dedekind domain, and K its field of fractions. Let L be a finite Galois extension of K and let B be the integral closure of A in L.

$$\begin{tikzcd}
L \arrow[d, dash] & \supset & B & \supset \mathfrak{q} \\
K & \supset & A \arrow[u, hook] & \supset \mathfrak{p}
\end{tikzcd}$$

The ring B is also a Dedekind domain, so we have unique factorization of prime ideals in B. For any prime $\mathfrak{p} \subset A$, $\mathfrak{p}B \subset B$ and so we can ask how the ideal $\mathfrak{p}$ factors in B.

Suppose

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\dots\mathfrak{q}_r^{e_r} = \prod_{i=1}^{r} \mathfrak{q}_i^{e(\mathfrak{q}_i/\mathfrak{p})}$$

with the $\mathfrak{q}_i \subset B$ prime ideals and $e(\mathfrak{q}_i/\mathfrak{p}) \in \mathbb{Z}_+$ the *inertial degree* of $\mathfrak{q}_i$ over $\mathfrak{p}$. We collect here some results about primes in such an extension.

Lemma 2.1.1. *[18, Section I.9] The ring B is stable under* $\mathrm{Gal}(L/K)$. *For any $\sigma \in \mathrm{Gal}(L/K)$ and $\mathfrak{q} \subset B$ prime, $\sigma(\mathfrak{q})$ is also prime; in fact, $B/\sigma(\mathfrak{q}) \cong B/\mathfrak{q}$.*

Lemma 2.1.2. *[16, Theorem 23] The group* $\mathrm{Gal}(L/K)$ *acts transitively on the set of primes of B lying over a prime $\mathfrak{p} \in A$.*

Since B is a Dedekind domain, any nonzero prime ideal $\mathfrak{q} \subset B$ is maximal and so $B/\mathfrak{q}$ is a field; we denote it by $\kappa(\mathfrak{q}) = B/\mathfrak{q}$ and call it the *residue field* of $\mathfrak{q}$. If $\mathfrak{q} \cap A = \mathfrak{p}$ then $\kappa(\mathfrak{q})$ is a finite extension of $\kappa(\mathfrak{p})$, and we call $f(\mathfrak{q}/\mathfrak{p}) = [\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]$ the *residue degree* of $\mathfrak{q}$ over $\mathfrak{p}$.

Corollary 2.1.3. *[16, Corollary to Theorem 23] If L/K is a finite Galois extension where $\mathfrak{q}$ and $\mathfrak{q}'$ lie over $\mathfrak{p}$, then*

$$f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}'/\mathfrak{p}) \quad \textit{and} \quad e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}'/\mathfrak{p}).$$

We will denote $f(\mathfrak{q}/\mathfrak{p})$ and $e(\mathfrak{q}/\mathfrak{p})$ as $f = f(\mathfrak{p})$ and $e = e(\mathfrak{p})$ respectively.

Proposition 2.1.4. *[18, Proposition I.8.2] Suppose*

$$\mathfrak{p}B = \prod_{\mathfrak{q}_i \big| \mathfrak{p}} \mathfrak{q}_i^{e(\mathfrak{q}_i/\mathfrak{p})} = \prod_{\mathfrak{q}_i \big| \mathfrak{p}} \mathfrak{q}_i^{e_i}$$

and let $f_i = f(\mathfrak{q}_i/\mathfrak{p})$. Then

$$\sum_i e_i f_i = [L : K] = n.$$

Corollary 2.1.5. *Suppose L/K is Galois and let $r(\mathfrak{p}) = \#\{\mathfrak{q} \subset B |\ \mathfrak{q}|\mathfrak{p}\}$. Then $r(\mathfrak{p})f(\mathfrak{p})e(\mathfrak{p}) = n$.*

Remark 2.1.6. If $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^e$ then we can use the Chinese Remainder Theorem [11, Proposition 12.3.1] to write

$$B/\mathfrak{p}B \cong \bigoplus_i B/\mathfrak{q}_i^e,$$

where $B/\mathfrak{p}B$ and each $B/\mathfrak{q}_i^e$ are vector spaces over $\kappa(\mathfrak{p})$.

The action of the Galois group $\mathrm{Gal}(L/K)$ on primes in B clearly governs the factorization in B of a prime $\mathfrak{p}$ of A. For the sake of convenience, let us make a few definitions here. We say that $\mathfrak{p}$ *splits completely* if $(e, f, r) = (1, 1, n)$ (i.e., $\mathfrak{p}B = \prod_{i=1}^{n} \mathfrak{q}_i$ with the $\mathfrak{q}_i$ distinct). We say that $\mathfrak{p}$ is *ramified* if $e > 1$, and that $\mathfrak{p}$ is *totally ramified* if $(e, f, r) = (n, 1, 1)$ (i.e., $\mathfrak{p}B = \mathfrak{q}^n$). We say that $\mathfrak{p}$ is *inert* if $(e, f, r) = (1, n, 1)$ (i.e., $\mathfrak{p}$ is prime in B). Many other factorizations are possible, depending on the factorization of n.

Now we define two subgroups of $\mathrm{Gal}(L/K)$ which control the structure of the factorization of $\mathfrak{p}$ and state some results about them which will be useful in chapters 5 and 7. The *decomposition group* at $\mathfrak{q}$ is the stabilizer of $\mathfrak{q}$ in $\mathrm{Gal}(L/K)$,

$$D(\mathfrak{q}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

and the *inertia group* at $\mathfrak{q}$ is

$$I(\mathfrak{q}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\beta) \equiv \beta \bmod \mathfrak{q}\ \forall \beta \in B\}.$$

Notice that $I(\mathfrak{q}/\mathfrak{p}) \leq D(\mathfrak{q}/\mathfrak{p}) \leq \mathrm{Gal}(L/K)$.

Theorem 2.1.7. *[18, Proposition I.9.4] There is an isomorphism*

$$D(\mathfrak{q}/\mathfrak{p})/I(\mathfrak{q}/\mathfrak{p}) \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})).$$

Lemma 2.1.8. *[18, Propositions I.9.3,I.9.6]*

$$\#D(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p}) \text{ and } \#I(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p}).$$

Corollary 2.1.9. *If $\mathfrak{p}$ is unramified, $D(\mathfrak{q}/\mathfrak{p}) \cong \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$.*

Recall that L and K are number fields over $\mathbb{Q}$. Then the residue fields $\kappa(\mathfrak{q})$ and $\kappa(\mathfrak{p})$ are finite fields and $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is a Galois extension of degree $f = f(\mathfrak{q}/\mathfrak{p})$ with $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \cong \mathbb{Z}/f$. Notably, this Galois group is cyclic and so must have a generator, the automorphism $x \mapsto x^{\#\kappa(\mathfrak{p})}$.

Let $\mathfrak{p}$ be unramified in L so that $D(\mathfrak{q}/\mathfrak{p}) \cong \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ by the previous corollary. There is an element $\sigma \in D(\mathfrak{q}/\mathfrak{p})$ that corresponds to this automorphism via the isomorphism from Theorem 2.1.7, and so has the property $\sigma(\beta) \equiv \beta^{\#\kappa(\mathfrak{p})} \bmod \mathfrak{q}$ for all $\beta \in B$. Since $\mathfrak{p}$ is unramified, this is the only σ with this property. We call σ the *Frobenius automorphism* of $\mathfrak{q}$ over $\mathfrak{p}$; the Frobenius automorphisms for the different $\mathfrak{q}$ dividing $\mathfrak{p}$ are conjugate as elements of $\mathrm{Gal}(L/K)$. Since the map $x \mapsto x^{\#\kappa(\mathfrak{p})}$ generates $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ it has order $f(\mathfrak{q}/\mathfrak{p})$, and thus σ does as well.

Then when $\mathfrak{p}$ is unramified, σ generates the decomposition group $D(\mathfrak{q}/\mathfrak{p})$, and the order of σ gives information about the factorization of $\mathfrak{p}$ in B. For example, an unramified prime $\mathfrak{p}$ splits completely in L if and only if $\sigma = 1$ (since $\sigma = 1$ if and only if $f(\mathfrak{p}) = 1$). This Frobenius automorphism will be a key tool in chapters 5 and 7 for determining how to match a prime $\ell \in \mathbb{Z}$ to a conjugacy class of $\mathrm{GL}_2(\mathbb{F}_\ell)$ or $\mathrm{GSp}_4(\mathbb{F}_\ell)$ based on its factorization in B.

Now consider a tower of fields $L/M/K$ with L/K Galois, A and B as before, and C the integral closure of A in M. Given a prime $\mathfrak{p} \subset A$, let $\mathfrak{r} \subset C$ be a prime lying over $\mathfrak{p}$ and $\mathfrak{q} \subset B$ be a prime lying over $\mathfrak{r}$.

$$\begin{tikzcd}
L & \supset & B & \supset \mathfrak{q} \\
M \arrow[u, dash] & \supset & C \arrow[u, hook] & \supset \mathfrak{r} \\
K \arrow[u, dash] & \supset & A \arrow[u, hook] & \supset \mathfrak{p}
\end{tikzcd}$$

Lemma 2.1.10. *[16, Chapter 3] With the above notation,*

$$f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{r})f(\mathfrak{r}/\mathfrak{p}) \quad \textit{and} \quad e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{r})e(\mathfrak{r}/\mathfrak{p}).$$

We also have relationships between the decomposition and inertia groups in such a tower of fields. We will make considerable use of these in chapter 7 to determine the structure of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$.

Lemma 2.1.11. *[19, Proposition I.22.a]*

$$\begin{aligned} D(\mathfrak{q}/\mathfrak{r}) =& D(\mathfrak{q}/\mathfrak{p}) \cap \mathrm{Gal}(L/M), \\ \textit{and} \quad I(\mathfrak{q}/\mathfrak{r}) =& I(\mathfrak{q}/\mathfrak{p}) \cap \mathrm{Gal}(L/M). \end{aligned}$$

Lemma 2.1.12. *[19, Proposition I.22.b] Suppose* $\mathrm{Gal}(L/M)$ *is normal and let* $\rho : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ *be the natural projection map. Then*

$$\begin{aligned} D(\mathfrak{r}/\mathfrak{p}) &= \rho(D(\mathfrak{q}/\mathfrak{p})), \\ \textit{and} \quad I(\mathfrak{r}/\mathfrak{p}) &= \rho(I(\mathfrak{q}/\mathfrak{p})). \end{aligned}$$

For the context of the problem we will address, A will be $\mathbb{Z}$ so that $K = \mathbb{Q}$. The number field L will be the splitting field of some monic irreducible polynomial $f(T) \in \mathbb{Z}[T]$ of degree $2g$, and we will rename it as $K = \mathrm{Split}(f)$. Then B will be the ring of integers of K, $\mathcal{O}_K$. The prime $\mathfrak{p} = \ell$ will be an odd rational prime (i.e., a prime number in $\mathbb{Z}$) and will have a collection of prime ideals $\lambda \subset \mathcal{O}_K$ lying above it. The residue fields will be $\kappa(\mathfrak{p}) = \kappa(\ell) = \mathbb{F}_\ell$ and so $\kappa(\lambda)$ will be isomorphic to $\mathbb{F}_{\ell f(\lambda)}$.

$$\begin{tikzcd}
K = \mathrm{Split}(f) \arrow[d, dash] & \supset & \mathcal{O}_K & \supset & \{\lambda_1, \lambda_2, \ldots, \lambda_r\} \\
\mathbb{Q} & \supset & \mathbb{Z} \arrow[u, hook] & \supset & \ell
\end{tikzcd}$$

2.2 Dirichlet characters, L-series, and the Dedekind zeta function

Almost all of the material in this section comes from Chapters 3 and 4 of Washington [25], supplemented with Chapter 16 in Ireland and Rosen [11].

A *Dirichlet character* is a multiplicative homomorphism $\chi : (\mathbb{Z}/m)^\times \to \mathbb{C}^\times$ which can be extended to a function on $\mathbb{Z}$ by

$$\chi(n) = \begin{cases} \chi(n \bmod m) & \text{if } \gcd(m,n) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

In fact, χ maps into μ_m, the group of the m^{th} roots of unity. The trivial character χ_0 is the constant map $\chi_0(n) = 1$ for all $n \in \mathbb{Z}$.

The *Dirichlet L-series* of a character χ is defined to be

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for $s \in \mathbb{C}$ with $Re(s) > 1$, and has an Euler product expansion on that half plane,

$$L(s,\chi) = \prod_{\ell \text{ prime}} \left(1 - \frac{\chi(\ell)}{\ell^s}\right)^{-1}.$$

Notice that $L(s,\chi_0) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$, the Riemann zeta function, which has a pole at $s = 1$.

Lemma 2.2.1. *[11, Proposition 16.1.2]*

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1.$$

Suppose G is a finite abelian group. The set of characters of G is the set of homomorphisms $X = \{\chi : G \to \mathbb{C}^\times\}$; X is a group under multiplication and is called the *character group* of G.

Lemma 2.2.2. *[25, Lemma 3.1] If G is a finite abelian group, then $X \cong G$.*

Any individual character $\chi \in X$ can be associated to a subfield M of a number field K by letting $M = \operatorname{Fix}(\ker(\chi))$. In particular, if G is the Galois group of K, then X is isomorphic to the group of characters associated to K itself. By abuse of notation, we call both of them X.

Let K be a number field with ring of integers $\mathcal{O}_K$. The *Dedekind zeta function* of K is defined to be

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{(\mathfrak{N}(\mathfrak{a}))^s}$$

where $\mathfrak{N}$ denotes the ideal norm.

In some special cases, we can give an equivalent factorization of $\zeta_K(s)$.

Theorem 2.2.3. *[25, Theorem 4.3] Let K be an abelian extension of $\mathbb{Q}$ and let X be the group of characters associated with K. Then*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).$$

Corollary 2.2.4. *[25, Corollary 4.4] For $\chi \in X$, $\chi \neq \chi_0$, $L(1, \chi)$ is nonvanishing.*

2.3 Class numbers

Now we use the material from the previous section to construct the class number of K, which is an invariant of the number field K. The results in this section are primarily from Marcus [16] and Neukirch [18].

For a number field K, a *fractional ideal* I of $\mathcal{O}_K$ is an $\mathcal{O}_K$ submodule of K such that for some $d \in \mathcal{O}_K$, $dI \subseteq \mathcal{O}_K$. In other words, a fractional ideal I can be written as $I = \left\{\frac{a}{d} | a \in \mathfrak{a}, \text{ an ideal of } \mathcal{O}_K\right\}$. The set of all fractional ideals forms a group, $\mathcal{J}$. Consider two elements of $\mathcal{J}$ equivalent if they differ by a principal ideal (i.e., I_1 and I_2 are equivalent if there exist principal ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ such that $\mathfrak{a}I_1 = \mathfrak{b}I_2$). We call the quotient group formed by this equivalence relation the *class group of* $\mathcal{O}_K$ and denote it $\mathcal{CL}(\mathcal{O}_K)$.

Theorem 2.3.1. *[18, Theorem I.6.3] The size of the class group of $\mathcal{O}_K$ is finite.*

We call the size of this group the *class number* and denote it h_K. Typically we think of the class number as a way to measure the failure of the ring of integers to have unique factorization; $\mathcal{O}_K$ is a unique factorization domain if and only if its class number is one.

The class group itself is difficult to compute, but there is an analytic formula to calculate the class number directly. Before stating the theorem, however, we define some invariants of a number field K.

A number field K of degree n can be embedded into either the real numbers or the complex numbers (or both). Let a map $\rho : K \to \mathbb{R}$ be a *real embedding* and a map $\sigma : K \to \mathbb{C}$ be a *complex embedding.* Complex embeddings come in complex conjugate pairs, and if there are r_1 real embeddings and r_2 pairs of complex embeddings for K, then

$$n = r_1 + 2r_2.$$

The following theorem of Dirichlet then tells us that the group of units of the ring of integers, $\mathcal{O}_K^\times$, has a very specific structure.

Theorem 2.3.2 (Dirichlet's Unit Theorem)**.** *[18, I.7.4] Let K be a number field of degree n with r_1 real and $2r_2$ complex embeddings and let $r = r_1 + r_2 - 1$. Then the group of units $(\mathcal{O}_K)^\times$ of $\mathcal{O}_K$ is of the form*

$$(\mathcal{O}_K)^\times \cong \mathbb{Z}/\omega_K\mathbb{Z} \times \mathbb{Z}^r$$

where ω_K is the number of roots of unity of $(\mathcal{O}_K)^\times$.

In other words, there are r units u_i called *fundamental units* so that any unit $u \in \mathcal{O}_K^\times$ can be written as

$$u = \zeta u_1^{n_1} u_2^{n_2} \dots u_r^{n_r}$$

with ζ a root of unity. These fundamental units generate a rank r lattice in $\mathbb{R}^{r_1+r_2}$ and we can compute the volume of the fundamental region for such a lattice as

$$\text{vol} = \sqrt{r_1 + r_2}\ R_K$$

where R_K is called the *regulator* of K and can be computed as a determinant in terms of the fundamental units [18]. The regulator R_K is typically difficult to find (due to the difficulty of producing the fundamental units), but in general it can be bounded for a certain field K.

Now we can compute the class number using Dirichlet's formula.

Theorem 2.3.3 (The Analytic Class Number Formula)**.** *[16, Chapter 7] Let K be a number field with Dedekind zeta function $\zeta_K(s)$, r_1 and $2r_2$ real and complex embeddings, respectively, regulator R_K, ω_K roots of unity in its integral closure, and discriminant d_K over $\mathbb{Q}$. Then*

$$\lim_{s\to 1^+} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\omega_K \sqrt{|d_K|}}.$$

If $K/\mathbb{Q}$ is a Galois extension, we can evaluate the left side of the equality rather precisely as

$$\begin{aligned}\lim_{s\to1^+}(s-1)\zeta_K(s) &= \lim_{s\to1^+}(s-1)\prod_{\chi\in X}L(s,\chi)\\ &= \lim_{s\to1^+}(s-1)L(s,\chi_0)\prod_{\substack{\chi\in X\\ \chi\neq\chi_0}}L(s,\chi)\\ &= \lim_{s\to1^+}\prod_{\substack{\chi\in X\\ \chi\neq\chi_0}}L(s,\chi) = \prod_{\substack{\chi\in X\\ \chi\neq\chi_0}}L(1,\chi),\end{aligned}$$

remembering that $L(s,\chi_0)=\zeta(s)$ so we have $\lim_{s\to1^+}(s-1)L(s,\chi_0)=1$ by Lemma 2.2.1. All other $L(s,\chi)$ are convergent and nonzero at $s=1$ (Corollary 2.2.4).

The analytic class number formula then says that

$$\prod_{\substack{\chi\in X\\ \chi\neq\chi_0}}L(1,\chi)=\frac{2^{r_1}(2\pi)^{r_2}h_KR_K}{\omega_K\sqrt{|d_K|}}=\xi_Kh_K$$

where

$$\xi_K=\frac{2^{r_1}(2\pi)^{r_2}R_K}{\omega_K\sqrt{|d_K|}}\in\mathbb{R}. \tag{2.3.1}$$

We note that if $K/\mathbb{Q}$ is Galois, then either all embeddings are real or all of them are complex, and so either r_1 or r_2 will be zero. Further, if K is totally imaginary ($r_1=0$) then K has a unique complex conjugation automorphism which we will denote cc. This is characterized by the fact that for every conjugate pair of complex embeddings σ and $\bar\sigma$ and for every $\alpha\in K$,

$$\sigma(cc(\alpha))=\bar\sigma(\alpha).$$

Example 2.3.4. Suppose we want to compute the class number of $K=\mathbb{Q}(i)$. Since K is an imaginary quadratic field, it has $r_1=0$ real and $2r_2=2$ complex embeddings, so the rank of the unit group is $r = r_1 + r_2 - 1 = 0$. Then we have no fundamental units and thus no lattice; R_K is defined to be 1 in this case. The roots of unity in $\mathbb{Q}(i)$ are $\{\pm 1, \pm i\}$, so $\omega_K = 4$, and the discriminant of K is $d_K = -4$ since K is a quadratic field of the form $\mathbb{Q}(\sqrt{d})$ for $d \equiv 3 \bmod 4$ [11, Proposition 13.1.2].

Then

$$\xi_{\mathbb{Q}(i)} = \frac{2^{r_1}(2\pi)^{r_2} R_K}{\omega_K \sqrt{|d_K|}} = \frac{2^0(2\pi)^1 \cdot 1}{4\sqrt{|-4|}} = \frac{\pi}{4}$$

and

$$\zeta_{\mathbb{Q}(i)}(s) = \prod_{\substack{\chi \in X \\ \chi \neq \chi_0}} L(1, \chi) = L(1, \chi)$$

for the nontrivial character $\chi = \left(\frac{d_K}{\ell}\right) = \left(\frac{-4}{\ell}\right)$ of K. As an infinite sum, $L(1, \chi)$ is difficult to compute. In Marcus [16], Theorems 46 and 47 give formulae for computing $L(1, \chi)$. Using them we can compute that in this case

$$|L(1, \chi)| = \frac{\pi}{|2 - \chi(2)| \sqrt{|d_K|}} |\chi(1)| = \frac{\pi}{2\sqrt{4}} \cdot 1 = \frac{\pi}{4}$$

since $\chi(1) = 1$ as usual and $\chi(2) = 0$. Then $h_{\mathbb{Q}(i)} = 1$. (Recall that $\mathcal{O}_K = \mathbb{Z}[i]$ has unique factorization, so this is expected.)

2.4 Abelian varieties and isogeny

Most of the material in this section can be found in Silverman's books [21, 20]. Additional information about generalizations to abelian varieties can be found in Milne's Abelian Varieties [17].

An *abelian variety* X of dimension g over a field k is a reduced and irreducible projective variety with a (commutative) group structure. It has an *endomorphism ring*,

$$\mathrm{End}(X) = \{\phi : X \to X | \phi \text{ is a homomorphism}\}.$$

Then $\mathrm{End}(X) \otimes \mathbb{Q}$ is an algebra, and we call it the *endomorphism algebra* of X.

An endomorphism of an abelian variety X induces a homomorphism on the group of points of X. Many of the endomorphisms have the following form. For $m \in \mathbb{Z}$, consider the associated multiplication by m map $[m] : X \to X$ where for $P \in X$, $[m] : P \mapsto mP = P + \cdots + P$. Each map $[m]$ is an endomorphism of X, and we have the following lemma.

Lemma 2.4.1. *[21] For X/k, $\mathbb{Z} \hookrightarrow End_k(X)$.*

Denote the group of points of order dividing m on X by $X[m]$. For a prime $\ell \nmid \mathrm{char}(k)$, we define the *$\ell$-adic Tate module* on X,

$$T_\ell(X) = \varprojlim_n X[\ell^n](\bar{k}), \tag{2.4.1}$$

a free $\mathbb{Z}_\ell$ module of rank $2g$ [17]. Then $\mathrm{End}(T_\ell(X))$ is contained in a matrix ring of dimension $2g$ and we can consider a map

$$\mathrm{End}(X) \longrightarrow \mathrm{End}(T_\ell(X)) \tag{2.4.2}$$

which is in fact a homomorphism of rings.

Some abelian varieties have endomorphisms that are not a multiplication-by-m map; consider the following example.

Example 2.4.2. An abelian variety of dimension one over k is an elliptic curve. If $\mathrm{char}(k) \neq 2, 3$, it has an affine equation of the form $y^2 = f(x)$ where $f(x)$ is a cubic polynomial. The elliptic curve over $\mathbb{C}$ with affine equation

$$E : y^2 = x^3 - x$$

has the extra endomorphism $(x, y) \mapsto (-x, iy)$ so $\mathbb{Z} \subsetneq \mathrm{End}_{\mathbb{C}}(E)$. In fact

$$\mathrm{End}_{\mathbb{Q}(i)}(E) = \mathrm{End}_{\mathbb{C}}(E) = \mathbb{Z}[i].$$

If an elliptic curve E is such that $\mathrm{End}(E) \neq \mathbb{Z}$, we say E has *complex multiplication.* Then in the previous example, we say that E has complex multiplication by $\mathbb{Z}[i]$. In fact, we can say something general about what the endomorphism ring of an elliptic curve can be.

Proposition 2.4.3. *[21] For E/k with $\mathrm{char}(k) = 0$, $End_k(E)$ is either $\mathbb{Z}$ or an order in a quadratic imaginary field.*

If K is a quadratic imaginary field, recall that an *order* is a subring $\mathcal{O}$ of K, finitely generated as a $\mathbb{Z}$-module, such that $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K (i.e., $\mathcal{O} \otimes \mathbb{Q} = K$). All orders of K are subrings of $\mathcal{O}_K$, the ring of integers of K and the maximal order of K.

We can define maps between abelian varieties of any dimension.

Definition 2.4.4. Let X_1, X_2 be abelian varieties of dimension g over k. A homomorphism $\phi : X_1 \to X_2$ is an *isogeny* if ϕ is surjective and nontrivial. We say the varieties X_1 and X_2 are *isogenous* if there exists an isogeny $\phi : X_1 \to X_2$.

Then isogeny induces an equivalence relation on the set of abelian varieties of dimension g. For elliptic curves over k with complex multiplication, the following proposition gives us a way to easily distinguish between the equivalence classes (called *isogeny classes*).

Proposition 2.4.5. *[20, Chapter II] Over a field of characteristic zero, two elliptic curves with complex multiplication are isogenous if and only if their endomorphism rings are orders in the same quadratic imaginary field.*

In this sense, a quadratic imaginary field K completely determines an isogeny class of elliptic curves over k. Over a field like $\mathbb{C}$, there are infinitely many elliptic curves in each isogeny class. However, if we are interested in elliptic curves with endomorphism ring exactly $\mathcal{O}_K$ there are only finitely many of them.

Theorem 2.4.6. *[21, Appendix C §11] Let K be a quadratic imaginary field with maximal order $\mathcal{O}_K$ and class number h_K. Then*

$$h_K = \#\mathcal{CL}(\mathcal{O}_K) = \#\left\{\textit{isomorphism classes of elliptic curves with End}(E) = \mathcal{O}_K\right\}.$$

For higher dimension abelian varieties over fields of characteristic zero, much of the story is the same. Suppose that an abelian variety X over k of dimension $g > 1$ has $\mathrm{End}_k(X) \cong \mathcal{O}$ with $\mathcal{O} \otimes \mathbb{Q} \cong K$ ($\mathcal{O}$ is an order in K) for some totally imaginary number field K of degree $2g$ over $\mathbb{Q}$. Then we say that X has complex multiplication by $\mathcal{O}$ and the isogeny class of X is determined by the action of $\mathcal{O}$ on the Lie algebra of X (a $g-$dimensional vector space over $\mathbb{C}$). Two abelian varieties with complex multiplication by orders in the same imaginary number field K are isogenous. (This statement is false if we remove the complex multiplication assumption.) Again, over $\mathbb{C}$, the isogeny class is infinite, but only finitely many abelian varieties have $\mathrm{End}_k(X) \cong \mathcal{O}_K$.

On the other hand, any abelian variety X of dimension g over a finite field $\mathbb{F}_q$ has an extra endomorphism in the form of a Frobenius element. By the representation of $\mathrm{End}(X)$ on $\mathrm{End}(T_\ell(X))$ (as in (2.4.2)), we can associate to the Frobenius endomorphism an element of $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ (see section 7.1). Certainly the characteristic polynomial of such a matrix has degree $2g$ and $\mathbb{Z}_\ell$-coefficients. Then we use Tate's theorem to determine the isogeny classes of abelian varieties of any dimension.

Theorem 2.4.7 (Tate,[22])**.** *Two abelian varieties of dimension g over $\mathbb{F}_q$ are isogenous if and only if their Frobenius elements are conjugate over $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$.*

In fact, the characteristic polynomial $f(T)$ of the matrix of Frobenius has $\mathbb{Z}$-coefficients, and the polynomial is independent of the choice of ℓ. The size of the reciprocal roots of $f(T)$ are given by the Weil conjectures [21, Theorem V.2.2], and so the coefficients of f are bounded independent of ℓ.

In the case of elliptic curves, the characteristic polynomial of the matrix of Frobenius is the quadratic polynomial $T^2 - a_q T + q$ with $a_q = q + 1 - \#E(\mathbb{F}_q)$ [21], which encodes the number of points on the curve. An abelian surface has a polarization which forces the matrix representation of the Frobenius element to lie in GSp_4 (section 7.1). Then its characteristic polynomial has the form

$$f(T) = T^4 + aT^3 + bT^2 + aqT + q^2 \in \mathbb{Z}[T]$$

(Lemma 6.2.2) with exactly two free coefficients a and b such that

$$|a| \leq 4\sqrt{q} \quad \text{and} \quad 2\,|a|\,\sqrt{q} - 2q \leq b \leq \frac{a^2}{4} + 2q.$$

These conditions (which stem from the Weil conjectures) ensure that f is a Weil polynomial, and in fact a possible characteristic polynomial of Frobenius [15, Lemma 2.1].

For most matrices, the characteristic polynomial is enough to determine its conjugacy class, so Tate's theorem gives us a connection between the conjugacy classes of the matrix groups $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r)$ and the isogeny classes of abelian varieties of dimension g over a finite field $\mathbb{F}_q$ with complex multiplication by orders in K. The following unpublished theorem of Everett Howe gives a formula for the number of abelian varieties with complex multiplication by the maximal order, a subset of the full isogeny class; we will eventually compare this to the sizes of conjugacy classes in $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r)$.

Theorem 2.4.8 (Howe,[10]). *Suppose K is an imaginary field of degree $2g$ over $\mathbb{Q}$. The set of isomorphism classes of principally polarized abelian varieties of dimension*

g with complex multiplication by the maximal order in K has cardinality h_K/h_{K^+}, where K^+ is the (unique) maximal totally real subfield of K.

This result generalizes Theorem 2.4.6 from elliptic curves to higher dimensional abelian varieties. A special case appears in [3] as Corollary 3.2.

3. MOTIVATION AND OVERVIEW: A THEOREM OF GEKELER

Gekeler [9] was interested in the number of isomorphism classes of elliptic curves $E/\mathbb{F}_p$ with a fixed number of points. Since the trace of Frobenius encodes this information, he reinterpreted the problem in terms of determining the proportion of matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with a given trace and determinant out of the "expected" number of elements with fixed trace and determinant. In 2009, Katz included a reformulation of Gekeler's work in [12]. In the notation of Katz, what Gekeler computed was the limit of a sequence of ratios

$$\nu_\ell(A,Q) = \lim_{r\to\infty} \frac{\#\left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r) \,|\, \operatorname{tr}\gamma \equiv A \bmod \ell^r, \det\gamma \equiv Q \bmod \ell^r\right\}}{\ell^{-r}\#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)},$$

where $A, Q \in \mathbb{Z}$ and $A^2 - 4Q < 0$. Gekeler proved that for each $\ell \nmid A^2 - 4Q$, this quantity $\nu_\ell(A,Q)$ is the ℓ^{th} Euler factor of the L-series $L(1,\chi)$ of the quadratic character χ. (In Gekeler's context, χ was the quadratic residue symbol associated to $A^2 - 4Q$.)

For our purposes, notice that the $L(1,\chi)$ in Gekeler's result occurs in the class number formula (Theorem 2.3.3)

$$\xi_K h_K = \prod_{\substack{\chi\in X\\ \chi\neq\chi_0}} L(1,\chi) = L(1,\chi)$$

for an imaginary quadratic field $K = \mathrm{Split}(T^2 - AT + Q)$ which has $X = \{\chi_0, \chi\}$. Recall Theorem 2.4.6 which says that h_K gives the size of the set of isomorphism classes of elliptic curves with complex multiplication by the maximal order in the field K.

In this paper we determine the conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ and $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$, reproduce Gekeler's result for elliptic curves, interpret it in terms of the size of this set, and then extend the heuristic to abelian surfaces using the following sequence of ideas.

Let $f(T) \in \mathbb{Z}[T]$ be monic of degree $2g$ and irreducible over $\mathbb{Q}$ such that f is a possible characteristic polynomial of the Frobenius endomorphism of an abelian variety over $\mathbb{F}_q$. Such an f has a totally imaginary splitting field $K = \mathrm{Split}(f)$; additionally, choose f so that $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. Then K has a unique maximal totally real subfield, which we will denote K^+.

The field K defines an isogeny class of abelian varieties $X/\mathbb{F}_q$ of dimension g with complex multiplication by an order in K. The theorem of Howe (Theorem 2.4.8) computes the number of elements of this isogeny class with complex multiplication by the maximal order $\mathcal{O}_K$ as h_K/h_{K^+}, the ratio of the class numbers of K and K^+.

The polynomial f also defines, for each odd prime ℓ and positive integer r, a set of matrices γ of $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r)$ with characteristic polynomial $\mathrm{charpol}(\gamma) \equiv f \bmod \ell^r$ that satisfy a correspondence with $f \bmod \ell$. We can find the size of such a set (a union of conjugacy classes), and then ask how much more often than we expect such a matrix occurs in $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r)$.

Then one might hope these two quantities, the size of the set of abelian varieties of dimension g over a finite field with complex multiplication by $\mathcal{O}_K$ and the excess probability that a matrix $\gamma \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r)$ has a fixed characteristic polynomial, might be related, as the diagram below shows.

$$\begin{tikzcd}
\mathrm{Frob}_q \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & f \arrow[r, leftrightarrow] & K = \mathrm{Split}(f) \arrow[d, leftrightarrow] \\
\# \left\{ \begin{array}{c} \gamma \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r) \text{ which} \\ \text{correspond to } f \bmod \ell \end{array} \right\} \arrow[d, leftrightarrow] & & \# \left\{ \begin{array}{c} \text{Abelian surfaces with} \\ \text{complex multiplication} \\ \text{by } \mathcal{O}_K \end{array} \right\} \arrow[d, leftrightarrow] \\
\text{Excess proportion for } \ell \arrow[rr, leftrightarrow, dashed] & & \dfrac{h_K}{h_{K^+}}
\end{tikzcd}$$

As in section 2.2, a totally imaginary number field K and its maximal real subfield K^+ each have a group of characters

$$X = \left\{\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times\right\} \quad \text{and} \quad X^+ = \left\{\chi : \mathrm{Gal}(K^+/\mathbb{Q}) \to \mathbb{C}^\times\right\};$$

notice that since $\mathrm{Gal}(K/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K^+/\mathbb{Q})$, $X^+ \subset X$. Recall from equation (2.3.1) that

$$\xi_K = \frac{2^{r_1}(2\pi)^{r_2} R_K}{\omega_K \sqrt{|d_K|}}$$

and let $\xi = \xi_K/\xi_{K^+}$. Then to compute the size of the set of abelian varieties with complex multiplication by $\mathcal{O}_K$ using Theorem 2.4.8, we evaluate

$$\frac{h_K}{h_{K^+}} = \frac{\xi_{K^+}}{\xi_K} \frac{\prod_{\substack{\chi \in X \\ \chi \neq \chi_0}} L(1,\chi)}{\prod_{\substack{\chi \in X^+ \\ \chi \neq \chi_0}} L(1,\chi)} = \frac{1}{\xi} \prod_{\chi \in X \smallsetminus X^+} L(1,\chi) = \frac{1}{\xi} \prod_{\chi \in X \smallsetminus X^+} \prod_{\ell} \frac{1}{1 - \frac{\chi(\ell)}{\ell}}. \qquad (3.0.1)$$

Thus, we need to evaluate the characters $\chi \in X \smallsetminus X^+$ on the primes of $\mathbb{Z}$.

Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and for any rational prime ℓ consider its factorization in K. Recall that for each prime $\lambda \subset \mathcal{O}_K$ lying above an unramified prime ℓ there is an element of G called the Frobenius element, and they are all conjugate in G. Since

G is abelian, these automorphisms are independent of λ and there is a well-defined Frobenius element $\mathrm{Frob}_K(\ell)$ associated with ℓ. This automorphism generates the Galois group of the extension of residue fields over ℓ (Theorem 2.1.7). The order of $\mathrm{Frob}_K(\ell)$ is the residue degree $f(\lambda/\ell)$ and thus encodes information about the splitting of ℓ in subfields of K. Then we define $\chi(\ell) = \chi(\mathrm{Frob}_K(\ell))$ for all odd unramified primes ℓ, and $\chi(\ell) = 0$ if ℓ is ramified in the field corresponding to χ (as in section 2.2).

Recall that we have $K = \mathrm{Split}(f)$ and so there exists some primitive element α with $\mathrm{minpol}(\alpha) = f(T) \in \mathbb{Z}[T]$ such that $K = \mathbb{Q}(\alpha)$. Then $\mathbb{Z}[\alpha]$ is a finite index subgroup of $\mathcal{O}_K$ as both are free abelian groups of rank $[K : \mathbb{Q}]$. For a rational prime we can find the polynomial $\bar{f}(T) \in \mathbb{F}_\ell[T]$ by reducing each coefficient of f mod ℓ. Then we have the following relationship.

Proposition 3.0.1. *[16, Theorem 27] Let f,$\bar{f}$, α, and K be as above and suppose $\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then the polynomial $\bar{f}(T)$ factors uniquely in $\mathbb{F}_\ell[T]$ as*

$$\bar{f}(T) = \bar{g_1}^{e_1} \bar{g}_2^{e_2} \dots \bar{g}_r^{e_r}$$

with each $\bar{g}_i$ a distinct monic irreducible element of $\mathbb{F}_\ell[T]$. Construct the distinct prime ideals $\lambda_i = (\ell, \bar{g}_i(\alpha)) \subset \mathcal{O}_K$. Then

$$\ell\mathcal{O}_K = \lambda_1^{e_1} \lambda_2^{e_2} \dots \lambda_r^{e_r}$$

and $f(\lambda_i/\ell) = f_i = \deg \bar{g}_i$.

In the cases we are concerned with, $[K : \mathbb{Q}] = 2$ or 4, and the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is 1, 2, or 4. Since we only consider odd primes ℓ, the condition $\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is unrestrictive for our purposes.

This proposition gives a bijection between the factorization of a prime element and the reduction of the polynomial that generated the field K; it will be used extensively in chapters 5 and 7.

For a fixed f we need to compute the number of elements γ of $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$ which correspond to $f \bmod \ell$. In most cases, $f \bmod \ell$ defines a unique conjugacy class $\mathcal{C}(f \bmod \ell)$ of all elements $\gamma \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$ with $\mathrm{charpol}(\gamma) \equiv f \bmod \ell$, and we can usually tell which class by the factorization of $f \bmod \ell$. (The extra information we may need is the eigenspace decomposition of an associated γ; see section 6.2 for more details.) Then counting the number of elements which are related to $f \bmod \ell$ is the same as finding the order of an appropriate union of conjugacy classes.

Proposition 3.0.1 will be used to connect a conjugacy class $\mathcal{C}$ to a prime ℓ in the following way. A factorization of a prime ℓ in the number field $K = \mathrm{Split}(f)$ corresponds to a factorization of $f \bmod \ell$ and has an associated ring $\mathcal{O}_K/\ell$ which is a vector space over $\mathbb{Z}/\ell = \mathbb{F}_\ell$. Then the factorization of $f \bmod \ell$ and the action of complex conjugation on the Frobenius element of $\mathcal{O}_K$ will define a (union of) conjugacy classes $\mathcal{C}(f \bmod \ell) \subset \mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$ which have characteristic polynomial $f \bmod \ell$.

Then, using centralizer orders, we can compute the sizes of the conjugacy classes $\mathcal{C}(f \bmod \ell)$. Once we understand these classes and their centralizers over $\mathbb{F}_\ell$, we can lift them to $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r)$.

We will then compute the proportion of these elements out of an "average" or "expected" number of $\gamma \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r)$ with a fixed characteristic polynomial f. In the case of elliptic curves we have $f = T^2 - aT + b$, and the "expected" number of matrices of $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ with this characteristic polynomial is approximated by $\ell^{-r}\#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)$. In this case, $\#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)$ is the number of matrices with a fixed determinant mod ℓ^r and then we normalize by ℓ^{-r} for the ℓ^r possible traces in $\mathbb{Z}/\ell^r$. More generally, this averaging term will be

$$\ell^{-nr}\#\,\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^r), \tag{3.0.2}$$

where $n+1$ is the number of free coefficients in the characteristic polynomial f of degree $2g$. Then we compute

$$\frac{\#\left\{\gamma \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^r) \middle| \operatorname{charpol}(\gamma) \equiv f \bmod \ell^r\right\}}{\ell^{-nr}\ \#\,\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^r)}$$

for a fixed g and each $r \in \mathbb{N}$.

The correspondence between the prime ℓ and the conjugacy classes $\mathcal{C}(f \bmod \ell)$ lets us evaluate the characters in the product of L-series that occurs in the formula for h_K/h_{K^+}. Then for each ℓ, we compute the ℓ^{th} Euler factor of equation (3.0.1), and compare this factor to the proportion of matrices computed above. We will see that, up to the real constant $\xi = \xi_K/\xi_{K^+}$, they will match. Then we can compute the number of abelian varieties with complex multiplication by the maximal order of K by taking the product over all ℓ of these proportions (Theorems 5.2.2 and 8.0.3).

To proceed, we first determine the conjugacy classes of $\mathrm{GSp}_2(\mathbb{Z}/\ell^r) = \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ and find their centralizer orders in section 4. Then in chapter 5 we determine the correspondence between primes and conjugacy classes, compute the proportion of elements with a fixed characteristic polynomial, and show that it matches the appropriate Euler factor for any ℓ, reinterpreting the result in terms of the size of a set of elliptic curves. Chapters 6, 7, and 8 contain the analogous results for $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ and abelian surfaces.

Remark 3.0.2. It should be noted that we will restrict to the matrices γ which are cyclic mod ℓ^r. The number of matrices with a given characteristic polynomial which are not cyclic is small relative to the total number of such matrices. See Appendix A for a calculation in $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ which says that if we include non-cyclic matrices with a fixed characteristic polynomial which happens to have repeated roots mod ℓ, there is a failure of matching between the proportion of matrices with this characteristic polynomial and the corresponding Euler factor.

4. THE CONJUGACY CLASSES OF $\mathrm{GL}_2(\mathbb{Z}/\ell^{\mathrm{r}})$

The conjugacy classes of $\mathrm{GL}_n(k)$, where k is a field, are well-understood as they are entirely characterized by their rational canonical form (RCF). The RCF of a matrix is data about the factorization of its characteristic polynomial together with partition data for repeated factors, and most importantly relies on the fact that $k[X]$ is a unique factorization domain ([8],[13],[27]). For example, RCF allows us to distinguish between

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

which both have characteristic polynomial $(T-2)^2$ but are not conjugate. In [27] (based on work of Fulman and Kung), we determined in which conjugacy class an element of $\mathrm{GL}_n(\mathbb{F}_q)$ belonged based on the irreducible components of its characteristic polynomial, their multiplicities, and the size of the corresponding blocks in its rational canonical form.

To review the construction of a matrix γ in rational canonical form, suppose $\mathrm{charpol}(\gamma) = \prod_{i=1}^{t} f_i(T)^{n_i}$ with all $n_i > 0$ and each $f_i(T)$ monic, distinct and irreducible. Clearly $n = \deg \mathrm{charpol}(\gamma) = \sum_{i=1}^{t} n_i \deg f_i$. We correspond to each f_i a partition $P_i = [p_{(i,1)}, p_{(i,2)}, \ldots, p_{(i,s)}]$ of n_i, so $\sum_j p_{(i,j)} = n_i$. Then the matrix $\gamma \in \mathrm{GL}_n(k)$ has a block of dimension $p_{(i,j)} \deg f_i$ corresponding to the irreducible polynomial f_i for each pair (i,j), and the set of partitions $P = \{P_1, P_2, \ldots, P_t\}$ together with the factorization of $\mathrm{charpol}(\gamma)$ uniquely defines a conjugacy class of $\mathrm{GL}_n(k)$. (See, for example, Chapter 12.2 of [5], for a complete treatment of RCF.)

With this notation, reconsider the above example. The partitions associated to the polynomial $T-2$ are $[1,1]$ in the first case (two blocks of size $1 \cdot \deg(T-2) = 1$) and $[2]$ in the second case (one block of size $2 \cdot \deg(T-2) = 2$).

For the specific case when $n = 2$ and $k = \mathbb{F}_\ell$, the following are all of the possible conjugacy classes.

Case 1: Regular semisimple elements

The regular semisimple elements are those with distinct roots over $\bar{\mathbb{F}}_\ell$.

- (**Split**) $\operatorname{charpol}(\gamma) = (T-a)(T-b)$ with $a \neq b \in \mathbb{F}_\ell^\times$. The partitions associated with each factor are $[1]$ (we denote the set of partitions by $\{[1],[1]\}$) so there is one block of size one for each factor of $\operatorname{charpol}(\gamma)$). Such a matrix has a representative $\left(\begin{smallmatrix} a & \\ & b \end{smallmatrix}\right)$. There are $\frac{1}{2}(\ell-1)(\ell-2)$ of these conjugacy classes.

- (**Nonsplit**) $\operatorname{charpol}(\gamma) = T^2 - aT + b$ with $T^2 - aT + b$ irreducible over $\mathbb{F}_\ell$. The partition associated with the irreducible factor is $[1]$ since it occurs with multiplicity one. Then the class has a representative $\left(\begin{smallmatrix} 0 & 1 \\ -b & a \end{smallmatrix}\right)$, which notice has one block of size $2 = \deg \operatorname{charpol}(\gamma)$. The number of irreducible monic polynomials of degree two, and thus the number of **Nonsplit** conjugacy classes, is $\frac{1}{2}\ell(\ell-1)$.

Case 2: Non-regular elements

These elements have repeated roots over $\mathbb{F}_\ell$, and so there is only one possible factorization of $\operatorname{charpol}(\gamma)$.

- (**RL**) (Repeated Linear) $\operatorname{charpol}(\gamma) = (T-a)^2$ with $a \in \mathbb{F}_\ell^\times$. Since the multiplicity of the irreducible factor is two there are two possible partitions, $[1,1]$ and $[2]$. Then there are $\ell - 1$ of each of the following class types.
  - If the partition is $[1,1]$, the representative has two blocks of dimension $1 \cdot \deg(T-a) = 1$, which is the matrix $\left(\begin{smallmatrix} a & \\ & a \end{smallmatrix}\right) = aI$. We will denote this class by **RL**[1,1], and we comment that these matrices are not cyclic (see Definition 4.2.1).

– If instead the partition is [2], the representative has one block of size $2 \cdot \deg(T - a) = 2$. In RCF, the matrix is $\left(\begin{smallmatrix} a & 1 \\ & a \end{smallmatrix}\right)$. This class will be called **RL**[2], and it should be noted that although $\operatorname{charpol}(\gamma)$ has a repeated root, the matrices in this class are cyclic.

4.1 The problem

Now let R be a local, possibly Artinian, ring. To determine in what conjugacy class an element of $\mathrm{GL}_2(R)$ belongs we need a new tactic as $R[X]$ is not necessarily a unique factorization domain. One interesting effect of this is that we cannot always distinguish conjugacy classes of this group based on their characteristic polynomial, as the following examples illustrate.

Example 4.1.1. Let $R = \mathbb{Z}_3/(3^2\mathbb{Z}_3) \cong \mathbb{Z}/9$ and consider $\mathrm{GL}_2(\mathbb{Z}/9)$. Let $A = \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 7 & 1 \\ & 4 \end{smallmatrix}\right)$. Then $\operatorname{charpol}(A) = (x-1)^2$ and $\operatorname{charpol}(B) = (x-4)(x-7)$ but notice that $\operatorname{charpol}(A) = x^2 - 2x + 1 \equiv \operatorname{charpol}(B) \bmod 9$. We would like to believe that these two matrices are in different conjugacy classes since it would seem that A has a repeated "eigenvalue" and B has distinct "eigenvalues" in R. However, if $C = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)$,

$$CAC^{-1} = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 27 & 4 \end{pmatrix} \equiv \begin{pmatrix} 7 & 1 \\ 0 & 4 \end{pmatrix} \bmod 9 = B$$

and so A is conjugate to B.

Remark 4.1.2. Throughout the paper we shall use the notation $A \sim_G B$ to mean that matrix A is conjugate (similar) to matrix B in the group G. When the group is clear, we will shorten this to $A \sim B$.

Example 4.1.3. Assume $R = \mathbb{Z}_5/(5^2\mathbb{Z}_5) \cong \mathbb{Z}/25$. Let $A = \left(\begin{smallmatrix} 1 & 5 \\ 15 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 5 \\ 10 & 1 \end{smallmatrix}\right)$. Then $\operatorname{charpol}(A) = \operatorname{charpol}(B) = x^2 - 2x + 1$, however these matrices are not conjugate. Let $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then A and B are conjugate by C if and only if

$$AC - CB = \begin{pmatrix} 5c - 10b & 5d - 5a \\ 15a - 10d & 15b - 5c \end{pmatrix} \equiv 0 \bmod 25$$

which is true if and only if $\left(\begin{smallmatrix} c-2b & d-a \\ 3a-2d & 3b-c \end{smallmatrix}\right) \equiv 0 \bmod 5$. These conditions are met if and only if all of a, b, c, d are multiples of 5 in $\mathbb{Z}/25$, and therefore C is not invertible ($C \notin \mathrm{GL}_2(\mathbb{Z}/25)$). Thus, A and B are not conjugate over $\mathrm{GL}_2(\mathbb{Z}/25)$. (We will see a much simpler reason for this in section 4.2.1.)

Because we cannot use the factorizations of characteristic polynomials or rational canonical forms in order to identify which conjugacy class a matrix belongs to in $\mathrm{GL}_2(R)$ for R not a field, we need to find another way to classify the matrices in this group.

4.2 A classification

We will rely on the constrained structure of the elements of $\mathrm{GL}_2(R)$ to find purchase on our problem. In this section we describe a decomposition of these elements that appears in [1], and give some basic results about the number of conjugacy classes of $\mathrm{GL}_2(R)$ and their representatives. The following definitions will be pivotal in this description.

Definition 4.2.1. A matrix $A \in \mathrm{GL}_n(R)$ is called *cyclic* if there exists some $v \in R^n$ such that

$$\{v, Av, A^2v, \dots, A^{n-1}v\}$$

is a basis for R^n. A matrix $B \in \mathrm{GL}_n(R)$ is called *scalar* if $B = dI$ for some $d \in R^\times$ where I is the identity matrix of $\mathrm{GL}_n(R)$. We call a conjugacy class *scalar* if the elements of the class are scalar. All other conjugacy classes are called *nonscalar*.

In particular, if $\alpha \in \mathrm{GL}_2(R)$ is cyclic with trace τ and determinant δ, then there exists some vector v such that $\{v, \alpha v\}$ is a basis for the R-module. Then if we rewrite α in this basis, we get a matrix $C = \left(\begin{smallmatrix} 0 & 1 \\ a & b \end{smallmatrix}\right)$ where $a, b \in R$. Since C is in the same conjugacy class as α, they must have the same trace and determinant and so

$$\tau := \operatorname{tr} \alpha = \operatorname{tr} \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} = b \quad \text{and} \quad \delta := \det \alpha = \det \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} = -a.$$

Then C is the companion matrix $\left(\begin{smallmatrix} 0 & 1 \\ -\delta & \tau \end{smallmatrix}\right)$ and any cyclic matrix is similar to a matrix of this form [5].

4.2.1 An overview of Section 2 of Avni, et al

In [1], the authors determine and enumerate the similarity classes of $\mathrm{Mat}_3(R)$, the ring of 3×3 matrices over a local principal ideal ring R. As an introduction to their method, they begin by describing the similarity classes of $\mathrm{Mat}_2(R)$; this is the classification in which we are interested.

Let R be a local principal ideal commutative ring with maximal ideal $\mathfrak{m} = (\mu)$. Let $\mathbb{F} = R/\mathfrak{m}$ be the residue field and $u \in \mathbb{N} \cup \{\infty\}$ be the *length* of the ideal $\mathfrak{m}$ (i.e., let u be the smallest positive integer for which $\mathfrak{m}^u = 0$). For $1 \leq i \leq u$ let $R_i := R/\mathfrak{m}^i$. Fix a section $\mathbb{F} = R_1 \hookrightarrow R$ which maps zero to zero with image $F_1 \subset R$. Then define compatible sections $R_i \hookrightarrow R$ for all $1 \leq i < u$ where R_i is identified with $F_i := \left\{ \sum_{j=0}^{i-1} a_j \mu^j | a_j \in F_1 \right\} \subset R$ as sets. We define F_0 to be $\{0\}$.

The key to the following description of the conjugacy classes of $\mathrm{GL}_2(R)$ is the fact that any element of $\mathrm{GL}_2(\mathbb{F})$ is either a scalar matrix or a cyclic matrix.

Lemma 4.2.2. *[1, Lemma 2.1] Any element $\alpha \in \mathrm{Mat}_2(R)$ can be written in the form $\alpha = dI + \mu^j \beta$ with $j \in \{0, \ldots, u\}$ maximal such that α is congruent to a scalar matrix modulo $\mathfrak{m}^j$, with unique $d \in F_j$ and unique $\beta \in \mathrm{Mat}_2(R_{u-j})$ cyclic.*

Proof. The only thing that needs to be shown is that β is cyclic. Let $\overline{x} := x \bmod \mathfrak{m}$. Let $M = R_{u-j} \oplus R_{u-j}$ a R_{u-j}-module, and identify $\mathrm{Mat}_2(R_{u-j})$ with $\mathrm{End}(M)$. The maximality of j implies that β is not scalar mod $\mathfrak{m}$. Then $\overline{\beta} = \beta \bmod \mathfrak{m} \in \mathrm{Mat}_2(\mathbb{F})$ is cyclic and thus there exists some $\overline{v} \in \overline{M}$ such that $\left\{\overline{v}, \overline{\beta}\overline{v}\right\}$ generates $\overline{M}$ (i.e., the smallest submodule of $\overline{M}$ stable under $\overline{\beta}$ is $\overline{M}$). Choose $v \in M$ such that $v \bmod \mathfrak{m} = \bar{v}$. Let N be the submodule of M generated by $\{v, \beta v\}$. Then

$$\overline{N} = \frac{N}{N \cap \mathfrak{m}M} \hookrightarrow \frac{M}{\mathfrak{m}M} = \overline{M}.$$

We have $N \subset M \Rightarrow \overline{N} \subset \overline{M}$ and $\overline{N} \neq 0$, but $\overline{M}$ was the smallest submodule of $\overline{M}$ stable under $\overline{\beta}$. Then we must have $\overline{N} = \overline{M}$ and by Nakayama's lemma, $N = M$. Thus we have $v \in M$ such that M is generated by $\{v, \beta v\}$, which implies that β is cyclic. □

Proposition 4.2.3. *A matrix $\alpha = dI + \mu^j\beta$ is similar to $\alpha' = d'I + \mu^j\beta'$ by an element of $\mathrm{GL}_2(R)$ if and only if $d = d'$ and β is similar to β' by an element of $\mathrm{Mat}_2(R_{u-j})$.*

Proof. First, suppose $d = d'$ and there exists a nonzero matrix $P \in \mathrm{Mat}_2(R_{u-j})$ such that $P\beta = \beta' P$. Lift P to an element of $\mathrm{Mat}_2(R)$. Then

$$\begin{aligned} P\alpha = &\ P(dI + \mu^j\beta) = dP + \mu^j P\beta \\ \alpha' P = &\ (d'I + \mu^j\beta')P = d'P + \mu^j\beta' P = dP + \mu^j P\beta \end{aligned}$$

so $P\alpha = \alpha' P$ which implies that $\alpha \sim \alpha'$.

Conversely, suppose that $\alpha \sim \alpha'$. Then there exists a $Q \in \mathrm{GL}_2(R)$ such that $Q\alpha = \alpha' Q$. Let $Q = eI + \mu^i\gamma$ as in Lemma 4.2.2 so that

$$\begin{aligned} Q\alpha =& (eI + \mu^i\gamma)(dI + \mu^j\beta) = edI + \mu^j e\beta + \mu^i d\gamma + \mu^{i+j}\gamma\beta \\ \alpha' Q =& (d'I + \mu^j\beta')(eI + \mu^i\gamma) = ed'I + \mu^j e\beta' + \mu^j d'\gamma + \mu^{i+j}\beta'\gamma. \end{aligned}$$

Since $Q\alpha = \alpha' Q$, we get $edI = ed'I$ which easily implies that $d = d'$. Then we have

$$\begin{aligned}
\mu^j e\beta + \mu^i d\gamma + \mu^{i+j}\gamma\beta &= \mu^j e\beta' + \mu^i d'\gamma + \mu^{i+j}\beta'\gamma \\
&= \mu^j e\beta' + \mu^i d\gamma + \mu^{i+j}\beta'\gamma \\
\implies \quad \mu^j e\beta + \mu^{i+j}\gamma\beta &= \mu^j e\beta' + \mu^{i+j}\beta'\gamma \\
[\mu^j(eI + \mu^i\gamma)]\beta &= \beta'[\mu^j(eI + \mu^i\gamma)] \\
[\mu^j Q]\beta &= \beta'[\mu^j Q]
\end{aligned}$$

and so we see that $\beta \sim \beta'$ via $\mu^j Q \in \mathrm{Mat}_2(R_{u-j})$, finishing the proof. □

Since we are working in only two dimensions, a companion matrix is uniquely determined by its determinant and trace as the characteristic polynomial of a 2×2 matrix β is $f(T) = T^2 - \mathrm{tr}(\beta)T + \det(\beta)$. Then, based on the previous proposition, the next theorem follows directly.

Theorem 4.2.4. *[1, Theorem 2.2] For any $\alpha \in \mathrm{Mat}_2(R)$, let j, d, β be as in Lemma 4.2.2. Then α is similar to the matrix*

$$dI + \mu^j \left(\begin{smallmatrix} 0 & 1 \\ -\det(\beta) & \mathrm{tr}(\beta) \end{smallmatrix}\right).$$

Thus the information $\{j, d, \mathrm{tr}(\beta), \det(\beta)\}$ completely determines a similarity class in $\mathrm{Mat}_2(R)$ or $\mathrm{GL}_2(R)$ with the condition that the similarity classes in $\mathrm{GL}_2(R)$ have $d \in F_j^\times$ for $j \geq 1$, or if $j = 0$ then $\det(\beta) \in R^\times$.

4.2.2 Enumerating similarity and conjugacy classes

Assume that the residue field $R/\mathfrak{m} = \mathbb{F}$ is finite of cardinality ℓ an odd prime. There are (at least) two ways to count the similarity classes of $\mathrm{GL}_2(R_i)$: One could count them directly via the previous theorem, or use a recursive approach.

Direct count

First, we count them simply using Theorem 4.2.4. Recall that $R_i = R/\mathfrak{m}^i$ and so $\# R_i = \ell^i$. Since any conjugacy class in $\mathrm{GL}_2(R_i)$ has a unique representative of the form $dI + \mu^j \left(\begin{smallmatrix} 0 & 1 \\ -\det(\beta) & \operatorname{tr}(\beta) \end{smallmatrix}\right)$, there are three (essentially) free variables for any choice of $j \in \{0, \dots, i\}$. Let ϕ denote the Euler totient function, and recall that when ℓ is prime, $\phi(\ell^r) = \ell^{r-1}(\ell - 1)$. Note that for F_r, $\phi(\ell^r)$ gives the number of units of the ring. For $\alpha = dI + \ell^j \beta$ in $\mathrm{GL}_2(R_i)$, we have $d \in F_j^\times$ when $j \geq 1$, and if $j = 0$ we have $d = 0$ and $\det \beta \in R_i^\times$ to guarantee invertibility. Recall that $\beta \in \mathrm{Mat}_2(R_{i-j})$ when $j \geq 1$. Consider the following table.

j	$\# d$	$\# \det \beta$	$\# \operatorname{tr} \beta$	Total classes
0	$\lvert\{0\}\rvert = 1$	$\phi(\ell^i) = \ell^{i-1}(\ell - 1)$	ℓ^i	$\ell^{2i-1}(\ell - 1)$
1	$\lvert F_1^\times \rvert = \lvert \mathbb{F}^\times \rvert = \ell - 1$	ℓ^{i-1}	ℓ^{i-1}	$\ell^{2i-2}(\ell - 1)$
2	$\lvert F_2^\times \rvert = \ell(\ell - 1)$	ℓ^{i-2}	ℓ^{i-2}	$\ell^{2i-3}(\ell - 1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i - 1$	$\lvert F_{i-1}^\times \rvert = \ell^{i-2}(\ell - 1)$	ℓ	ℓ	$\ell^i(\ell - 1)$
i	$\lvert F_i^\times \rvert = \ell^{i-1}(\ell - 1)$	1	1	$\ell^{i-1}(\ell - 1)$
			Sum =	$\sum_{n=i}^{2i} \phi(\ell^n)$

Then the total number of conjugacy classes in $\mathrm{GL}_2(R_i)$ is

$$\sum_{n=i}^{2i} \phi(\ell^n) = \sum_{n=i}^{2i} \ell^{n-1}(\ell - 1) = \ell^{2i} - \ell^{i-1}.$$

If instead we want to count the similarity classes of $\mathrm{Mat}_2(R_i)$, then we choose $d \in F_j$ and $\operatorname{tr}(\beta), \det(\beta) \in R_{i-j}$.

j	$\#d$	$\#\det\beta$	$\#\operatorname{tr}\beta$	Total classes
0	$\lvert\{0\}\rvert = 1$	ℓ^i	ℓ^i	ℓ^{2i}
1	$\lvert F_1\rvert = \lvert\mathbb{F}\rvert = \ell$	ℓ^{i-1}	ℓ^{i-1}	ℓ^{2i-1}
2	$\lvert F_2\rvert = \ell^2$	ℓ^{i-2}	ℓ^{i-2}	ℓ^{2i-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$i-1$	$\lvert F_{i-1}\rvert = \ell^{i-1}$	ℓ	ℓ	ℓ^{i+1}
i	$\lvert F_i\rvert = \ell^i$	1	1	ℓ^i
			Sum $=$	$\sum_{n=i}^{2i} \ell^n$

Then the total number of similarity classes of $\mathrm{Mat}_2(R_i)$ is $\sum_{n=i}^{2i} \ell^n = \ell^i \left(\frac{\ell^{i+1}-1}{\ell-1}\right)$.

Recursive approach

Next, we use a rather clever recursion (from [1]). Let $\eta : \mathrm{Mat}_2(R_{i+1}) \longrightarrow \mathrm{Mat}_2(R_i)$ be the natural reduction map, and let $\mathcal{C} \subset \mathrm{Mat}_2(R_i)$ be a similarity class. Then $\eta^{-1}(\mathcal{C})$ is a disjoint union of classes in $\mathrm{Mat}_2(R_{i+1})$. Since we are working in two dimensions, we only have two types of classes to track: the scalar classes, and the nonscalar classes. Let a_i be the number of scalar similarity classes and b_i be the number of nonscalar similarity classes in $\mathrm{Mat}_2(R_i)$. We use the map η^{-1} to determine what types of classes and how many of each lie above a class of $\mathrm{Mat}_2(R_i)$. To do this, we look at some "branching rules".

Remark 4.2.5. The following branching descriptions hold also in reducing elements of $\mathrm{GL}_2(R_{i+1})$ to $\mathrm{GL}_2(R_i)$ via η since any reduction of an invertible matrix is also invertible.

A scalar class in $\mathrm{Mat}_2(R_{i+1})$ can only reduce via η to a scalar class in $\mathrm{Mat}_2(R_i)$. Then $a_{i+1} = \ell a_i$.

A nonscalar class $\mathcal{C}$ in $\mathrm{Mat}_2(R_{i+1})$ could reduce to a scalar class of $\mathrm{Mat}_2(R_i)$ (in which case the class $\mathcal{C}$ is scalar mod μ^i but not mod μ^{i+1}), or to a nonscalar class of

$\mathrm{Mat}_2(R_i)$. If $\mathcal{C}$ lies over a scalar class $\bar{d}I$, there are ℓ^2 nonscalar lifts $dI + \mu^{i+1}\beta$ of dI with $\beta \in \mathrm{Mat}_2(R_1)$ since there are ℓ^2 cyclic matrices in $\mathrm{Mat}_2(R_1)$. If $\mathcal{C}$ lies over a nonscalar class represented by $dI + \mu^i\beta$, there are also ℓ^2 lifts since there are ℓ ways to lift each of the trace and determinant of β. Then $b_{i+1} = \ell^2 a_i + \ell^2 b_i$.

Then we have that

$$\begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix} = \begin{bmatrix} \ell & 0 \\ \ell^2 & \ell^2 \end{bmatrix} \begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} \ell a_i \\ \ell^2 a_i + \ell^2 b_i \end{bmatrix}$$

as a recurrence relation. We have initial values v_M and v_G for the similarity classes of $M = \mathrm{Mat}_2(R_1) = \mathrm{Mat}_2(\mathbb{F})$ and the conjugacy classes of $G = \mathrm{GL}_2(R_1) = \mathrm{GL}_2(\mathbb{F})$ from what we know about similarity classes over a field (see the beginning of chapter 4):

$$v_M = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} = \begin{bmatrix} \ell \\ \ell^2 \end{bmatrix} \qquad \text{and} \qquad v_G = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} = \begin{bmatrix} \ell - 1 \\ \ell^2 - \ell \end{bmatrix}.$$

Let $T = \left[\begin{smallmatrix} \ell & 0 \\ \ell^2 & \ell^2 \end{smallmatrix}\right]$. To find

$$\begin{bmatrix} a_i \\ b_i \end{bmatrix} = T^{i-1} \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}$$

we will use the following lemma, which follows by a simple calculation.

Lemma 4.2.6.

$$\textit{For} \;\; S = \begin{bmatrix} 1-\ell & 0 \\ \ell & 1 \end{bmatrix} \; \textit{and} \; D = \begin{bmatrix} \ell & \\ & \ell^2 \end{bmatrix}, \quad T = SDS^{-1}.$$

Then we compute

$$T^{i-1} = \left(SDS^{-1}\right)^{i-1} = SD^{i-1}S^{-1} = S \begin{bmatrix} \ell^{i-1} & \\ & (\ell^2)^{i-1} \end{bmatrix} S^{-1} = \begin{bmatrix} \ell^{i-1} & \\ \ell^i \left(\frac{\ell^{i-1}-1}{\ell-1}\right) & \ell^{2(i-1)} \end{bmatrix},$$

so for $\mathrm{GL}_2(R_i)$,

$$\begin{bmatrix} a_i \\ b_i \end{bmatrix} = T^{i-1}v_G = \begin{bmatrix} \ell^{i-1} & 0 \\ \ell^i\left(\frac{\ell^{i-1}-1}{\ell-1}\right) & \ell^{2i-2} \end{bmatrix} \begin{bmatrix} \ell-1 \\ \ell^2-\ell \end{bmatrix} = \begin{bmatrix} \ell^i-\ell^{i-1} \\ \ell^{2i}-\ell^i \end{bmatrix}.$$

The total number of conjugacy classes in $\mathrm{GL}_2(R_i)$ is the sum of these, or

$$(\ell^i-\ell^{i-1})+(\ell^{2i}-\ell^i)=\ell^{2i}-\ell^{i-1}.$$

Also, for $\mathrm{Mat}_2(R_i)$,

$$\begin{bmatrix} a_i \\ b_i \end{bmatrix} = T^{i-1}v_M = \begin{bmatrix} \ell^{i-1} & 0 \\ \ell^i\left(\frac{\ell^{i-1}-1}{\ell-1}\right) & \ell^{2i-2} \end{bmatrix} \begin{bmatrix} \ell \\ \ell^2 \end{bmatrix} = \begin{bmatrix} \ell^i \\ \ell^{i+1}\frac{\ell^i-1}{\ell-1} \end{bmatrix}.$$

The total number of similarity classes in $\mathrm{Mat}_2(R_i)$ is then

$$\ell^i+\ell^{i+1}\frac{\ell^i-1}{\ell-1}=\ell^i\left(\frac{\ell^{i+1}-1}{\ell-1}\right).$$

Notice that these values match those in the tables in the previous section.

4.3 The order of a conjugacy class of $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$

We have now seen how to determine the conjugacy classes of the group $\mathrm{GL}_2(R)$ for some local principal ideal commutative ring R. In [1], the authors only showed how to determine a representative for each conjugacy class and counted the total number of conjugacy classes. We would also like to find the number of elements in each of these conjugacy classes, and in fact we have two approaches to this enumerative problem.

In the language of the previous section, let $R=\mathbb{Z}_\ell$ for some ℓ an odd prime. Then $\mathfrak{m}=(\ell)$ and each $R_r=R/\mathfrak{m}^r=\mathbb{Z}_\ell/(\ell^r\mathbb{Z}_\ell)\cong\mathbb{Z}/\ell^r$, a finite ring of order ℓ^r. We also have $F_0 = \{0\}$, $F_1 \cong \mathbb{F}_\ell$, and for each $j > 1$,

$$F_j = \left\{ \sum_{i=0}^{j-1} a_i \ell^i | a_i \in F_1 \cong \mathbb{F}_\ell \right\} \leftrightarrow \mathbb{Z}_\ell/(\ell^j \mathbb{Z}_\ell) \cong \mathbb{Z}/\ell^j.$$

Each element of $\mathrm{GL}_2(R_r) = \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ can be written as $\alpha = dI + \ell^j\beta$ for some $j \in \{0, \ldots, r\}$, where $d \in F_j^\times = (\mathbb{Z}/\ell^j)^\times$, and $\beta \in \mathrm{Mat}_2(R_{r-j}) = \mathrm{Mat}_2(\mathbb{Z}/\ell^{r-j})$ cyclic. Let us return to our earlier examples (Examples 4.1.1 and 4.1.3) to see how our classification could be used.

Example 4.3.1 (Example 4.1.1, revisited)**.** Consider $\mathrm{GL}_2(\mathbb{Z}/9)$, so that $\ell = 3$ and $r = 2$. With our decomposition,

$$A = \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right) = 0I + 3^0 \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right) \quad \text{and} \quad B = \left(\begin{smallmatrix} 7 & 1 \\ & 4 \end{smallmatrix}\right) = 0I + 3^0 \left(\begin{smallmatrix} 7 & 1 \\ & 4 \end{smallmatrix}\right).$$

Then $\{j, d, \operatorname{tr}\beta, \det\beta\}_A = \{0, 0, 2, 1\}$ and $\{j, d, \operatorname{tr}\beta, \det\beta\}_B = \{0, 0, 11, 28\}$. But notice that $\{j, d, \operatorname{tr}\beta, \det\beta\}_B \equiv \{0, 0, 2, 1\} \bmod 9$ so since these sets of invariants match, the matrices A and B are in the same conjugacy class.

Example 4.3.2 (Example 4.1.3, revisited)**.** Working in $\mathrm{GL}_2(\mathbb{Z}/25)$, let $A = \left(\begin{smallmatrix} 1 & 5 \\ 15 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 5 \\ 10 & 1 \end{smallmatrix}\right)$. Then $\ell = 5$ and $r = 2$. Rewrite both matrices so that

$$A = 1I + 5^1 \left(\begin{smallmatrix} 0 & 1 \\ 3 & 0 \end{smallmatrix}\right) \quad \text{and} \quad B = 1I + 5^1 \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right).$$

Then $\{j, d, \operatorname{tr}\beta, \det\beta\}_A = \{1, 1, 0, -3\}$ and $\{j, d, \operatorname{tr}\beta, \det\beta\}_B = \{1, 1, 0, -2\}$ are not the same, so these matrices are not in the same conjugacy class.

Now we will use these representatives for the conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ to compute the size of each class. As an example, consider the smallest possible example, $\mathrm{GL}_2(\mathbb{Z}/\ell^2)$.

Example 4.3.3. A matrix in $\mathrm{GL}_2(\mathbb{Z}/\ell^2)$ has the form $dI + \ell^j\beta$ where $j \in \{0, 1, 2\}$

and $F_0 = \{0\}, F_1 \cong \mathbb{F}_\ell, F_2 = \{0, 1, \ldots, \ell^2 - 1\} \leftrightarrow \mathbb{Z}/\ell^2$. Since there are only three cases, let's consider them separately.

- First, let $j = 2$. This is perhaps the easiest case, because if $j = 2$ then $d \in (\mathbb{Z}/\ell^2)^\times$ and $\beta \in \mathrm{Mat}_2(F_0) = \mathrm{Mat}_2(0)$, so $\beta = (0)$ (i.e., these are the scalar matrices dI in $\mathrm{GL}_2(\mathbb{Z}/\ell^2)$). Each d determines its own conjugacy class, and so there are $\phi(\ell^2) = \ell(\ell - 1)$ of these "full scalar" classes, each with only itself in the class (since these are the elements of the center of $\mathrm{GL}_2(\mathbb{Z}/\ell^2)$).

- Now, let $j = 1$. A conjugacy class is determined by $d \in F_1^\times \cong \mathbb{F}_\ell^\times$ and cyclic $\beta \in \mathrm{Mat}_2(\mathbb{Z}/\ell) = \mathrm{Mat}_2(\mathbb{F}_\ell)$. There are $\ell - 1$ possible values of d and ℓ^2 different similarity classes of cyclic matrices in $\mathrm{Mat}_2(\mathbb{F}_\ell)$, so there are $\ell^2(\ell - 1)$ different conjugacy classes of elements that have the form $dI + \ell\beta$. To determine the number of elements in each of these classes, we will enumerate its centralizer and use the orbit-stabilizer theorem. Let $\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^r)}(\beta)$ denote the centralizer of β in $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$.

  Consider an element $\alpha = dI + \ell\beta$ and an element $A \in \mathrm{GL}_2(\mathbb{Z}/\ell^2)$. We can write $A = A_0 + \ell A_1$ where $A_0 \in \mathrm{GL}_2(\mathbb{Z}/\ell)$ and $A_1 \in \mathrm{Mat}_2(\mathbb{Z}/\ell)$. Then

$$\begin{aligned} A\alpha - \alpha A &= (A_0 + \ell A_1)(dI + \ell\beta) - (dI + \ell\beta)(A_0 + \ell A_1) \\ &\equiv (dA_0 + \ell(A_0\beta + dA_1)) - (dA_0 + \ell(dA_1 + \beta A_0)) \pmod{\ell^2} \\ &= \ell(A_0\beta - \beta A_0). \end{aligned}$$

  Thus $A \in \mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^2)}(\alpha)$ exactly when $A_0 \in \mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell)}(\beta)$. We have no constraints on A_1, so $\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^2)}(dI + \ell\beta)$ is in bijection with $\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell)}(\beta) \times \mathrm{Mat}_2(\mathbb{Z}/\ell)$.

  Recall the taxonomy of conjugacy classes in $\mathrm{GL}_2(\mathbb{F}_\ell)$ at the beginning of chapter 4. We rely on previous knowledge of the orders of the centralizers of each type of cyclic β to proceed.

Case 1: Say β lies in a **Split** conjugacy class, which has centralizer order $(\ell-1)^2$ in $\mathrm{GL}_2(\mathbb{Z}/\ell)$. Then the order of the centralizer of $\alpha = dI + \ell\left(\begin{smallmatrix} a & \\ & b \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Z}/\ell^2)$ is $(\ell-1)^2 \cdot \ell^4$ and the number of elements in each of these classes is $\frac{\ell^4(\ell^2-\ell)(\ell^2-1)}{\ell^4(\ell-1)^2} = \ell(\ell+1)$.

Case 2: Say β is **Nonsplit**; such a β has centralizer order ℓ^2-1 in $\mathrm{GL}_2(\mathbb{Z}/\ell)$. Thus

$$\#\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^2)}(dI + \ell\left(\begin{smallmatrix} 0 & 1 \\ -b & a \end{smallmatrix}\right)) = (\ell^2-1)\cdot\ell^4$$

and the size of such a conjugacy class is $\frac{\ell^4(\ell^2-\ell)(\ell^2-1)}{\ell^4(\ell^2-1)} = \ell(\ell-1)$.

Case 3: Say β is in a $\mathbf{RL}[2]$ conjugacy class. The centralizer of β in $\mathrm{GL}_2(\mathbb{Z}/\ell)$ has order $\ell(\ell-1)$, so $\#\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^2)}(dI + \ell\left(\begin{smallmatrix} a & 1 \\ & a \end{smallmatrix}\right)) = \ell(\ell-1)\cdot\ell^4$. Then each conjugacy class $dI + \ell\left(\begin{smallmatrix} a & 1 \\ & a \end{smallmatrix}\right)$ has order $\frac{\ell^4(\ell^2-\ell)(\ell^2-1)}{\ell^4\ell(\ell-1)} = \ell^2-1$.

- Lastly, let $j = 0$. These are the matrices where $d = 0$ and $\beta \in \mathrm{GL}_2(\mathbb{Z}/\ell^2)$ cyclic, and so are not scalar mod any power of ℓ. Since β is cyclic, it can be represented by a companion matrix. There are $\ell^2 \cdot \ell(\ell-1)$ of these conjugacy classes determined by the trace and determinant of β. Computing the centralizer (and thus its order) of one of these elements will be the subject of the following two sections.

4.3.1 A number theoretic approach

We are interested in computing the order of the centralizer of a cyclic element β of $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$. Since it is cyclic, β can be representated as a companion matrix. Let this matrix be

$$C := \begin{pmatrix} 0 & 1 \\ -\delta & \tau \end{pmatrix}$$

where $\delta = \det(\beta)$ and $\tau = \mathrm{tr}(\beta)$. Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$. We will determine conditions on $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ so that it is an element of $\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^r)}(C)$. Consider

$$\begin{aligned}\begin{pmatrix} a & b \\ c & d \end{pmatrix} C - C \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -\delta & \tau \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ -\delta & \tau \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} -(c+b\delta) & a+b\tau-d \\ (a-d)\delta - c\tau & c+b\delta \end{pmatrix}. \end{aligned} \tag{4.3.1}$$

Then (4.3.1) is the zero matrix if and only if $d = a + b\tau$ and $c = -b\delta$, so

$$A = \begin{pmatrix} a & b \\ -b\delta & a+b\tau \end{pmatrix}$$

centralizes C in $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ when it is invertible. The size of the centralizer of C is then

$$\#\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^r)}(C) = \#\left\{\left(\begin{smallmatrix} a & b \\ -b\delta & a+b\tau \end{smallmatrix}\right) | D(a,b) \in (\mathbb{Z}/\ell^r)^\times\right\},$$

where $D(a,b) = a^2 + ab\tau + b^2\delta$ is the determinant of A. Notice that finding the size of $\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^r)}(C)$ also gives the size of the centralizer of β since they are elements of the same conjugacy class.

Definition 4.3.4. Let $\Delta = \tau^2 - 4\delta = \Delta(\mathrm{charpol}(C))$. The quadratic character of discriminant Δ is

$$\chi_\Delta(\ell) = \begin{cases} -1 & \text{if } \Delta \text{ is not a square mod } \ell, \\ 0 & \text{if } \ell | \Delta, \\ 1 & \text{if } \Delta \text{ is a square mod } \ell. \end{cases}$$

Remark 4.3.5. Notice that $\chi_\Delta(\ell)$ is the Legendre symbol and often denoted $\left(\frac{\Delta}{\ell}\right)$.

Lemma 4.3.6.

$$\#\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell)}(C) = (\ell-1)(\ell-\chi_{\Delta}(\ell)).$$

Proof. We count pairs $a, b \in \mathbb{Z}/\ell$ so that $D(a,b) = a^2 + ab\tau + b^2\delta \in (\mathbb{Z}/\ell)^{\times}$.

Suppose $b = 0$. Then $D(a,b) = D(a,0) = a^2$, which is a unit in $\mathbb{Z}/\ell$ exactly when a is a unit, so we get $\ell - 1$ centralizer elements.

Now suppose that $b \in (\mathbb{Z}/\ell)^{\times}$. For a fixed b, $D(a,b)$ is quadratic in a and has discriminant $b^2(\tau^2 - 4\delta)$. The number of solutions of $D(a,b) = 0$ then depends on whether $\Delta = \tau^2 - 4\delta$ is square or not mod ℓ. Using the definition of $\chi_{\Delta}(\ell)$, there are $1 + \chi_{\Delta}(\ell)$ solutions to $D(a,b) = 0$ for a fixed b, so there are $(\ell - (1 + \chi_{\Delta}(\ell))) \cdot (\ell - 1)$ additional centralizer elements.

Then

$$\#\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell)}(C) = (\ell-1) + (\ell - (1+\chi_{\Delta}(\ell)))(\ell-1) = (\ell-1)(\ell-\chi_{\Delta}(\ell)).$$

□

Proposition 4.3.7.

$$\#\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^r)}(C) = \ell^{2(r-1)}(\ell-1)(\ell-\chi_{\Delta}(\ell)).$$

Proof. Now we find pairs $a, b \in \mathbb{Z}/\ell^r$ so that $D(a,b) \in (\mathbb{Z}/\ell^r)^{\times}$. Any such pair is a lift of a solution (a,b) mod ℓ, and so we lift both a and b from $\mathbb{Z}/\ell$ to $\mathbb{Z}/\ell^r$. Using the previous lemma we have the result. □

Proposition 4.3.7 only gives the order of the centralizer in $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ for a cyclic matrix in $\mathrm{Mat}_2(\mathbb{Z}/\ell^r)$ (i.e., one for which $j = 0$). To find the centralizer order for any element $\alpha = dI + \ell^j\beta \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ we need to determine what happens when $1 \leq j \leq r$.

Let $\alpha = dI + \ell^j\beta$ for $j \in \{1, \ldots, r-1\}$, and let $A = \sum_{i=0}^{r-1} \ell^i A_i$ where $A_0 \in \mathrm{GL}_2(\mathbb{F}_\ell)$

and $A_i \in \mathrm{Mat}_2(\mathbb{F}_\ell)$ for $i \geq 1$ so that $A \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$. Then

$$\begin{aligned} A\alpha - \alpha A &= \left(\sum_{i=0}^{r-1} \ell^i A_i\right)\left(dI + \ell^j\beta\right) - \left(dI + \ell^j\beta\right)\left(\sum_{i=0}^{r-1} \ell^i A_i\right) \\ &= d\sum_{i=0}^{r-1} \ell^i A_i + \ell^j \left(\sum_{i=0}^{r-1} \ell^i A_i\right)\beta - d\sum_{i=0}^{r-1} \ell^i A_i - \ell^j\beta\left(\sum_{i=0}^{r-1} \ell^i A_i\right) \\ &\equiv \ell^j \left(\left(\sum_{i=0}^{r-j-1} \ell^i A_i\right)\beta - \beta\left(\sum_{i=0}^{r-j-1} \ell^i A_i\right)\right) \pmod{\ell^r}. \end{aligned}$$

Notice that the centralizer only depends on $A' = \sum_{i=0}^{r-j-1} \ell^i A_i \in \mathrm{GL}_2(\mathbb{Z}/\ell^{r-j})$ and so $A_{r-j}, \ldots, A_{r-1}$ are all free. In addition, $A \in \mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^r)}(\alpha)$ if and only if A' is an element of $\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^{r-j})}(\beta)$. Then the centralizer in $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ of any $\alpha = dI + \ell^j\beta$ is in bijection with $\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^{r-j})}(\beta) \times (\mathrm{Mat}_2(\mathbb{F}_\ell))^j$ and it has order

$$\#\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^{r-j})}(\beta) \cdot (\ell^4)^j = \ell^{4j}\left[\ell^{(r-j)-1}(\ell-1)\left(\ell^{r-j} - \ell^{(r-j)-1}\ \chi_\Delta\right)\right],$$

where we define

$$\Delta(\beta) := \mathrm{tr}(\beta)^2 - 4\det(\beta), \tag{4.3.2}$$

the discriminant of $\mathrm{charpol}(\beta) = T^2 - \mathrm{tr}(\beta)T + \det(\beta)$.

When $j = r$, $\alpha = dI + \ell^r\beta \equiv dI \bmod \ell^r$. Then α is scalar, and thus is in the center of the group, so $\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^r)}(\alpha) = \mathrm{GL}_2(\mathbb{Z}/\ell^r)$.

Then we have proved the following theorem.

Theorem 4.3.8.

$$\#\mathcal{Z}_{\mathrm{GL}_2(\mathbb{Z}/\ell^r)}(dI + \ell^j\beta) = \begin{cases} \ell^{2(r-1)}(\ell-1)(\ell-\chi_\Delta(\ell)) & \text{if } j = 0, \\ \ell^{2(r+j-1)}(\ell-1)(\ell-\chi_\Delta(\ell)) & \text{if } 1 \leq j \leq r-1, \\ \#\mathrm{GL}_2(\mathbb{Z}/\ell^r) = \ell^{4(r-1)}(\ell^2-1)(\ell^2-\ell) & \text{if } j = r. \end{cases}$$

4.3.2 An algebraic geometric approach: Smoothness

Let R be a complete discrete valuation ring with maximal ideal $\mathfrak{m} = (\mu)$ and consider the group scheme GL_2 over R. Define $\mathscr{Z}_G(\alpha)$ to be the centralizer in G of the element α. Then $\mathscr{Z}_G(\alpha)$ is a group scheme over R. Our goal in this section will be to prove the following theorem.

Theorem 4.3.9. *Let $G = \mathrm{GL}_{2,R}$ with $\alpha \in \mathrm{GL}_2(R)$. Consider $X = \mathscr{Z}_G(\alpha)$ as a group scheme over R. Then X is smooth if and only if α is either scalar or cyclic.*

Before we prove Theorem 4.3.9, we will use the following results to reduce the problem.

Theorem 4.3.10. *[14] Suppose that G is a group scheme over a discrete valuation ring S. Then G is smooth if and only if G is flat and reduced.*

Then to prove Theorem 4.3.9 we need to show that these centralizers are flat and reduced group schemes. To show they are reduced, we will show that there are no nilpotents. For flatness, we refer to the next proposition.

Proposition 4.3.11. *[14, Proposition 4.3.9] Consider a local ring R with maximal ideal $\mathfrak{m}$, and a reduced scheme X over R.*

$$\begin{tikzcd}
& X \arrow[d, "f"] & \\
\operatorname{Spec}(\operatorname{Frac} R) \arrow[r, hook, "\eta"] & \operatorname{Spec} R & \operatorname{Spec} R/\mathfrak{m} \arrow[l, hook', "s"']
\end{tikzcd}$$

Then the morphism f is flat if and only if every irreducible component of X dominates $\operatorname{Spec} R$*.*

In other words, f is flat if and only if no irreducible component of X lies purely over the closed point $\operatorname{Spec} R/\mathfrak{m}$. We can show that f is flat by computing the fibers of X over each of the points s and η and checking that they are equidimensional and topologically equivalent.

Recall that the operator $[x, y]$ denotes the Lie bracket operator, $[x, y] = xy - yx$.

Proof. (of Theorem 4.3.9)
We want to show that $\mathcal{Z}_G(\alpha)$ is flat, but we can make one further reduction and instead prove that for $M = \mathrm{Mat}_{2,R}$, $X = \mathcal{Z}_M(\alpha)$ is flat. The map $\mathcal{Z}_G(\alpha) \to \mathcal{Z}_M(\alpha)$ is an open immersion and so is flat. Then since the composition of two flat maps is flat, if the map $\mathcal{Z}_M(\alpha) \to \operatorname{Spec} R$ is flat then the map $\mathcal{Z}_G(\alpha) \to \operatorname{Spec} R$ is flat and so $\mathcal{Z}_G(\alpha)$ is flat. Thus in this proof we only compute the fibers in $\mathrm{Mat}_{2,R}$.

By way of notation, let $\mathcal{F} = \operatorname{Frac} R$ and let $k = R/\mathfrak{m}$.

Let $X = \mathcal{Z}_M(\alpha)$. We begin by proving that if α is scalar or cyclic then X is smooth. Suppose α is scalar, so $\alpha = dI$ for some d. Then

$$X = \mathcal{Z}_M(\alpha) = \operatorname{Spec} \frac{R[w, x, y, z]}{[\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right), dI]}.$$

But since

$$[\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right), dI] = d\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) - d\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) = (0)$$

regardless of the values of $d, w, x, y,$ or z, we have that

$$X \cong \operatorname{Spec} R[w, x, y, z].$$

Then $X \cong \mathrm{Mat}_{2,R}$ and it is clear that X is smooth over $\operatorname{Spec} R$.

Suppose that $\alpha \in \mathrm{GL}_2(R)$ is cyclic ($j = 0$) with trace τ and determinant δ. Then α is conjugate to a companion matrix $\left(\begin{smallmatrix} 0 & 1 \\ -\delta & \tau \end{smallmatrix}\right)$, and

$$X = \mathcal{Z}_M(\alpha) = \operatorname{Spec} \frac{R[w, x, y, z]}{[\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -\delta & \tau \end{smallmatrix}\right)]}.$$

Here,

$$[\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -\delta & \tau \end{smallmatrix}\right)] = \begin{pmatrix} -(y+x\delta) & w+x\tau-z \\ (w-z)\delta-y\tau & y+x\delta \end{pmatrix}$$

so we get that

$$X = \operatorname{Spec} \frac{R[w,x,y,z]}{(w + x\tau - z, (w-z)\delta - y\tau, y + x\delta)} = \operatorname{Spec} \frac{R[w,x,y,z]}{(w + x\tau - z, y + x\delta)}.$$

Now

$$X_\eta = X \times_{\operatorname{Spec} R} \eta = \operatorname{Spec} \left(\frac{R[w,x,y,z]}{(w + x\tau - z, y + x\delta)} \otimes_R \mathcal{F} \right) = \operatorname{Spec} \frac{\mathcal{F}[w,x,y,z]}{(w + x\tau - z, y + x\delta)}$$

and

$$X_s = X \times_{\operatorname{Spec} R} s = \operatorname{Spec} \left(\frac{R[w,x,y,z]}{(w + x\tau - z, y + x\delta)} \otimes_R k \right) = \operatorname{Spec} \frac{k[w,x,y,z]}{(w + x\tau - z, y + x\delta)}.$$

Since there are no components supported only over s, we see that $\mathcal{Z}_M(\alpha)$ is flat, and hence smooth, when α is cyclic.

In the other direction, we show that if α is neither scalar nor cyclic, then X is in fact not smooth. Let $\alpha = dI + \mu^j \beta$ where $j > 0$ and $\beta \neq (0)$ so that α has nontrivial scalar and cyclic parts. Then

$$X = \mathcal{Z}_M(\alpha) = \operatorname{Spec} \frac{R[w,x,y,z]}{\left[\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right), dI + \mu^j \beta\right]}.$$

Calculating the Lie bracket, we get that

$$\left[\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right), dI + \mu^j \beta\right] = \left(d \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) + \mu^j \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) \beta\right) - \left(d \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) + \mu^j \beta \left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right)\right) = \mu^j \left[\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right), \beta\right]$$

so

$$X = \operatorname{Spec} \frac{R[w,x,y,z]}{\mu^j \left[\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right), \beta\right]} = \operatorname{Spec} \frac{R[w,x,y,z]}{\mu^j (w + x\tau - z, y + x\delta)}.$$

Then

$$\begin{aligned} X_\eta = X \times_{\operatorname{Spec} R} \eta &= \operatorname{Spec}\left(\frac{R[w,x,y,z]}{\mu^j(w+x\tau-z, y+x\delta)} \otimes_R \mathcal{F}\right) \\ &= \operatorname{Spec}\frac{\mathcal{F}[w,x,y,z]}{\mu^j(w+x\tau-z, y+x\delta)} \\ &= \operatorname{Spec}\frac{\mathcal{F}[w,x,y,z]}{(w+x\tau-z, y+x\delta)} \end{aligned}$$

since μ is a unit in $\mathcal{F}$. Additionally

$$\begin{aligned} X_s = X \times_{\operatorname{Spec} R} s &= \operatorname{Spec}\left(\frac{R[w,x,y,z]}{\mu^j(w+x\tau-z, y+x\delta)} \otimes_R k\right) \\ &= \operatorname{Spec}\frac{k[w,x,y,z]}{\mu^j(w+x\tau-z, y+x\delta)} \\ &= \operatorname{Spec} k[w,x,y,z] \end{aligned}$$

since $\mu \equiv 0$ in k. Then we see that X_η and X_s have different dimensions, and so $\mathcal{Z}_M(\alpha)$ is not flat for α not cyclic or scalar, and thus $\mathcal{Z}_M(\alpha)$ is not smooth. □

Let $R = \mathbb{Z}_\ell$, so $\mu = \ell$ and for $\alpha \in G(R) = \mathrm{GL}_2(\mathbb{Z}_\ell)$, $\alpha = dI + \ell^j\beta$. In general, suppose we have the following diagram for a fiber product.

$$\begin{tikzcd} X \times_A B \arrow[r] \arrow[d, "g"'] & X \arrow[d, "f"] \\ B \arrow[r] & A \end{tikzcd}$$

If f is a smooth map, so is g. Then if $\mathcal{Z}_G(\alpha) \longrightarrow \operatorname{Spec}\mathbb{Z}_\ell$ is smooth, so is

$$\mathcal{Z}_G(\alpha) \times_{\operatorname{Spec}\mathbb{Z}_\ell} \operatorname{Spec}\mathbb{Z}_\ell/\ell^r \longrightarrow \operatorname{Spec}\mathbb{Z}_\ell/\ell^r.$$

Corollary 4.3.12. *Let $\alpha \in G(\mathbb{Z}_\ell), \alpha = dI + \ell^j\beta$. The map*

$$\mathcal{Z}_G(\alpha) \times_{\operatorname{Spec}\mathbb{Z}_\ell} \operatorname{Spec}\mathbb{Z}_\ell/\ell^r \longrightarrow \operatorname{Spec}\mathbb{Z}_\ell/\ell^r$$

is smooth if $j = 0$ or $r \leq j$, and is not smooth if $r > j \neq 0$.

Proof. If $j = 0$ (α is cyclic), then $\mathcal{Z}_G(\alpha)$ is smooth by the previous theorem, so $\mathcal{Z}_G(\alpha) \times_{\operatorname{Spec}\mathbb{Z}_\ell} \operatorname{Spec}\mathbb{Z}_\ell/\ell^r \longrightarrow \operatorname{Spec}\mathbb{Z}_\ell/\ell^r$ is also smooth.

If $r \leq j$, then α mod ℓ^r is scalar in $G(\mathbb{Z}_\ell/\ell^r)$. Then

$$\mathcal{Z}_G(\alpha) \times_{\operatorname{Spec}\mathbb{Z}_\ell} \operatorname{Spec}\mathbb{Z}_\ell/\ell^r = \mathcal{Z}_{\mathrm{GL}_{2,\mathbb{Z}_\ell/\ell^r}}(\alpha)$$

which is smooth by Theorem 4.3.9.

Otherwise, $\mathcal{Z}_G(\alpha) \to \operatorname{Spec}\mathbb{Z}_\ell$ is not smooth, and α mod ℓ^r is neither cyclic nor scalar, so $\mathcal{Z}_{\mathrm{GL}_{2,\mathbb{Z}_\ell/\ell^r}}(\alpha)$ is not smooth either. □

Remark 4.3.13. We can also show that for $\alpha = dI + \ell^j\beta$, $\mathcal{Z}_M(\alpha)$ is not formally smooth by finding a $\gamma \in \mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^j)$ so that there is no lift of γ into $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{j+1})$. Notice that α is scalar mod ℓ^j but cyclic mod ℓ^{j+1}, and let $\gamma = \sum_{i=0}^{j-1} \ell^i A_i \in \mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^j)$. Then consider $\tilde{\gamma} = \sum_{i=0}^{j} \ell^i A_i = \gamma + \ell^j A_j$, a lift of γ.

$$\begin{aligned}
\tilde{\gamma}\alpha - \alpha\tilde{\gamma} &= (\gamma + \ell^j A_j)(dI + \ell^j\beta) - (dI + \ell^j\beta)(\gamma + \ell^j A_j) \\
&= \gamma(dI + \ell^j\beta) + \ell^j A_j(dI + \ell^j\beta) - (dI + \ell^j\beta)\gamma - (dI + \ell^j\beta)\ell^j A_j \\
&= d\gamma + \ell^j\gamma\beta + \ell^j dA_j + \ell^{2j}A_j\beta - d\gamma - \ell^j\beta\gamma - \ell^j dA_j - \ell^{2j}\beta A_j \\
&\equiv \ell^j(\gamma\beta - \beta\gamma) \bmod \ell^{j+1}.
\end{aligned}$$

Then we see that if we choose $\gamma \notin \mathcal{Z}_G(\beta)(\mathbb{Z}_\ell/\ell)$ then there exists no lift of γ in $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{j+1})$.

Suppose we are interested in the centralizer of some cyclic or scalar $\tilde{\alpha} \in G(\mathbb{Z}_\ell/\ell^r)$. There exists an $\alpha \in G(\mathbb{Z}_\ell)$ such that $\alpha \equiv \tilde{\alpha}$ mod ℓ^r and $\mathcal{Z}_G(\alpha)$ is smooth; if $\tilde{\alpha}$ is cyclic, any lift α will also be cyclic. If instead $\tilde{\alpha}$ is scalar of the form $\tilde{d}I$, lift $\tilde{d} \in \mathbb{Z}_\ell/\ell^r$

to any d in $\mathbb{Z}_\ell$ where $d \bmod \ell^r \equiv \tilde{d}$ and let $\alpha = dI$. The smoothness of $\mathcal{Z}_G(\alpha)$ implies

$$\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^i) \to \mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{i-1})$$

is surjective for all i, or that any element of a centralizer has as many lifts as possible that will still centralize α. In particular we can find $\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) = \#\mathcal{Z}_G(\tilde{\alpha})$ using this surjectivity and the proof of Theorem 4.3.9.

Suppose $\alpha \in G(\mathbb{Z}_\ell)$ is scalar. From the proof of the previous theorem, $\mathcal{Z}_M(\alpha)$ is formally smooth and of relative dimension four over $\operatorname{Spec} \mathbb{Z}_\ell$. Then the reduction map $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) \to \mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{r-1})$ is an ℓ^4-to-1 map. Since any element of $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{r-1})$ has ℓ^4 lifts in $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r)$, we see that

$$\begin{aligned}\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) &= \ell^4 \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{r-1}) = \cdots = \ell^{4(r-1)} \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell) \\ &= \ell^{4(r-1)} \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{F}_\ell).\end{aligned}$$

We know the order of the centralizer of any element of $G(\mathbb{F}_\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$, and since in this case α is scalar mod ℓ we know it must commute with all of $G(\mathbb{F}_\ell)$. Then $\#\mathcal{Z}_G(\alpha)(\mathbb{F}_\ell) = (\ell^2-1)(\ell^2-\ell)$, and

$$\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) = \ell^{4(r-1)} \cdot (\ell^2-1)(\ell^2-\ell).$$

Notice that $\ell^{4(r-1)}(\ell^2-1)(\ell^2-\ell) = \#\,\mathrm{GL}_2(\mathbb{Z}_\ell/\ell^r)$, which is the expected centralizer order for a scalar element.

Now suppose $\alpha \in G(\mathbb{Z}_\ell)$ is cyclic. We know $\mathcal{Z}_M(\alpha) = \operatorname{Spec} \frac{\mathbb{Z}_\ell[w,x,y,z]}{(w+x\tau-z,y+x\delta)}$, which is formally smooth by Theorem 4.3.9 and of relative dimension two over $\operatorname{Spec} \mathbb{Z}_\ell$ since y and z are completely determined by w and x. Then the reduction map $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) \to \mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{r-1})$ is ℓ^2-to-1. By similar reasoning as above, any element of $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell)$ has $\ell^{2(r-1)}$ lifts in $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r)$. Since α is cyclic, we know that

$\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell) = \#\mathcal{Z}_G(\alpha)(\mathbb{F}_\ell) = (\ell-1)(\ell-\chi_{\Delta}(\ell))$ by Lemma 4.3.6, where $\Delta = \Delta(\beta)$ as in equation (4.3.2). Thus,

$$\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) = \ell^{2(r-1)} \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{F}_\ell) = \ell^{2(r-1)}(\ell-1)(\ell-\chi_{\Delta}(\ell)).$$

The third case is when $\alpha \in G(\mathbb{Z}_\ell)$ is neither scalar nor cyclic mod ℓ^r, and so we know that $\mathcal{Z}_G(\alpha) \longrightarrow \operatorname{Spec}\mathbb{Z}_\ell$ is not formally smooth. However, if $\alpha = dI + \ell^j\beta$ has $0 < j < r$ then $\mathcal{Z}_G(\alpha) \times_{\operatorname{Spec}\mathbb{Z}_\ell} \operatorname{Spec}\mathbb{Z}_\ell/\ell^j \longrightarrow \operatorname{Spec}\mathbb{Z}_\ell/\ell^j$ is smooth, and so $\mathcal{Z}_G(\alpha)(\mathbb{Z}/\ell^i) \longrightarrow \mathcal{Z}_G(\alpha)(\mathbb{Z}/\ell^{i-1})$ is surjective and ℓ^2-to-1 for $2 \leq i \leq j$. Thus

$$\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^j) = \ell^{4(j-1)} \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell) = \ell^{4(j-1)} \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{F}_\ell)$$

as α is scalar mod ℓ^i for $i \leq j$.

As α is cyclic mod ℓ^i for $j+1 \leq i \leq r$, $\mathcal{Z}_G(\alpha) \times_{\operatorname{Spec}\mathbb{Z}_\ell} \operatorname{Spec}\mathbb{Z}_\ell/\ell^i \longrightarrow \operatorname{Spec}\mathbb{Z}_\ell/\ell^i$ is smooth for such i and so the maps $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^i) \longrightarrow \mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{i-1})$ are surjective and ℓ^4-to-1 for $j+2 \leq i \leq r$. Then

$$\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) = \ell^{2(r-(j+1))} \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{j+1}).$$

Since α is cyclic mod ℓ^{j+1} but scalar mod ℓ^j, $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{j+1}) \longrightarrow \mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^j)$ is not surjective, so we cannot count lifts as we did above. However, since $\alpha = dI + \ell^j\beta$ in $G(\mathbb{Z}_\ell)$, an element of $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{j+1})$ centralizes $\beta \neq (0)$ instead of just the scalar part of α. Since $\beta \in M(\mathbb{Z}_\ell/\ell) = M(\mathbb{F}_\ell)$, $\#\mathcal{Z}_G(\beta)(\mathbb{Z}_\ell/\ell) = (\ell-1)(\ell-\chi_{\Delta}(\ell))$ (Lemma 4.3.6), and so $\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{j+1}) = (\ell-1)(\ell-\chi_{\Delta}(\ell)) \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^j)$. Then

$$\begin{aligned}
\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) &= \ell^{2(r-(j+1))} \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^{j+1}) \\
&= \ell^{2(r-(j+1))} \cdot (\ell-1)(\ell-\chi_{\Delta}(\ell)) \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^j) \\
&= \ell^{2(r-(j+1))} \cdot (\ell-1)(\ell-\chi_{\Delta}(\ell)) \cdot \ell^{4(j-1)} \cdot \#\mathcal{Z}_G(\alpha)(\mathbb{F}_\ell).
\end{aligned}$$

Although α is scalar mod ℓ, $\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell)$ is not $G(\mathbb{F}_\ell)$ but is instead $M(\mathbb{F}_\ell)$. Any $\gamma \in \mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r)$ is such that γ mod ℓ^r is in $G(\mathbb{Z}_\ell/\ell^r) \cong G(\mathbb{F}_\ell) \times M(\mathbb{Z}_\ell/\ell^{r-1})$, but notice that in the reduction $\mathcal{Z}_G(\alpha)(\mathbb{Z}/\ell^{j+1}) \longrightarrow \mathcal{Z}_G(\alpha)(\mathbb{Z}/\ell^j)$ we use the centralizer of β in $G(\mathbb{F}_\ell)$, and so we are free to choose the centralizer component over $\mathbb{F}_\ell$ in $M(\mathbb{F}_\ell)$ since any centralizer element already has this invertible component. Then we have

$$\begin{aligned}\#\mathcal{Z}_G(\alpha)(\mathbb{Z}_\ell/\ell^r) &= \ell^{2(r-(j+1))} \cdot (\ell-1)(\ell-\chi_\Delta(\ell)) \cdot \ell^{4(j-1)} \cdot \ell^4 \\ &= \ell^{4j}\ell^{2(r-(j+1))}(\ell-1)(\ell-\chi_\Delta(\ell)),\end{aligned}$$

and we have proved the following theorem.

Theorem 4.3.14. *Let $\alpha = dI + \ell^j\beta \in G(\mathbb{Z}_\ell/\ell^r)$ and $\Delta = \Delta(\beta)$, the discriminant of* charpol(β) *as in equation* (4.3.2)*. Then*

$$\#\mathcal{Z}_G(\alpha)(\mathbb{Z}/\ell^r) = \begin{cases} \ell^{2(r-1)}(\ell-1)\,(\ell-\chi_\Delta(\ell)) & \text{if } j = 0, \\ \ell^{4j}\left[\ell^{2(r-j-1)}(\ell-1)\,(\ell-\chi_\Delta(\ell))\right] & \text{if } 0 < j < r, \\ \ell^{4(r-1)}(\ell^2-1)(\ell^2-\ell) & \text{if } j = r. \end{cases}$$

Notice that this matches Theorem 4.3.8.

5. THE NUMBER OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION BY THE MAXIMAL ORDER

Fix a polynomial $f(T) = T^2 - aT + q$, a possible characteristic polynomial of the Frobenius endomorphism of an elliptic curve over $\mathbb{F}_q$ and let $K = \mathrm{Split}(f)$. As stated in section 3, we want to compare the ℓ^{th} Euler factor of the L-series $L(1, \chi)$ appearing in Theorem 2.3.3 to the excess proportion of matrices $\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ with $\mathrm{charpol}(\gamma) \equiv f \bmod \ell^r$. First we consider how primes split in such a K and associate to each factorization a conjugacy class of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

5.1 Primes, conjugacy classes, and characters

Suppose $K = \mathrm{Split}(f)$ is a totally imaginary quadratic field over $\mathbb{Q}$.

$$\begin{tikzcd} K \arrow[r, phantom, "\supset"] & \mathcal{O}_K \arrow[r, phantom, "\supset"] & \lambda \\ \mathbb{Q} \arrow[u, dash] \arrow[r, phantom, "\supset"] & \mathbb{Z} \arrow[u, hook] \arrow[r, phantom, "\ni"] & \ell \end{tikzcd}$$

Then $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma = cc\} = \langle \sigma \rangle$ where cc is complex conjugation. Choose ℓ, a rational prime. We want to associate a conjugacy class of $\mathrm{GL}_2(\mathbb{F}_\ell)$ to the factorization of the prime ℓ, and so we use inertia and decomposition groups (see section 2.1) to enumerate and describe these factorizations.

Let (e, f, r) be the factorization invariants of a prime $\lambda \subset \mathcal{O}_K$ over ℓ. Recall that

$$I(\lambda/\ell) \leq D(\lambda/\ell) \leq \mathrm{Gal}(K/\mathbb{Q}),$$
$$\#I(\lambda/\ell) = e(\lambda) = e \ \text{ and } \ \#D(\lambda/\ell) = e(\lambda)f(\lambda) = ef$$

by Lemma 2.1.8, and $efr = n = 2$ from Corollary 2.1.5. To the factorization of ℓ we associate a factorization of f mod ℓ using Proposition 3.0.1, and then we can determine the cyclic conjugacy class type $\mathcal{C}(f \bmod \ell)$ of a matrix $\gamma \in \mathrm{GL}_2(\mathbb{F}_\ell)$ with characteristic polynomial f mod ℓ. If ℓ is unramified in K we determine the Frobenius element $\mathrm{Frob}_K(\ell) \in \mathrm{Gal}(K/\mathbb{Q})$ that generates the Galois group of the extension of residue fields $\kappa(\lambda)/\kappa(\ell)$ (Theorem 2.1.7).

1. Suppose $D(\lambda/\ell) = \{1\}$, so $I(\lambda/\ell) = \{1\}$. Since ℓ is unramified, use Theorem 2.1.7 to see

$$\{1\} = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell)) \;\Rightarrow\; \mathrm{Frob}_K(\ell) = 1.$$

   Notice that $(e, f, r) = (1, 1, 2)$ so this factorization of ℓ corresponds to the factorization f mod $\ell = (T - a)(T - b)$ by Proposition 3.0.1. The conjugacy class with this characteristic polynomial is **Split**.

2. Suppose $D(\lambda/\ell) = \langle cc \rangle$.

   (a) Suppose $I(\lambda/\ell) = \{1\}$. Then by Theorem 2.1.7

$$\langle cc \rangle = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell)) \;\Rightarrow\; \mathrm{Frob}_K(\ell) = cc.$$

   We have $(e, f, r) = (1, 2, 1)$ so f mod ℓ is an irreducible quadratic by Proposition 3.0.1, which then implies that $\mathcal{C}(f \bmod \ell)$ is **Nonsplit**.

   (b) Suppose $I(\lambda/\ell) = \langle cc \rangle$. This gives $(e, f, r) = (2, 1, 1)$ and so ℓ is ramified in $\mathcal{O}_K$. Then by Proposition 3.0.1, f mod $\ell = (T - a)^2$ and an element of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with this characteristic polynomial is **RL**.

The character group associated to K is $X = \{\chi_0, \chi\}$ where χ is defined on elements of $\mathrm{Gal}(K/\mathbb{Q})$ by $\chi : \sigma \mapsto -1$. Recall from chapter 3 that we define $\chi(\ell)$ to be

$\chi(\mathrm{Frob}_K(\ell))$ for unramified primes ℓ and $\chi(\ell) = 0$ if ℓ is ramified in K. Then for $K = \mathrm{Split}(f)$ an imaginary quadratic field, we can define $\chi \in X$ on primes ℓ via

$$\chi(\ell) = \begin{cases} \chi(1) = 1 & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{Split} \\ \chi(\sigma) = -1 & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{Nonsplit}, \\ 0 & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{RL}. \end{cases} \tag{5.1.1}$$

Remark 5.1.1. One could also define this χ (or any quadratic character) on primes of $\mathbb{Z}$ by $\chi(\ell) = \left(\frac{\Delta(f)}{\ell}\right) = \left(\frac{d_K}{\ell}\right)$, the Legendre symbol. This definition corresponds with $\chi_{\Delta(f)} = \chi_{\Delta}(\ell)$ in the notation of section 4.3.1 (see equation (4.3.2)).

5.2 The proportion of Frobenius elements and elliptic curves with complex multiplication by $\mathcal{O}_K$

If $K = \mathrm{Split}(T^2 - aT + q)$ is an imaginary quadratic field, as in the previous section, then K defines an isogeny class of elliptic curves over $\mathbb{F}_q$ with complex multiplication by orders in K. Theorem 2.4.6 gives the number of elliptic curves with complex multiplication by $\mathcal{O}_K$ as the class number h_K of K, which can be computed (via Theorem 2.3.3) as

$$h_K = \frac{1}{\xi_K} L(1, \chi)$$

where χ is the nontrivial character associated to K and ξ_K is defined by equation (2.3.1).

We now proceed to compare the ℓ^{th} Euler factor of $L(1, \chi)$ to the proportion of matrices $\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ with characteristic polynomial $f = T^2 - aT + q$. To do so, we make use of Definition 5.1.1 for $\chi(\ell)$ and Theorem 4.3.8, the formula for the order of the centralizer of $\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$.

Recall that

$$\frac{\#\operatorname{GL}_2(R)}{\#\operatorname{SL}_2(\mathbb{R})} = \#R^\times \quad \text{and} \quad \#\mathcal{C}(\gamma) = \frac{\#G}{\#\mathcal{Z}_G(\gamma)}.$$

Theorem 5.2.1. *Let $f(T) = T^2 - aT + q$ be a possible characteristic polynomial of Frobenius over $\mathbb{F}_q$, $K = \operatorname{Split}(f)$ an imaginary quadratic field, and χ the nontrivial character of $\operatorname{Gal}(K/\mathbb{Q}) = \{1, \sigma = cc\}$ extended to $\mathbb{Z}$ by Definition 5.1.1. Then for any $r \geq 1$*

$$\frac{\#\left\{\textit{cyclic } \gamma \in \operatorname{GL}_2(\mathbb{Z}/\ell^r) | \operatorname{charpol}(\gamma) \equiv f \textit{ mod } \ell^r\right\}}{\ell^{-r}\ \#\operatorname{SL}_2(\mathbb{Z}/\ell^r)} = \frac{1}{1 - \frac{\chi(\ell)}{\ell}}.$$

Proof. Let ℓ be an odd prime. Recall that we are only considering purely cyclic matrices γ in $\operatorname{GL}_2(\mathbb{Z}/\ell^r)$ (chapter 3), so we only use the $j = 0$ entry of the formula in Theorem 4.3.8. In general,

$$\begin{aligned}
&\frac{\#\left\{\gamma \in \operatorname{GL}_2(\mathbb{Z}/\ell^r) | \operatorname{charpol}(\gamma) \equiv f \text{ mod } \ell^r\right\}}{\ell^{-r}\ \#\operatorname{SL}_2(\mathbb{Z}/\ell^r)} \\
&= \frac{\#\mathcal{C}(\gamma)}{\ell^{-r}\ \#\operatorname{SL}_2(\mathbb{Z}/\ell^r)} \\
&= \frac{\#\operatorname{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)(\ell-\chi_\Delta(\ell)) \cdot \ell^{-r}\ \#\operatorname{SL}_2(\mathbb{Z}/\ell^r)} \\
&= \frac{\ell^r \cdot \ell^{r-1}(\ell-1)}{\ell^{2(r-1)}(\ell-1)(\ell-\chi_\Delta(\ell))} \\
&= \frac{\ell}{\ell - \chi_\Delta(\ell)} = \frac{1}{1 - \frac{\chi_\Delta(\ell)}{\ell}}.
\end{aligned}$$

Then the theorem is true if $\chi_\Delta(\ell) = \chi(\ell)$. By the definition of $\chi_\Delta(\ell)$ (definition 4.3.4) in section 4.3.1, we could say

$$\chi_\Delta(\ell) = \begin{cases} 1 & \text{if } f \text{ mod } \ell = (T-a)(T-b), \\ 0 & \text{if } f \text{ mod } \ell = (T-a)^2, \\ -1 & \text{if } f \text{ mod } \ell \text{ is irreducible,} \end{cases} = \begin{cases} 1 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{Split}, \\ 0 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{RL}, \\ -1 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{Nonsplit}, \end{cases}$$

using the taxonomy in section 4.1. This definition is identical to the values of $\chi(\ell)$ given in equation (5.1.1) based on the factorization of the prime ℓ in K, and the theorem is proven. □

This was the result of Gekeler in [9]. Let us reinterpret this theorem in the context of finding the number of elliptic curves over a finite field with complex multiplication by $\mathcal{O}_K$ for $K = \mathrm{Split}(f)$.

Theorem 5.2.2. *Let f and K be as above. Then the set $\mathcal{E}$ of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}_K$ has order*

$$\#\mathcal{E} = \frac{1}{\xi_K} \prod_{\ell \in \mathbb{Z}} \frac{\#\left\{\textit{cyclic } \gamma \in \mathrm{GL}_2(\mathbb{F}_\ell) \middle| \, \mathrm{charpol}(\gamma) \equiv f \ \textit{mod } \ell\right\}}{\ell^{-1} \, \# \, \mathrm{SL}_2(\mathbb{F}_\ell)}.$$

Proof. Notice that the term

$$\frac{1}{1 - \frac{\chi(\ell)}{\ell}}$$

from the previous theorem is exactly the ℓ^{th} Euler factor of the L-series occurring in the class number formula (Theorem 2.3.3) for h_K. By Theorem 2.4.6, h_K is the size of the set $\mathcal{E}$, and taking a product over the odd primes ℓ finishes the result. □

Remark 5.2.3. For K an imaginary quadratic field, we have $r_1 = 0$ and $r_2 = 1$ implying that the rank of the unit group of $\mathcal{O}_K$ is $r = 0$. Then $R_K = 1$ for any such field. If we consider the normalized class number (so we ignore the value of ω_K) then

$$\xi_K = \frac{2\pi}{\sqrt{|d_K|}} = \frac{2\pi}{\sqrt{|a^2 - 4q|}}.$$

Recall that a family of elliptic curves is one-dimensional over $\mathbb{F}_q$. Thus

$$\frac{1}{\xi_K} = \frac{1}{2\pi}\sqrt{4q - a^2} = q\mu_{ST}(a),$$

the expected number of elliptic curves with trace of Frobenius a by the Sato-Tate conjecture. (See Appendix B for details of the computation of $\mu_{ST}(a)$.)

6. THE CONJUGACY CLASSES OF $\mathrm{GSp}_4(\mathbb{Z}/\ell^{\mathrm{r}})$

Before we begin describing and enumerating the conjugacy classes of $\mathrm{GSp}_4(\mathbb{Z}/\ell^{\mathrm{r}})$, we give an introduction to the group from the point of view of linear algebra.

6.1 A brief introduction to the symplectic groups

Let V be a $2g$-dimensional vector space over a ring R and define the $2g \times 2g$ matrix

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

where I_g is the $g \times g$ identity matrix. For $\mathbf{x}, \mathbf{y} \in V$, the map

$$\langle \cdot, \cdot \rangle : V \times V \to R \text{ given by } \langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T J \mathbf{y}$$

defines a skew-symmetric bilinear form on V (which we will alternatively call a *pairing*). For a matrix A, let A^T denote the transpose of A.

Definition 6.1.1.

$$\begin{aligned} \mathrm{Sp}_{2g}(R) &= \{\gamma \in \mathrm{GL}_{2g}(R) | \langle \gamma\mathbf{x}, \gamma\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle\} = \left\{\gamma \in \mathrm{GL}_{2g}(R) | \gamma^T J \gamma = J\right\}, \\ \text{and } \mathrm{GSp}_{2g}(R) &= \left\{\gamma \in \mathrm{GL}_{2g}(R) | \ \exists\ m \in R^\times : \langle \gamma\mathbf{x}, \gamma\mathbf{y} \rangle = m \langle \mathbf{x}, \mathbf{y} \rangle\right\} \\ &= \left\{\gamma \in \mathrm{GL}_{2g}(R) | \ \exists\ m \in R^\times : \gamma^T J \gamma = mJ\right\}. \end{aligned}$$

We call the value m the *multiplier* of the matrix γ. In practice, the condition on the value of $\gamma^T J\gamma$ in these definitions forces pairs of eigenvalues of γ to have the same product (product one in the case of $\mathrm{Sp}_{2g}(R)$ and product m in the case of $\mathrm{GSp}_{2g}(R)$). Alternatively, consider γ as a block matrix

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

where $A, B, C, D \in \mathrm{Mat}_g(R)$. Then $\gamma \in \mathrm{GSp}_{2g}(R)$ if and only if

$$A^T C = C^T A, \quad B^T D = D^T B, \text{ and } A^T D - C^T B = mI. \tag{6.1.1}$$

It should be noted that we made a choice of J above. However, all groups arising from nondegenerate skew-symmetric bilinear forms in this way are isomorphic (i.e., there is only one symplectic group of dimension $2g$ up to isomorphism) [4].

Suppose that $V = W_1 \oplus W_2$, where the W_i are nontrivial subspaces of V. Consider the following two possibilities for how these subspaces sit with respect to the pairing.

- First suppose that $W_1 \perp W_2$, so that $\langle w_1, w_2\rangle = 0$ for all $w_i \in W_i$ (i.e., $\langle \cdot, \cdot \rangle |_{W_i}$ is nondegenerate). Then the subspaces W_1 and W_2 are themselves *symplectic* vector spaces, and there are isomorphisms from W_i to its dual, W_i^*, given by

$$\begin{aligned} \phi : W_i &\longrightarrow W_i^* \\ w_i &\mapsto f_{w_i} : w_i' \mapsto \langle w_i, w_i' \rangle . \end{aligned}$$

  The map ϕ is clearly linear, and injective since

$$\begin{aligned} \ker\phi &= \{w_i \in W_i | \phi(w_i) = f_{w_i} \text{ is the trivial map}\} \\ &= \{w_i \in W_i | f_{w_i}(w_i') = \langle w_i, w_i'\rangle = 0 \;\forall\; w_i' \in W_i\} = (0) \end{aligned}$$

by the nondegeneracy of the pairing on the W_i.

- Now suppose that $W_i \perp W_i$ for each i, so the subspaces are *totally isotropic* (i.e., $\langle W_i, W_i \rangle = 0$). Because of the symplectic basis for the space, $\langle w_1, w_2 \rangle = 0$ if and only if one of w_1, w_2 is itself zero. We can show that

$$\begin{aligned} \phi : W_1 &\longrightarrow W_2^* \\ w_1 &\mapsto f_{w_1} : w_2 \mapsto \langle w_1, w_2 \rangle \end{aligned}$$

is an isomorphism. The map is linear, and injective since

$$\begin{aligned} \ker \phi &= \{w_1 \in W_2 | \phi(w_1) = f_{w_1} \text{ is the trivial map}\} \\ &= \{w_1 \in W_1 | f_{w_1}(w_2) = \langle w_1, w_2 \rangle = 0 \; \forall \; w_2 \in W_2\} = (0) \end{aligned}$$

by the statement above.

6.2 The conjugacy classes of $\mathrm{GSp}_4(\mathbb{F}_\ell)$

Let $R = k$, a field. The conjugacy classes of $\mathrm{Sp}_{2g}(k)$ and $\mathrm{GSp}_{2g}(k)$ are parameterized similarly to the conjugacy classes of $\mathrm{GL}_n(k)$, by the factorization of the characteristic polynomial of a representative matrix along with some additional partition data for repeated factors. This parameterization was considered in 1963 by Wall [24] and more recently by Fulman [6, 7] who used Wall's work to construct the cycle index function for $\mathrm{Sp}_{2g}(\mathbb{F}_q)$ and Breeding [2] who computed the irreducible representations of $\mathrm{GSp}_4(\mathbb{F}_q)$.

Recall from section 4.1 that if $\mathrm{charpol}(\gamma) = \prod_{i=1}^{t} f_i(T)^{n_i}$ we can associate a partition $P_i = [p_{(i,1)}, p_{(i,2)}, \ldots, p_{(i,s)}]$ to each $n_i > 0$ so that the matrix γ has a block of size $p_{(i,j)} \deg f_i$ for each pair (i, j).

There are two prominent differences between partition data for elements of $\mathrm{GL}_n(k)$

versus $\mathrm{Sp}_{2g}(k)$ or $\mathrm{GSp}_{2g}(k)$. First, if P_i is a partition associated with $\gamma \in \mathrm{GSp}_{2g}(k)$, then the odd parts of the partition have even multiplicity. For example, if $\gamma \in \mathrm{GSp}_4(k)$ has $\mathrm{charpol}(\gamma) = (T-a)^4$, $[1,1,1,1]$ and $[1,1,2]$ are two of the possible partitions, but $[1,3]$ is not. This condition reflects the symplectic pairing on the vector space.

The second difference is the presence of signed partitions. For an element of $\mathrm{Sp}_{2g}(k)$ or $\mathrm{GSp}_{2g}(k)$, a partition may include a $+$ or $-$ to distinguish between two non-conjugate classes of matrices with the same characteristic polynomial and actual partition.

Example 6.2.1. Consider a matrix in $\mathrm{GSp}_4(\mathbb{R})$ which has characteristic polynomial $(x-2)^4$. For partition [2,2] there are two different conjugacy classes, [2,2]+ and [2,2]− with representatives

$$\begin{pmatrix} 2 & & 1 & \\ & 2 & & 1 \\ & & 2 & \\ & & & 2 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & & 1 & \\ & 2 & & -1 \\ & & 2 & \\ & & & 2 \end{pmatrix},$$

respectively. These matrices are conjugate over $\mathrm{GL}_4(\mathbb{R})$ by an element of the form

$$\begin{pmatrix} r_1 & r_2 & r_5 & r_6 \\ r_3 & r_4 & r_7 & r_8 \\ & & r_1 & -r_2 \\ & & r_3 & -r_4 \end{pmatrix}.$$

This matrix is an element of $\mathrm{GSp}_4(\mathbb{R})$ if and only if $r_1^2 + r_3^2 = -(r_2^2 + r_4^2)$ with not all $r_i = 0$, which is impossible over $\mathbb{R}$. Then the matrices are elements of different classes in $\mathrm{GSp}_4(\mathbb{R})$.

In $\mathrm{Sp}_{2g}(k)$, the even parts of any partition have a sign $+$ or $-$ to distinguish between conjugacy classes [7]. In $\mathrm{GSp}_{2g}(k)$, some of these signed classes coalesce in the larger group; in other words, perhaps the matrix which conjugates a class with a [4]+ partition to one with a [4]− partition lies in $\mathrm{GSp}_{2g}(k)$ but not $\mathrm{Sp}_{2g}(k)$. In $\mathrm{GSp}_4(\mathbb{F}_\ell)$ specifically, only three conjugacy class types retain a signed partition.

As a final statement on the topic of partitions, it is worth noting that we can identify classes of cyclic matrices based on partitions. A matrix is cyclic if each partition is "maximal" in some sense; that is, a matrix is cyclic if

$$P = \{P_1, P_2, \ldots, P_t\} = \{[n_1], [n_2], \ldots, [n_t]\},$$

so the matrix has a single block corresponding to each irreducible factor of $\mathrm{charpol}(\gamma)$.

The form of the characteristic polynomial of $\gamma \in \mathrm{GSp}_4(k)$ is constrained by the condition $\gamma^T J\gamma = mJ$.

Lemma 6.2.2. *Let $\gamma \in \mathrm{GSp}_4(k)$ with multiplier $m \in k^\times$. Then for $a, b \in k$*

$$\mathrm{charpol}(\gamma) = T^4 + aT^3 + bT^2 + amT + m^2.$$

Proof. Since $\gamma \in \mathrm{GSp}_4(k)$ the degree of $\mathrm{charpol}(\gamma)$ is exactly four, and over a sufficient extension of k, $\mathrm{charpol}(\gamma)$ factors as

$$(T - \alpha_1)(T - \alpha_2)(T - \alpha_3)(T - \alpha_4)$$

where $\alpha_1\alpha_3 = \alpha_2\alpha_4 = m \in k^\times$. Replace α_3 and α_4 with $\frac{m}{\alpha_1}$ and $\frac{m}{\alpha_2}$, respectively. Multiplying, we get

$$T^4 - \left(\alpha_1 + \tfrac{m}{\alpha_1} + \alpha_2 + \tfrac{m}{\alpha_2}\right) T^3 + \left(\tfrac{m\alpha_2}{\alpha_1} + \tfrac{m^2}{\alpha_1\alpha_2} + \alpha_1\alpha_2 + \tfrac{m\alpha_1}{\alpha_2} + 2m\right) T^2 \\ - \left(m\alpha_1 + \tfrac{m^2}{\alpha_1} + m\alpha_2 + \tfrac{m^2}{\alpha_2}\right) T + m^2.$$

Let the coefficient on T^3 be a and the coefficient on T^2 be b. Notice that the coefficient of the linear term is $-(m\alpha_1 + \frac{m^2}{\alpha_1} + m\alpha_2 + \frac{m^2}{\alpha_2}) = ma$. □

Let $k = \mathbb{F}_\ell$ for an odd prime ℓ. Then (from [7])

$$\begin{aligned} \# \operatorname{Sp}_4(\mathbb{F}_\ell) &= \ell^4(\ell^4-1)(\ell^2-1), \\ \text{and } \# \operatorname{GSp}_4(\mathbb{F}_\ell) &= \ell^4(\ell^4-1)(\ell^2-1)(\ell-1). \end{aligned}$$

We will determine the conjugacy classes of $\operatorname{GSp}_4(\mathbb{F}_\ell)$, but first we will prove two short counting lemmas that will be useful.

Lemma 6.2.3. *The number of pairs of distinct elements of $\mathbb{F}_\ell^\times$ which multiply to a fixed $m \in \mathbb{F}_\ell^\times$ is*

$$\begin{cases} \frac{\ell-3}{2} & \textit{if } m \textit{ is square,} \\ \frac{\ell-1}{2} & \textit{if } m \textit{ is not square.} \end{cases}$$

Proof. If m is a square there are $\ell - 3$ elements $a \in \mathbb{F}_\ell^\times$ such that $a^2 \neq m$, so there are $\frac{\ell-3}{2}$ pairs of distinct elements which multiply to m. If m is not a square there are no elements of $\mathbb{F}_\ell^\times$ such that $a^2 = m$ so there are $\frac{\ell-1}{2}$ pairs of distinct elements which multiply to m. □

Lemma 6.2.4. *The number of monic irreducible quadratic polynomials in $\mathbb{F}_\ell[x]$ with constant term $m \in \mathbb{F}_\ell^\times$ is*

$$\begin{cases} \frac{\ell-1}{2} & \textit{if } m \textit{ is square,} \\ \frac{\ell+1}{2} & \textit{if } m \textit{ is not square.} \end{cases}$$

Proof. A polynomial $T^2 + aT + m$ only factors if a is the sum of two numbers which multiply to give m. Suppose m is a square. There are $\frac{\ell-3}{2} + 2 = \frac{\ell+1}{2}$ pairs of numbers which multiply to m (taking the previous lemma and adding the two pairs for the square roots of m), and ℓ total monic quadratics with constant term m. Then there are $\ell - \frac{\ell+1}{2} = \frac{\ell-1}{2}$ irreducible monic quadratic polynomials with a square constant term.

Now suppose m is not square. By the previous lemma there are $\frac{\ell-1}{2}$ pairs of elements in $\mathbb{F}_\ell^\times$ which multiply to m and thus $\frac{\ell-1}{2}$ factorable monic quadratics, implying there are $\ell - \frac{\ell-1}{2} = \frac{\ell+1}{2}$ irreducible monic quadratic polynomials with a nonsquare constant term. □

Any $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ has four eigenvalues (over $\bar{\mathbb{F}}_\ell$), two pairs of which have the same product $m \in \mathbb{F}_\ell^\times$. As $\mathbb{F}_\ell$ is not algebraically closed, the usual definition of *eigenspace* may not apply to $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$. Instead, suppose $\mathrm{charpol}(\gamma) = \prod_i f_i(T)^{n_i}$ as above. Then consider a decomposition of the vector space V as

$$V = \bigoplus_i V_{f_i} \quad \text{such that} \quad \mathrm{charpol}(\gamma|_{V_{f_i}}) = f_i(T)^{n_i}. \tag{6.2.1}$$

Then, with some abuse of language, we will call the V_{f_i} *eigenspaces* of γ.

Recall that the dimensions of the eigenspaces of a matrix γ are preserved by matrix conjugation, so we can at least partially identify conjugacy classes by the eigenspaces of a representative of the class. Eigenspaces are also subspaces of V which are invariant under the action of γ, and so we can use them to interpret the action of the pairing on the eigenvalues of γ. Using the language of section 6.1, if the eigenvalues with product m lie in a single eigenspace, then the eigenspaces of γ are symplectic. On the other hand, a matrix whose eigenvalues with product m lie in distinct eigenspaces has isotropic eigenspaces.

The following is a complete characterization of the conjugacy classes in $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Let $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ and let $\mathrm{charpol}(\gamma)$ be its characteristic polynomial. For all of the following classes, let a fixed $m \in \mathbb{F}_\ell^\times$ be the multiplier. Let a *conjugacy class type* be given by the factorization of the characteristic polynomial and any pertinent pairing information, and be denoted by the bolded abbreviation. A *conjugacy class* will then be determined by its type and a partition (if necessary).

We split the conjugacy classes into two cases for later reference.

Case 1: Regular semisimple elements

The regular semisimple elements are the ones with four distinct roots over $\bar{\mathbb{F}}_\ell$. An important attribute of these classes is that they are completely determined by their characteristic polynomial and multiplier.

- **(Full Split)** $\mathrm{charpol}(\gamma) = (T-a_1)(T-a_2)(T-a_3)(T-a_4)$ such that all $a_i \in \mathbb{F}_\ell^\times$ distinct and $a_1a_3 = a_2a_4 = m \in \mathbb{F}_\ell^\times$. To define such a class we choose two different pairs of elements from $\mathbb{F}_\ell^\times$ with the same product m. By Lemma 6.2.3, the number of these classes is

$$\binom{\frac{\ell-3}{2}}{2}\frac{\ell-1}{2} + \binom{\frac{\ell-1}{2}}{2}\frac{\ell-1}{2} = \frac{(\ell-1)(\ell-3)^2}{8}.$$

- **(IQ/Split)** (Irreducible Quadratic/Split) $\mathrm{charpol}(\gamma) = g(T)(T-a_1)(T-a_2)$ with $g(T)$ a monic irreducible quadratic polynomial with constant term m, $a_i \in \mathbb{F}_\ell^\times$ distinct, and $a_1a_2 = m$. These classes have two eigenvalues in $\mathbb{F}_\ell$ and two in $\mathbb{F}_{\ell^2} \smallsetminus \mathbb{F}_\ell$. Note that such a polynomial corresponds (via Proposition 3.0.1) to a prime ℓ with a factorization which is impossible to achieve in a Galois extension (the factors of ℓ would have different residue degrees, see Corollary 2.1.3). Combining Lemmas 6.2.3 and 6.2.4 we have

$$\left[\frac{\ell-1}{2}\cdot\frac{\ell-3}{2}\right]\frac{\ell-1}{2} + \left[\frac{\ell+1}{2}\cdot\frac{\ell-1}{2}\right]\frac{\ell-1}{2} = \frac{(\ell-1)^3}{4}$$

such classes.

- **(DIQ SR)** (Double Irreducible Quadratic) $\mathrm{charpol}(\gamma) = g_1(T)g_2(T)$ with $g_i(T)$ distinct monic irreducible quadratic polynomials with constant term m. A matrix of this type has eigenspaces corresponding to g_1 and g_2, and the eigenvalues in each multiply to m implying that the eigenspaces are symplectic. These elements have distinct roots in $\mathbb{F}_{\ell^2}$ such that pairs have product m. Then by Lemma 6.2.4, there are

$$\binom{\frac{\ell-1}{2}}{2}\frac{\ell-1}{2}+\binom{\frac{\ell+1}{2}}{2}\frac{\ell-1}{2}=\frac{(\ell-1)^3}{8}$$

conjugacy classes of this type.

- **(DIQ NSR)** (Double Irreducible Quadratic) charpol(γ) $= g_1(T)g_2(T)$ with $g_i(T)$ distinct irreducible monic quadratic polynomials such that neither of the constant terms is m but their product is m^2. This class also has two distinct eigenspaces, but the paired eigenvalues lie in different eigenspaces, so the eigenspaces are isotropic. Because of this, $g_2(T)$ is uniquely determined by $g_1(T)$ and a choice of m, and in fact the constant terms must be both square or both nonsquare. Fix m. The number of irreducible quadratics with constant term *not* equal to m is

$$\begin{cases} \frac{\ell(\ell-1)}{2}-\frac{\ell-1}{2}=\frac{(\ell-1)^2}{2} & \text{if } m \text{ is square,}\\ \frac{\ell(\ell-1)}{2}-\frac{\ell+1}{2}=\frac{(\ell-1)^2}{2}-1 & \text{if } m \text{ is not square.}\end{cases}$$

by Lemma 6.2.4. Notice that this is even when m is square and odd when m is not square. Choosing $g_1(T)$ determines $g_2(T)$ so we get

$$\frac{1}{2}\left[\frac{(\ell-1)^2}{2}\right]\frac{\ell-1}{2}+\frac{1}{2}\left[\left(\frac{(\ell-1)^2}{2}-1\right)-1\right]\frac{\ell-1}{2}=\frac{(\ell-1)(\ell^2-2\ell-1)}{4}$$

total classes of this type.

- **(Irred Quartic)** charpol$(\gamma) = h(T)$ where $h(T)$ is a monic quartic polynomial with constant term m^2, irreducible over $\mathbb{F}_\ell$. Note that this means that the roots $t_1, \ldots, t_4 \in \mathbb{F}_{\ell^4}$ are in a single Galois orbit under the Galois group of $\mathbb{F}_{\ell^4}$ over

$\mathbb{F}_\ell$. Then $t_1^\ell = t_2$, $t_2^\ell = t_3$, etc, and

$$t_1 t_3 = t_1 t_1^{\ell^2} = t_1^{\ell^2+1} = m \in \mathbb{F}_\ell^\times.$$

Thus t_1 has order ℓ^2+1 in a cyclic group of order ℓ^4-1, implying there are $\frac{\ell^4-1}{\ell^2+1} = \ell^2-1$ choices for t_1. Since t_2, t_3, t_4 are uniquely determined by t_1, this means there are $\frac{\ell^2-1}{4}$ unique sets of roots for the quartic charpol(γ) for each choice of m, or

$$\frac{\ell^2-1}{4}\cdot(\ell-1)$$

total classes of this type.

Case 2: Non-regular elements

The non-regular conjugacy classes are the ones for which charpol(γ) has a repeated root over some extension of $\mathbb{F}_\ell$, or equivalently, those where charpol$(\gamma) \in \mathbb{F}_\ell[T]$ is not squarefree. These classes are not fully determined by their characteristic polynomial; we also need the data of their signed partition.

- **Repeated Irreducible Quadratics**

  - **(RIQ)** charpol$(\gamma) = [g(T)]^2$ where $g(T)$ is an irreducible monic quadratic polynomial. The multiplier m is the constant term of $g(T)$, so the eigenvalues with product m are the roots of $g(T)$. A class of this type has two possible partitions, [1,1] or [2]. Then by Lemma 6.2.4 there are

    $$2\cdot\left(\frac{\ell-1}{2}\cdot\frac{\ell-1}{2}+\frac{\ell+1}{2}\cdot\frac{\ell-1}{2}\right) = \ell(\ell-1)$$

    such classes.

  - **(RIQ*)** charpol$(\gamma) = [g(T)]^2$ with $g(T) = T^2 - m$ for some nonsquare m (so g is irreducible). The roots of $g(T)$ do not have product m; instead, each root of $T^2 - m$ (over $\mathbb{F}_{\ell^2}$) is an eigenvalue which squares to m. A representative of this class type has the form

$$\begin{pmatrix} 0 & 1 & * & * \\ m & 0 & * & * \\ & & 0 & m \\ & & 1 & 0 \end{pmatrix}$$

where the choice of the $*$'s determines the partition: [1,1] or [2]±. Since we only have m nonsquare there are $3 \cdot \frac{\ell-1}{2}$ classes of this type.

- **Repeated linear factors**

  - **(RL/IQ)** (Repeated Linear/Irred Quadratic) $\mathrm{charpol}(\gamma) = g(T)(T-a)^2$ where $g(T)$ a monic irreducible quadratic polynomial with constant term $m = a^2$ and corresponding partition data [1,1] or [2] for $(T-a)$. Note that this $\mathrm{charpol}(\gamma)$ corresponds to a prime ℓ with a factorization which is impossible in a Galois extension (its factors would have different residue degrees, see Corollary 2.1.3). This class only occurs with square multipliers but there are two possible values of a for each m. Then by Lemma 6.2.4 there are
$$2 \cdot \left(2 \cdot \frac{\ell-1}{2} \cdot \frac{\ell-1}{2}\right) = (\ell-1)^2$$
such conjugacy classes.

  - **(RL/Split)** $\mathrm{charpol}(\gamma) = (T-a_1)(T-a_2)(T-a_3)^2$, all $a_i \in \mathbb{F}_\ell^\times$ distinct, with $a_1 a_2 = (a_3)^2 = m$ and partition [1,1] or [2] corresponding to $(T-a_3)$. Note that the factorization of $\mathrm{charpol}(\gamma)$ corresponds to a factorization of the prime ℓ which is impossible in a Galois extension (the factors of ℓ would have different ramification degrees, see Corollary 2.1.3). This class type has square m, two choices of a_3, and $\frac{\ell-3}{2}$ choices for the pair a_1, a_2 by

Lemma 6.2.3, so we get

$$2 \cdot \left(2 \cdot \frac{\ell-3}{2} \cdot \frac{\ell-1}{2}\right) = (\ell-1)(\ell-3)$$

classes.

- **(DRL Ⓐ)** (Double Repeated Linear) charpol(γ) = $[(T-a_1)(T-a_2)]^2$, so that the multiplier is $m = a_1 a_2$, $a_1 \neq a_2$. Then the eigenvalues with product m lie in separate eigenspaces and the eigenspaces of this matrix are isotropic. The class has corresponding partition [1,1] or [2] on the block corresponding to $[(T-a_1)(T-a_2)]$, so the total number of classes is (by Lemma 6.2.3)

$$2 \cdot \left(\frac{\ell-1}{2} \cdot \frac{\ell-3}{2} + \frac{\ell-1}{2} \cdot \frac{\ell-1}{2}\right) = (\ell-1)(\ell-2).$$

- **(DRL Ⓑ)** (Double Repeated Linear) charpol(γ) = $[(T-a)^2]\,[(T+a)^2]$, $a \in \mathbb{F}_\ell^\times$, with a set of partitions $\{[1,1],[1,1]\}$, $\{[1,1],[2]\}$, $\{[2],[1,1]\}$, or $\{[2],[2]\}\pm$. The multiplier $m = a^2$ is the product of eigenvalues within each eigenspace, so they are symplectic subspaces of V. Since m is totally determined by a choice of $a \in \mathbb{F}_\ell^\times$, there are $5 \cdot \frac{\ell-1}{2}$ classes of this type.

- **(QRL)** (Quadruply Repeated Linear) charpol(γ) = $(T-a)^4$, with partition data [1,1,1,1] (the scalar matrices aI), [1,1,2], [2,2]±, or [4] (cyclic). The multiplier is $m = a^2$. For each choice of (square) m we have two choices for a so the number of **QRL** conjugacy classes is

$$5 \cdot \left(2 \cdot \frac{\ell-1}{2}\right) = 5(\ell-1).$$

6.3 Centralizer orders: Regular semisimple classes

A regular semisimple matrix γ is an element of a unique maximal torus of $\mathrm{GSp}_4(\mathbb{F}_\ell)$, and the centralizer of such a γ is that maximal torus [4]. We use the structure of these maximal tori to compute the sizes of the centralizers of regular semisimple elements.

Recall that $\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma)$ is the centralizer of γ in $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Proposition 6.3.1. *Let γ be a regular semisimple element of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$. *Then*

$$\#\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma) = \begin{cases} (\ell-1)^3 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{Full Split}, \\ (\ell+1)^2(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{DIQ SR}, \\ (\ell+1)(\ell-1)^2 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{DIQ NSR}, \\ (\ell^2+1)(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{Irred Quartic}, \end{cases}$$

Proof. Suppose γ is **Full Split**. The centralizer of γ in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is the torus of diagonal matrices over $\mathbb{F}_\ell^\times$. The first three entries of these matrices are free in $\mathbb{F}_\ell^\times$, and the fourth is completely determined by the pairing. Then the size of the torus and centralizer is $(\ell-1)^3$.

If $\mathcal{C}(\gamma)$ is **DIQ SR**, γ is diagonalizable over $\mathbb{F}_{\ell^2}$ with two pairs of Galois conjugate roots on the diagonal such that each conjugate pair has the same product m in $\mathbb{F}_\ell^\times$. Notice that the product of an element t of $\mathbb{F}_{\ell^2}$ with its Galois conjugate t^ℓ gives the norm of t from $\mathbb{F}_{\ell^2}$ to $\mathbb{F}_\ell$. Then any element of this torus is defined by two elements of $\mathbb{F}_{\ell^2}$ with the same norm in $\mathbb{F}_\ell^\times$. The norms of the units in $\mathbb{F}_{\ell^2}$ are equally distributed among the elements of $\mathbb{F}_\ell^\times$, so there are $\frac{\ell^2-1}{\ell-1} = \ell+1$ such elements. Then the centralizer has order $(\ell^2-1)(\ell+1) = (\ell+1)^2(\ell-1)$.

Let $\gamma \in$**DIQ NSR**; such a γ is also diagonalizable over $\mathbb{F}_{\ell^2}$ with two pairs of Galois conjugate roots on the diagonal. Certainly, the conjugate pairs also have their product in $\mathbb{F}_\ell^\times$, but the products need not match; instead, pairs of non-conjugate roots have product m. An element of this torus is then determined by one element of $\mathbb{F}_{\ell^2}$ which has its norm in $\mathbb{F}_\ell^\times$ and a choice of $m \in \mathbb{F}_\ell^\times$. Then the size of this torus is $(\ell^2 - 1)(\ell - 1) = (\ell + 1)(\ell - 1)^2$.

Lastly, let $\mathcal{C}(\gamma)$ be of type **Irred Quartic**. The element γ has eigenvalues t, t^ℓ, t^{ℓ^2}, and t^{ℓ^3} in $\mathbb{F}_{\ell^4}$ in one orbit under the action of Galois. Two pairs of eigenvalues have product in $\mathbb{F}_\ell^\times$ by the multiplier condition; if $tt^\ell \in \mathbb{F}_\ell^\times$ then we have that t lies in a degree two extension of $\mathbb{F}_\ell$, which is a contradiction. Thus $tt^{\ell^2} = m \in \mathbb{F}_\ell^\times$. Notice that the map $t \mapsto tt^{\ell^2}$ is the norm map of $\mathbb{F}_{\ell^4}$ over $\mathbb{F}_{\ell^2}$, so we count elements of $\mathbb{F}_{\ell^4}^\times$ whose norm over $\mathbb{F}_{\ell^2}$ lies in $\mathbb{F}_\ell^\times$. There are $\frac{\ell^4-1}{\ell^2-1} \cdot (\ell - 1) = (\ell^2 + 1)(\ell - 1)$ of these, which is then the size of the torus and thus the centralizer. □

Take a regular semisimple matrix γ from $\mathrm{GSp}_4(\mathbb{F}_\ell)$, and consider the elements $\tilde{\gamma} \in \mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ such that $\tilde{\gamma} \equiv \gamma \bmod \ell$ (we call $\tilde{\gamma}$ a *lift* of γ).

Lemma 6.3.2. *For any regular semisimple conjugacy class $\mathcal{C}$ in $\mathrm{GSp}_4(\mathbb{F}_\ell)$, there are $\ell^{3(r-1)}$ regular semisimple conjugacy classes in $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ which reduce to $\mathcal{C}$ mod ℓ.*

Proof. Let $\gamma \in \mathcal{C}$. The conjugacy class of a regular semisimple element is entirely determined by its characteristic polynomial charpol(γ) and the multiplier m. Since charpol(γ) has distinct roots mod ℓ, any $\tilde{f}(T) \in (\mathbb{Z}/\ell^r)[T]$ with $\tilde{f} \equiv \mathrm{charpol}(\gamma) \bmod \ell$ will also have distinct roots. Every lift of

$$\mathrm{charpol}(\gamma) = T^4 + aT^3 + bT^2 + amT + m^2$$

can be constructed by lifting each of a, b, m. There are ℓ^{r-1} lifts of any element of $\mathbb{F}_\ell$ to $\mathbb{Z}/\ell^r$, so there are $\ell^{3(r-1)}$ distinct lifts $\tilde{f}$ of charpol(γ), each of which determines a unique conjugacy class. Then there are $\ell^{3(r-1)}$ regular semisimple conjugacy classes in $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ over each regular semisimple class in $\mathrm{GSp}_4(\mathbb{F}_\ell)$. □

6.4 Centralizer orders: Non-regular classes

In this section we will determine the centralizer orders of elements of the cyclic non-regular classes. We will ignore class types where $f \in \mathbb{Z}[T]$ with $f \equiv \operatorname{charpol}(\gamma) \bmod \ell$ is such that the field $\operatorname{Split}(f)$ is not Galois. Thus we only consider the conjugacy classes **DRL** $\textcircled{\textbf{A}}[2]$, **DRL** $\textcircled{\textbf{B}}\{[2],[2]\}\pm$, **RIQ**[2], **RIQ***[2]±, and **QRL**[4].

Since these classes are non-regular, we cannot find their centralizer orders as we did in Proposition 6.3.1. Instead, we find the orders of their centralizers by finding an explicit representative of the class and the centralizer. We begin over $\mathbb{F}_\ell$.

Proposition 6.4.1. *Suppose $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ is a cyclic non-regular matrix in one of the conjugacy classes listed above. Then*

$$\#\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma) = \begin{cases} \ell(\ell-1)^2 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{DRL } \textcircled{\textbf{A}}[2], \\ 2\ell^2(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{DRL}\textcircled{\textbf{B}}\{[2],[2]\}+ \text{ or } \textbf{DRL}\textcircled{\textbf{B}}\{[2],[2]\}-, \\ \ell(\ell^2-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{RIQ}[2], \\ 2\ell^2(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{RIQ*}[2]+ \text{ or } \textbf{RIQ*}[2]-, \\ \ell^2(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{QRL}[4]. \end{cases}$$

Proof. For each listed conjugacy class, we will provide a conjugacy class representative γ such that $\operatorname{charpol}(\gamma)$ is of the correct form, $\operatorname{minpol}(\gamma) = \operatorname{charpol}(\gamma)$, and γ satisfies $\gamma^T J \gamma = mJ$ where m is the multiplier of γ. (Alternatively, the blocks of γ satisfy the conditions of (6.1.1).) We will also list a generic member C of the centralizer of γ, so that we can find the size of $\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma)$. The conditions to show that γ is a representative of the right class, and that C is an element of the centralizer of γ in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ are straightforward to verify, and so we omit them here.

- An element $\gamma \in$**DRL** $\textcircled{\textbf{A}}[2]$ has characteristic polynomial $[(T-a)(T-b)]^2$ with

$a \neq b \in \mathbb{F}_\ell^\times$ and multiplier $m = ab$. Let

$$\gamma = \begin{pmatrix} a & a & & \\ & a & & \\ & & b & \\ & & -b & b \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} c_1 & c_3 & & \\ & c_1 & & \\ & & c_2 & \\ & & z & c_2 \end{pmatrix}$$

where $c_1, c_2 \in (\mathbb{F}_\ell)^\times$, $c_3 \in \mathbb{F}_\ell$, and $z = -\frac{c_2 c_3}{c_1}$. Then we see $\#\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma) = \ell(\ell-1)^2$.

• For $\gamma \in$**DRL** $\textcircled{\textbf{B}}\{[2],[2]\}+$ or **DRL** $\textcircled{\textbf{B}}\{[2],[2]\}-$, $\mathrm{charpol}(\gamma) = (T-a)^2(T+a)^2$ with $a \in \mathbb{F}_\ell^\times$ and γ has multiplier $m = a^2$. The plus and minus denote separate classes with the same characteristic polynomial, so we provide two representatives,

$$\gamma_1 = \begin{pmatrix} a & & 1 & \\ & -a & & 1 \\ & & a & \\ & & & -a \end{pmatrix} \quad \text{and} \quad \gamma_2 = \begin{pmatrix} a & & 1 & \\ & -a & & x \\ & & a & \\ & & & -a \end{pmatrix}$$

where $\gamma_1 \in$**DRL** $\textcircled{\textbf{B}}\{[2],[2]\}+$, $\gamma_2 \in$**DRL** $\textcircled{\textbf{B}}\{[2],[2]\}-$, and $x \in \mathbb{F}_\ell^\times$ is nonsquare. These matrices are not conjugate in $\mathrm{GSp}_4(\mathbb{F}_\ell)$; over $\mathrm{GL}_4(\mathbb{F}_\ell)$ there exists a matrix

$$Z = \begin{pmatrix} z_1 & & z_3 & \\ & z_2 & & z_4 \\ & & z_1 & \\ & & & z_2 x \end{pmatrix}$$

such that $\gamma_1 \sim \gamma_2$ via Z. If Z is an element of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ then $z_1^2 = z_2^2 x$, which is impossible since x is nonsquare. The matrix

$$C = \begin{pmatrix} c_1 & & c_3 & \\ & c_2 & & c_4 \\ & & c_1 & \\ & & & c_2 \end{pmatrix}$$

centralizes both γ_1 and γ_2 with the conditions that $c_1, c_2 \in (\mathbb{F}_\ell)^\times$, $c_3, c_4 \in \mathbb{F}_\ell$, and $c_1^2 = c_2^2 \Rightarrow c_1 = \pm c_2$. Then each class has a centralizer of order $2\ell^2(\ell - 1)$.

• Suppose $\gamma \in$**RIQ**[2]. Then charpol(γ) $= (T^2 - \tau T + m)^2 = g(T)^2$ for $g(T)$ irreducible, and the multiplier of γ is m. Let

$$\gamma = \begin{pmatrix} 0 & 1 & x & y \\ -m & \tau & 0 & -mx + \tau y \\ & & \tau & m \\ & & -1 & 0 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ -mc_2 & c_1 + \tau c_2 & v & w \\ & & c_1 + \tau c_2 & mc_2 \\ & & -c_2 & c_1 \end{pmatrix}$$

where $v = -a\tau c_2 + bc_2 + \tau c_3 - c_4$ and $w = -2amc_2 + b\tau c_2 + mc_3$. The matrix C is an element of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ if and only if c_1, c_2, c_3, c_4 satisfy the following conditions:

$$c_1^2 + \tau c_1 c_2 + mc_2^2 \neq 0 \tag{6.4.1}$$

$$vc_1 + wc_2 + mc_2c_3 - \tau c_2 c_4 + c_1 c_4 = 0. \tag{6.4.2}$$

One can verify the following quadruples satisfy both of these conditions and account for all possible such quadruples.

c_1	c_2	c_3	c_4
$\in \mathbb{F}_\ell^\times$	0	$\in \mathbb{F}_\ell$	$\frac{\tau c_3}{2}$
0	$\in \mathbb{F}_\ell^\times$	$\frac{1}{2m}\left(2amc_2 - \tau bc_2 + \tau c_4\right)$	$\in \mathbb{F}_\ell$
$\frac{-\tau c_2}{2}$	$\in \mathbb{F}_\ell^\times$	$ac_2 - \frac{b\tau c_2}{\tau^2-4m}$	$\in \mathbb{F}_\ell$
$\in \mathbb{F}_\ell^\times, \neq \frac{-\tau c_2}{2}$	$\in \mathbb{F}_\ell^\times$	$\in \mathbb{F}_\ell$	c_4

$$\text{where } \ c_4 = \frac{2mc_2c_3 - 2amc_2^2 + \tau bc_2^2 - a\tau c_1c_2 + bc_1c_2 + \tau c_1c_3}{2c_1 + \tau c_2}.$$

Since $g(T) = T^2 - \tau T + m$ is irreducible by assumption, $\tau^2 - 4m = \Delta(g) \neq 0$. Then we have

$$\ell(\ell-1) + \ell(\ell-1) + \ell(\ell-1) + \ell(\ell-1)(\ell-2) = \ell(\ell^2-1)$$

elements which satisfy conditions (6.4.1) and (6.4.2).

• If $\gamma \in$**RIQ***[2]+ or **RIQ***[2]−, charpol$(\gamma) = (T^2 - m)^2$ where m is nonsquare in $(\mathbb{F}_\ell)^\times$ and is the multiplier of γ. This type has two conjugacy classes, but we give two representatives $\gamma_{2,1}$ and $\gamma_{2,2}$ for **RIQ***[2]− because the representatives we give depend on the congruence class of ℓ mod 4. Let

$$\gamma_1 = \begin{pmatrix} & 1 & & 1+m \\ m & & 2m & \\ & & & m \\ & & 1 & \end{pmatrix}, \gamma_{2,1} = \begin{pmatrix} & 1 & -x & \\ m & & ym & -xm \\ & & & m \\ & & 1 & \end{pmatrix}, \gamma_{2,2} = \begin{pmatrix} & 1 & -1 & \\ m & & & -m \\ & & & m \\ & & 1 & \end{pmatrix}$$

with $x, y \in \mathbb{F}_\ell^\times$ such that $-4x^2 + my^2 = w$ is a square in $\mathbb{F}_\ell^\times$. We will use $\gamma_{2,1}$ if $\ell \equiv 3$ mod 4 and $\gamma_{2,2}$ if $\ell \equiv 1$ mod 4.

Over $\mathrm{GL}_4(\mathbb{F}_\ell)$, γ_1 and $\gamma_{2,1}$ are conjugate via

$$Z_1 = \begin{pmatrix} \frac{v}{w}(yz_1 + 2xz_2) & \frac{v}{wm}(2xz_1 + ymz_2) & z_3 & z_4 \\ \frac{v}{w}(2xz_1 + ymz_2) & \frac{v}{w}(yz_1 + 2xz_2) & \frac{1}{w}t & \frac{1}{w}u \\ & & z_1 & mz_2 \\ & & z_2 & z_1 \end{pmatrix}$$

where

$$\begin{aligned} t &= vxyz_1 - (2(m-1)x^2 - 2y^2m^2)z_2 - wz_4, \\ u &= (2(1-m)x^2 - (m+1)y^2m)z_1 - vxyz_2 - mwz_3, \end{aligned}$$

and $v = 3m + 1$. The matrix Z_1 is in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ if and only if

$$4xz_1z_2 + y(z_1^2 + mz_2^2) \neq 0 \tag{6.4.3}$$

$$\text{and} \ \ ymz_1z_2 + x(z_1^2 + mz_2^2) = 0. \tag{6.4.4}$$

When $\ell \equiv 3 \bmod 4$, there exist pairs z_1, z_2 so that $z_1^2 + mz_2^2 \equiv 0 \bmod \ell$ with both of z_1 and z_2 nonzero (for example, let $\ell = 7, z_1 = 1, z_2 = 3, m = 3$). Then to guarantee condition (6.4.3) we must have $z_1z_2 \neq 0$. However, if $z_1z_2 \neq 0$ condition (6.4.4) fails. Thus, Z_1 does not conjugate γ to $\gamma_{2,1}$ in $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Over $\mathrm{GL}_4(\mathbb{F}_\ell)$, γ and $\gamma_{2,2}$ are conjugate by

$$Z_2 = \begin{pmatrix} \frac{-v}{2}z_1 & \frac{-v}{2m}z_2 & z_3 & z_4 \\ \frac{-v}{2}z_2 & \frac{-v}{2}z_1 & \frac{m-1}{2}z_1 + z_4 & \frac{m+1}{2}z_2 + mz_3 \\ & & z_2 & mz_1 \\ & & z_1 & z_2 \end{pmatrix}$$

where $v = 3m+1$. We have that Z_2 is an element of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ if and only if $-vz_1z_2 \neq 0$

and $\frac{-v}{2}(mz_1^2 + z_2^2) = 0$; then both $z_1, z_2 \neq 0$ and $mz_1^2 = -z_2^2$. Recall m is nonsquare; when $\ell \equiv 1 \bmod 4$, mz_1^2 is nonsquare, but $-z_2^2$ is square. Then γ_1 and $\gamma_{2,2}$ are not conjugate over $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

The centralizers of the three representatives are nearly identical. Let

$$C_i = \begin{pmatrix} c_1 & c_2 & c_3 & c_4 - s_i c_2 \\ mc_2 & c_1 & c_4 & mc_3 \\ & & c_1 & mc_2 \\ & & c_2 & c_1 \end{pmatrix}$$

where $s_1 = m - 1$, $s_{2,1} = ym$, and $s_{2,2} = 0$ so that C_i centralizes γ_i. Each $C_i \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ if $c_1^2 + mc_2^2 \neq 0$ and $c_1 c_2 = 0$; then exactly one of c_1, c_2 is zero and the other is a unit in $\mathbb{F}_\ell$, and $c_3, c_4 \in \mathbb{F}_\ell$. Thus each centralizer has order $2\ell^2(\ell - 1)$.

• Lastly, if $\gamma \in$(**QRL**[4]) then $\mathrm{charpol}(\gamma) = (T-a)^4$ for $a \in (\mathbb{F}_\ell)^\times$ and γ has multiplier $m = a^2$. Then we have representatives

$$\gamma = \begin{pmatrix} a & -1 & & \\ & a & 1 & a \\ & & a & \\ & & 1 & a \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} z & c_1 & c_2 & c_3 \\ & z & -(c_1 + c_3) & -ac_1 \\ & & z & 0 \\ & & -c_1 & z \end{pmatrix}$$

where $z = \frac{-ac_1^2}{c_1 + 2c_3}$ with $c_1 \in (\mathbb{F}_\ell)^\times$ and $c_2, c_3 \in \mathbb{F}_\ell$. Then $\#\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma) = \ell^2(\ell - 1)$.

□

Remark 6.4.2. Notice that all of the conjugacy classes we have identified (both these cyclic non-regular conjugacy classes and the regular semisimple classes) have centralizers which are three dimensional. All of them are also connected, except for the classes **DRL** Ⓑ{[2], [2]} ± and **RIQ***[2]± which have two components each. Notice that the failure of connectedness coincides exactly with class types which have the ±

conjugacy classes.

Now consider any lift $\tilde{\gamma}$ of a γ in one of these cyclic non-regular classes. We want to construct a result similar to Lemma 6.3.2 for these non-regular elements, and then count the number of lifts of any cyclic $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$. Notice that any lift of a cyclic matrix is also cyclic (use Nakayama's Lemma to lift the basis).

We begin with a classical result about decomposing modules over certain rings.

Lemma 6.4.3 (Fitting's Lemma)**.** *[5, §15.1] Let R be a finite local ring, and let α be a linear transformation on a module V of dimension n over R. There exists a (unique) decomposition of V as $V = X \oplus Y$ such that α acts nilpotently on X and bijectively on Y. In particular, there exists an $N \in \mathbb{N}$ such that*

$$V = \ker \alpha^N \oplus \operatorname{im} \alpha^N.$$

Let α be defined in terms of a matrix $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ such that $\ker \alpha^N$ gives an eigenspace of γ (as defined in (6.2.1)). Then $\dim \ker \alpha^N$ is fixed for a choice of γ and eigenspace, and since γ is cyclic, $\ker \alpha^N$ has a basis of the form $\{\gamma^i x\}_{i \in I}$ for some set I and vector x. For a lift $\tilde{\gamma}$ of γ then $\{\tilde{\gamma}^i \tilde{x}\}_{i \in I}$ is a basis for $\ker \tilde{\alpha}^N$ with the same dimension and so eigenspaces are stable under lifting for cyclic matrices.

Then we have the following results

Proposition 6.4.4. *For every lift $\tilde{\gamma} \in \mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ of a cyclic $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$, $\mathcal{C}(\tilde{\gamma})$ is of the same type as $\mathcal{C}(\gamma)$.*

Proof. Since $\tilde{\gamma}$ reduces to γ mod ℓ, $\mathrm{charpol}(\tilde{\gamma}) \equiv \mathrm{charpol}(\gamma) \bmod \ell$. A factorization of a polynomial mod ℓ^r reduces to one mod ℓ, so the degrees of the irreducible factors of $\mathrm{charpol}(\tilde{\gamma})$ are the same as those of $\mathrm{charpol}(\gamma)$. The eigenspaces of γ are preserved under lifting and so the action of the symplectic pairing on the eigenspaces is preserved under lifting. Thus, the multiplier of $\tilde{\gamma}$ is a lift of the multiplier of γ and is computed using corresponding eigenvalues of $\tilde{\gamma}$.

If the factors of charpol(γ) are distinct then so are the factors of charpol($\tilde{\gamma}$), and so a regular semisimple $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ has that $\mathcal{C}(\tilde{\gamma})$ is of the same type as $\mathcal{C}(\gamma)$ for all $\tilde{\gamma}$.

Otherwise, consider a non-regular cyclic $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$. A matrix $\tilde{\gamma}$ in one of the regular semisimple classes is diagonalizable over an extension of $\mathbb{Z}/\ell^r$, but a non-regular cyclic γ is not diagonalizable over any extension of $\mathbb{F}_\ell$, so no reduction of a regular semisimple element can be non-regular and cyclic. Then, every lift $\tilde{\gamma}$ of a non-regular cyclic γ must be of the same class type as γ. □

Proposition 6.4.5. *[Lemma 6.3.2, generalized] Given a cyclic matrix in* $\mathrm{GSp}_4(\mathbb{F}_\ell)$*, denote its conjugacy class by* $\mathcal{C}$*. Then there are* $\ell^{3(r-1)}$ *cyclic conjugacy classes* $\tilde{\mathcal{C}}$ *in* $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ *which reduce to* $\mathcal{C}$ *mod* ℓ*.*

Proof. Let γ be any cyclic matrix in $\mathrm{GSp}_4(\mathbb{F}_\ell)$. The conjugacy class $\mathcal{C}$ of γ is completely determined by its characteristic polynomial and the action of the pairing on the eigenspace decomposition of γ. As stated in the proof of Lemma 6.3.2, each lift of

$$\mathrm{charpol}(\gamma) = T^4 + aT^3 + bT^2 + amT + m^2$$

is distinct, so there are $\ell^{3(r-1)}$ distinct cyclic conjugacy classes $\tilde{\mathcal{C}}$ in $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ which reduce to $\mathcal{C}$ mod ℓ. □

Proposition 6.4.6. *Let* $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ *be a cyclic matrix and choose* $\tilde{\gamma} \in \mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ *a lift of* γ*. Then*

$$\#\mathcal{C}(\tilde{\gamma}) = \ell^{8(r-1)} \cdot \#\mathcal{C}(\gamma).$$

Proof. Let γ and $\tilde{\gamma}$ be as stated. By Lemma 6.4.4, every $\tilde{\gamma}$ is of the same conjugacy class type as γ; then every $\tilde{\gamma}$ is of the same type and thus have conjugate centralizers, so each $\mathcal{C}(\tilde{\gamma})$ has the same order. The previous lemma gives that there are $\ell^{3(r-1)}$ such conjugacy classes $\mathcal{C}(\tilde{\gamma})$ lying above $\mathcal{C}(\gamma)$. There are $\ell^{11(r-1)}$ total lifts of γ in

$\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ since the dimension of GSp_4 is 11. Then

$$\#\mathcal{C}(\tilde{\gamma}) = \frac{\#\left\{\text{Lifts of elements of } \mathcal{C}(\gamma)\right\}}{\#\left\{\text{Conjugacy classes of lifts}\right\}} = \frac{\ell^{11(r-1)} \cdot \#\mathcal{C}(\gamma)}{\ell^{3(r-1)}} = \ell^{8(r-1)} \cdot \#\mathcal{C}(\gamma).$$

□

Remark 6.4.7. The non-cyclic Case 2 conjugacy classes have more complicated lifting. In general, the invariant spaces that are forced to stay separate in cyclic elements could combine for non-cyclic classes with repeated roots. For example, a non-regular matrix γ with partition [1,1] could have a lift $\tilde{\gamma}$ into a class with a [2] partition. This is analogous to the situation in $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ where a scalar matrix dI can lift to a nonscalar matrix $dI + \ell^j\beta$ (see Appendix A). Unfortunately, without the nice decomposition we had in section 4, tracking such lifts becomes more complicated.

7. PRIMES, CONJUGACY CLASSES, AND CHARACTERS IN IMAGINARY QUARTIC EXTENSIONS

Fix a polynomial $f(T) = T^4 + aT^3 + bT^2 + amT + m^2$, a possible characteristic polynomial of the Frobenius endomorphism of an abelian surface over a finite field and let $K = \mathrm{Split}(f)$ so that K is a totally imaginary quartic Galois extension of $\mathbb{Q}$, with either $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4$ or $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. In this section we consider how primes split in each such K and associate to each splitting a cyclic conjugacy class of $\mathrm{GSp}_4(\mathbb{F}_\ell)$, and use this association to extend the characters $\chi \in X \smallsetminus X^+$ to maps on $\mathbb{Z}$.

The correspondence between primes of $\mathbb{Z}$ and cyclic conjugacy classes of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is determined as follows. Proposition 3.0.1 gives a bijection between the factorization of a rational prime ℓ in $\mathcal{O}_K$ and the factorization of f mod ℓ from which we can determine the type and multiplicity of the eigenvalues of $\gamma \in \mathcal{C}(f \bmod \ell)$. Then to uniquely determine a cyclic class of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ we need to understand the eigenspace decomposition of the vector space V that was discussed in section 6.2. In other words, we need to understand how $\gamma \in \mathcal{C}(f \bmod \ell)$ acts on V.

For each prime ℓ, we also compute $\mathcal{O}_K/\ell$, a vector space over $\mathbb{F}_\ell$. To complete the association between primes ℓ and conjugacy classes, we relate the structure of $\mathcal{O}_K/\ell$ as a vector space and the action of complex conjugation on its subspaces to the eigenspace decomposition of V under γ and the action of the pairing on that decomposition.

As we are only concerned with the cyclic conjugacy classes of $\mathrm{GSp}_4(\mathbb{F}_\ell)$, the information of the factorization of f mod ℓ and the action of the pairing on the eigenspaces is enough to fully determine a conjugacy class.

In order to define $\chi \in X \smallsetminus X^+$ on primes ℓ, we will also identify, when possible, a Frobenius element which generates the extension of residue fields of a prime in the factorization of $\ell\mathcal{O}_K$.

7.1 Complex conjugation in $\mathcal{O}_K$ and eigenspaces of γ

Suppose that an abelian surface $A/\mathbb{F}_q$ has complex multiplication by $\mathcal{O}_K \subseteq \mathrm{End}(A)$. The variety A has a polarization which is compatible with the action of complex conjugation on $\mathcal{O}_K$ in the following way [20, 17].

For each rational prime, $\mathcal{O}_K$ acts on $T_\ell(A)$ (defined by (2.4.1)), producing a homomorphism

$$\rho_\ell : \mathcal{O}_K \longrightarrow \mathrm{End}(T_\ell(A)) \cong \mathrm{Mat}_{2g}(\mathbb{Z}_\ell)$$

as in (2.4.2). The polarization induces a skew-symmetric map

$$\begin{array}{ccc} T_\ell(A) \times T_\ell(A) & \longrightarrow & \mathbb{Z}_\ell \\ x \times y & \mapsto & \langle x, y \rangle \end{array}$$

so that if $\bar{\alpha}$ is the image under complex conjugation of $\alpha \in \mathcal{O}_K$,

$$\langle \rho_\ell(\alpha)x, y \rangle = \langle x, \rho_\ell(\bar{\alpha})y \rangle .$$

Extend ρ_ℓ to

$$\mathcal{O}_K \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{End}(T_\ell(A))$$

and thus to

$$\bar{\rho}_\ell : \mathcal{O}_K \otimes \mathbb{Z}/\ell \longrightarrow \mathrm{End}(A[\ell][\bar{K}]).$$

If $\alpha \in \mathcal{O}_K$ is the Frobenius element of $A/\mathbb{F}_q$, the matrix $\gamma = \bar{\rho}_\ell(\alpha)$ has characteristic polynomial $f(T) \in \mathbb{Z}[T]$. Over an algebraic closure, γ has an eigenvalue $z \in \bar{\mathbb{F}}_\ell$ with eigenspace V_z; then V_z and $V_{\bar{z}}$ are dual as vector spaces.

Since we are not working over an algebraic closure of $\mathbb{F}_\ell$, we instead use the eigenspace decomposition given by (6.2.1) corresponding to the irreducible factors of

$$f = \mathrm{charpol}(\gamma) = \prod_i f_i(T)^{n_i}.$$

We will consider the eigenspaces V_{f_i} and determine if V_{f_i} is its own dual, or if distinct V_{f_i} are dual to each other, as in section 6.1.

The result of this information is that we can relate the action of complex conjugation on the factors of ℓ in $\mathcal{O}_K$ with how the eigenspaces of γ sit with respect to the pairing. This in turn will give us a way to distinguish between the conjugacy classes with the same factorization of their characteristic polynomial.

7.2 Cyclic quartic extensions

Suppose $K = \mathrm{Split}(f)$ is cyclic (i.e., $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4$). Then K has just one subfield of degree (and index) two. It is a totally real quadratic field, and it we denote it by K^+.

$$\begin{tikzcd}
K \arrow[d, dash] & \supset & \mathcal{O}_K & \lambda \\
K^+ \arrow[d, dash] & \supset & \mathcal{O}_{K^+} \arrow[u, hook] & \lambda^+ \\
\mathbb{Q} & \supset & \mathbb{Z} \arrow[u, hook] & \ell
\end{tikzcd}$$

We have $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \sigma^2 = cc, \sigma^3\} = \langle\sigma\rangle$, where σ has order four and $\sigma^2 = cc$ is complex conjugation. Note that $\mathrm{Gal}(K/K^+) = \langle\sigma^2\rangle$ and $\mathrm{Gal}(K^+/\mathbb{Q}) = \langle\sigma\rangle \mod \sigma^2$.

We will consider all possible combinations of decomposition and inertia groups for a prime $\lambda \subset \mathcal{O}_K$ which lies over ℓ. Recall from section 2.1 that

$$I(\lambda/\ell) \leq D(\lambda/\ell) \leq \mathrm{Gal}(K/\mathbb{Q}),$$
$$\#D(\lambda/\ell) = e(\lambda)f(\lambda),\ \#I(\lambda/\ell) = e(\lambda), \text{ and } efr = n = 4$$

by Lemmas 2.1.8 and 2.1.5. We also will use Lemma 2.1.12; let

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(K^+/\mathbb{Q})$$

be the natural projection such that $\psi : \sigma \mapsto \sigma \bmod \sigma^2$. Then in this context Lemma 2.1.12 says

$$D(\lambda^+/\ell) = \psi(D(\lambda/\ell)) = D(\lambda/\ell) \bmod \sigma^2,$$
$$\text{and } I(\lambda^+/\ell) = \psi(I(\lambda/\ell)) = I(\lambda/\ell) \bmod \sigma^2.$$

Let ℓ be a rational prime, let (e, f, r) be the factorization invariants of $\lambda \subset \mathcal{O}_K$ over ℓ, and let $(e, f, r)^+$ be the factorization invariants of $\lambda^+ \subset \mathcal{O}_{K^+}$ over ℓ.

1. Suppose $D(\lambda/\ell) = \{1\}$; then $I(\lambda/\ell) = \{1\}$ also. Since ℓ is unramified in K, we use the corollary to Theorem 2.1.7 and the fact that $\mathrm{Frob}_K(\ell)$ generates $\mathrm{Gal}(\kappa(\lambda)/\kappa(\ell))$ to say that

   $$\{1\} = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell)) \Rightarrow \mathrm{Frob}_K(\ell) = 1.$$

   Notice that in this case $(e, f, r) = (1, 1, 4)$, so ℓ splits completely in K. By Proposition 3.0.1, $f \bmod \ell$ factors completely and this corresponds to a conjugacy class of type **Full Split**.

2. Suppose $D(\lambda/\ell) = \langle\sigma^2\rangle$.

   (a) Suppose $I(\lambda/\ell) = \{1\}$. Then using the same argument as above,

   $$\langle\sigma^2\rangle = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell)) \Rightarrow \mathrm{Frob}_K(\ell) = \sigma^2.$$

Using Lemma 2.1.12, $D(\lambda^+/\ell) = D(\lambda/\ell) \bmod \sigma^2 = \{1\}$ so the action of complex conjugation is trivial on λ^+. Since $(e, f, r) = (1, 2, 2)$ and $f^+ = 1$, we have that $\mathcal{O}_K/\ell \cong \mathbb{F}_{\ell^2} \oplus \mathbb{F}_{\ell^2}$ where complex conjugation acts independently on each summand. Then $f \bmod \ell$ has two distinct quadratic factors and the conjugacy class has symplectic eigenspaces, so the class type is **DIQ SR**.

(b) Suppose $I(\lambda/\ell) = \langle\sigma^2\rangle$. Now $(e, f, r) = (2, 1, 2)$ and

$$\mathcal{O}_K/\ell \cong \frac{\mathbb{F}_\ell[T]}{(T)^2} \oplus \frac{\mathbb{F}_\ell[T]}{(T)^2}.$$

As above, $D(\lambda^+/\ell) = \{1\}$ so $(e, f, r)^+ = (1, 1, 2)$ implies $\mathcal{O}_{K^+}/\ell \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell$. Complex conjugation acts trivially on λ^+ and so acts independently on each summand of $\mathcal{O}_K/\ell$. By Proposition 3.0.1, $f \bmod \ell = (T-a)^2(T-b)^2$, and $\mathcal{C}(f \bmod \ell)$ has symplectic eigenspaces, so $\mathcal{C}(f \bmod \ell)$ is a class of the type **DRL** Ⓑ.

3. Suppose $D(\lambda/\ell) = \langle\sigma\rangle$.

(a) Suppose $I(\lambda/\ell) = \{1\}$. Then by Theorem 2.1.7 we have

$$\langle\sigma\rangle = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell));$$

in this case, since $\langle\sigma\rangle = \langle\sigma^3\rangle$, we only know that $\mathrm{Frob}_K(\ell) = \sigma$ or σ^3. (For our purposes, this is enough information; see Remark 7.2.1.) This factorization has $(e, f, r) = (1, 4, 1)$ so ℓ is inert in K. Then $f \bmod \ell$ is irreducible by Proposition 3.0.1 and the corresponding conjugacy class type is **Irred Quartic**.

(b) Suppose $I(\lambda/\ell) = \langle\sigma^2\rangle$. Lemma 2.1.12 gives that $I(\lambda^+/\ell) = \{1\}$ and $D(\lambda^+/\ell) = \langle\sigma\rangle \bmod \sigma^2$ (a group of order two), so $(e, f, r)^+ = (1, 2, 1)$ and

$\mathcal{O}_{K^+}/\lambda^+ \cong \mathcal{O}_{K^+}/\ell \cong \mathbb{F}_{\ell^2}$. Complex conjugation acts trivially on $\lambda^+ \subset K^+$ (and thus on $\mathcal{O}_{K^+}/\ell$), and since $cc \in I(\lambda/\ell)$, cc acts trivially mod λ. However, the higher ramification group

$$G_1 = \left\{\sigma \in \operatorname{Gal}(K/\mathbb{Q}) | \sigma(x) \equiv x \bmod \lambda^2\right\}$$

is an ℓ-group by Corollary 3 to Proposition 7 in Chapter IV of Serre [19]. Since $\ell > 2$, G_1 (a subgroup of $\operatorname{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4$) must be trivial, and so cc acts nontrivially mod λ^2. As a ring,

$$\mathcal{O}_K/\ell \cong \mathcal{O}_K/\lambda^2 \cong \frac{\mathbb{F}_{\ell^2}[T]}{(T)^2}$$

so f mod ℓ factors as a quadratic squared by Proposition 3.0.1. As a module over $\mathbb{F}_{\ell^2}$,

$$\mathcal{O}_K/\ell \cong \mathcal{O}_K/\lambda^2 \cong \mathbb{F}_{\ell^2} \oplus T\mathbb{F}_{\ell^2}$$

and the nontrivial action of cc is given by $a + bT \mapsto a - bT$.

A representative γ of the corresponding class acts on $(\mathbb{F}_\ell)^{\oplus 4} = (\mathbb{F}_{\lambda^+})^{\oplus 2}$ since ℓ is inert in K^+. The characteristic polynomial of γ over $\mathbb{F}_{\lambda^+}$ is $(T-\mu)^2$, where $\mu \in \mathbb{F}_{\lambda^+} \cong \mathbb{F}_{\ell^2}$ such that $\mu^2 = m$, so $\gamma = \left(\begin{smallmatrix} \mu & * \\ & \mu \end{smallmatrix}\right)$ over $\mathbb{F}_{\lambda^+}$ (where $*$ is a unit so that the matrix γ is cyclic). Then γ acting on $(\mathbb{F}_\ell)^{\oplus 4}$ is given by

$$\gamma = \begin{pmatrix} 0 & 1 & * & * \\ m & 0 & * & * \\ & & 0 & m \\ & & 1 & 0 \end{pmatrix}$$

and thus the associated conjugacy class type is **RIQ***.

(c) Suppose $I(\lambda/\ell) = \langle\sigma\rangle$. Then $(e, f, r) = (4, 1, 1)$ and ℓ is totally ramified in

K. Proposition 3.0.1 says that $f \bmod \ell = (T-a)^4$, so the corresponding conjugacy class type is **QRL**.

The character group is $X = \{\chi_0, \chi, \chi^2, \chi^3 = \bar{\chi}\} = \langle \chi \rangle$ and without loss of generality, $\chi : \sigma \mapsto i$ so $\chi^2 : \sigma \mapsto -1$ and $\chi^3 = \bar{\chi} : \sigma \mapsto -i$. As stated in section 2.2, to each of these characters χ^i we associate the subfield of K that is fixed by $\ker(\chi^i)$:

$$\chi \longleftrightarrow K, \quad \chi^2 \longleftrightarrow K^+, \text{ and } \quad \chi^3 = \bar{\chi} \longleftrightarrow K.$$

Then $X^+ = \{\chi_0, \chi^2\}$ is the set of characters associated to K^+.

We define (as stated in section 3)

$$\chi(\ell) = \begin{cases} \chi(\mathrm{Frob}_K(\ell)) & \text{if } \ell \text{ is unramified in } K, \\ 0 & \text{if } \ell \text{ is ramified in } K. \end{cases}$$

Then for K a totally imaginary cyclic quartic number field, we see that

$$\chi(\ell) = \begin{cases} \chi(1) = 1 & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{Full Split} \\ \chi(\sigma^2) = -1 & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{DIQ SR}, \\ \chi(\sigma) = i \text{ or } \chi(\sigma^3) = -i & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{Irred Quartic}, \\ 0 & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{QRL}, \textbf{DRL } \textcircled{\textbf{B}}, \text{ or } \textbf{RIQ*}. \end{cases} \tag{7.2.1}$$

Remark 7.2.1. In the **Irred Quartic** case, the ambiguity of the Frobenius element has no effect on the product of Euler factors

$$\frac{1}{1 - \frac{\chi(\ell)}{\ell}} \cdot \frac{1}{1 - \frac{\bar{\chi}(\ell)}{\ell}}.$$

7.3 Biquadratic quartic extensions

Suppose $K = \text{Split}(f)$ is biquadratic (i.e., $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$). Then K has three subfields of degree two; two imaginary quadratic fields, K_1 and K_2, and one real quadratic field, K^+. Let $a \neq b$ be positive squarefree integers.

$$\begin{tikzcd}
 & K = \mathbb{Q}(\sqrt{-a}, \sqrt{-b}) \arrow[dl, dash, "\langle\sigma\rangle"'] \arrow[d, dash, "\langle\sigma\tau\rangle"'] \arrow[dr, dash, "\langle\tau\rangle"] & \\
K_1 = \mathbb{Q}(\sqrt{-a}) \arrow[dr, dash] & K^+ = \mathbb{Q}(\sqrt{ab}) \arrow[d, dash] & K_2 = \mathbb{Q}(\sqrt{-b}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \lambda \subset \mathcal{O}_K & \\
\lambda_1 \subset \mathcal{O}_{K_1} \arrow[ur, hook] & \lambda^+ \subset \mathcal{O}_{K^+} \arrow[u, hook] & \lambda_2 \subset \mathcal{O}_{K_2} \arrow[ul, hook] \\
 & \ell \in \mathbb{Z} \arrow[ul, hook] \arrow[u, hook] \arrow[ur, hook] &
\end{tikzcd}$$

We have $\text{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau = cc\}$ with

$$\sigma : \begin{cases} \sqrt{-a} \mapsto -\sqrt{-a} \\ \sqrt{-b} \mapsto \sqrt{-b} \end{cases}, \tau : \begin{cases} \sqrt{-a} \mapsto \sqrt{-a} \\ \sqrt{-b} \mapsto -\sqrt{-b} \end{cases}, \text{ and } \sigma\tau : \begin{cases} \sqrt{-a} \mapsto -\sqrt{-a} \\ \sqrt{-b} \mapsto -\sqrt{-b} \end{cases} = cc.$$

As in the previous section, we need to compute $\mathcal{O}_K/\ell$ to understand the structure of the conjugacy class associated to ℓ. We will again consider the possible decomposition and inertia groups and use Lemmas 2.1.11 and 2.1.12 to determine how ℓ factors in K and determine (when possible) a Frobenius element $\text{Frob}_K(\ell)$ which generates $\text{Gal}(\kappa(\lambda)/\kappa(\ell))$. For this field K, we have

$$\begin{gathered} \text{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle\,,\ \text{Gal}(K/K_1) = \langle \sigma \rangle\,, \\ \text{Gal}(K/K_2) = \langle \tau \rangle\,, \ \text{ and } \ \text{Gal}(K/K^+) = \langle \sigma\tau \rangle\,. \end{gathered}$$

Let ℓ be a rational prime and let (e, f, r) be the factorization invariants of a prime $\lambda \subset \mathcal{O}_K$ over ℓ.

1. Suppose $D(\lambda/\ell) = \{1\}$; then $I(\lambda/\ell) = \{1\}$. We have that

   $$\{1\} = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell)) \;\Rightarrow\; \mathrm{Frob}_K(\ell) = 1$$

   by Theorem 2.1.7 and the definition of $\mathrm{Frob}_K(\ell)$. Since $(e, f, r) = (1, 1, 4)$, ℓ is totally split in K and thus by Proposition 3.0.1, $f \bmod \ell$ factors completely. Then the corresponding conjugacy class type is **Full Split**.

2. Suppose $D(\lambda/\ell) = \langle\sigma\rangle$.

   (a) Suppose $I(\lambda/\ell) = \{1\}$. Using Theorem 2.1.7 again we have

   $$\langle\sigma\rangle = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell)) \;\Rightarrow\; \mathrm{Frob}_K(\ell) = \sigma.$$

   By Lemma 2.1.12, $D(\lambda_1/\ell) = D(\lambda/\ell) \bmod \sigma = \{1\}$ so $\mathcal{O}_{K_1}/\ell \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell$ and complex conjugation acts by exchanging the summands. This factorization has $(e, f, r) = (1, 2, 2)$ so $\mathcal{O}_K/\ell \cong \mathbb{F}_{\ell^2} \oplus \mathbb{F}_{\ell^2}$, and the action of *cc* exchanges the summands, which corresponds to a conjugacy class with isotropic eigenspaces. By Proposition 3.0.1, $f \bmod \ell$ factors as distinct irreducible quadratics and so this class type must be **DIQ NSR**.

   (b) Suppose $I(\lambda/\ell) = \langle\sigma\rangle$. Lemma 2.1.12 gives $D(\lambda_1/\ell) = I(\lambda_1/\ell) = \{1\}$ and so $\mathcal{O}_{K_1}/\ell \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell$ where *cc* acts by permuting the summands. Since $(e, f, r) = (2, 1, 2)$,

   $$\mathcal{O}_K/\ell \cong \frac{\mathbb{F}_\ell[T]}{(T)^2} \oplus \frac{\mathbb{F}_\ell[T]}{(T)^2}$$

   and the action of *cc* exchanges the summands. Then the corresponding polynomial factorization is $f \bmod \ell = (T-a)^2(T-b)^2$ by Proposition 3.0.1 and the associated class has isotropic eigenspaces, so $\mathcal{C}(f \bmod \ell)$ is of type **DRL** $\textcircled{\textbf{A}}$.

3. Suppose $D(\lambda/\ell) = \langle\tau\rangle$; then notice that any factorizations here are symmetric with the ones for $D(\lambda/\ell) = \langle\sigma\rangle$.

4. Suppose $D(\lambda/\ell) = \langle\sigma\tau\rangle$.

   (a) Suppose $I(\lambda/\ell) = \{1\}$. Then Theorem 2.1.7 gives

   $$\langle\sigma\tau\rangle = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell)) \;\Rightarrow\; \mathrm{Frob}_K(\ell) = \sigma\tau$$

   and $(e, f, r) = (1, 2, 2)$ implies that $\mathcal{O}_K/\ell \cong \mathbb{F}_{\ell^2} \oplus \mathbb{F}_{\ell^2}$. By Lemma 2.1.12 we have $D(\lambda^+/\ell) = I(\lambda^+/\ell) = \{1\}$, so $\mathcal{O}_{K^+}/\ell \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell$. Complex conjugation acts trivially on K^+ and so fixes each of these summands. Then $f \bmod \ell$ factors as a product of distinct quadratics and the corresponding conjugacy class has symplectic eigenspaces, implying that the class type is **DIQ SR**.

   (b) Suppose $I(\lambda/\ell) = \sigma\tau$. Lemma 2.1.12 gives $\mathcal{O}_{K^+}/\ell \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell$ as above, where *cc* preserves the summands of $\mathcal{O}_{K^+}/\ell$. Since $(e, f, r) = (2, 1, 2)$, we have

   $$\mathcal{O}_K/\ell \cong \frac{\mathbb{F}_\ell[T]}{(T)^2} \oplus \frac{\mathbb{F}_\ell[T]}{(T)^2}$$

   where complex conjugation fixes each subspace. Then ℓ corresponds to $f \bmod \ell = (T - a)^2(T - b)^2$ and the associated conjugacy class has symplectic eigenspaces, so ℓ corresponds to the **DRL** Ⓑ class type.

5. Suppose $D(\lambda/\ell) = \langle\sigma, \tau\rangle$.

   (a) Suppose $I(\lambda/\ell) = \{1\}$. Then Theorem 2.1.7 implies

   $$\langle\sigma, \tau\rangle = D(\lambda/\ell) \cong \mathrm{Gal}(\kappa(\lambda)/\kappa(\ell))$$

   which is a contradiction since $\mathrm{Gal}(\kappa(\lambda)/\kappa(\ell))$ is a cyclic group. Thus this is not a possible factorization of ℓ in K.

(b) Suppose $I(\lambda/\ell) = \langle\sigma\rangle$, so that $(e, f, r) = (2, 2, 1)$. Then

$$\mathcal{O}_K/\ell \cong \mathcal{O}_K/\lambda^2 \cong \frac{\mathbb{F}_{\ell^2}[T]}{(T)^2}$$

as a ring, so Proposition 3.0.1 implies that f mod ℓ factors as $[g(T)]^2$. Complex conjugation acts trivially on λ^+ and thus on $\mathcal{O}_{K^+}/\lambda^+ \cong \mathbb{F}_\ell$. By Lemma 2.1.11, $I(\lambda/\lambda^+) = \langle\sigma\rangle \cap \langle\sigma\tau\rangle = \{1\}$ so complex conjugation acts nontrivially on the extension from $\mathcal{O}_{K^+}/\lambda^+$ to $\mathcal{O}_K/\lambda \cong \mathbb{F}_{\ell^2}$. Then cc acts as a generator for $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$ and its action on the module $\mathcal{O}_K/\ell \cong \mathbb{F}_{\ell^2} \oplus T\mathbb{F}_{\ell^2}$ is given by $a + bT \mapsto \bar{a} + \bar{b}T$. This action preserves the summands of $\mathcal{O}_K/\ell$ and so ℓ corresponds to a class of type **RIQ**.

(c) Suppose $I(\lambda/\ell) = \langle\tau\rangle$; this factorization is symmetric with the one above, and produces the same conjugacy class type.

(d) Suppose $I(\lambda/\ell) = \langle\sigma\tau\rangle$. Once again we have $(e, f, r) = (2, 2, 1)$ so

$$\mathcal{O}_K/\ell \cong \mathcal{O}_K/\lambda^2 \cong \frac{\mathbb{F}_{\ell^2}[T]}{(T)^2}$$

as a ring. We also have that $I(\lambda^+/\ell) = \{1\}$ and $D(\lambda^+/\ell) = \langle\sigma, \tau\rangle \mod \sigma\tau$ (a group of order two) using Lemma 2.1.12 so $\mathcal{O}_{K^+}/\lambda^+ = \mathcal{O}_{K^+}/\ell \cong \mathbb{F}_{\ell^2}$ and has a trivial action by cc. This factorization is the same as 3(b) of the previous section, so by the same argument the class type corresponding to ℓ is **RIQ***.

(e) Suppose $I(\lambda/\ell) = \langle\sigma, \tau\rangle$. Each of $I(\lambda_i/\ell)$ and $I(\lambda^+/\ell)$ have order two by Lemma 2.1.12, implying that ℓ ramifies in each of the subfields of K. A prime ℓ ramifies in K_1 and K_2 if it divides each of a and b; then $\ell^2|ab$, and we can rewrite $K^+ = \mathbb{Q}(\sqrt{ab}) = \mathbb{Q}(\ell\sqrt{ab/\ell^2}) \cong \mathbb{Q}(\sqrt{ab/\ell^2})$ where $\ell \nmid ab/\ell^2$. Then ℓ cannot also ramify in K^+, so this is a contradiction.

Recall $X = \{\chi_0, \chi_1, \chi_2, \chi_3\}$ where each χ_i is a quadratic character defined by

$$\chi_1 : \begin{cases} 1 \mapsto 1 \\ \sigma \mapsto 1 \\ \tau \mapsto -1 \\ \sigma\tau \mapsto -1 \end{cases}, \quad \chi_2 : \begin{cases} 1 \mapsto 1 \\ \sigma \mapsto -1 \\ \tau \mapsto 1 \\ \sigma\tau \mapsto -1 \end{cases}, \text{ and } \chi_3 : \begin{cases} 1 \mapsto 1 \\ \sigma \mapsto -1 \\ \tau \mapsto -1 \\ \sigma\tau \mapsto 1 \end{cases}.$$

Recall from section 2.2 that to each of these characters χ_i we can associate the subfield of K that is fixed by the kernel of χ_i:

$$\chi_1 \longleftrightarrow K_1, \quad \chi_2 \longleftrightarrow K_2, \text{ and } \chi_3 \longleftrightarrow K^+,$$

and so $X^+ = \{\chi_0, \chi_3\}$. If a prime ℓ ramifies in, for example, K_1, then $\chi_1(\ell) = 0$.

As before, define $\chi(\ell)$ as $\chi(\mathrm{Frob}_K(\ell))$ for unramified primes and zero otherwise. Then for K a totally imaginary biquadratic quartic number field, we have

$$(\chi_1, \chi_2)(\ell) = \begin{cases} (\chi_1, \chi_2)(1) = (1, 1) & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{Full Split}, \\ (\chi_1, \chi_2)(\sigma) = (-1, 1) & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{DIQ NSR}, \\ (\chi_1, \chi_2)(\sigma\tau) = (-1, -1) & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{DIQ SR}, \\ (-1, 0) & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{RIQ}, \\ (1, 0) & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{DRL } \textcircled{\textbf{A}}, \\ (0, 0) & \text{if } \mathcal{C}(f \bmod \ell) \text{ is } \textbf{RIQ*} \text{ or } \textbf{DRL } \textcircled{\textbf{B}}. \end{cases} \tag{7.3.1}$$

Remark 7.3.1. Without loss of generality, we list the values of (χ_1, χ_2) that correspond to the list above, but as noted there is symmetry between cases where either a decomposition group or an inertia group is $\langle\sigma\rangle$ or $\langle\tau\rangle$. In particular, in the cases where $\mathcal{C}(f \bmod \ell)$ is **DRL** Ⓐ, **DIQ NSR**, or **RIQ**, the values of χ_1 and χ_2 could be reversed. Notice that this exchange does not affect the value of

$$\frac{1}{1-\frac{\chi_1(\ell)}{\ell}}\,\frac{1}{1-\frac{\chi_2(\ell)}{\ell}}.$$

Remark 7.3.2. Since each of the χ_i are quadratic characters, we can define each of them as a Legendre symbol of the appropriate field discriminant. Recall that ℓ splits in a quadratic ring $\mathbb{Q}(\sqrt{d})$ if d is a nonzero square mod ℓ (i.e., if $\left(\frac{d}{\ell}\right)=1$), is inert if d is not a square mod ℓ (i.e., if $\left(\frac{d}{\ell}\right)=-1$), and ramifies if $\ell|d$ [16]. Note that $\left(\frac{ab}{\ell}\right)=\left(\frac{-a}{\ell}\right)\left(\frac{-b}{\ell}\right)$. Then the splitting of the prime ℓ in K^+ completely depends on its splitting in K_1 and K_2.

7.4 The constant ξ

In this section we consider the real constant $\xi = \xi_K/\xi_{K^+}$. In section 2.3, we defined (equation (2.3.1))

$$\xi_K = \frac{2^{r_1}(2\pi)^{r_2}R_K}{\omega_K\sqrt{|d_K|}}$$

where r_1 is the number of real embeddings of K, $2r_2$ is the number of complex embeddings, R_K is the regulator, ω_K is the number of roots of unity in K, and d_K is the field discriminant.

As K is a totally imaginary quartic field, K has $r_1 = 0$ and $r_2 = 2$. Similarly, K^+ is quadratic and totally real so it has $r_1 = 2$ and $r_2 = 0$. The only roots of unity in K^+ are $\{\pm 1\}$ so $\omega_{K^+} = 2$. Assume $\omega_K = \omega_{K^+}$. Then

$$\xi = \frac{\xi_K}{\xi_{K^+}} = \frac{\frac{4\pi^2 R_K}{\omega_K\sqrt{|d_K|}}}{\frac{4R_{K^+}}{\omega_{K^+}\sqrt{|d_{K^+}|}}} = \pi^2\frac{R_K}{R_{K^+}}\sqrt{\left|\frac{d_{K^+}}{d_K}\right|}. \tag{7.4.1}$$

The ratio of regulators, R_K/R_{K^+}, is given by the following pair of theorems.

Theorem 7.4.1. *[25, Theorem 4.12] Let K be a totally imaginary number field of* *degree $2g$ over $\mathbb{Q}$ and let $E = (\mathcal{O}_K)^\times$ be its unit group. Let $E^+ = (\mathcal{O}_K)^\times$ be the unit group of K^+ and let W be the group of roots of unity of K. Then*

$$Q := [E : WE^+] = 1 \text{ or } 2.$$

Theorem 7.4.2. *[25, Proposition 4.16] Let K be as above and let K^+ be its maximal real subfield. Then*

$$\frac{R_K}{R_{K^+}} = \frac{1}{Q} 2^{(r_2 - 1)}.$$

For K a totally imaginary quartic field, $r_2 = 2$ so $R_K/R_{K^+} = 1$ or 2. Since we have assumed $\omega_K = \omega_{K^+}$, $W = \{\pm 1\}$ and so $Q = [E : WE^+] = 1$. Then using the second theorem we see that $R_K/R_{K^+} = 2$.

Recall that the moduli space of abelian surfaces over $\mathbb{F}_q$ has dimension three. Then

$$\xi = 2\pi^2 \sqrt{\left| \frac{d_{K^+}}{d_K} \right|}$$

and

$$\frac{1}{\xi} = \frac{1}{2\pi^2} \sqrt{\left| \frac{d_K}{d_{K^+}} \right|} = 2q^3 \mu_{ST}(a, b),$$

the expected number of abelian surfaces with such a polynomial of Frobenius. (See Appendix B for details of the computation of $\mu_{ST}(a, b)$.)

8. THE NUMBER OF ABELIAN SURFACES WITH COMPLEX MULTIPLICATION BY THE MAXIMAL ORDER

If K is a totally imaginary quartic number field, generated as $K = \mathrm{Split}(f)$ as in chapter 7, then we can identify an isogeny class of principally polarized abelian surfaces over a finite field with complex multiplication by an order in K. With all definitions and notation as before, we have

$$\xi \frac{h(K)}{h(K^+)} = \frac{\lim_{s\to 1^+}(s-1)\zeta_K(s)}{\lim_{s\to 1^+}(s-1)\zeta_{K^+}(s)} = \frac{\prod_{\chi_0 \neq \chi \in X} L(1,\chi)}{\prod_{\chi_0 \neq \chi \in X^+} L(1,\chi)} = \prod_{\chi \in X \smallsetminus X^+} L(1,\chi).$$

Since $\deg(f) = 4$, $\# X = 4$, and $\# X^+ = 2$, this simplifies to $L(1,\chi)L(1,\chi')$ for $\chi, \chi' \in X \smallsetminus X^+$.

We will now proceed to use the definitions (7.2.1) and (7.3.1) of χ, χ_1, and χ_2 on primes ℓ from the previous two sections to prove the following theorems.

Theorem 8.0.1. *Let $f = T^4 + aT^3 + bT^2 + amT + m^2$ a possible polynomial of Frobenius such that $K = \mathrm{Split}(f)$ is a totally imaginary quartic field, and let X and X^+ the groups of characters associated to K and K^+, respectively. Let χ, χ_1, χ_2 be defined as in chapter 7, with $\{\chi, \chi'\} = X \smallsetminus X^+$. Then for all odd primes ℓ,*

$$\frac{\#\left\{\text{cyclic } \gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell) | \mathcal{C}(\gamma) \leftrightarrow f \text{ mod } \ell\right\}}{\ell^{-2}\, \#\, \mathrm{Sp}_4(\mathbb{F}_\ell)} = \frac{1}{1-\frac{\chi(\ell)}{\ell}} \frac{1}{1-\frac{\chi'(\ell)}{\ell}}.$$

Proof. We proceed by cases, fitting together the values of the characters in $X \smallsetminus X^+$ on ℓ as in (7.2.1) and (7.3.1) with the orders of the centralizers of the corresponding conjugacy class types determined in Propositions 6.3.1 and 6.4.1. For the non-regular classes, we will only consider the cyclic versions of these matrices (the ones for which $\operatorname{minpol}(\gamma) = \operatorname{charpol}(\gamma)$) for reasons discussed in Remark 3.0.2.

To avoid repetition, we list the pertinent results in the following table. We compute the size of a conjugacy class as

$$\#\mathcal{C}(\gamma) = \frac{\#\operatorname{GSp}_4(\mathbb{Z}/\ell)}{\#\mathcal{Z}(\gamma)}$$

and recall that $\#\operatorname{GSp}_4(\mathbb{F}_\ell) = (\ell - 1)\,\#\operatorname{Sp}_4(\mathbb{F}_\ell)$. Empty cells correspond to factorizations that are impossible in the associated field type. The characters $\chi, \bar{\chi}, \chi_2$, and χ_2 are evaluated at ℓ. In the final column we compute

$$\frac{1}{1 - \frac{\chi(\ell)}{\ell}} \cdot \frac{1}{1 - \frac{\chi'(\ell)}{\ell}} = \frac{\ell}{\ell - \chi(\ell)} \cdot \frac{\ell}{\ell - \chi'(\ell)}$$

where $\{\chi, \chi'\} = \{\chi, \bar{\chi}\}$ in the cyclic quartic case or $\{\chi, \chi'\} = \{\chi_1, \chi_2\}$ in the biquadratic case.

Class type	$\#\mathcal{Z}(\gamma)$	$\frac{\#\mathcal{C}(\gamma)}{\ell^{-2}\ \#\operatorname{Sp}_4(\mathbb{F}_\ell)}$	$(\chi, \bar{\chi})$	(χ_1, χ_2)	$\frac{\ell}{\ell-\chi(\ell)} \cdot \frac{\ell}{\ell-\chi'(\ell)}$
Full Split	$(\ell - 1)^3$	$\frac{\ell^2}{(\ell-1)^2}$	$(1, 1)$	$(1, 1)$	$\frac{\ell}{\ell-1} \cdot \frac{\ell}{\ell-1}$
DIQ SR	$(\ell + 1)^2(\ell - 1)$	$\frac{\ell^2}{(\ell+1)^2}$	$(-1, -1)$	$(-1, -1)$	$\frac{\ell}{\ell+1} \cdot \frac{\ell}{\ell+1}$
DIQ NSR	$(\ell + 1)(\ell - 1)^2$	$\frac{\ell^2}{\ell^2-1}$		$(-1, 1)$	$\frac{\ell}{\ell+1} \cdot \frac{\ell}{\ell-1}$
Irred Quartic	$(\ell^2 + 1)(\ell - 1)$	$\frac{\ell^2}{\ell^2+1}$	$(i, -i)$		$\frac{\ell}{\ell-i} \cdot \frac{\ell}{\ell+i}$
DRL Ⓐ	$\ell(\ell - 1)^2$	$\frac{\ell}{\ell-1}$		$(1, 0)$	$\frac{\ell}{\ell-1} \cdot 1$
DRL Ⓑ±	$2\ell^2(\ell - 1)$	1	$(0, 0)$	$(0, 0)$	$1 \cdot 1$
RIQ	$\ell(\ell^2 - 1)$	$\frac{\ell}{\ell+1}$		$(-1, 0)$	$\frac{\ell}{\ell+1} \cdot 1$
RIQ*±	$2\ell^2(\ell - 1)$	1	$(0, 0)$	$(0, 0)$	$1 \cdot 1$
QRL	$\ell^2(\ell - 1)$	1	$(0, 0)$		$1 \cdot 1$

Since the third and sixth columns match, the theorem is proved. □

Take a cyclic matrix γ from $\mathrm{GSp}_4(\mathbb{F}_\ell)$, and consider elements $\tilde{\gamma} \in \mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ such that $\tilde{\gamma} \equiv \gamma \bmod \ell$ (we call $\tilde{\gamma}$ a *lift* of γ). We will show that Theorem 8.0.1 generalizes to $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$.

Corollary 8.0.2. *With the same setup as above, for all odd primes ℓ and any $r \in \mathbb{Z}_+$*

$$\frac{\#\{\textit{cyclic } \gamma \in \mathrm{GSp}_4(\mathbb{Z}/\ell^r) | \mathcal{C}(\gamma) \leftrightarrow f \textit{ mod } \ell^r\}}{\ell^{-2r}\ \#\,\mathrm{Sp}_4(\mathbb{Z}/\ell^r)} = \frac{1}{1-\frac{\chi(\ell)}{\ell}}\frac{1}{1-\frac{\chi'(\ell)}{\ell}}.$$

Proof. Using Proposition 6.4.6, we know that for these cyclic elements,

$$\#\mathcal{C}(\tilde{\gamma}) = \ell^{8(r-1)} \cdot \#\mathcal{C}(\gamma).$$

Recall that $\#\,\mathrm{Sp}_4(\mathbb{Z}/\ell^r) = \ell^{10(r-1)}\#\,\mathrm{Sp}_4(\mathbb{F}_\ell)$ as the dimension of Sp_4 is 10. Then

$$\begin{aligned}
&\frac{\#\{\gamma \in \mathrm{GSp}_4(\mathbb{Z}/\ell^r) | \mathcal{C}(\gamma) \leftrightarrow f \text{ mod } \ell^r\}}{\ell^{-2r}\ \#\,\mathrm{Sp}_4(\mathbb{Z}/\ell^r)}\\
=&\frac{\ell^{8(r-1)}\#\{\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell) | \mathcal{C}(\gamma) \leftrightarrow f \text{ mod } \ell\}}{\ell^{-2r}\ (\ell^{10(r-1)}\#\,\mathrm{Sp}_4(\mathbb{F}_\ell))}\\
=&\frac{\ell^{8(r-1)}}{\ell^{-2(r-1)}\ell^{10(r-1)}} \cdot \frac{\#\{\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell) | \mathcal{C}(\gamma) \leftrightarrow f \text{ mod } \ell\}}{\ell^{-2}\#\,\mathrm{Sp}_4(\mathbb{F}_\ell)}\\
=&\frac{\#\{\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell) | \mathcal{C}(\gamma) \leftrightarrow f \text{ mod } \ell\}}{\ell^{-2}\#\,\mathrm{Sp}_4(\mathbb{F}_\ell)}\\
=&\frac{1}{1-\frac{\chi(\ell)}{\ell}}\frac{1}{1-\frac{\chi'(\ell)}{\ell}}.
\end{aligned}$$

□

We can interpret the Euler factors appearing in Theorem 8.0.1 in terms of the size of the set of principally polarized abelian surfaces over a finite field with complex multiplication by $\mathcal{O}_K$ via Theorem 2.4.8 of Howe. Recall that this theorem gives the size of such a set as the ratio of class numbers of K and K^+. Then by applying Howe's result to Theorem 8.0.1, we get the main result of the paper.

Theorem 8.0.3 (Main Theorem)**.** *Suppose $f(T) \in \mathbb{Z}[T]$ is irreducible and quartic such that $K = \mathrm{Split}(f)$ is a totally imaginary quartic field. Let $\mathcal{I}_K$ be the set of isomorphism classes of principally polarized abelian surfaces over $\mathbb{F}_q$ with complex multiplication by the maximal order of K. Then for the real constant $\xi = \xi_K/\xi_{K^+}$ defined by equation* (7.4.1)*,*

$$\#\mathcal{I}_K = \frac{1}{\xi} \prod_{\ell \in \mathbb{Z} \ prime} \frac{\# \{ cyclic\ \gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell) | \mathcal{C}(\gamma) \leftrightarrow f \ mod\ \ell \}}{\ell^{-2} \, \# \mathrm{Sp}_4(\mathbb{F}_\ell)}.$$

Proof. Use Theorem 8.0.1 and take a product over all odd primes $\ell \in \mathbb{Z}$ so

$$\begin{aligned}
\prod_{\ell \in \mathbb{Z}} \frac{\# \{ \gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell) | \mathcal{C}(\gamma) \leftrightarrow f \text{ mod } \ell \}}{\ell^{-2} \, \# \mathrm{Sp}_4(\mathbb{F}_\ell)} &= \prod_{\ell \in \mathbb{Z}} \frac{1}{1 - \frac{\chi(\ell)}{\ell}} \frac{1}{1 - \frac{\chi'(\ell)}{\ell}} \\
&= \prod_{\ell \in \mathbb{Z}} \frac{1}{1 - \frac{\chi(\ell)}{\ell}} \prod_{\ell \in \mathbb{Z}} \frac{1}{1 - \frac{\chi'(\ell)}{\ell}} \\
&= L(1, \chi) L(1, \chi') = \prod_{\chi \in X \smallsetminus X^+} L(1, \chi).
\end{aligned}$$

Equation (3.0.1) in chapter 3 gives

$$\frac{1}{\xi} \prod_{\chi \in X \smallsetminus X^+} L(1, \chi) = \frac{h_K}{h_{K^+}}$$

which is the number of principally polarized abelian surfaces with complex multiplication by $\mathcal{O}_K$ by Theorem 2.4.8. □

9. CONCLUSIONS AND FUTURE WORK

We have determined the conjugacy classes of the finite matrix groups $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ and $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ and found their orders. We showed, by creating a correspondence between rational primes and conjugacy classes of these groups, that the proportion of matrices with a given characteristic polynomial out of the expected number of such matrices is constant and equal to the ℓ^{th} Euler factor of a product of L-series. Using a theorem of Howe (Theorem 2.4.8), we know that the product of these L-series is, up to a real constant, the number of abelian varieties with certain characteristics.

For $g = 1$ or 2, let

$$\begin{aligned} \nu_\ell(f) &= \frac{\#\left\{\text{cyclic } \gamma \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell) | \mathcal{C}(\gamma) \leftrightarrow f \bmod \ell\right\}}{\ell^{-g} \# \, \mathrm{Sp}_{2g}(\mathbb{F}_\ell)} \\ \text{and } \nu_\infty(f) &= q^d \mu_{ST}(f) \end{aligned}$$

where $d = 1$ if $g = 1$ and $d = 3$ if $g = 2$ and $\mu_{ST}(f)$ is the generalized Sato-Tate measure on the Frobenius polynomial f (see Appendix B). Then $\nu_\infty(f)$ is the expected number of abelian varieties with polynomial of Frobenius f via the Sato-Tate heuristic. Notice that in both the elliptic curve and the abelian surface setting, the constant ξ_K or ξ related to the class number formula is the reciprocal of $\nu_\infty(f)$. Let $\mathcal{I}_K$ be the set of abelian varieties of fixed dimension over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}_K$. Then Theorems 5.2.2 and 8.0.3 could be restated as follows.

Theorem 9.0.1. *Let $g = 1$ or 2 and suppose $f(T) \in \mathbb{Z}[T]$ is a Weil polynomial of degree $2g$ which is irreducible such that $K = \mathrm{Split}(f)$ is a totally imaginary field. Let $\mathcal{I}_K$ be the set of isomorphism classes of principally polarized abelian varieties of* *dimension g over $\mathbb{F}_q$ with complex multiplication by the maximal order of K. Then for the real constant $\xi = \xi_K/\xi_{K^+}$ defined by equation* (7.4.1),

$$\#\mathcal{I}_K = \nu_\infty(f) \prod_{\ell \in \mathbb{Z} \ prime} \nu_\ell(f).$$

Then interpret this restatement in terms of the proportion of such abelian varieties out of the expected number:

$$\frac{\#\mathcal{I}_K}{\nu_\infty(f)} = \prod_{\ell \in \mathbb{Z} \text{ prime}} \nu_\ell(f).$$

One way to view the main result (Theorem 8.0.3) is that it provides a new way to compute the number of principally polarized abelian varieties over $\mathbb{F}_q$ of dimension g with complex multiplication by the maximal order in a totally imaginary field. Rather than computing a ratio of class numbers using techniques from number theory, we can instead use group theory to compute the probabilities of certain matrices occurring in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Perhaps a different interpretation is as follows. Consider the Frobenius endomorphism of an abelian variety over $\mathbb{F}_q$ of dimension g as a matrix in $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ with characteristic polynomial $f(T)$. Certainly these matrices cannot be literally equidistributed in the matrix group; there are only finitely many abelian varieties over any $\mathbb{F}_q$, so if q is small relative to ℓ the proportion of Frobenius elements in the matrix group will be very small. However, the Frobenius elements are uniformly distributed in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ if $\ell \ll q$.

Suppose we allow ourselves to make equidistribution and independence assumptions on these endomorphisms in general and use them to compute the local contribution for each ℓ. Then we find that the proportion of abelian varieties with complex multiplication out of the expected number of abelian varieties with a fixed number of points is given precisely by the product of proportions of Frobenius endomorphisms for each ℓ.

We believe this heuristic will extend to abelian varieties of all dimensions with complex multiplication in a totally imaginary field. As we restrict to utilizing only the purely cyclic elements of the matrix group, counting elements reduces to determining the sizes of conjugacy classes. The conjugacy classes of maximal tori in a matrix group are parameterized by conjugacy classes in the Weyl group [4]. From this, one can obtain a formula for the size of the centralizer of a torus and thus compute the necessary proportions of matrices at least for regular semisimple elements. Then using the characters of imaginary fields and Theorem 2.4.8, a general statement can, we believe, be made.

BIBLIOGRAPHY

[1] N. Avni, U. Onn, A. Prasad, and L. Vaserstein. Similarity classes of 3 × 3 matrices over a local principal ideal ring. *Comm. Algebra*, 37(8):2601–2615, 2009.

[2] J. Breeding, II. Irreducible characters of GSp(4, Fq). *ArXiv e-prints*, Apr. 2011.

[3] R. Bröker, D. Gruenewald, and K. Lauter. Explicit CM theory for level 2-structures on abelian surfaces. *Algebra Number Theory*, 5(4):495–528, 2011.

[4] R. W. Carter. *Finite groups of Lie type*. Wiley Classics Library. John Wiley & Sons Ltd., Chichester, 1993. Conjugacy classes and complex characters, Reprint of the 1985 original, A Wiley-Interscience Publication.

[5] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[6] J. Fulman. Cycle indices for the finite classical groups. *J. Group Theory*, 2(3):251–289, 1999.

[7] J. Fulman. A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups. *J. Algebra*, 234(1):207–224, 2000.

[8] J. Fulman. Random matrix theory over finite fields. *Bull. Amer. Math. Soc. (N.S.)*, 39(1):51–85 (electronic), 2002.

[9] E.-U. Gekeler. Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.*, (37):1999–2018, 2003.

[10] E. W. Howe. Personal communication, 2000.

[11] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[12] N. M. Katz. Lang-Trotter revisited. *Bull. Amer. Math. Soc. (N.S.)*, 46(3):413–457, 2009.

[13] J. P. S. Kung. The cycle structure of a linear transformation over a finite field. *Linear Algebra Appl.*, 36:141–155, 1981.

[14] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[15] D. Maisner and E. Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.

[16] D. A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[17] J. S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[18] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[19] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[20] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[21] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[22] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[23] S. G. Vlăduţ. Isogeny class and Frobenius root statistics for abelian varieties over finite fields. *Mosc. Math. J.*, 1(1):125–139, 2001.

[24] G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Austral. Math. Soc.*, 3:1–62, 1963.

[25] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[26] W. C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

[27] C. L. Williams. The cycle index of $\mathrm{GL}(n, \mathbb{F}_q)$, its generating function, and applications. Master's thesis, Colorado State University, Fort Collins, Colorado, September 2008.

APPENDICES

A. A FAILURE OF MATCHING

In [9], Gekeler matched the proportion of matrices

$$\frac{\#\left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r) \middle| \operatorname{tr}\gamma \equiv A \bmod \ell^r, \det\gamma \equiv Q \bmod \ell^r\right\}}{\ell^{-r}\#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)}$$

to the Euler factor

$$\frac{1}{1-\frac{\chi(\ell)}{\ell}}$$

which appears in the L-series $L(1,\chi)$ for rational primes $\ell \nmid A^2-4Q$. This condition on ℓ meant that he was only concerned with matrices which had distinct eigenvalues mod ℓ.

We have shown (Theorem 5.2.1) that if we restrict to only cyclic matrices, those with $\ell | A^2-4Q$ (i.e., those with repeated eigenvalues) also produce the Euler factor for ℓ in $L(1,\chi)$. In this appendix, we show that (for $\mathrm{GL}_2(Z/\ell^r)$) including in

$$\begin{aligned}&\left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r) \middle| \operatorname{tr}\gamma \equiv A \bmod \ell^r, \det\gamma \equiv Q \bmod \ell^r\right\}\\ =&\left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r) \middle| \operatorname{charpol}(\gamma) \equiv T^2-AT+Q \bmod \ell^r\right\}\end{aligned}$$

more than the purely cyclic (i.e., $j=0$) non-regular matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ produces a failure of matching between the proportion

$$\frac{\#\left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r) \middle| \operatorname{charpol}(\gamma) \equiv T^2-AT+Q \bmod \ell^r\right\}}{\ell^{-r}\#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)}$$

and the Euler factor for ℓ.

In the notation of section 4, let the local ring R be $\mathbb{Z}_\ell$, so that $\mathfrak{m} = (\ell)$ where ℓ is an odd prime. Then $R/\mathfrak{m}^r = \mathbb{Z}_\ell/\ell^r\mathbb{Z}_\ell \cong \mathbb{Z}/\ell^r$. Fix $A, Q \in \mathbb{Z}$ such that $A^2 - 4Q < 0$, and choose an odd prime ℓ such that $\ell | A^2 - 4Q$. We wish to compute

$$\nu_\ell(A,Q) = \lim_{r\to\infty} \frac{\#\left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r) \middle| \operatorname{tr}\gamma \equiv A \bmod \ell^r, \det\gamma \equiv Q \bmod \ell^r\right\}}{\ell^{-r}\#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)},$$

the proportion of invertible matrices γ with $\operatorname{charpol}(\gamma) \equiv f(T) = T^2 - AT + Q \bmod \ell^r$ as r tends to infinity. To simplify notation, define

$$\begin{aligned} N(f,r) &= \#\left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r) \middle| \operatorname{tr}\gamma \equiv A, \det\gamma \equiv Q \bmod \ell^r\right\} \\ &= \#\left\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r) \middle| \operatorname{charpol}(\gamma) \equiv f \bmod \ell^r\right\}. \end{aligned}$$

Let $\gamma = dI + \ell^j\beta \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ as in section 4. Then $d \in (\mathbb{Z}/\ell^j)^\times$ and β is cyclic in $\mathrm{Mat}_2(\mathbb{Z}/\ell^{r-j})$.

If $\ell|\Delta(f) = A^2 - 4Q$, then f defines a unique cyclic conjugacy class for each r with repeated roots mod ℓ. For some values of i, there are multiple conjugacy classes with $\operatorname{charpol}(\gamma) \equiv f \bmod \ell^i$, and we can count how many such elements γ there are.

Proposition A.0.1. *Suppose $\ell|\Delta(f) = A^2 - 4Q$. Let $M \geq 1$ be the greatest integer such that $\ell^M|\Delta(f)$. Let $\gamma = dI + \ell^j\beta$ such that* $\operatorname{charpol}(\gamma) \equiv f$ *mod ℓ^r and let $\chi_\Delta(\ell)$ be defined as in section 4 by $\Delta(\beta)$. Then*

$$N(f,r) = \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)(\ell-\chi_{r,0})} + \sum_{j=1}^{N} \ell^j \cdot \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r+j-1)}(\ell-1)(\ell-\chi_{r,j})} + S(r)$$

where $\chi_{r,j} = \chi_\Delta(\ell), N = \min\left\{\left\lfloor\frac{r-1}{2}\right\rfloor \left\lfloor\frac{M}{2}\right\rfloor\right\}$

$$\chi_{r,0} = \begin{cases} 0 & \textit{if } r \leq M \\ -1 & \textit{if } r > M \end{cases}, \quad \textit{and} \quad S(r) = \begin{cases} 1 & \textit{if } r \leq M \\ 0 & \textit{if } r > M \end{cases}.$$

Proof. For any r and any $1 \leq j \leq r-1$, $\gamma = dI + \ell^j \beta \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ has

$$\mathrm{tr}(\gamma) = 2d + \ell^j \,\mathrm{tr}\,\beta \text{ and } \det(\gamma) = d^2 + \ell^j d \,\mathrm{tr}\,\beta + \ell^{2j} \det \beta,$$

with $d \in (\mathbb{Z}/\ell^j)^\times$ and $\mathrm{tr}\,\beta, \det \beta \in \mathbb{Z}/\ell^{r-j}$. We need to determine, for each j, for how many pairs (d, β) are $\mathrm{tr}(\gamma) \equiv A \pmod{\ell^r}$ and $\det(\gamma) \equiv Q \pmod{\ell^r}$. This will determine how many conjugacy classes have trace and determinant A and Q, and how to classify them, and thus will allow us to count these elements.

Notice that if $A \equiv \mathrm{tr}\,\gamma \bmod \ell^r = 2d + \ell^j \,\mathrm{tr}\,\beta$, then A uniquely determines both d and $\mathrm{tr}\,\beta$.

Suppose $2j < r$ (i.e., suppose that j is small). We need to determine the values of $\det \beta$ so that $Q \equiv \det \gamma \bmod \ell^r$. The natural projection map $\ell^{2j}\ \mathbb{Z}/\ell^{r-j} \to \mathbb{Z}/\ell^r$ has kernel

$$\begin{aligned} \left\{a \in \ell^{2j}\ \mathbb{Z}/\ell^{r-j} | a \equiv 0 \bmod \ell^r\right\} &= \left\{a = b\ell^{2j} | b \in \mathbb{Z}/\ell^{r-j}\right\} \\ &= \left\{a = b\ell^{2j} | b \equiv 0 \bmod \mathbb{Z}/\ell^{r-2j}\right\}, \end{aligned}$$

which has size ℓ^j. So there are ℓ^j values of $\det \beta$ which produce the same value of $\ell^{2j} \det \beta$, and thus Q, mod ℓ^r. Then for a fixed A and Q, there are ℓ^j conjugacy classes with trace A and determinant Q, each with the same value of $\chi_{r,j} = \chi_{\Delta}(\ell)$ where $\Delta = \Delta(\beta)$. (To see why, notice that $\chi_\Delta(\ell)$ depends on the value of Δ mod ℓ, and $\det \beta$ is constant mod ℓ when $2j < r$.) This in turn tells us that each of these ℓ^j conjugacy classes have the same size.

Now suppose that

$$A \equiv \mathrm{tr}\,\gamma = 2d + \ell^j \,\mathrm{tr}\,\beta \text{ and } Q \equiv \det \gamma = d^2 + \ell^j d \,\mathrm{tr}\,\beta + \ell^{2j} \det \beta \bmod \ell^r.$$

Recall that $\ell^M | A^2 - 4Q$ exactly, so write $A^2 - 4Q = \ell^M \cdot v$ where $\ell \nmid v$. Then

$$\begin{aligned} A^2 - 4Q &\equiv (2d + \ell^j \operatorname{tr}\beta)^2 - 4(d^2 + \ell^j d \operatorname{tr}\beta + \ell^{2j} \det\beta) \bmod \ell^r \\ &= \ell^{2j}\left((\operatorname{tr}\beta)^2 - 4\det\beta\right) \in \ell^{2j}\mathbb{Z}/\ell^{r-j} \bmod \ell^r \\ \Rightarrow \ell^M \cdot v &= \ell^{2j}\left((\operatorname{tr}\beta)^2 - 4\det\beta\right) \in \left\{0, \ell^{2j}, 2\ell^{2j}, \dots, (\ell^{r-2j} - 1)\ell^{2j}\right\} \end{aligned}$$

If $M < 2j$, then $\ell^M \cdot v \notin \ell^{2j}\mathbb{Z}/\ell^{r-j}$ and so there is no $\det\beta$ such that

$$A^2 - 4Q \equiv \ell^{2j} \equiv \ell^{2j}\left((\operatorname{tr}\beta)^2 - 4\det\beta\right)$$

and in particular such that $Q \equiv \det\gamma \bmod \ell^r$. Then we will have no $\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ with $\operatorname{charpol}\gamma \equiv f \bmod \ell^r$ for j such that $M < 2j$.

Any $f = T^2 - AT + Q$ defines a cyclic class of $\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)$ with $j = 0$ and representative

$$C := \begin{pmatrix} 0 & 1 \\ -Q & A \end{pmatrix} \bmod \ell^r.$$

If $r \leq M$, $\ell^r | \Delta(f) = A^2 - 4Q = \ell^M \cdot v$ and there exists an $a \in (\mathbb{Z}/\ell^r)^\times$ such that $f \equiv (T - a)^2 \bmod \ell^r$. Then

$$C = \begin{pmatrix} 0 & 1 \\ -Q & A \end{pmatrix} \sim \begin{pmatrix} a & 1 \\ & a \end{pmatrix}$$

over $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ and $\chi_{r,0} = 0$. If on the other hand $r > M$, $\ell^r \nmid \Delta(f) = A^2 - 4Q$, and $f \bmod \ell^r$ does not have multiple roots, so $C \not\sim \left(\begin{smallmatrix} a & 1 \\ & a \end{smallmatrix}\right)$ for any $a \in \mathbb{Z}/\ell^r$ and $\chi_{r,0} = -1$ as $\Delta(f)$ is nonsquare in $\mathbb{Q}$, and so $\Delta(f)$ will be nonsquare mod ℓ^r once $r > M$.

The $j = r$ classes are those where $\gamma = dI, d \in (\mathbb{Z}/\ell^r)^\times$ and $\operatorname{charpol}(\gamma) \equiv f \bmod \ell^r$. If $r \leq M$, then $f \equiv (T-a)^2 \bmod \ell^r$ so $d = a$ and we have such a matrix. If $r > M$ then we have no such factorization of f and so there is no scalar matrix with characteristic polynomial f.

We will ignore the case where $r \leq 2j < 2r$. These elements can only increase the size of $N(f,r)$ and we will see shortly that the ones for which $2j < r$ is already enough to give a failure of matching.

Thus we are considering matrices γ with $2j < r$ and $2j \leq M$, and using Theorem 4.3.14 we have proven the theorem. □

Using this counting result, we proceed to compute

$$\nu_\ell(A,Q) = \lim_{r\to\infty} \frac{N(f,r)}{\ell^{-r}\ \#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)}$$

when $\ell | A^2 - 4Q$.

Suppose $M \geq 1$ is as before, and let $j \leq \min\left\{\left\lfloor \frac{r-1}{2}\right\rfloor, \left\lfloor \frac{M}{2}\right\rfloor\right\}$. Since $r \to \infty$ we say

$$N(f,r) = \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)(\ell-\chi_{r,0})} + \sum_{j=1}^{\lfloor M/2\rfloor} \ell^j \cdot \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r+j-1)}(\ell-1)(\ell-\chi_{r,j})}$$

by Proposition A.0.1. We know from Theorem 4.3.14 that

$$\frac{\left(\frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)(\ell-\chi_{r,0})}\right)}{\ell^{-r}\ \#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)} = \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)(\ell-\chi_{r,0})\cdot\ell^{-r}\ \#\,\mathrm{SL}_2(\mathbb{Z}/\ell^r)} = \frac{1}{1-\frac{\chi(\ell)}{\ell}}$$

since the numerator represents the number of purely cyclic classes with characteristic polynomial $T^2 - AT + Q$.

$$\begin{aligned}\sum_{j=1}^{\lfloor M/2\rfloor} \ell^j \cdot \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r+j-1)}(\ell-1)(\ell-\chi_{r,j})} &= \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)} \sum_{j=1}^{\lfloor M/2\rfloor} \frac{\ell^j}{\ell^{2j}(\ell-\chi_{r,j})} \\ &= \frac{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)} \sum_{j=1}^{\lfloor M/2\rfloor} \ell^{-j}\frac{1}{\ell-\chi_{r,j}}\end{aligned}$$

Recall that $\chi_{r,j}$ is constant for each j and notice that $\ell - 1 \leq \ell - \chi_{r,j} \leq \ell + 1$. Then

$$\sum_{j=1}^{\lfloor M/2 \rfloor} \ell^{-j} \frac{1}{\ell + 1} \leq \sum_{j=1}^{\lfloor M/2 \rfloor} \ell^{-j} \frac{1}{\ell - \chi_{r,j}} \leq \sum_{j=1}^{\lfloor M/2 \rfloor} \ell^{-j} \frac{1}{\ell - 1}$$

$$\frac{\ell^{-1}(1 - \ell^{-\lfloor M/2 \rfloor})}{(\ell+1)(1-\ell^{-1})} \leq \sum_{j=1}^{\lfloor M/2 \rfloor} \ell^{-j} \frac{1}{\ell - \chi_{r,j}} \leq \frac{\ell^{-1}(1 - \ell^{-\lfloor M/2 \rfloor})}{(\ell-1)(1-\ell^{-1})}$$

Taking the limit as $r \to \infty$ of the bounding terms gives

$$\lim_{r\to\infty} \frac{(1 - \ell^{-\lfloor M/2 \rfloor}) \ \# \operatorname{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)^2(\ell+1) \ \ell^{-r} \ \# \operatorname{SL}_2(\mathbb{Z}/\ell^r)} = \frac{\ell(1 - \ell^{-\lfloor M/2 \rfloor})}{(\ell-1)(\ell+1)}$$

$$\text{and} \quad \lim_{r\to\infty} \frac{(1 - \ell^{-\lfloor M/2 \rfloor}) \ \# \operatorname{GL}_2(\mathbb{Z}/\ell^r)}{\ell^{2(r-1)}(\ell-1)^2(\ell-1) \ \ell^{-r} \ \# \operatorname{SL}_2(\mathbb{Z}/\ell^r)} = \frac{\ell(1 - \ell^{-\lfloor M/2 \rfloor})}{(\ell-1)(\ell-1)}$$

so that we have

$$\frac{1}{1 - \frac{\chi(\ell)}{\ell}} + \frac{\ell(1 - \ell^{-\lfloor M/2 \rfloor})}{(\ell-1)(\ell+1)} \leq \lim_{r\to\infty} \frac{N(f,r)}{\ell^{-r} \ \# \operatorname{SL}_2(\mathbb{Z}/\ell^r)} \leq \frac{1}{1 - \frac{\chi(\ell)}{\ell}} + \frac{\ell(1 - \ell^{-\lfloor M/2 \rfloor})}{(\ell-1)(\ell-1)}.$$

Notice that the error terms in the previous statement are each positive. Since M is constant for any choice of A and Q, we see that including more than the matrices which are purely cyclic in $\operatorname{GSp}_4(\mathbb{Z}/\ell^r)$ leads to an error term and a failure of the proportion to match the Euler factor.

B. THE SATO-TATE CONJECTURE

Take a family of abelian varieties over $\mathbb{F}_q$. Each has a Frobenius endomorphism with a characteristic polynomial f. Weil's theorem implies we can write

$$f(T) = \prod_{i=1}^{g}(T - \sqrt{q}e^{i\theta_i})(T - \sqrt{q}e^{-i\theta_i})$$

where $0 \leq \theta_1 \leq \theta_2 \leq \cdots \leq \theta_g \leq \pi$. For elliptic curves, the Sato-Tate conjecture stated that the angle θ_1 is uniformly distributed in $P := [0, \pi]$ with respect to the Sato-Tate measure $\mu_{ST}(\theta) = \frac{2}{\pi}\sin^2\theta d\theta$. In higher dimensions there is a generalization of this measure, as presented in [23]. For a family of abelian varieties, the generalization of the Sato-Tate conjecture for (motives of) abelian varieities of dimension g claims that $\{\theta_1, \theta_2, \ldots, \theta_g\}$ is uniformly distributed in $P^g \subset \mathbb{R}^g$ with respect to the Sato-Tate measure

$$\mu_{ST}(\theta_1, \theta_2, \ldots, \theta_g) = 2^{g^2}\left(\prod_{j<k}(\cos\theta_j - \cos\theta_k)^2\right) \cdot \prod_i \left(\frac{1}{\pi}\sin^2\theta_i d\theta_i\right). \qquad \text{(B.0.1)}$$

Choose an elliptic curve $E/\mathbb{F}_q$. It has a Frobenius endomorphism with characteristic polynomial $f(T) = T^2 - aT + q$ with $a = q + 1 - \#E/\mathbb{F}_q$ and $|a| \leq 2\sqrt{q}$ so $\frac{a}{2\sqrt{q}} \in [-1, 1]$. If we make a histogram of the number of elliptic curves with a fixed value of $a/2\sqrt{q}$, the Sato-Tate measure gives an area of $\frac{1}{2\pi}\sqrt{4q - a^2}$.

Alternatively, Weil's theorem gives $f(T)$ for some $\theta \in [0, \pi]$ as

$$f = (T - \sqrt{q}e^{i\theta})(T - \sqrt{q}e^{-i\theta}) = T^2 - \sqrt{q}(e^{i\theta} + e^{-i\theta})T + q = T^2 - (2\sqrt{q}\cos\theta)T + q.$$

Equation B.0.1 gives the usual Sato-Tate measure in terms of θ:

$$\mu_{ST}(\theta) = 2\frac{1}{\pi}\sin^2(\theta)d\theta.$$

Then $a = 2\sqrt{q}\cos\theta$, so $\cos\theta = a/2\sqrt{q}$ and $-\sin\theta d\theta = \frac{da}{2\sqrt{q}}$. A quick computation shows $\sin\theta = \frac{\sqrt{4q-a^2}}{2\sqrt{q}}$. Then, changing variables from θ to a,

$$\begin{aligned}\mu_{ST}(\theta) &= 2\frac{1}{\pi}\sin^2(\theta)d\theta \\ &= \frac{2}{\pi}\left(\frac{\sqrt{4q-a^2}}{2\sqrt{q}}\right)\left(-\frac{da}{2\sqrt{q}}\right) \\ &= \frac{1}{2q\pi}\sqrt{4q-a^2}da = \mu_{ST}(a).\end{aligned}$$

Recall that a family of elliptic curves can be given by $y^2 = x(x-1)(x-\lambda)$ over U, where $\#U(\mathbb{F}_q) = q$. Then we expect a given a to occur with frequency

$$\#U(\mathbb{F}_q)\cdot\mu_{ST}(a) = q\cdot\mu_{ST}(a) = q\cdot\frac{1}{2q\pi}\sqrt{4q-a^2}da = \frac{1}{2\pi}\sqrt{4q-a^2}da.$$

Notice that $\mathrm{disc}(f) = a^2-4q < 0$ and recall that $\mathrm{disc}(f) = d_K$ where $K = \mathrm{Split}(f)$ when E has complex multiplication by $\mathcal{O}_K$. Then

$$q\mu_{ST}(a) = \frac{1}{2\pi}\sqrt{4q-a^2}da = \frac{1}{2\pi}\sqrt{|d_K|}da = \frac{1}{\xi_K}da$$

with ξ_K as in section 2.3 for an imaginary quadratic field K.

Now let $A/\mathbb{F}_q$ be a (principally polarized) abelian surface. It has a Frobenius endomorphism with characteristic polynomial $f(T) = T^4 - aT^3 + bT^2 - aqT + q^2$

under the conditions (from Weil's theorem)

$$\begin{aligned} |a| &\leq 4\sqrt{q}, \\ 2\,|a|\,\sqrt{q} - 2q \leq \quad b &\leq \frac{a^2}{4} + 2q. \end{aligned}$$

By Weil's theorem, we also have

$$\begin{aligned} f(T) &= (T - \sqrt{q}e^{i\theta_1})(T - \sqrt{q}e^{-i\theta_1})(T - \sqrt{q}e^{i\theta_2})(T - \sqrt{q}e^{-i\theta_2}) \\ &= T^4 - (2\sqrt{q}\cos\theta_1 + 2\sqrt{q}\cos\theta_2)T^3 + (2q + 4q\cos\theta_1\cos\theta_2)T^2 \\ &\qquad - (2q\sqrt{q}\cos\theta_1 + 2q\sqrt{q}\cos\theta_2)T + q^2 \end{aligned}$$

with $0 \leq \theta_1 \leq \theta_2 \leq \pi$. Then

$$a = 2\sqrt{q}(\cos\theta_1 + \cos\theta_2) \quad \text{and} \quad b = 2q + 4q\cos\theta_1\cos\theta_2, \tag{B.0.2}$$

$$\Rightarrow \frac{a}{2\sqrt{q}} = \cos\theta_1 + \cos\theta_2 \quad \text{and} \quad \frac{b}{2q} - 1 = 2\cos\theta_1\cos\theta_2. \tag{B.0.3}$$

Now equation B.0.1 gives

$$\mu_{ST}(\theta_1, \theta_2) = 2^4(\cos\theta_2 - \cos\theta_1)^2 \cdot \left(\frac{1}{\pi}\sin^2\theta_1 d\theta_1\right)\left(\frac{1}{\pi}\sin^2\theta_2 d\theta_2\right).$$

We proceed to change variables to a and b.

From (B.0.3),

$$\left(\frac{a}{2\sqrt{q}}\right)^2 = \frac{a^2}{4q} = \cos^2\theta_1 + 2\cos\theta_1\cos\theta_2 + \cos^2\theta_2$$

so

$$\begin{aligned}(\cos\theta_2 - \cos\theta_1)^2 &= \cos^2\theta_1 - 2\cos\theta_1\cos\theta_2 + \cos^2\theta_2 \\ &= \frac{a^2}{4q} - 2\left(\frac{b}{2q} - 1\right) = \frac{a^2 - 4b + 8q}{4q}.\end{aligned}$$

Also

$$\begin{aligned}\sin^2\theta_1\sin^2\theta_2 &= (1-\cos^2\theta_1)(1-\cos^2\theta_2) \\ &= 1 - (\cos^2\theta_1 + \cos^2\theta_2) + \cos^2\theta_1\cos^2\theta_2 \\ &= 1 - \left(\frac{a^2}{4q} - \left(\frac{b}{2q} - 1\right)\right) + \left(\frac{1}{2}\left(\frac{b}{2q} - 1\right)\right)^2 \\ &= \frac{b^2 + 4bq + 4q^2 - 4qa^2}{16q^2}.\end{aligned}$$

We will need the value of $\sin\theta_i$ as well; solve (B.0.3) for $\cos\theta_2 = \frac{a}{2\sqrt{q}} - \cos\theta_1$ and substitute into $\frac{b}{2q} - 1 = 2\cos\theta_1\cos\theta_2$ so that

$$0 = 2\cos^2\theta_1 - \frac{a}{\sqrt{q}}\cos\theta_1 + \left(\frac{b}{2q} - 1\right).$$

The quadratic formula gives

$$\cos\theta_1 = \frac{\frac{a}{\sqrt{q}} \pm \sqrt{\frac{a^2}{q} - 4\left(\frac{b}{2q} - 1\right)\cdot 2}}{4} = \frac{a \pm \sqrt{a^2 - 4b + 8q}}{4\sqrt{q}}$$

and so

$$\cos\theta_2 = \frac{a}{2\sqrt{q}} - \cos\theta_1 = \frac{a \mp \sqrt{a^2 - 4b + 8q}}{4\sqrt{q}}.$$

Then let $\cos\theta_1 = \frac{a + \sqrt{a^2 - 4b + 8q}}{4\sqrt{q}}$ and $\cos\theta_2 = \frac{a - \sqrt{a^2 - 4b + 8q}}{4\sqrt{q}}$. Using a right triangle we find that

$$\begin{aligned}\sin\theta_1 &= \frac{\sqrt{16q-(a+\sqrt{a^2-4b+8q})^2}}{4\sqrt{q}}\\ \text{and }\ \sin\theta_2 &= \frac{\sqrt{16q-(a-\sqrt{a^2-4b+8q})^2}}{4\sqrt{q}}.\end{aligned}$$

Using (B.0.2) we construct the Jacobian matrix of the transformation:

$$J = \begin{pmatrix} -2\sqrt{q}\sin\theta_1 & -2\sqrt{q}\sin\theta_2 \\ -4q\sin\theta_1\cos\theta_2 & -4q\sin\theta_2\cos\theta_1 \end{pmatrix}$$

which has determinant $8q\sqrt{q}\sin\theta_1\sin\theta_2(\cos\theta_1-\cos\theta_2)$. Thus,

$$\begin{aligned} dadb &= |\det(J)|\, d\theta_1 d\theta_2 \\ &= |8q\sqrt{q}\sin\theta_1\sin\theta_2(\cos\theta_1-\cos\theta_2)|\, d\theta_1 d\theta_2 \\ &= \left| 8q\sqrt{q}\frac{\sqrt{4q^2+b^2+4qb-4qa^2}}{4q}\cdot\frac{\sqrt{a^2-4b+8q}}{2\sqrt{q}}\right| d\theta_1 d\theta_2 \\ &= \sqrt{(4q^2+b^2+4qb-4qa^2)(a^2-4b+8q)}d\theta_1 d\theta_2 \end{aligned}$$

Then

$$\begin{aligned} \mu_{ST}(a,b) &= \frac{2^4}{\pi^2}\left(\frac{a^2-4b+8q}{4q}\right)\left(\frac{b^2+4bq+4q^2-4aq^2}{16q^2}\right)\cdot \\ &\qquad \left(\frac{1}{\sqrt{(4q^2+b^2+4qb-4qa^2)(a^2-4b+8q)}}dadb\right) \\ &= \frac{1}{4q^3\pi^2}\sqrt{(a^2-4b+8q)(4q^2+b^2+4qb-4qa^2)}dadb. \end{aligned}$$

The discriminant of $f(T)$ such that A has complex multiplication by a maximal order in a number field is

$$\mathrm{disc}(f) = (a^2 - 4b + 8q)^2(4q^2 + b^2 + 4qb - 4qa^2).$$

In fact, if A has complex multiplication by the maximal order of $K = \mathrm{Split}(f)$, then $\mathrm{disc}(f) = d_K$, and $a^2 - 4b + 8q$ is the discriminant of the real subfield K^+. Recall that the dimension of the moduli space of abelian varieties of dimension g is $g(g+1)/2$ and so for $g = 2$ this dimension is three. Then the expected frequency of an abelian surface with polynomial of Frobenius $f(T)$ is

$$\begin{aligned} q^3\mu_{ST}(a,b) &= \frac{1}{4\pi^2}\sqrt{(a^2 - 4b + 8q)(4q^2 + b^2 + 4qb - 4qa^2)}dadb \\ &= \frac{1}{4\pi^2}\sqrt{\left|\frac{d_K}{d_{K^+}}\right|}dadb = \frac{1}{2\xi}dadb \end{aligned}$$

where $\xi = \xi_K/\xi_{K^+}$ as first introduced in chapter 3.