Hecke algebras, Galois representations, and abelian varieties

Thesis committee:
Prof. dr. F. Beukers, Universiteit Utrecht
Prof. dr. J. Hartmann, University of Pennsylvania
Prof. dr. E. Mantovan, California Institute of Technology
Prof. dr. B. de Smit, Universiteit Leiden
Dr. M. S. Solleveld, Radboud Universiteit

ISBN: 978-90-393-6563-2

Hecke algebras, Galois representations, and abelian varieties

Hecke algebra's, Galois voorstellingen en abelse variëteiten
(met een samenvatting in het Nederlands)

Proefschrift

ter verkrijging van de graad van doctor aan de Universiteit Utrecht op gezag van de rector magnificus, prof. dr. G. J. van der Zwaan, ingevolge het besluit van het college voor promoties in het openbaar te verdedigen op maandag 13 juni 2016 des middags te 2.30 uur

door
Valentijn Zoë Karemaker
geboren op 13 april 1990 te Utrecht

Promotor: Prof. dr. G. L. M. Cornelissen

This thesis has been financially supported by the Netherlands Organisation for Scientific Research (NWO) under the research project “Quantum statistical mechanics and anabelian geometry”.

Contents

CHAPTER 1

Introduction

One of the main objects of study of modern algebraic number theory is the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ of a local or global field K with separable closure $\overline{K}$. In particular, one wants to understand the absolute Galois group of the rational numbers, $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. This is a very large group, yet it is compact with respect to the profinite topology.

One way of gaining insight into G_K is by studying its representations. These may arise in different ways. First of all, through the Langlands correspondence, they can come from automorphic representations, or equivalently, from representations of certain Hecke algebras. Secondly, by considering the action of G_K on vector spaces associated to varieties (e.g. the geometric torsion points of an abelian variety), one finds geometric Galois representations.

This thesis treats three questions related to G_K and its representations. The first of these, which is anabelian in nature, asks to what extent the representation theory of a Hecke algebra of a field K (which is either a number field or a local non-archimedean field of characteristic zero) determines K. The second question concerns Galois representations attached to abelian varieties, and especially those with surjective image, which realise symplectic groups as Galois groups. The third question focuses on supersingular abelian varieties over finite fields, and arithmetic properties of these varieties which are determined by the characteristic polynomial of the Frobenius endomorphism; the topological Frobenius map is a generator of G_K for finite fields K.

1.1 Hecke algebras and adelic points

Let K be a field and let G_K denote its absolute Galois group. First suppose that K is a number field. When K is Galois over $\mathbf{Q}$, Neukirch [78] proved that G_K determines K, in the sense that any isomorphism $G_K \cong G_L$ (as profinite groups) induces a unique field isomorphism $K \cong L$. Uchida [117] later proved this result when K is not necessarily Galois; as Neukirch points out in [79], the same result was obtained independently by Iwasawa (unpublished), using results by Ikeda [47].

By contrast, the abelianisation G_K^{ab}, corresponding to the one-dimensional representations of G_K, does not determine K, cf. [83] or [3].

Now suppose that K is a non-archimedean local field of characteristic zero. In this case, Yamagata showed in [129] that the analogous statement of the result by Neukirch and Uchida is false. Jarden and Ritter [52] prove that G_K determines the absolute field degree $[K\colon \mathbf{Q}_p]$ and the maximal abelian subextension of K over $\mathbf{Q}_p$. In addition, Mochizuki [76] proved that the absolute Galois group together with its ramification filtration *does* determine a local field of characteristic 0, and Abrashkin [1], [2] extended this result to any characteristic $p > 0$.

A couple of natural questions then arise: when K is a number field, do irreducible *two-dimensional* (being the "lowest-dimensional non-abelian") representations of G_K determine K? When K is a non-archimedean local field of characteristic zero, to what extent does the representation theory of G_K determine K?

By the philosophy of the Langlands programme, n-dimensional irreducible representations of G_K (or, more generally, of the Weil group W_K) should be in correspondence with certain automorphic representations of GL_n, while preserving L-series.

Over non-archimedean local fields of characteristic zero, the local Langlands correspondence was proven by Harris and Taylor [40] and Henniart [42]. More precisely, their results state that equivalence classes of admissible irreducible representations of $\mathrm{GL}_n(K)$ are in bijection with equivalence classes of n-dimensional Frobenius semisimple representation of the Weil-Deligne group W_K' of K, see e.g. [122]; W_K' is a group extension of the Weil group W_K, from which there exists a continuous homomorphism to G_K with dense image.

When K is a number field, no analogous result is known, although various special cases have been considered. One believes that irreducible n-dimensional representations of G_K should correspond to cuspidal representations of $\mathrm{GL}_n(\mathbf{A}_K)$ "of Galois type" [22, p. 244]. Moreover, *all* cuspidal representations of $\mathrm{GL}_n(\mathbf{A}_K)$ should be in correspondence with irreducible n-dimensional representations of the so-called Langlands group, which is the conjectural global analogue of the Weil-Deligne group.

Automorphic (admissible) representations of $\mathrm{GL}_n(\mathbf{A}_K)$ in turn correspond to (admissible) modules over the Hecke algebra $\mathscr{H}_{\mathrm{GL}_n}(K)$. Therefore, our questions inspire the next question.

Question 1.1. Let K be either a number field or a non-archimedean local field of characteristic zero. To what extent does (the representation theory of) the Hecke algebra $\mathscr{H}_{\mathrm{GL}_n}(K)$ determine K?

For $n = 2$, the following result (Theorem 4.11) provides a partial answer.

Theorem A (Theorem 4.11)**.** *Let K and L be two non-archimedean local fields of characteristic zero and let $G = \mathrm{GL}_2$. Then there is always a Morita equivalence $\mathscr{H}_G(K) \sim_M \mathscr{H}_G(L)$.*

The Morita equivalence means that the respective categories of modules over the Hecke algebras of K and L are isomorphic. That is, the module structure of the complex representations of GL_2 over a local field as above does not depend on the local field. The proof uses the Bernstein decomposition of the Hecke algebra.

Hecke algebras exist for any linear algebraic group G over $\mathbf{Q}$. When K is a number field, we will work with the finite-adelic real Hecke algebra, and when K is a non-archimedean local field of characteristic zero, we use the local Hecke algebra. These are defined as follows:

$$\mathscr{H}_G(K) = \begin{cases} C_c^\infty(G(\mathbf{A}_{K,f}), \mathbf{R}) & \text{if } K \text{ is a number field,} \\ C_c^\infty(G(K), \mathbf{C}) & \text{if } K \text{ is non-arch. local of char. 0.} \end{cases}$$

(We could replace $\mathbf{R}$ by $\mathbf{C}$ in the number fields case; this does not affect our results.) Such Hecke algebras are equipped with an L^1-norm, which is induced from the Haar measure on the (locally compact) point group; an *L^1-isomorphism* will be an algebra isomorphism which respects this norm.

Using Stone-Weierstrass and results by Kawada [55] and Wendel [127], we prove in Theorem 4.6 that there is an L^1-isomorphism of finite-adelic Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if there is an isomorphism of finite-adelic point groups $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$, and that there is an L^1-isomorphism of local Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if there is an isomorphism of local point groups $G(K) \cong G(L)$.

The question whether $G(R) \cong G(S)$ for algebraic groups G and rings R, S implies a ring isomorphism $R \cong S$ has been considered before (following seminal work of van der Waerden and Schreier from 1928 [97]), most notably when $G = \mathrm{GL}_n$ for $n \geq 3$ or when G is a Chevalley group and R and S are integral domains (see, e.g., [31], [88] and the references therein). The methods employed there make extensive use of root data and Lie algebras.

When $G = \mathrm{GL}_n$ for $n \geq 2$ and K and L are non-archimedean local of characteristic zero, $G(K) \cong G(L)$ implies $K \cong L$ by Theorem 5.6.10 of [82]. That is, the following result provides another partial answer to Question 1.1.

Theorem B (Corollary 4.9). *Let K and L be two non-archimedean local fields of characteristic zero and let $G = \mathrm{GL}_n$, $n \geq 2$. Then there is an L^1-isomorphism of local Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if there is a field isomorphism $K \cong L$.*

In the case of number fields, we introduce the following technical condition on the groups G: we call G *fertile* for a field $K/\mathbf{Q}$ if G contains a Borel group B which is split over K as $B = T \ltimes U$, such that over K, the split maximal torus $T \neq \{1\}$ acts nontrivially by conjugation on the abelianisation of the maximal unipotent group $U \neq \{0\}$. In particular, GL_n is fertile for any K and all $n \geq 2$.

Now we can state the main result of Chapter 3.

Theorem C (Theorem 3.1). *Let K and L be two number fields, and let G denote a linear algebraic group over $\mathbf{Q}$ which is fertile for K and L. There is a topological group isomorphism of finite-adelic point groups $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ if and only if there is a topological ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$.*

Our proof of Theorem C uses number theory in adele rings and, by not passing to Lie algebras, applies to a more general class of (not necessarily reductive) algebraic groups. First, we prove in general that maximal divisible subgroups $\mathbf{D}$ of $G(\mathbf{A}_{K,f})$ and maximal unipotent point groups are the same up to conjugacy (Proposition 3.10; note that this does not apply at the archimedean places). The torus $\mathbf{T}$ (as a quotient of the normaliser $\mathbf{N}$ of the unipotent point group $\mathbf{D}$ by itself) acts on the abelian group $\mathbf{V} = [\mathbf{N}, \mathbf{D}]/[\mathbf{D}, \mathbf{D}]$, that decomposes as a sum of one-dimensional $\mathbf{T}$-modules, on which $\mathbf{T}$ acts by multiplication with powers. Now we use a formula of Siegel, which allows us to express any adele as a linear combination of fixed powers, to show how this implies that the centre of the endomorphism ring of the $\mathbf{T}$-module $\mathbf{V}$ is a a cartesian power of the finite adele ring. We then use the structure of the maximal principal ideals in the finite adele ring to find from these data the adele ring itself.

For example, consider $G = \mathrm{GL}(2)$. Then $\mathbf{D} = \left(\begin{smallmatrix} 1 & \mathbf{A}_{K,f} \\ 0 & 1 \end{smallmatrix}\right) \cong (\mathbf{A}_{K,f}, +)$ is (conjugate to) a group of strictly upper triangular matrices, $\mathbf{N} = \left(\begin{smallmatrix} \mathbf{A}^*_{K,f} & \mathbf{A}_{K,f} \\ 0 & \mathbf{A}^*_{K,f} \end{smallmatrix}\right)$ and $\mathbf{T} \cong (\mathbf{A}^*_{K,f}, \cdot)^2$ (represented as diagonal matrices) acts on $\mathbf{V} \cong \mathbf{D}$ (represented as upper triangular matrices) by conjugation. Now $\mathrm{End}_{\mathbf{T}}\mathbf{V} \cong \mathbf{A}_{K,f}$ as (topological) rings.

Hence, we have proved the following global version of Theorem B (Theorem 4.7), providing a partial answer to Question 1.1 for number fields.

Theorem D. *Let K and L be two number fields, and let G denote a linear algebraic group over $\mathbf{Q}$ that is fertile for K and L. There is an L^1-isomorphism of Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if there is a ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$.*

It is not clear to us for precisely which (linear) algebraic groups G Theorem C holds. However, the following example illustrates why a condition like fertility is needed: if $G = \mathbf{G}_a^r \times \mathbf{G}_m^s$ for integers r, s, then for any two distinct imaginary quadratic fields K and L of discriminant < -8 we have an isomorphism of topological groups $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ while $\mathbf{A}_K \not\cong \mathbf{A}_L$.

To prove this, one determines separately the abstract structures of the additive (Section 2.2) and multiplicative (Section 2.3) groups of the adele ring $\mathbf{A}_K$ and sees that they depend on only a few arithmetic invariants, allowing for a lot of freedom in "exchanging local factors". In particular, the additive structure depends only on the field degree $[K\colon \mathbf{Q}]$, and the multiplicative structure on the field degree, the residue field degrees and the roots of unity in K.

Finally, we make some remarks on the condition $\mathbf{A}_K \cong \mathbf{A}_L$, cf. Section 2.1. When such an isomorphism exists, K and L are said to be locally isomorphic. Local isomorphism implies, but is generally stronger than, arithmetic equivalence of K and L. Recall that K and L are arithmetically equivalent if their Dedekind zeta functions coincide: $\zeta_K = \zeta_L$. Moreover, if K or L is Galois over $\mathbf{Q}$, both local isomorphism and arithmetic equivalence imply that K and L are isomorphic as fields.

Therefore, if K and L are Galois over $\mathbf{Q}$, and G is fertile for K and L, Theorem D shows that there is an L^1-isomorphism of Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if $K \cong L$. This result can be seen as an automorphic analogue of Neukirch's theorem.

Chapter overview

- In Chapter 2, we discuss the notions of arithmetic equivalence and local isomorphism between number fields, and we study the additive and multiplicative structures of the adele ring of a number field.

- In Chapter 3, we consider finite-adelic point groups for number fields K and L and a fertile linear algebraic group $G/\mathbf{Q}$, and we prove Theorem C.

- In Chapter 4, we introduce Hecke algebras over global and local fields, as well as the notion of an L^1-isomorphism, and prove Theorem B, Theorem D, and Theorem A.

1.2 Galois representations

The Inverse Galois Problem asks whether, for a given finite group G, there exists a Galois extension $K/\mathbf{Q}$ with Galois group isomorphic to G. In other words, it asks whether a finite group G occurs as a quotient of $G_{\mathbf{Q}}$. It is an open problem whether this holds for any finite group G. The origin of this problem can be traced back to Hilbert. In 1892, he proved in [44] that the symmetric group S_n and the alternating group A_n are Galois groups over $\mathbf{Q}$, for all n. We also have an affirmative answer to the Inverse Galois Problem for some other families of finite groups. For instance, all finite solvable groups (Shafarevich, [94]) and all sporadic simple groups, except the Mathieu group M_{23}, are known to be Galois groups over $\mathbf{Q}$; cf. [53, Section 0.2] for an overview.

A Galois representation is a continuous homomorphism

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_n(R),$$

where R is a topological ring, e.g. $\mathbf{C}$, $\mathbf{Z}/n\mathbf{Z}$ or $\mathbf{F}_q$ with the discrete topology, or $\mathbf{Q}_\ell$ with the ℓ-adic topology.

Since $G_{\mathbf{Q}}$ is compact, the image of ρ is finite when the topology of R is discrete. As a consequence, images of Galois representations yield Galois realisations over $\mathbf{Q}$ of finite linear groups

$$\mathrm{Gal}(\overline{\mathbf{Q}}^{\ker\rho}/\mathbf{Q}) \simeq \rho(G_{\mathbf{Q}}) \subseteq \mathrm{GL}_n(R).$$

This gives us an interesting connection between the Inverse Galois Problem and Galois representations, and hence a strategy to address the Inverse Galois Problem, namely, to construct Galois representations with a given image.

This strategy has been employed in the literature, to obtain Galois realisations of, for instance, $\mathrm{GL}_2(\mathbf{F}_\ell)$ for all ℓ [102], $\mathrm{GSp}_4(\mathbf{F}_\ell)$ for $\ell > 3$ [10] , $\mathrm{PGSp}_4(\mathbf{F}_{\ell^3})$ and $\mathrm{PSp}_4(\mathbf{F}_{\ell^2})$ for explicit infinite families of primes ℓ [34], and $\mathrm{PGSp}_{2n}(\mathbf{F}_{\ell^r})$ and $\mathrm{PSp}_{2n}(\mathbf{F}_{\ell^r})$ for each $n \geq 2$, for either a fixed prime ℓ and infinitely many positive integers r [56], or a fixed r and a positive density set of primes ℓ [5].

If A is an abelian variety of dimension g defined over $\mathbf{Q}$, and ℓ is a prime number, let $A[\ell] = A(\overline{\mathbf{Q}})[\ell]$ denote the ℓ-torsion subgroup of $\overline{\mathbf{Q}}$-points of A. The natural action of $G_{\mathbf{Q}}$ on $A[\ell]$ gives rise to a continuous Galois representation $\overline{\rho}_{A,\ell}$ taking values in $\mathrm{GL}(A[\ell]) \simeq \mathrm{GL}_{2g}(\mathbf{F}_\ell)$. If the abelian variety A is moreover principally polarised, the image of $\overline{\rho}_{A,\ell}$ lies inside the general symplectic group $\mathrm{GSp}(A[\ell])$ of $A[\ell]$ with respect to the symplectic pairing induced by the Weil pairing and the polarisation of A; thus, we have a representation

$$\overline{\rho}_{A,\ell} \, : \, G_{\mathbf{Q}} \longrightarrow \mathrm{GSp}(A[\ell]) \simeq \mathrm{GSp}_{2g}(\mathbf{F}_\ell),$$

providing a realisation of $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ as a Galois group over $\mathbf{Q}$, *if* $\overline{\rho}_{A,\ell}$ is surjective.

Let us fix a dimension g. The setup above leads to the following questions.

Question 1.2. (a) If we are given a principally polarised g-dimensional abelian variety A, for which prime numbers ℓ is the representation $\overline{\rho}_{A,\ell}$ surjective?

(b) If we are instead given a prime number ℓ, can we always find a principally polarised g-dimensional abelian variety A such that $\overline{\rho}_{A,\ell}$ is surjective?

The image of Galois representations attached to the ℓ-torsion points of abelian varieties has received a lot of attention. Let us briefly mention a few known results.

For an abelian variety A defined over a number field, a classical result by Serre ensures surjectivity for almost all primes ℓ when $\mathrm{End}_{\overline{\mathbf{Q}}}(A) = \mathbb{Z}$ and the dimension of A is 2, 6 or odd [105].

More recently, Hall [38] proved a result for any dimension, under some additional conditions on the abelian variety which are explained below. This result has been further generalised by Arias-de-Reyna, Gajda, and Petersen, to the case of abelian varieties over finitely generated fields [7]. Le Duff [60] has also applied it to Jacobian varieties of genus 2 curves, to obtain realisations of $\mathrm{GSp}_4(\mathbf{F}_\ell)$ for all odd primes $\ell \leq 500000$.

Arias-de-Reyna and Vila (cf. [9], [10]) have solved the Inverse Galois Problem for $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ when $g = 1, 2$ and $\ell \geq 5$ is any prime number, by constructing a family of genus g curves C such that the Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the Jacobian variety $\mathrm{Jac}(C)$ is surjective. Moreover, these representations are tamely ramified for every curve in the family.

Suppose that we have a representation $\overline{\rho}_{A,\ell} \colon G_{\mathbf{Q}} \to \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ as above. A *transvection* $T \in \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ is an element which acts as the identity on a hyperplane $H \subset A[\ell]$. The structure theory of the general symplectic group (Section 5.1) gives us that $\mathrm{Im}(\overline{\rho}_{A,\ell}) = \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ if $\mathrm{Im}(\overline{\rho}_{A,\ell})$ contains both a nontrivial transvection and an element whose characteristic polynomial is irreducible and has a nonzero trace. Thus, to answer Question 1.2, it suffices to find primes ℓ (when $A/\mathbf{Q}$ is given), resp. abelian varieties $A/\mathbf{Q}$ (when ℓ is given), such that $\mathrm{Im}(\overline{\rho}_{A,\ell})$ contains these two kinds of elements.

By a result of Hall [38], if there is a finite extension $K/\mathbf{Q}$ so that the Néron model of A/K over the ring of integers $\mathscr{O}_K$ of K has a semistable fibre at some prime $\mathfrak{p}$ with toric dimension 1, then $\mathrm{Im}(\overline{\rho}_{A,\ell})$ contains a transvection. If this holds, we say that A satisfies condition (T).

We prove the following surjectivity result.

Theorem E (Theorem 5.15)**.** *Let $A/\mathbf{Q}$ be a principally polarised g-dimensional abelian variety which satisfies condition* (T) *for some rational prime p. Denote by Φ_p the group of connected components of the special fibre of the Néron model of A over $\mathbf{Q}_p$. In addition, let q be a prime of good reduction of A, let A_q be the special fibre of the Néron model of A over $\mathbf{Q}_q$, and let $P_q(X) \in \mathbf{Z}[X]$ be the characteristic polynomial of the Frobenius endomorphism of A_q.*

Then $\mathrm{Im}(\overline{\rho}_{A,\ell}) = \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ for all primes ℓ which divide neither $6pq|\Phi_p|$ nor the coefficient of X^{2g-1} in $P_q(X)$, and satisfy that the reduction of $P_q(X) \bmod \ell$ is irreducible in $\mathbf{F}_\ell$.

We now restrict to the case $g = 3$. Our first main result, answering Question 1.2(a), can be summarised as follows.

Theorem F. *Let $A = \mathrm{Jac}(C)$ be the Jacobian variety of a hyperelliptic curve $C\colon Y^2 = f(X)$ of genus 3 over $\mathbf{Q}$ which satisfies condition* (T) *for some prime p. Then there exists an algorithm which provides a non-empty list of primes ℓ for which $\overline{\rho}_{A,\ell}$ is surjective.*

First, we remark that in this special case where $A = \mathrm{Jac}(C)$ is the Jacobian variety of a hyperelliptic curve $C\colon Y^2 = f(X)$ of genus g, condition (T) simplifies; now, A satisfies condition (T) as soon as there is a (rational) prime p such that the coefficients of $f(X)$ have p-adic valuation greater than or equal to zero, and $f(X) \bmod p$ has one double zero and otherwise simple zeroes.

The algorithm uses an auxiliary prime q, which is a prime of good reduction for A. For each prime ℓ, the algorithm determines whether ℓ satisfies the conditions of Theorem E.

Note that the list of primes ℓ we obtain in this way is not necessarily exhaustive. However, in Chapter 6, we compute an example, which realises $\mathrm{GSp}_6(\mathbf{F}_\ell)$ as a Galois group over $\mathbf{Q}$ for all $\ell \in [11, 500000]$.

Our second main result provides an answer to Question 1.2(b) and can be phrased as follows.

Theorem G (Theorem 7.1)**.** *For any prime number $\ell \geq 5$, there exist infinitely many curves $C/\mathbf{Q}$ of genus 3 defined over $\mathbf{Q}$ such that $\mathrm{Im}(\overline{\rho}_{\mathrm{Jac}(C),\ell}) = \mathrm{GSp}_6(\mathbf{F}_\ell)$.*

This theorem provides an explicit and constructive solution to the Inverse Galois Problem for the symplectic groups $\mathrm{GSp}_6(\mathbf{F}_\ell)$.

The proof again uses two auxiliary primes p and q. Firstly, we construct a curve $C_p/\mathbf{Q}_p$, such that $\mathrm{Jac}(C_p)$ satisfies condition (T) for p and such that $|\Phi_p| = 2$. We do this by forcing its defining equation to have a very particular form after reduction modulo p^2. Then, we construct a second curve C_q over $\mathbf{F}_q$, such that the Jacobian $\mathrm{Jac}(C_q)$ has a Frobenius endomorphism whose characteristic polynomial modulo ℓ is irreducible and has nonzero trace. In fact, we show that for any $\ell \geq 3$, there exists a suitable q, by counting Weil q-polynomials. Finally, the defining equation for the curve $C/\mathbf{Q}$ is obtained by lifting that of C_q to $\mathbf{Z}$, and then imposing the same conditions modulo p^2 as for that of C_p. (This is always possible by the Chinese Remainder Theorem.) The representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ is therefore immediately seen to be surjective.

Chapter overview

- In Chapter 5, we introduce Galois representations attached to abelian varieties, and state results about their surjectivity, including Theorem E.
- In Chapter 6, we explain the algorithm from Theorem F which, for a given three-dimensional abelian variety $A/\mathbf{Q}$, computes a list of prime numbers ℓ for which the Galois representation $\overline{\rho}_{A,\ell}$ is surjective.
- In Chapter 7, we construct, for a given prime number ℓ, a family of three-dimensional abelian varieties $A/\mathbf{Q}$ for which the Galois representations $\overline{\rho}_{A,\ell}$ are surjective, proving Theorem G.

1.3 Abelian varieties

Let us fix a finite field $K = \mathbf{F}_q$ of characteristic p, i.e., such that $q = p^r$ for some r, and let $k = \overline{\mathbf{F}}_p$ be an algebraic closure.

Let V be a smooth projective g-dimensional variety over K. By the Riemann hypothesis over function fields [33], the roots of the characteristic polynomial of the Frobenius endomorphism of V all have absolute value $\sqrt{q}$. These roots are called the *Weil numbers* of V; dividing them by $\sqrt{q}$ yields the *normalised Weil numbers*.

In our situation, V will be either a g-dimensional abelian variety A/K or a smooth projective connected curve X/K of genus g. For such a curve X/K we then consider its Jacobian $\mathrm{Jac}(X)$; this is a g-dimensional abelian variety, and the Weil numbers of X are the roots of the characteristic polynomial of the Frobenius endomorphism of $\mathrm{Jac}(X)$.

An abelian variety is determined up to K-isogeny by the characteristic polynomial of its Frobenius endomorphism. Moreover, Honda-Tate theory implies that the set of K-isogeny classes of simple abelian varieties over K is in bijection with the set of K-Weil numbers up to Galois conjugacy.

An elliptic curve E over any field of characteristic p is called *supersingular* if $E[p^r] = 0$ for one (hence all) $r \geq 1$, cf. [107, Theorem V.3.1]. Equivalently, E is supersingular if and only if its Weil numbers $(\alpha, \overline{\alpha})$ satisfy $\alpha = \sqrt{q}\zeta$ (and $\overline{\alpha} = \sqrt{q}\overline{\zeta}$), where ζ is some root of unity.

More generally, a principally polarised g-dimensional abelian variety A/K is called supersingular if its normalised Weil numbers are all roots of unity, and a curve X/K is supersingular if $\mathrm{Jac}(X)$ is supersingular.

Thus, the Weil numbers tell us whether an abelian variety or a curve is supersingular. This part of the thesis studies some other arithmetic properties of supersingular abelian varieties and (Jacobians of) curves over finite fields, which are determined by their (normalised) Weil numbers.

First of all, we see that the Riemann hypothesis over function fields has immediate consequences for the number of K-points of an abelian variety or a curve over K. The Hasse-Weil bound for curves X/K of genus g says that

$$|X(K) - (q+1)| \leq 2g\sqrt{q}.$$

When X reaches the upper bound $|X(K)| = (q+1) + 2g\sqrt{q}$, we say it is *maximal* over K; when it reaches the lower bound, we call it *minimal*. The normalised Weil numbers of a maximal (resp. minimal) curve X/K are all -1 (resp. 1). Analogously, we say an abelian variety A/K is maximal (resp. minimal) if all its normalised Weil numbers are -1 (resp. 1).

We see that an abelian variety A/K, or a curve X/K, is supersingular if and only if it is minimal over some finite field extension of K. Now we would like to study the following problem.

Question 1.3. When is a supersingular abelian variety A/K or curve X/K *maximal* over some finite extension of K?

The *(K-)period* of an abelian variety A/K or curve X/K is the degree of the smallest extension of K over which A resp. X is either maximal or minimal. The *(K-)parity* is 1 in the first case and -1 in the second case. A quadratic twist of a maximal abelian variety or curve can be minimal, and this introduces some subtlety to the problem.

Let $\Theta(A/K)$ denote the set of K-twists of A, i.e., the set of abelian varieties A_0/K such that A_0 is isomorphic to A over k. We define A to be (i) *fundamentally* *maximal* or (ii) *partially maximal* or (iii) *fundamentally minimal* if A_0 has parity 1 for (i) all or (ii) some or (iii) none of $A_0 \in \Theta(A/K)$. Taking $A = \mathrm{Jac}(X)$, we define the same three types for curves X.

We show how the type of a supersingular abelian variety or curve is related to its Weil numbers. These Weil numbers $\{\alpha_1, \ldots, \alpha_{2g}\}$ are of the form $\alpha_i = \sqrt{q}\zeta_{N_i}^{j_i}$ (where $\gcd(N_i, j_i) = 1$), for some $N_i = 2^{e_i}o_i$ with o_i odd. We call e_i the *binary value of* α_i.

Proposition H (Propositions 9.11 and 9.12). *Let A/K be a supersingular g-dimensional abelian variety.*

1. *If A/K is fundamentally maximal, then all e_i equal the same value $e \geq 2$.*

2. *If A/K is fundamentally minimal, then not all e_i are the same.*

   Conversely, we have:

3. *If $e_i = 0$ for all i, or $e_i = 1$ for all i, then A/K is partially maximal.*

4. *If all $e_i \geq 2$ are the same, the parity of A/K is not affected by quadratic twists.*

5. *If not all e_i are the same, the twist by* $[-1]$ *does not affect the parity of A/K.*

When $g = 1$, we completely analyse the isogeny classes of supersingular elliptic curves and determine their types. When $g = 2$, we compute the parities and periods for each isogeny class of abelian surfaces (in Proposition 9.22).

Secondly, we investigate the relation between Weil numbers and the dimension of the corresponding abelian variety. Honda-Tate theory yields that for every complex root of unity z, there exists a simple supersingular abelian variety A_z/K whose Weil numbers are $\alpha = \sqrt{q}z$ and its conjugates. We ask the following question.

Question 1.4 (Question 10.1). Suppose that $z_1, \ldots, z_s$ are s randomly chosen roots of unity and consider the supersingular abelian variety $A = A_{z_1} \times \ldots \times A_{z_s}$. What is the probability that A has dimension g?

For simplicity, we study the case where $\{z_1, \ldots, z_s\} \subseteq \mu_{2^N}$ for some N. Now, "randomly chosen" means that we equip μ_{2^N} with the uniform measure.

Recall that $K = \mathbf{F}_q$ with $q = p^r$. Our answer to question 1.4 depends on whether r is odd or even, and on whether $p = 2$ or $p > 2$. Here we give one case of our main result.

Proposition I (Proposition 10.7(1)). *Let $q = p^r$ with r odd and $p > 2$, and fix N. Randomly pick $z = \zeta_{2^m}^j \in \mu_{2^N}$ and let $A = A_z$ be the corresponding simple supersingular abelian variety over K. Then*

$$\dim(A) = \begin{cases} 1 \\ 2 \\ 2^{m-2} \text{ \textit{if} } 4 \leq m \leq N \end{cases} \qquad \textit{with probability} \begin{cases} \frac{1}{2^{N-1}} \\ \frac{3}{2^{N-1}} \\ \frac{1}{2^{N+1-m}} \end{cases}.$$

Chapter overview

- In Chapter 8, we collect some results on supersingular abelian varieties and curves and their Weil numbers. We introduce twists and study how these affect the Frobenius endomorphism.

- In Chapter 9, we define the period and the parity, as well as the types (fundamentally maximal, fundamentally minimal, partially maximal). To provide answers to Question 1.3, we state and prove some properties of these notions, including Proposition H. In Section 9.2, we analyse the $g = 1$ and $g = 2$ situations.

- In Chapter 10, we consider Question 1.4, and we prove Proposition I.

Part I

Hecke algebras and adelic points

CHAPTER 2

Arithmetic equivalence and local isomorphism

In this chapter, we discuss the group structure of the additive and multiplicative groups of adeles of a number field, and we recall the notions of local isomorphism of number fields and its relation to isomorphism of adele rings and arithmetic equivalence. We introduce *local* additive and multiplicative isomorphisms and prove that their existence implies arithmetic equivalence.

2.1 Arithmetic equivalence and local isomorphism

Notation/Definitions 2.1. If K is a number field with ring of integers $\mathcal{O}_K$, let M_K denote the set of all places of K, $M_{K,f}$ the set of non-archimedean places of K, and $M_{K,\infty}$ the set of archimedean places. If $\mathfrak{p} \in M_{K,f}$ is a prime ideal, then $K_\mathfrak{p}$ denotes the completion of K at $\mathfrak{p}$, and $\mathcal{O}_{K,\mathfrak{p}}$ its ring of integers. Let $e(\mathfrak{p})$ and $f(\mathfrak{p})$ denote the ramification and residue degrees of $\mathfrak{p}$ over the rational prime p below $\mathfrak{p}$, respectively. The *decomposition type* of a rational prime p in a field K is the sequence $(f(\mathfrak{p}))_{\mathfrak{p}|p}$ of residue degrees of the prime ideals of K above p, in increasing order, with multiplicities.

For an archimedean place $\mathfrak{p}$ of K, we have $K_\mathfrak{p} = \mathbf{R}$ or $\mathbf{C}$ and we let $\mathcal{O}_{K,\mathfrak{p}} = K_\mathfrak{p}$.

Definition 2.2. We use the notation $\prod'(G_i, H_i)$ for the restricted product of the group G_i with respect to the subgroups H_i. We denote by

$$\mathbf{A}_K = \prod_{\mathfrak{p}\in M_K}{}' (K_\mathfrak{p}, \mathcal{O}_{K,\mathfrak{p}})$$

the adele ring of K, and by

$$\mathbf{A}_{K,f} = \prod_{\mathfrak{p}\in M_{K,f}}{}' (K_\mathfrak{p}, \mathcal{O}_{K,\mathfrak{p}})$$

its ring of finite adeles.

This chapter is based on parts of the article [32], joint work with Gunther Cornelissen.

Two number fields K and L are *arithmetically equivalent* if for all but finitely many prime numbers p, the decomposition types of p in K and L coincide.

Two number fields K and L are called *locally isomorphic* if there is a bijection $\varphi\colon M_{K,f} \to M_{L,f}$ between their sets of prime ideals such that the corresponding local fields are topologically isomorphic, i.e. $K_{\mathfrak{p}} \cong L_{\varphi(\mathfrak{p})}$ for all $\mathfrak{p} \in M_{K,f}$.

The *Dedekind zeta function* of a number field K is defined as

$$\zeta_K(s) = \sum_{I \subseteq \mathscr{O}_K} \frac{1}{N_{K/\mathbf{Q}}(I)^s},$$

where the sum ranges over the nonzero ideals of $\mathscr{O}_K$.

The main properties are summarised in the following proposition (see e.g. [57, III.1 and VI.2]):

Proposition 2.3. Let K and L be number fields. Then:

(i) K and L are locally isomorphic if and only if the adele rings $\mathbf{A}_K$ and $\mathbf{A}_L$ are isomorphic as topological rings, if and only if the rings of finite adeles $\mathbf{A}_{K,f}$ and $\mathbf{A}_{L,f}$ are isomorphic as topological rings.

(ii) K and L are arithmetically equivalent if and only if $\zeta_K = \zeta_L$, if and only if there is a bijection $\varphi\colon M_{K,f} \to M_{L,f}$ such that the local fields $K_{\mathfrak{p}} \cong L_{\varphi(\mathfrak{p})}$ are isomorphic for *all but finitely many* $\mathfrak{p} \in M_{K,f}$.

(iii) We have $K \cong L \Rightarrow \mathbf{A}_K \cong \mathbf{A}_L$ (as topological rings) $\Rightarrow \zeta_K = \zeta_L$ and none of the implications can be reversed in general, but if K or L is Galois over $\mathbf{Q}$, then all implications can be reversed. □

2.2 The additive group of adeles

Proposition 2.4. If H is a number field, then there are topological isomorphisms of additive groups

$$(\mathbf{A}_{H,f}, +) \cong (\mathbf{A}_{\mathbf{Q},f}^{[H:\mathbf{Q}]}, +)$$

and

$$(\mathbf{A}_H, +) \cong (\mathbf{A}_{\mathbf{Q}}^{[H:\mathbf{Q}]}, +).$$

Proof. If $\mathfrak{p}$ is a prime of H above the rational prime p, then $\mathscr{O}_{H,\mathfrak{p}}$ is a free $\mathbf{Z}_p$-module of rank $e(\mathfrak{p})f(\mathfrak{p})$ (cf. [30, 5.3-5.4]), and tensoring with $\mathbf{Q}$ gives a compatible diagram of isomorphisms of additive groups

$$\begin{tikzcd}
(\mathscr{O}_{H,\mathfrak{p}}, +) \arrow[r, "\sim"'] \arrow[d, hook] & (\mathbf{Z}_p^{e(\mathfrak{p})f(\mathfrak{p})}, +) \arrow[d, hook] \\
(H_{\mathfrak{p}}, +) \arrow[r, "\sim"'] & (\mathbf{Q}_p^{e(\mathfrak{p})f(\mathfrak{p})}, +)
\end{tikzcd}$$

which we can sum over all $\mathfrak{p} \mid p$ for fixed p, to find

$$\begin{tikzcd}
(\bigoplus\limits_{\mathfrak{p}|p} \mathscr{O}_{H,\mathfrak{p}}, +) \arrow[r, "\sim"'] \arrow[d, hook] & (\mathbf{Z}_p^n, +) \arrow[d, hook] \\
(\bigoplus\limits_{\mathfrak{p}|p} H_{\mathfrak{p}}, +) \arrow[r, "\sim"'] & (\mathbf{Q}_p^n, +)
\end{tikzcd}$$

for $n = [H : \mathbf{Q}]$; here, we use the fact that $\sum_{\mathfrak{p}|p}[H_{\mathfrak{p}} : \mathbf{Q}_p] = [H : \mathbf{Q}]$. It follows that

$$\begin{aligned}
(\mathbf{A}_{H,f}, +) &= \prod_{p \in M_{\mathbf{Q},f}}{}^{\prime} (\bigoplus_{\mathfrak{p}|p}(H_{\mathfrak{p}}, +), \bigoplus_{\mathfrak{p}|p}(\mathscr{O}_{H,\mathfrak{p}}, +)) \\
&\cong \prod_{p \in M_{\mathbf{Q},f}}{}^{\prime} ((\mathbf{Q}_p^n, +), (\mathbf{Z}_p^n, +)) \\
&\cong (\mathbf{A}_{\mathbf{Q},f}^n, +)
\end{aligned}$$

and hence

$$\begin{aligned}
(\mathbf{A}_H, +) &= (\mathbf{A}_{H,f}, +) \times (\mathbf{R}^n, +) \\
&\cong (\mathbf{A}_{\mathbf{Q},f}^n, +) \times (\mathbf{R}^n, +) \cong (\mathbf{A}_{\mathbf{Q}}^n, +).
\end{aligned}$$

□

Corollary 2.5. The additive groups $(\mathbf{A}_K, +)$ and $(\mathbf{A}_L, +)$ are isomorphic (as topological groups) for two number fields K and L if and only if K and L have have the same degree over $\mathbf{Q}$. For finite adeles, $[K\colon \mathbf{Q}] = [L\colon \mathbf{Q}]$ implies $(\mathbf{A}_{K,f}, +) \cong (\mathbf{A}_{L,f}, +)$.

Proof. By Proposition 2.4, we know that $[K : \mathbf{Q}] = [L : \mathbf{Q}]$ implies that $(\mathbf{A}_{K,f}, +) \cong (\mathbf{A}_{L,f}, +)$ and $(\mathbf{A}_K, +) \cong (\mathbf{A}_L, +)$.

Conversely, a topological isomorphism $(\mathbf{A}_K, +) \cong (\mathbf{A}_L, +)$ of additive groups induces a homeomorphism between their respective connected components of the identity, i.e.,

$$\mathbf{R}^{[K:\mathbf{Q}]} \cong \mathbf{R}^{[L:\mathbf{Q}]}.$$

Since homotopic groups have isomorphic homology [71, Theorem 4.2] and $\mathbf{R}^n - \{0\}$ is homotopic to the sphere S^{n-1} for any $n \geq 1$ (e.g. [20, Example 14.7], we find (e.g. in [126, Lemma 4.1.3]) that

$$H_k(\mathbf{R}^n - \{0\}) = \begin{cases} \mathbf{Z} \text{ when } k = 0, n \\ 0 \text{ otherwise} \end{cases} .$$

In particular, if $m \neq n$, then $\mathbf{R}^m - \{0\}$ and $\mathbf{R}^n - \{0\}$ have different homology groups. Hence, we deduce that $[K : \mathbf{Q}] = [L : \mathbf{Q}]$. □

If, additionally, the isomorphism is "local", i.e. induced by local additive isomorphisms, then we have the following result.

Proposition 2.6. Let K and L be number fields such that there is a bijection

$$\varphi \colon M_{K,f} \to M_{L,f}$$

with, for almost all places $\mathfrak{p}$, isomorphisms of topological groups

$$\Phi_\mathfrak{p} \colon (K_\mathfrak{p}, +) \cong (L_{\varphi(\mathfrak{p})}, +).$$

Then K and L are arithmetically equivalent.

Proof. We may view each $K_\mathfrak{p}$ as a $[K_\mathfrak{p} : \mathbf{Q}_p] = e(\mathfrak{p})f(\mathfrak{p})$-dimensional topological $\mathbf{Q}_p$-vector space, where $p \in \mathbf{Q}$ is the prime lying below $\mathfrak{p}$. Similarly, for $q \in \mathbf{Q}$ the prime lying below $\varphi(\mathfrak{p}) \in L_{\varphi(\mathfrak{p})}$, we find that $L_{\varphi(\mathfrak{p})}$ is a topological $\mathbf{Q}_q$-vector space of dimension $[L_{\varphi(\mathfrak{p})} : \mathbf{Q}_q] = e(\varphi(\mathfrak{p}))f(\varphi(\mathfrak{p}))$. We will write $n = e(\mathfrak{p})f(\mathfrak{p})$ and $m = e(\varphi(\mathfrak{p}))f(\varphi(\mathfrak{p}))$. Thus, we have an isomorphism of topological groups

$$\Phi_\mathfrak{p} \colon (\mathbf{Q}_p^n, +) \xrightarrow{\sim} (\mathbf{Q}_q^m, +).$$

which must map $\mathbf{Z}^n$ injectively onto a subgroup of $\mathbf{Q}_q^m$ of the form $\bigoplus_{i=1}^n \nu_i \mathbf{Z}$, where the ν_i are $\mathbf{Z}$-linearly independent.

We indicate topological closure by a bar. Since the group of integers $\mathbf{Z}$ is dense in both $\mathbf{Z}_p$ and $\mathbf{Z}_q$ and $\Phi_\mathfrak{p}$ is a homeomorphism, we have

$$\Phi_\mathfrak{p}(\mathbf{Z}_p^n) = \Phi_\mathfrak{p}(\overline{\mathbf{Z}}^n) = \overline{\Phi_\mathfrak{p}(\mathbf{Z}^n)} = \overline{\bigoplus_{i=1}^n \nu_i \mathbf{Z}} = \sum_{i=1}^n \nu_i \mathbf{Z}_q \cong \mathbf{Z}_q^{n'},$$

where $n' \leq n$. In the last step, we have used that since $\mathbf{Z}_p$ is a principal ideal domain, any submodule of the free module $\mathbf{Z}_p^n$ is free. Thus, $\Phi_\mathfrak{p}$ restricts to a group isomorphism

$$\Phi'_\mathfrak{p} \colon (\mathbf{Z}_p^n, +) \xrightarrow{\sim} (\mathbf{Z}_q^{n'}, +).$$

We know (cf. [95, Lemma 52.6]) that the only p-divisible subgroup of $(\mathbf{Z}_p^n, +)$ is $\{0\}$, whereas for $q \neq p$, every element of $(\mathbf{Z}_p^n, +)$ is q-divisible. This group theoretic property ensures that $p = q$, that is,

$$\Phi'_{\mathfrak{p}} \colon (\mathbf{Z}_p^n, +) \xrightarrow{\sim} (\mathbf{Z}_p^{n'}, +) \subset (\mathbf{Q}_p^m, +).$$

As a group homomorphism, $\Phi'_{\mathfrak{p}}$ preserves the subgroup $p\mathbf{Z}_p^n$, and by considering the quotient, we find an isomorphism $(\mathbf{F}_p^n, +) \cong (\mathbf{F}_p^{n'}, +)$, which, by counting elements, implies that $n = n'$. Moreover, we see that $n = n' \leq m$, and since the isomorphism is invertible, we also obtain $m \leq n$, hence $n = m$.

We conclude that for all non-archimedean places $\mathfrak{p} \in M_{K,f}$, we must have

$$e(\mathfrak{p})f(\mathfrak{p}) = e(\varphi(\mathfrak{p}))f(\varphi(\mathfrak{p})).$$

At all but finitely many primes p, both K and L are unramified, so the local maps $\Phi_{\mathfrak{p}}$ will ensure that $f(\mathfrak{p}) = f(\varphi(\mathfrak{p}))$ for all but finitely many residue field degrees $f(\mathfrak{p})$. This implies that K and L are arithmetically equivalent. □

Remark 2.7. If all but finitely many residue field degrees of K and L match, then in fact *all* residue field degrees match, by a result of Perlis (the equivalence of (b) and (c) in [87, Theorem 1]). This in turn implies that all ramification degrees match. So whereas two arithmetically equivalent number fields may have different ramification degrees at finitely many places, the above isomorphism excludes this possibility. However, this is still weaker than local isomorphism, since the ramification degree does not uniquely determine the ramified part of a local field extension.

2.3 The multiplicative group of adeles

Proposition 2.8. If H is a number field with r_1 real and r_2 complex places, then there is a topological group isomorphism

$$(\mathbf{A}_H^*, \cdot) \cong (\mathbf{R}^*)^{r_1} \times (\mathbf{C}^*)^{r_2} \times \left(\bigoplus_{\mathbf{Z}} \mathbf{Z}\right) \times \hat{\mathbf{Z}}^{[H:\mathbf{Q}]} \times \prod_{\mathfrak{p} \in M_{H,f}} (\overline{H}_{\mathfrak{p}}^* \times \mu_{p^\infty}(H_{\mathfrak{p}}))$$

where $\overline{H}_{\mathfrak{p}}^*$ is the multiplicative group of the residue field of H at $\mathfrak{p}$ (a cyclic group of order $p^{f(\mathfrak{p})} - 1$) and $\mu_{p^\infty}(H_{\mathfrak{p}})$ is the (finite cyclic p-)group of p-th power roots of unity in $H_{\mathfrak{p}}$.

Proof. We have

$$\mathbf{A}_H^* \cong (\mathbf{R}^*)^{r_1} \times (\mathbf{C}^*)^{r_2} \times \mathbf{A}_{H,f}^*$$

and

$$\mathbf{A}^*_{H,f} \cong J_H \times \hat{\mathscr{O}}^*_H.$$

Here, J_H is the topologically discrete group of fractional ideals of H, so

$$J_H \cong \bigoplus_{\mathbf{Z}} \mathbf{Z},$$

where the index runs over the set of prime ideals, and the entry of $\mathfrak{n} \in J_H$ corresponding to a prime ideal $\mathfrak{p}$ is given by $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n})$. Furthermore,

$$\hat{\mathscr{O}}^*_H = \prod_{\mathfrak{p} \in M_{H,f}} \mathscr{O}^*_{H,\mathfrak{p}}$$

is the group of finite idelic units. To determine the isomorphism type of the latter, we quote [41], Kapitel 15: let $\pi_{\mathfrak{p}}$ be a local uniformiser at $\mathfrak{p}$ and let $\overline{H}_{\mathfrak{p}} = \mathscr{O}_{H,\mathfrak{p}}/\mathfrak{p}$ denote the residue field; then the unit group is

$$\mathscr{O}^*_{H,\mathfrak{p}} \cong \overline{H}^*_{\mathfrak{p}} \times (1 + \pi_{\mathfrak{p}} \mathscr{O}_{H,\mathfrak{p}}) \tag{2.1}$$

and the one-unit group

$$1 + \pi_{\mathfrak{p}} \mathscr{O}_{H,\mathfrak{p}} \cong \mathbf{Z}_p^{[H_{\mathfrak{p}}:\mathbf{Q}_p]} \times \mu_{p^\infty}(H_{\mathfrak{p}}) \tag{2.2}$$

where $\mu_{p^\infty}(H_{\mathfrak{p}})$ is the group of p-th power roots of unity in $H_{\mathfrak{p}}$. □

It remains to determine the exact structure of the p-th power roots of unity, e.g.:

Example 2.9. [3, Lemma 3.1 and Lemma 3.2] If $H \neq \mathbf{Q}(i)$ and $H \neq \mathbf{Q}(\sqrt{-2})$, then there is an isomorphism of topological groups

$$\prod_{\mathfrak{p} \in M_{H,f}} (\overline{H}^*_{\mathfrak{p}} \times \mu_{p^\infty}(H_{\mathfrak{p}})) \cong \prod_{n \geq 1} \mathbf{Z}/n\mathbf{Z}.$$

Hence we conclude: *If K and L are two imaginary quadratic number fields different from $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$, then we have a topological group isomorphism $\mathbf{A}^*_K \cong \mathbf{A}^*_L$.*

Combining Proposition 2.4 and Example 2.9, we obtain the following corollary.

Corollary 2.10. For any two imaginary quadratic number fields K and L different from $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-2})$ and for any integers r and s, there are topological group isomorphisms

$$(\mathbf{A}_{K,f})^r \times (\mathbf{A}^*_{K,f})^s \cong (\mathbf{A}_{L,f})^r \times (\mathbf{A}^*_{L,f})^s.$$

and

$$(\mathbf{A}_K)^r \times (\mathbf{A}^*_K)^s \cong (\mathbf{A}_L)^r \times (\mathbf{A}^*_L)^s.$$

□

On the other hand, we again have a "local" result (and Remark 2.7 also applies in this case):

Proposition 2.11. Let K and L be number fields such that there is a bijection $\varphi\colon M_{K,f} \to M_{L,f}$ with, for almost all places $\mathfrak{p}$, isomorphisms of topological groups $\Phi_{\mathfrak{p}}\colon (K_{\mathfrak{p}}^*, \cdot) \xrightarrow{\sim} (L_{\varphi(\mathfrak{p})}^*, \cdot)$. Then K and L are arithmetically equivalent.

Proof. From (2.1) and (2.2), for a given $\mathfrak{p}$ lying above $p \in \mathbf{Q}$, we find that

$$K_{\mathfrak{p}}^* \cong \mathbf{Z} \times \overline{K}_{\mathfrak{p}}^* \times \mathbf{Z}_p^{[K_{\mathfrak{p}}:\mathbf{Q}_p]} \times \mu_{p^\infty}(K_{\mathfrak{p}}).$$

Dividing out by the torsion elements yields

$$K_{\mathfrak{p}}^*/K_{\mathfrak{p},\mathrm{tors}}^* \cong \mathbf{Z} \times \mathbf{Z}_p^{[K_{\mathfrak{p}}:\mathbf{Q}_p]}.$$

Hence, $\Phi_{\mathfrak{p}}$ will induce a map

$$\Phi'_{\mathfrak{p}}\colon K_{\mathfrak{p}}^*/K_{\mathfrak{p},\mathrm{tors}}^* \xrightarrow{\sim} L_{\varphi(\mathfrak{p})}^*/L_{\varphi(\mathfrak{p}),\mathrm{tors}}^*$$

which equals

$$\Phi'_{\mathfrak{p}}\colon \mathbf{Z} \times \mathbf{Z}_p^{[K_{\mathfrak{p}}:\mathbf{Q}_p]} \xrightarrow{\sim} \mathbf{Z} \times \mathbf{Z}_q^{[L_{\varphi(\mathfrak{p})}:\mathbf{Q}_q]}$$

where $q \in \mathbf{Q}$ is the rational prime below $\varphi(\mathfrak{p})$. Now we form the quotient

$$(\mathbf{Z} \times \mathbf{Z}_p^{[K_{\mathfrak{p}}:\mathbf{Q}_p]})/p \cdot (\mathbf{Z} \times \mathbf{Z}_p^{[K_{\mathfrak{p}}:\mathbf{Q}_p]}) \cong \mathbf{Z}/p\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^{[K_{\mathfrak{p}}:\mathbf{Q}_p]} \tag{2.3}$$

which, under $\Phi'_{\mathfrak{p}}$, will map isomorphically onto

$$(\mathbf{Z} \times \mathbf{Z}_q^{[L_{\varphi(\mathfrak{p})}:\mathbf{Q}_q]})/p \cdot (\mathbf{Z} \times \mathbf{Z}_q^{[L_{\varphi(\mathfrak{p})}:\mathbf{Q}_q]}) = \begin{cases} \mathbf{Z}/p\mathbf{Z} \times (\mathbf{Z}/q\mathbf{Z})^{[L_{\varphi(\mathfrak{p})}:\mathbf{Q}_q]} & \text{if } p = q \\ \mathbf{Z}/p\mathbf{Z} & \text{if } p \neq q \end{cases}. \tag{2.4}$$

Thus, from comparing the right hand sides of equations (2.3) and (2.4), a counting argument shows that we must have $p = q$ and $[K_{\mathfrak{p}} : \mathbf{Q}_p] = [L_{\varphi(\mathfrak{p})} : \mathbf{Q}_p]$. For all but finitely many primes, the extensions $K_{\mathfrak{p}}/\mathbf{Q}_p$ and $L_{\varphi(\mathfrak{p})}/\mathbf{Q}_p$ are unramified. Hence, we find that the bijection φ matches the decomposition types of all but finitely many primes. This implies that K and L are arithmetically equivalent. □

Chapter 3

Adelic points on algebraic groups

In this chapter, we prove the following theorem.

Theorem 3.1. Let K and L be two number fields, and let G denote a linear algebraic group over $\mathbf{Q}$ which is fertile for K and L. There is a topological group isomorphism of finite-adelic point groups $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ if and only if there is a topological ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$.

Fertility for linear algebraic groups over number fields is defined in Definition 3.4, and discussed further below.

Remark 3.2. Suppose that K and L are Galois over $\mathbf{Q}$. By Proposition 2.3(iii), Theorem 3.1 then says that there is a topological group isomorphism of finite-adelic point groups $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ if and only if $K \cong L$.

3.1 Algebraic groups and fertility

First, we collect some notations and terminology from the theory of algebraic groups, and we elaborate on the notion of a group being fertile for a pair of number fields.

Algebraic groups

Notation/Definitions 3.3. Let G denote a linear (viz., affine) algebraic group over $\mathbf{Q}$. We denote the multiplicative group by $\mathbf{G}_m$ and the additive group by $\mathbf{G}_a$. An *n-dimensional torus* T is a linear algebraic group which is isomorphic, over $\overline{\mathbf{Q}}$, to $\mathbf{G}_m^r$, for some integer r, called the *rank* of T. When T is an algebraic subgroup of G and moreover a maximal torus inside G, then the *rank* of G is r as well. Suppose that a maximal torus *splits* over a field $F/\mathbf{Q}$, meaning that there exists an isomorphism $T \cong \mathbf{G}_m^r$ defined over F. All maximal F-split tori of G are $G(F)$-conjugate (cf. [17, Theorem 4.2.1] and [109, Theorem 15.2.6]) and have the same dimension, called the (F-)*rank* of G. A subgroup U of G is *unipotent* if $U(\overline{\mathbf{Q}})$ consists of unipotent elements. Every unipotent subgroup of $G/\mathbf{Q}$ splits over $\mathbf{Q}$, meaning that it has a

This chapter is based on parts of the article [32], joint work with Gunther Cornelissen.

composition series over $\mathbf{Q}$ in which every successive quotient is isomorphic to $\mathbf{G}_a$. Alternatively, it is isomorphic over $\mathbf{Q}$ to a subgroup of a group of strictly upper triangular matrices. Any connected group G that is not unipotent contains a nontrivial torus. A *Borel subgroup* B of G is a maximal connected solvable subgroup of G. If all successive quotients in the composition series of B over F are isomorphic to $\mathbf{G}_a$ or $\mathbf{G}_m$, then B is conjugate, over F, to a subgroup of an upper triangular matrix group, by the Lie-Kolchin theorem. Moreover, over F, for some split maximal torus T and maximal unipotent group U, we can write $B \cong T \ltimes U$ as a semi-direct product induced by the adjoint representation $\rho\colon T \to \mathrm{Aut}(U)$ (i.e., by the conjugation action of T on U). Furthermore, given U, B is the normaliser of U in G, and $T \cong B/U$.

Definition 3.4. We call a linear algebraic group G over $\mathbf{Q}$ *fertile* for a number field K if there exists a Borel K-subgroup B of G which is split over K, i.e., $B \cong_K T \ltimes U$ for $T \neq \{1\}$ a K-split maximal torus and $U \neq \{0\}$ a maximal unipotent group, such that T acts nontrivially (by conjugation) on the abelianisation U^{ab} of U.

The following equivalent definition was pointed out to us by Wilberd van der Kallen:

Proposition 3.5. *G is fertile over K if and only if it contains a K-split maximal torus, and the connected component of the identity G^0 is not a direct product of a torus and a unipotent group.*

Proof. Indeed, suppose G is fertile in the sense of Definition 3.4. Since Borel groups are connected, the identity component G^0 contains a Borel group, which is not a direct product of a torus and a unipotent group because all Borel subgroups are conjugate over $\overline{K}$, hence neither is G^0.

Conversely, suppose G^0 is not a direct product $T \times U$. There is a short exact sequence of algebraic groups

$$1 \to R_u(G) \to G^0 \to S \to 1$$

where $R_u(G)$ is the unipotent radical of G and S is a reductive group. Moreover, we may assume that S is a torus. Otherwise, S would contain a Borel group $\overline{B}$ whose abelian unipotent group $\overline{U}^{\mathrm{ab}}$ contains a nontrivial eigenspace for the maximal torus $\overline{T} \subset \overline{B}$. This eigenspace lifts to a nontrivial eigenspace inside U^{ab}, so G is fertile in the sense of Definition 3.4.

Thus, we may assume G^0 is itself a Borel subgroup (since it is solvable and connected, and maximal for these properties) with torus $S = T$ and unipotent subgroup $U = R_u(G)$, and consider the short exact sequence

$$1 \to U \to B \to T \to 1. \tag{3.1}$$

Now we claim that T acts nontrivially on U if and only if T acts nontrivially on U^{ab}, which will finish the proof. Necessity is clear. For the converse, let $\{U_i\}_i$ be the lower central series for U, i.e. $U_0 = U$ and $U_i = [U, U_{i-1}]$ for all $i \geq 1$. Let U_n be the last nontrivial subgroup occurring in this series. Then in particular $U_n \subseteq Z(U)$. Since T acts by conjugation, it preserves the lower central series. Furthermore, suppose that T acts trivially on $U^{\mathrm{ab}} = U/U_1$. We will show that T then acts trivially on U.

In fact, if T acts trivially on some U/U_{j-1} with $j \geq 2$, then T also acts trivially on U/U_j. Indeed, T acts trivially on the subgroup $U_{j-2}/U_{j-1} \leq U/U_{j-1}$. The commutator map $[\cdot,\cdot]\colon U \times U_{j-2} \to U_{j-1}$ factors through to give a surjective map

$$[\cdot,\cdot]\colon U/U_{j-1} \times U_{j-2}/U_{j-1} \to U_{j-1}/U_j.$$

Hence, T acts trivially on U_{j-1}/U_j. Now consider the short exact sequence

$$1 \to U_{j-1}/U_j \to U/U_j \to U/U_{j-1} \to 1.$$

Since T acts trivially on both U_{j-1}/U_j and U/U_{j-1}, we find that T acts trivially on U/U_j, as required.

Since $U_k = \{0\}$ for $k > n$, we have $U/U_k = U$ for such k. But by the above, T acts trivially on $U/U_k = U$, since it acts trivially on U/U_1, by assumption. □

Examples 3.6.

(i) Tori and unipotent groups are *not* fertile for any K, and neither are direct product of such groups.

(ii) The general linear group $\mathrm{GL}(n)$ for $n \geq 2$ is fertile for any K. Here, T is the group of diagonal matrices, split over $\mathbf{Q}$, which acts nontrivially on the group of strictly upper triangular matrices. Similarly, the Borel group of (non-strictly) upper triangular matrices is fertile.

(iii) Let $G = \mathrm{Res}^F_{\mathbf{Q}}(\mathbf{G}_m \ltimes \mathbf{G}_a)$ denote the "$ax+b$"-group of a number field F, as an algebraic group over $\mathbf{Q}$. This group is fertile for any number field K that contains F.

Adelic point groups

Definition 3.7. Let G denote a linear algebraic group over $\mathbf{Q}$ and let K a number field with adele ring $\mathbf{A}_K$. As described in [81, Section 3] (compare [67]) we may use any of the following equivalent definitions for the *group of adelic points of G over K* (also called the *adelic point group*), denoted $G(\mathbf{A}_K)$:

1. Since $\mathbf{A}_K$ is a $\mathbf{Q}$-algebra, $G(\mathbf{A}_K)$ is its scheme theoretic set of points.

2. Let S be a suitable finite set of places of $\mathbf{Q}$, including the archimedean place, and let $\mathscr{G}$ be a smooth separated group scheme of finite type over the S-integers $\mathbf{Z}_S$, whose generic fibre is G. Then
$$G(\mathbf{A}_K) = \varinjlim_{S' \supset S} \prod_{\mathfrak{p} \in S'} G(K_\mathfrak{p}) \times \prod_{\mathfrak{p} \notin S'} \mathscr{G}(\mathscr{O}_\mathfrak{p})$$
where S' runs over subsets of $M_{K,f}$ that contain divisors of primes in S.

3. Choose a $\mathbf{Q}$-isomorphism $\varphi\colon G \hookrightarrow \mathbb{A}^N$ of G onto a closed subvariety of a suitable affine space $\mathbb{A}^N$. For every $\mathfrak{p} \in M_{K,f}$, we define $G(\mathscr{O}_\mathfrak{p})$ to be the set of points $x \in G(K_\mathfrak{p})$ for which $\varphi(x) \in \mathscr{O}_\mathfrak{p}^N$. Then $G(\mathbf{A}_K)$ is the restricted product
$$G(\mathbf{A}_K) = \prod_{\mathfrak{p} \in M_{K,f}}{}' (G(K_\mathfrak{p}), G(\mathscr{O}_\mathfrak{p}))) \times \prod_{\mathfrak{p} \in M_{K,\infty}} G(K_\mathfrak{p}).$$

The second and third definitions immediately provide $G(\mathbf{A}_K)$ with a topology induced from the $\mathfrak{p}$-adic topologies. Also, the algebraic group law on G induces a topological group structure on $G(\mathbf{A}_K)$. The definitions are, up to isomorphism, independent of the choices of S, $\mathscr{G}$ and φ.

We define the *finite-adelic point group* $G(\mathbf{A}_{K,f})$ completely analogously.

Remark 3.8. In Chapter 2, we considered the group of adelic points on $\mathbf{G}_a$ and $\mathbf{G}_m$.

3.2 Divisibility and unipotency

In this section, we show how to characterise maximal unipotent point groups inside finite-adelic point groups in a purely group theoretic fashion, using divisibility. This is used later to deduce an isomorphism of unipotent point groups from an isomorphism of ambient point groups.

Definition 3.9. If $\mathbf{H}$ is a subgroup of a group $\mathbf{G}$, an element $h \in \mathbf{H}$ is called *divisible in* $\mathbf{G}$ if for every integer $n \in \mathbf{Z}_{>0}$, there exists an element $g \in \mathbf{G}$ such that $h = g^n$. The subgroup $\mathbf{H} \leq \mathbf{G}$ is called divisible (in $\mathbf{G}$) if all of its elements are divisible in $\mathbf{G}$.

Proposition 3.10. Suppose that G is fertile for K. Let U be a maximal unipotent algebraic subgroup of G. Then any maximal divisible subgroup of $G(\mathbf{A}_{K,f})$ is conjugate to $U(\mathbf{A}_{K,f})$ in $G(\mathbf{A}_{K,f})$.

Proof. We fix an embedding $G \hookrightarrow GL_N$ throughout, and consider elements of G as matrices. We start the proof with a sequence of lemmas about the local case. Fix a place $\mathfrak{p} \in M_{K,f}$.

Lemma 3.11. All divisible elements of $G(K_\mathfrak{p})$ are unipotent.

Proof. Let v denote a divisible element of $G(K_\mathfrak{p})$, and, for each $n \in \mathbf{Z}_{>0}$, let $w_n \in G(K_\mathfrak{p})$ satisfy $w_n^n = v$ for $n \in \mathbf{Z}_{>0}$. The splitting field L_n of the characteristic polynomial of w_n (seen as $N \times N$-matrix) has *bounded* degree $[L_n : K] \leq N!$. Since by Krasner's Lemma (e.g. [80, 8.1.6]), there are only finitely many extensions of $K_\mathfrak{p}$ of bounded degree, the compositum L of all L_n is a discretely valued field, in which all the eigenvalues λ_i of v are n-th powers (namely, of eigenvalues of w_n) for all integers n. Since L is non-archimedean,

$$\bigcap_{n \geq 1} L^n = \{1\},$$

by discreteness of the absolute value and the structure of $\mathscr{O}_H^*$ as described in the proof of Proposition 2.8. We conclude that all eigenvalues of v are 1 and v is unipotent. □

Remark 3.12. The lemma (and hence the proposition) is not true for archimedean places. To give an example at a real place, the rotation group $\mathrm{SO}(2, \mathbf{R}) \subseteq \mathrm{SL}(2, \mathbf{R})$ is divisible but contains non-unipotent elements.

Lemma 3.13. The group $U(K_\mathfrak{p})$ is divisible in $G(K_\mathfrak{p})$.

Proof. Since all $K_\mathfrak{p}$ are fields of characteristic zero, the exponential map

$$\exp \colon \mathfrak{N} \to U(K_\mathfrak{p})$$

from the nilpotent Lie algebra $\mathfrak{N}$ of $U(K_\mathfrak{p})$ to $U(K_\mathfrak{p})$ is an isomorphism (cf. [75, Theorem 6.5]). For an integer $n \in \mathbf{Z}_{>0}$ and an element $\mathfrak{n} \in \mathfrak{N}$,

$$\exp(n\mathfrak{n}) = \exp(\mathfrak{n})^n$$

by the Baker-Campbell-Hausdorff formula, since multiples of the same $\mathfrak{n}$ commute, so that (multiplicative) divisibility in the unipotent algebraic group corresponds to (additive) divisibility in the nilpotent Lie algebra $\mathfrak{N}$. Since the latter is a $K_\mathfrak{p}$-vector space and any integer n is invertible in $K_\mathfrak{p}$, we find the result. □

We will also need the following global version:

Lemma 3.14. The group $U(\mathbf{A}_{K,f})$ is divisible in $G(\mathbf{A}_{K,f})$.

Proof. Let $v = (v_{\mathfrak{p}})_{\mathfrak{p}} \in U(\mathbf{A}_{K,f})$, $n \in \mathbf{Z}_{\geq 0}$, and for every $\mathfrak{p} \in M_{K,f}$, let $w_{\mathfrak{p}} \in U(K_{\mathfrak{p}})$ be such that $w_{\mathfrak{p}}^n = v_{\mathfrak{p}}$ (which exists by the previous lemma). We claim that $w_{\mathfrak{p}} \in U(\mathscr{O}_{\mathfrak{p}})$ for all but finitely many $\mathfrak{p}$, which shows that $w = (w_{\mathfrak{p}})_{\mathfrak{p}} \in U(\mathbf{A}_{K,f})$ and proves the lemma. Indeed, it suffices to prove that $w_{\mathfrak{p}} \in GL_N(\mathscr{O}_{\mathfrak{p}})$ for all but finitely many $\mathfrak{p}$. This follows from the Taylor series

$$w_{\mathfrak{p}} = \sqrt[n]{1 + (v_{\mathfrak{p}} - 1)} = \sum_{k=0}^{\infty} \binom{1/n}{k} (v_{\mathfrak{p}} - 1)^k,$$

which is a finite sum since $v_{\mathfrak{p}} - 1$ is nilpotent, by noting that for fixed n, the binomial coefficients introduce denominators at only finitely many places. □

Lemma 3.15. Any maximal divisible subgroup of $G(K_{\mathfrak{p}})$ is conjugate to $U(K_{\mathfrak{p}})$ in $G(K_{\mathfrak{p}})$.

Proof. Let $\mathbf{D}$ denote a maximal divisible subgroup of $G(K_{\mathfrak{p}})$. By Lemma 3.11, it consists of unipotent elements. Since unipotency is defined by polynomial equations in the affine space of $N \times N$ matrices, the Zariski closure of $\mathbf{D}$ in $G_{K_{\mathfrak{p}}}$ is a unipotent algebraic subgroup U' of $G_{K_{\mathfrak{p}}}$. Moreover, Lemma 3.13 implies that $U(K_{\mathfrak{p}})$ consists of divisible elements, so by maximality of $\mathbf{D}$, we find that U' is a *maximal* unipotent algebraic subgroup of $G_{K_{\mathfrak{p}}}$. Theorem 8.2 of Borel-Tits [17] implies that there exists an element $\gamma_{\mathfrak{p}} \in G(K_{\mathfrak{p}})$ such that $\gamma_{\mathfrak{p}} U' \gamma_{\mathfrak{p}}^{-1} = U$, for U any chosen maximal unipotent subgroup of G. Hence, $\gamma_{\mathfrak{p}} \mathbf{D} \gamma_{\mathfrak{p}}^{-1} \subseteq U(K_{\mathfrak{p}})$. Since $\gamma_{\mathfrak{p}}^{-1} U(K_{\mathfrak{p}}) \gamma_{\mathfrak{p}}$ is maximal divisible, the result follows. □

We could not find a proof for the following result in the literature, so we include one inspired by an answer by Bhargav Bhatt on `mathoverflow.net/a/2231`:

Lemma 3.16. Let $B \subset G$ denote a K-split Borel subgroup of G and let $\mathscr{B} \subset \mathscr{G}$ denote any corresponding inclusion of smooth finite-type separated group schemes over the ring of S-integers $\mathbf{Z}_S$ for a suitable finite set of primes S, so that the generic fibre of $\mathscr{B}$ is B and that of $\mathscr{G}$ is G. Then for $\mathfrak{p} \in M_{K,f}$ not dividing any prime in S, we have

$$G(K_{\mathfrak{p}}) = B(K_{\mathfrak{p}}) \mathscr{G}(\mathscr{O}_{\mathfrak{p}}).$$

Proof. It suffices to show that

$$G(K_{\mathfrak{p}})/B(K_{\mathfrak{p}}) = \mathscr{G}(\mathscr{O}_{\mathfrak{p}})/\mathscr{B}(\mathscr{O}_{\mathfrak{p}}). \tag{3.2}$$

We will prove this by arguing that both sides of (3.2) equal $(\mathscr{G}/\mathscr{B})(\mathscr{O}_{\mathfrak{p}})$.

First consider the long exact sequence in fppf-cohomology associated to the exact sequence

$$1 \to \mathscr{B} \to \mathscr{G} \to \mathscr{G}/\mathscr{B} \to 1$$

of smooth group schemes (cf. [90, p. 151-152 and Theorem 6.5.10]), over $M = K_\mathfrak{p}$ or $M = \mathscr{O}_\mathfrak{p}$:

$$1 \to \mathscr{B}(M) \to \mathscr{G}(M) \to (\mathscr{G}/\mathscr{B})(M) \to H^1(M, \mathscr{B}) \to \dots$$

To rewrite the left hand side of (3.2), we take $M = K_\mathfrak{p}$, so we are dealing with $\mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p})$-cohomology. Recall from equation (3.1) that we have a short exact sequence

$$1 \to U \to B \to T \to 1,$$

for U a unipotent group and T a maximal K-split torus. This induces a long exact sequence

$$1 \to U(K_\mathfrak{p}) \to B(K_\mathfrak{p}) \to T(K_\mathfrak{p}) \to H^1(K_\mathfrak{p}, U) \to H^1(K_\mathfrak{p}, B) \to H^1(K_\mathfrak{p}, T) \\ \to \dots.$$

Since T is split over K, hence split (and a fortiori quasisplit) over $K_\mathfrak{p}$, and $K_\mathfrak{p}$ is a perfect field, applying [89, Lemma 2.4] yields $H^1(K_\mathfrak{p}, T) = 1$. Moreover, since $K_\mathfrak{p}$ has characteristic zero, $H^1(K_\mathfrak{p}, U) = 1$ by [89, Lemma 2.7]. Thus, we find that

$$H^1(K_\mathfrak{p}, B) = 1.$$

Hence,

$$G(K_\mathfrak{p})/B(K_\mathfrak{p}) = (G/B)(K_\mathfrak{p}).$$

Since G/B is projective, it follows from the valuative criterion of properness that

$$(G/B)(K_\mathfrak{p}) = (\mathscr{G}/\mathscr{B})(\mathscr{O}_\mathfrak{p}).$$

For the right hand side of (3.2), we set $M = \mathscr{O}_\mathfrak{p}$ and argue as in Step 3 of [90, Theorem 6.5.12]: $H^1(\mathscr{O}_\mathfrak{p}, \mathscr{B})$ classifies $\mathscr{B}$-torsors over $\mathscr{O}_\mathfrak{p}$; let $\mathscr{T} \to \operatorname{Spec} \mathscr{O}_\mathfrak{p}$ denote such a torsor. By Lang's theorem, its special fibre $\mathscr{T}_\mathfrak{p} \to \operatorname{Spec} \mathbf{F}_\mathfrak{p}$ over the finite residue field $\mathbf{F}_\mathfrak{p}$ has a rational point. Since $\mathscr{B}$ smooth, so is $\mathscr{T}$, so we can lift the rational point by Hensel's Lemma. Hence, $\mathscr{T}$ is also trivial. We conclude that $H^1(\mathscr{O}_\mathfrak{p}, \mathscr{B}) = 1$, so

$$(\mathscr{G}/\mathscr{B})(\mathscr{O}_\mathfrak{p}) = \mathscr{G}(\mathscr{O}_\mathfrak{p})/\mathscr{B}(\mathscr{O}_\mathfrak{p})$$

as claimed. □

To finish the proof of the proposition, let $\mathbf{D}$ denote a maximal divisible subgroup of $G(\mathbf{A}_{K,f})$ and let $\mathbf{D}_\mathfrak{p} = \mathbf{D} \cap G(K_\mathfrak{p})$ be its local component for $\mathfrak{p} \in M_{K,f}$. Let $\gamma_\mathfrak{p} \in G(K_\mathfrak{p})$ be as in Lemma 3.16, i.e., such that $\gamma_\mathfrak{p} \mathbf{D}_\mathfrak{p} \gamma_p^{-1} = U(K_\mathfrak{p})$. Let $B = N_G(U)$ be a Borel subgroup containing U; we may choose these such that B is a *split* Borel K-subgroup of G. Lemma 3.16 implies that for all but finitely many $\mathfrak{p}$, we may replace $\gamma_\mathfrak{p}$ by an element in $\mathscr{G}(\mathscr{O}_\mathfrak{p})$, which we again denote by $\gamma_\mathfrak{p}$ for ease of notation. This way, we find $\gamma = \prod_{\mathfrak{p}\in M_{K,f}} \gamma_\mathfrak{p} \in G(\mathbf{A}_{K,f})$ with

$$\mathbf{D} \subseteq \gamma^{-1} \prod U(K_\mathfrak{p})\gamma \cap G(\mathbf{A}_{K,f}) = \gamma^{-1}U(\mathbf{A}_{K,f})\gamma \subseteq \mathbf{D},$$

where the last inclusion holds by Lemma 3.14. □

3.3 Proof of Theorem 3.1

We now turn to the proof of Theorem 3.1.

Proof. Let $\mathbf{G} := G(\mathbf{A}_{K,f})$ as a topological group. We will apply a purely group theoretic construction to $\mathbf{G}$, to end up with the adele ring $\mathbf{A}_K$; this shows that the isomorphism type of the adele ring is determined by the topological group $\mathbf{G}$. Let $\mathbf{D}$ denote a maximal divisible subgroup of $\mathbf{G}$. Consider the normaliser $\mathbf{N} := N_\mathbf{G}\mathbf{D}$ of $\mathbf{D}$ in $\mathbf{G}$. Let $\mathbf{V} := [\mathbf{N}, \mathbf{D}]/[\mathbf{D}, \mathbf{D}] \leq \mathbf{D}^{\mathrm{ab}}$, and let $\mathbf{T} := \mathbf{N}/\mathbf{D}$. Note that $\mathbf{T}$ acts naturally on $\mathbf{V}$ by conjugation. Since $\mathbf{V}$ is locally compact Hausdorff, we can give $\mathrm{End}\mathbf{V}$, the endomorphisms of the abelian group $\mathbf{V}$, the compact-open topology.

Proposition 3.17. There exists an integer $\ell \geq 1$ such that there is a topological ring isomorphism

$$Z(\mathrm{End}_\mathbf{T}\mathbf{V}) \cong \mathbf{A}_{K,f}^\ell,$$

where the left hand side is the centre of the ring of continuous endomorphisms of the $\mathbf{T}$-module $\mathbf{V}$.

Proof of Proposition 3.17. First, we relate the subgroups of $\mathbf{G}$ to points groups of algebraic subgroups of G. From Proposition 3.10, we may assume that $\mathbf{D} = U(\mathbf{A}_{K,f})$ for a fixed maximal unipotent algebraic subgroup of G. The normaliser of U in G as an algebraic group is a Borel group B inside the fertile group G (Theorem of Chevalley, e.g. [16], 11.16); again, we choose U such that B is split over K. Since taking points and taking normalisers commute ([74], Proposition 6.3), we obtain that

$$\mathbf{N} = N_\mathbf{G}\mathbf{D} = N_{G(\mathbf{A}_{K,f})}U(\mathbf{A}_{K,f}) = (N_G U)(\mathbf{A}_{K,f}) = B(\mathbf{A}_{K,f}).$$

and $\mathbf{T} \cong T(A_{K,f})$ for T any maximal torus in B, which is K-split by assumption.

Next, we analyse the action of $\mathbf{T}$ on $\mathbf{V}$, knowing the action of T on U. The hypothesis that T splits over K implies that $T \cong \mathbf{G}_m^r$ over K for some r. The adjoint action of T by conjugation on U maps commutators to commutators, so it induces an action on the abelianisation U^{ab}, and we can consider the linear adjoint action $\rho\colon T \to \mathrm{Aut}(U^{\mathrm{ab}})$ over K. Note that $U^{\mathrm{ab}} \cong \mathbf{G}_a^k$ for some integer k, so we have an action over K

$$\rho\colon T(\cong \mathbf{G}_m^r) \to \mathrm{Aut}(\mathbf{G}_a^k) = \mathrm{GL}(k), \tag{3.3}$$

which is diagonalisable over K as a direct sum $\rho = \oplus\chi_i$ of k characters $\chi_i \in \mathrm{Hom}_K(T, \mathbf{G}_m)$ of algebraic groups. In coordinates $t = (t_1, \dots, t_r) \in \mathbf{G}_m^r = T$, any such character is of the form

$$\chi(t) = \chi(t_1, \dots, t_r) = t_1^{n_1} \cdot \ldots \cdot t_r^{n_r} \tag{3.4}$$

for some $n_1, \dots, n_r \in \mathbf{Z}$. Since the action of $\mathbf{T}$ on $\mathbf{V}$ is given by specialisation from the action of T on a subspace of U^{ab}, we find an isomorphism of $\mathbf{T}$-modules

$$\mathbf{V} \cong \bigoplus_{i=1}^{\ell} \mathbf{A}_{K,f,\chi_i}^{\mu_i},$$

where χ_i $(i = 1, \dots \ell)$ are the distinct nontrivial characters that occur in $\mathbf{V}$, μ_i is the multiplicity of χ_i in $\mathbf{V}$, and $\mathbf{A}_{K,f,\chi_i}$ is the $\mathbf{T}$-module $\mathbf{A}_{K,f}$ where $\mathbf{T}$ acts via χ_i. Hence,

$$\mathrm{End}_{\mathbf{T}}\mathbf{V} = \prod_{i=1}^{\ell}\prod_{j=1}^{\ell} \mathrm{Mat}_{\mu_j \times \mu_i}\left(\mathrm{Hom}_{\mathbf{T}}(\mathbf{A}_{K,f,\chi_i}, \mathbf{A}_{K,f,\chi_j})\right). \tag{3.5}$$

The assumption of fertility means precisely that $\ell \geq 1$.

Lemma 3.18. If χ_i and χ_j are nontrivial characters occurring in the above decomposition, then there is a topological ring isomorphism

$$\mathrm{Hom}_{\mathbf{T}}(\mathbf{A}_{K,f,\chi_i}, \mathbf{A}_{K,f,\chi_j}) \cong \begin{cases} \mathbf{A}_{K,f} & \text{if } \chi_i = \chi_j \\ \{0\} & \text{otherwise .} \end{cases}$$

Proof. A homomorphism between additive groups $f\colon (\mathbf{A}_{K,f,\chi_i}, +) \to (\mathbf{A}_{K,f,\chi_j}, +)$ is $\mathbf{T}$-equivariant precisely if $f(\chi_i(t)(u)) = \chi_j(t)f(u)$ for all $t \in \mathbf{T}$ and $u \in \mathbf{A}_{K,f}$. The χ are specialisations of algebraic characters as in (3.4), and some powers are nonzero by the assumption of fertility. If $\chi_i \neq \chi_j$, this means that

$$f(t^n u) = t^m f(u), \forall t \in \mathbf{A}_{K,f}^*,\ \forall u \in \mathbf{A}_{K,f} \tag{3.6}$$

for some $n, m > 0$, $n \neq m$, which is impossible unless $f = 0$: indeed, choose $t \in \mathbf{Z}_{>0}$; then the equation says that $t^n f(u) = t^m f(u)$ for any u, so $m = n$. So we must have $\chi_i = \chi_j$, and we find that

$$f(t^n u) = t^n f(u), \forall t \in \mathbf{A}_{K,f}^*,\ \forall u \in \mathbf{A}_{K,f} \tag{3.7}$$

for some $n > 0$.

We now reinterpret a formula of Siegel [106, p. 134] as saying the following: *Let R denote a ring and n a positive integer such that $n!$ is invertible in R. Then any element of R belongs to the $\mathbf{Z}$-linear span of the n-th powers in R. In particular, we have the following explicit formula for any $z \in R$:*

$$z = \sum_{k=0}^{n-1} (-1)^{n-k-1} \binom{n-1}{k} \left\{ \left(\frac{z}{n!} + k \right)^n - k^n \right\}.$$

Applied to $R = \mathbf{A}_{K,f}$, in which $n!$ is invertible, Siegel's formula expresses any element of $\mathbf{A}_{K,f}$ as $\mathbf{Z}$-linear combination of n-th powers in $\mathbf{A}_{K,f}$. We conclude from (3.7) and additivity of f that

$$f(tu) = tf(u), \forall t \in \mathbf{A}^*_{K,f},\ \forall u \in \mathbf{A}_{K,f}. \tag{3.8}$$

Hence, $f(t) = tf(1)$ is completely determined by specifying a value for $f(1) \in \mathbf{A}_{K,f}$, and

$$\mathrm{End}_{\mathbf{T}}(\mathbf{A}_{K,f,\chi}) \to \mathbf{A}_{K,f} \colon f \mapsto f(1)$$

is the required ring isomorphism. It is continuous, since evaluation maps (such as this one) are continuous in the compact-open topology on $\mathrm{End}_{\mathbf{T}}(\mathbf{A}_{K,f,\chi})$. The inverse map is $\alpha \mapsto (x \mapsto \alpha x)$, which is also continuous in the finite-adelic topology on $\mathbf{A}_{K,f}$. Hence, we find an isomorphism of topological groups, as required. □

To finish the proof of Proposition 3.17, combine Lemma 3.18 with equation (3.5) and construct the centre:

$$Z\left(\mathrm{End}_{\mathbf{T}}\mathbf{V}\right) = Z\left(\prod_{i=0}^{\ell} M_{\mu_i}\left(\mathbf{A}_{K,f}\right)\right) = \mathbf{A}^{\ell}_{K,f}.$$

□

If R is a ring, let $\mathscr{M}(R)$ denote its set of principal maximal ideals. Observe that $\mathscr{M}(R^\ell) = \mathscr{M}(R) \times \mathbf{Z}/\ell\mathbf{Z}$, since a maximal ideal in R^ℓ is of the form $R^{\ell_1} \times \mathfrak{m} \times R^{\ell_2}$ for some maximal ideal $\mathfrak{m}$ of R and a decomposition $\ell = \ell_1 + \ell_2 + 1$. Now we recall the description of the principal maximal ideals in an adele ring $\mathbf{A}_{K,f}$ as given by Iwasawa and Lochter ([65, Satz 8.6] and [48, p. 340–342], cf. [57, VI.2.4]):

$$\mathscr{M}(\mathbf{A}_{K,f}) = \{\mathfrak{m}_{\mathfrak{p}} = \ker\left(\mathbf{A}_{K,f} \to K_{\mathfrak{p}}\right)\}.$$

Note that $\mathbf{A}_{K,f}/\mathfrak{m}_{\mathfrak{p}} \cong K_{\mathfrak{p}}$. Hence the multiset

$$\{\mathbf{A}^{\ell}_{K,f}/\mathfrak{m} \colon \mathfrak{m} \in \mathscr{M}(\mathbf{A}^{\ell}_{K,f})\}$$

contains a copy of the local field $K_{\mathfrak{p}}$ exactly $\ell r_{\mathfrak{p}}$ times, where $r_{\mathfrak{p}}$ is the number of local fields of K isomorphic to $K_{\mathfrak{p}}$. Thus, we have constructed the multiset of local fields

$$\{K_{\mathfrak{p}} \colon \mathfrak{p} \in M_{K,f}\}$$

of K, up to isomorphism of local fields.

Now if K and L are two number fields with $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ as topological groups, then these multisets are in bijection, i.e., there exists a bijection of places $\varphi \colon M_{K,f} \to M_{L,f}$ such that $K_{\mathfrak{p}} \cong L_{\varphi(\mathfrak{p})}$ for all $\mathfrak{p} \in M_{K,f}$. Hence K and L are locally isomorphic (in the sense of Section 2.1), and we find ring isomorphisms $\mathbf{A}_{K,f} \cong \mathbf{A}_{L,f}$ and $\mathbf{A}_K \cong \mathbf{A}_L$, by Proposition 2.3.

For the reverse implication $\mathbf{A}_K \cong \mathbf{A}_L \Rightarrow G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$, we use that a topological ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$ implies the existence of topological isomorphisms $\Phi_{\mathfrak{p}} \colon K_{\mathfrak{p}} \cong L_{\varphi(\mathfrak{p})}$ of local fields for some bijection of places $\varphi \colon M_{K,f} \to M_{L,f}$ (again by Proposition 2.3). The fact that all $\Phi_{\mathfrak{p}}$ are homeomorphisms implies in particular that $\Phi_{\mathfrak{p}}(\mathscr{O}_{K,\mathfrak{p}}) = \mathscr{O}_{L,\varphi(\mathfrak{p})}$ for all $\mathfrak{p}$. Now $G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f})$ is immediate from the definition of finite-adelic point groups (with topology) in 3.7(2) or, equivalently, 3.7(3). This finishes the proof of Theorem 3.1. □

3.4 Discussion

One may wonder in what exact generality Theorem 3.1 holds.

1. The theorem does not hold for all linear algebraic groups; e.g., it does not hold for $G = \mathbf{G}_a^r \times \mathbf{G}_m^s$. Is it possible to characterise *precisely* the linear algebraic groups for which $G(\mathbf{A}_K) \cong G(\mathbf{A}_L)$ implies $\mathbf{A}_K \cong \mathbf{A}_L$?

2. What happens if G is not a linear algebraic group, but any algebraic group? It follows from Chevalley's structure theorem that such G have a unique maximal linear subgroup H; can we deduce $H(\mathbf{A}_K) \cong H(\mathbf{A}_L)$ from $G(\mathbf{A}_K) \cong G(\mathbf{A}_L)$?

3. What happens if there is no linear part, i.e., G is an abelian variety, e.g., an elliptic curve? For every number field, is there a sufficiently interesting elliptic curve $E/\mathbf{Q}$ such that $E(\mathbf{A}_K)$ determines all localisations of K?

4. Is the theorem true without imposing that a maximal torus T of G splits over K and L?

5. What happens over global fields of positive characteristic?

CHAPTER 4

Hecke algebras over global and local fields

Throughout this chapter, $G/\mathbf{Q}$ will denote a linear algebraic group. Moreover, K will be either a number field, or a non-archimedean local field of characteristic zero.

4.1 Hecke algebras

Finite-adelic Hecke algebras

Let $K/\mathbf{Q}$ be a number field. Recall that we defined the adelic (resp. finite-adelic) point groups $G(\mathbf{A}_K)$ (resp. $G(\mathbf{A}_{K,f})$) in Definition 3.7.

Definition 4.1. Because $\mathbf{A}_{K,f}$ is locally compact, $\mathbf{G}_K := G(\mathbf{A}_{K,f})$ is a locally compact topological group for the topology described in Definition 3.7. Hence, it is equipped with a (left) invariant Haar measure $\mu_{\mathbf{G}_K}$. The *finite-adelic (real) Hecke algebra* $\mathscr{H}_G(K) = C_c^\infty(\mathbf{G}_K, \mathbf{R})$ of G over K is the algebra of all real-valued locally constant compactly supported functions $\Phi : \mathbf{G}_K \to \mathbf{R}$ with the convolution product

$$\Phi_1 * \Phi_2 : g \mapsto \int_{\mathbf{G}_K} \Phi_1(gh^{-1})\Phi_2(h) d\mu_{\mathbf{G}_K}(h).$$

(Replacing $\mathbf{R}$ by $\mathbf{C}$ yields the finite-adelic complex Hecke algebra; the results in this section also hold in the complex setting.)

Every element of $\mathscr{H}_G(K)$ is a finite linear combination of characteristic functions on double cosets $\mathbf{K}h\mathbf{K}$, for $h \in \mathbf{G}_K$ and $\mathbf{K}$ a compact open subgroup of $\mathbf{G}_K$. Alternatively, we may write

$$\mathscr{H}_G(K) = \varinjlim_{\mathbf{K}} \mathscr{H}(\mathbf{G}_K /\!\!/ \mathbf{K}),$$

where $\mathscr{H}(\mathbf{G}_K /\!\!/ \mathbf{K})$ is the Hecke algebra of $\mathbf{K}$-biinvariant smooth functions on $\mathbf{G}_K$ (for example, if $\mathbf{K}$ is maximally compact, this is the spherical Hecke algebra).

This chapter is based on parts of the articles [54] and [32], the latter being joint work with Gunther Cornelissen.

Local Hecke algebras

Now, let K a non-archimedean local field of characteristic zero, whose ring of integers is denoted by $\mathscr{O}_K$.

Definition 4.2. Since K is locally compact, $G(K)$ is a locally compact topological group, whose topology is induced by the topology of K. Its group structure is induced by that of G. Moreover, it is equipped with a (left) invariant Haar measure $\mu_{G(K)}$ which satisfies $\mu_{G(K)}(G(\mathscr{O}_K)) = 1$.

Definition 4.3. The *(local) Hecke algebra* $\mathscr{H}_G(K) = C_c^\infty(G(K), \mathbf{C})$ of G over K is the algebra of locally constant compactly supported complex-valued functions on $G(K)$, with the convolution product

$$\Phi_1 * \Phi_2 : g \mapsto \int_{G(K)} \Phi_1(gh^{-1})\Phi_2(h) d\mu_{G(K)}(h) \tag{4.1}$$

for $\Phi_1, \Phi_2 \in \mathscr{H}_G(K)$.

4.2 L^1-isomorphisms

Definition 4.4. Let $\mathbf{G}$ be a locally compact topological group equipped with a Haar measure $\mu_{\mathbf{G}}$. We define an L^1*-norm* on functions on $\mathbf{G}$, through

$$||f||_1 = \int_{\mathbf{G}} |f| d\mu_{\mathbf{G}}.$$

Then let $L^1(\mathbf{G})$ denote the *group algebra*, i.e., the algebra of real-valued L^1-functions on $\mathbf{G}$ with respect to the Haar measure $\mu_{\mathbf{G}}$, under convolution.

(For example, $\mathbf{G} = G(K)$ for a linear algebraic group G and a non-archimedean local field K of characteristic zero, or $\mathbf{G} = \mathbf{G}_K = G(\mathbf{A}_{K,f})$ for a linear algebraic group G and a number field $K/\mathbf{Q}$.)

Definition 4.5. Let K and L be either both number fields, or both non-archimedean local fields of characteristic zero.

An isomorphism of Hecke algebras $\Psi \colon \mathscr{H}_G(K) \xrightarrow{\sim} \mathscr{H}_G(L)$ which is an isometry for the L^1-norms arising from the Haar measures (i.e., which satisfies $||\Psi(f)||_1 = ||f||_1$ for all $f \in \mathscr{H}_G(K)$) is called an L^1*-isomorphism.* We will denote this by

$$\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L).$$

The first main result in this section is the following theorem.

Theorem 4.6. Let K and L be either both number fields, or both non-archimedean local fields of characteristic zero.

Then there is an L^1-isomorphism of finite-adelic, resp. local Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if there is an isomorphism

$$\begin{cases} G(\mathbf{A}_{K,f}) \cong G(\mathbf{A}_{L,f}) & \text{if } K, L \text{ are number fields} \\ G(K) \cong G(L) & \text{if } K, L \text{ are local fields.} \end{cases}$$

Proof. We will first prove the theorem for K and L number fields, and again write $G_K = G(\mathbf{A}_{K,f})$ and $G_L = G(\mathbf{A}_{L,f})$.

The proof consists of two steps: first we show, using the Stone-Weierstrass theorem, that the Hecke algebras are dense in the group algebras, and then we use results on reconstructing a locally compact group from its group algebra due to Wendel.

Step 1: An isomorphism $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ implies that $L^1(\mathbf{G}_K) \cong_{L^1} L^1(\mathbf{G}_L)$.

By the locally compact real version of the Stone-Weierstrass theorem [43, 7.37(b)], $\mathscr{H}_G(K)$ is dense in $C_0(\mathbf{G}_K)$ for the sup-norm, where $C_0(\mathbf{G}_K)$ denotes the functions that vanish at infinity, i.e., such that $|f(x)| < \varepsilon$ outside a compact subset of $\mathbf{G}_K$. Indeed, one needs to check the nowhere vanishing and point separation properties of the algebra. Since $\mathscr{H}_G(K)$ contains the characteristic function of any compact subset $\mathbf{K} \subseteq \mathbf{G}_K$, the algebra vanishes nowhere, and the point separating property follows since $\mathbf{G}_K$ is Hausdorff.

A fortiori, $\mathscr{H}_G(K)$ is dense in the compactly supported functions $C_c(\mathbf{G}_K)$ for the sup-norm, and hence also in the L^1-norm. Now $C_c(\mathbf{G}_K)$ is dense in $L^1(\mathbf{G}_K)$, and the claim follows.

Step 2: An isometry $L^1(\mathbf{G}_K) \cong_{L^1} L^1(\mathbf{G}_L)$ implies an isomorphism $\mathbf{G}_K \cong \mathbf{G}_L$

Indeed, an L^1-isometry $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ implies an L^1-isometry of group algebras $L^1(\mathbf{G}_K) \cong_{L^1} L^1(\mathbf{G}_L)$. Hence the result follows from a theorem due to Wendel [127, Theorem 1], which says that an L^1-isometry of group algebras of locally compact topological groups is always induced by an isomorphism of the topological groups.

The proof for local non-archimedean fields of characteristic zero is analogous, once one replaces the real Stone-Weierstrass theorem by the complex version [43, 7.37(c)]. Moreover, both Step 1 and Step 2 of the proof go through for *complex* (finite-adelic) Hecke algebras. □

When K and L are number fields, and G is fertile for K and L (cf. Definition 3.4), Theorem 3.1 and Theorem 4.6 combine to prove the following result.

Theorem 4.7. Let K and L be two number fields, and let G denote a linear algebraic group over $\mathbf{Q}$ that is fertile for K and L. There is an L^1-isomorphism of Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if there is a ring isomorphism $\mathbf{A}_K \cong \mathbf{A}_L$. □

Remark 4.8. When K and L are Galois over $\mathbf{Q}$, Theorem 4.7 holds if and only if $K \cong L$, cf. Remark 3.2.

When K and L are local non-archimedean fields of characteristic zero, we only consider $G = \mathrm{GL}_n$ for some $n \geq 2$. In this case, [82, Theorem 5.6.10] shows that $G(K) \cong G(L)$ implies that $K \cong L$. Hence, we immediately obtain the following corollary of Theorem 4.6.

Corollary 4.9. Let K and L be two non-archimedean local fields of characteristic zero and let $G = \mathrm{GL}_n$, $n \geq 2$. Then there is an L^1-isomorphism of local Hecke algebras $\mathscr{H}_G(K) \cong_{L^1} \mathscr{H}_G(L)$ if and only if there is a field isomorphism $K \cong L$. □

Remark 4.10. Instead of citing [82], we could also adapt the proof of Theorem 4.7 to local fields - note that GL_n is fertile for all $n \geq 2$.

4.3 Morita equivalences

In this section, let K and L be local non-archimedean fields of characteristic zero and let $G = \mathrm{GL}_2$. We prove the following theorem.

Theorem 4.11. Let K and L be two non-archimedean local fields of characteristic zero and let $G = \mathrm{GL}_2$. Then there is a Morita equivalence

$$\mathscr{H}_G(K) \sim_M \mathscr{H}_G(L).$$

Remark 4.12. The Morita equivalence in Theorem 4.11 implies that the module category of a Hecke algebra over a local field K is independent of K (up to isomorphism). By contrast, as soon as we impose the analytic condition of an L^1-isomorphism, Corollary 4.9 shows that the Hecke algebra for a local field K uniquely determines K.

The proof of Theorem 4.11 will make use of the representation theory of p-adic reductive groups, and the decomposition of the Hecke algebra into Bernstein blocks. We start by collecting some preliminaries on these topics.

Representation theory of GL_n

We will write $\mathbf{G} = G(K)$ from now on, and study and classify representations $\pi\colon \mathbf{G} \to V$ where V is a (possibly infinite-dimensional) complex vector space. More details can be found in e.g. [13], [15].

Definition 4.13. The representation $\pi\colon \mathbf{G} \to V$ is called *admissible* if it satisfies the following two conditions:

1. the stabiliser $\mathrm{Stab}_{\mathbf{G}}(v)$ of any $v \in V$ is an open subgroup of $\mathbf{G}$,
2. for any open subgroup $\mathbf{G}' \subset G(\mathscr{O}_K)$, the space
$$\{v \in V\colon \pi(g')v = v \text{ for all } g' \in \mathbf{G}'\}$$
is finite-dimensional.

Remark 4.14. A representation π as in Definition 4.13 is called *smooth* if it satisfies only the first condition. Clearly, every admissible representations is smooth. Proposition 2 of [15] (due to M.-F. Vignéras) shows that any smooth irreducible complex representation is admissible. Hence, "smooth irreducible" and "admissible irreducible" will be used interchangeably.

Definition 4.15. A representation $\pi'\colon \mathscr{H}_G(K) \to V$ is called *admissible* if it satisfies the following two conditions:

1. for every $v \in V$, there is an element $f \in \mathscr{H}_G(K)$ such that $\pi(f)v = v$,
2. for every $f \in \mathscr{H}_G(K)$, we have $\dim(\pi(f)V) < \infty$.

Smooth representations of $\mathbf{G}$ correspond to representations π' for which V is a nondegenerate $\mathscr{H}_G(K)$-module [12]. Analogously, admissible representations of $\mathbf{G}$ correspond to admissible representations of $\mathscr{H}_G(K)$ and vice-versa, see e.g. [122, 2.1.13].

Definition 4.16. A *quasicharacter* χ of $K^\times$ is a continuous homomorphism
$$\chi\colon K^\times \to \mathbf{C}^*.$$

It is called *unramified* if it is trivial on $\mathscr{O}_K^\times$. Any unramified quasicharacter is of the form $|\cdot|^z$ for some $z \in \mathbf{C}$.

Lemma 4.17. [122, 2.1.18] Every irreducible admissible representation π which is finite-dimensional is in fact one-dimensional and there exists a quasicharacter χ such that $\pi(g) = \chi(\det g)$ for all $g \in \mathbf{G}$. □

Now we turn our attention to the infinite-dimensional representations.

Definition/Proposition 4.18. A *parabolic subgroup* $\mathbf{P}$ of $\mathbf{G}$ is such that $\mathbf{G}/\mathbf{P}$ is complete. Equivalently, $\mathbf{P}$ contains a Borel subgroup $\mathbf{B}$. Parabolic subgroups are the normalisers of their unipotent radicals, and every $\mathbf{P}$ is the semidirect product of this unipotent radical and a K-closed reductive group $\mathbf{L}$. This $\mathbf{L}$ is called a *Levi subgroup* of $\mathbf{P}$. □

Remark 4.19. The proper parabolic subgroups of $\mathrm{GL}_n(K)$ are the block upper triangular matrices and their conjugates. For instance, when $n = 2$, these are precisely the Borel subgroups, which are $\mathbf{T} \ltimes \mathbf{U}$ with $\mathbf{T}$ a maximal torus and $\mathbf{U}$ a maximal unipotent subgroup. That is, all the Levi subgroups in $\mathrm{GL}_2(K)$ are the maximal tori, i.e., the diagonal 2×2 matrices.

Definition 4.20. Let τ be a smooth representation of a Levi subgroup $\mathbf{L}$ of a parabolic subgroup $\mathbf{P}$ of $\mathbf{G}$. After inflation, we may assume that τ is a representation of $\mathbf{P}$. The *parabolic induction* $\mathrm{ind}_{\mathbf{P}}^{\mathbf{G}}(\tau)$, also denoted $\rho(\tau)$, is the space of locally constant functions ϕ on $\mathbf{G}$ which satisfy

$$\phi(pg) = \delta_P(p)^{\frac{1}{2}}\tau(p)\phi(g)$$

for all $g \in \mathbf{G}$ and $p \in \mathbf{P}$. The normalising factor $\delta_P = \Delta_P^{-1}$ is the inverse of the *modular character* Δ_P which satisfies

$$\Delta_P(\mathrm{diag}(a_1, \dots, a_n)) = |a_1|^{1-n}|a_2|^{3-n} \dots |a_n|^{n-1},$$

cf. [91, Ex. 2.6]. Parabolic induction preserves smoothness and admissibility but not necessarily irreducibility.

Definition 4.21. We call an infinite-dimensional irreducible admissible representation $\pi\colon \mathbf{G} \to V$ *(absolutely) cuspidal* or *supercuspidal* if it is not a subquotient of a representation that is parabolically induced from a *proper* parabolic subgroup of $\mathbf{G}$.

Definition 4.22. Using the notation of [13], a *partition* $(n_1, \dots, n_r)$ of n means a partition of $\{1, 2, \dots, n\}$ into segments

$$(1, \dots, n_1), (n_1 + 1, \dots, n_1 + n_2), \dots, (n_1 + n_2 + \dots + n_{r-1} + 1, \dots, n)$$

of respective lengths n_i. We will write $(n_1, \dots, n_r) \perp n$ for such a partition.

For any n_i appearing in a partition of n, write $\Delta_i = \{\sigma_i, \sigma_i|\cdot|, \dots, \sigma_i|\cdot|^{n_i-1}\}$ for $i = 1, \dots, r$ and σ_i an irreducible supercuspidal representation of $\mathrm{GL}_{n_i}(K)$. The Δ_i are also called segments, and we say that Δ_i *precedes* Δ_j if $\Delta_i \not\subset \Delta_j$ and $\Delta_j \not\subset \Delta_i$, if $\Delta_i \cup \Delta_j$ is also a segment, and $\sigma_i = \sigma_j|\cdot|^k$ for some $k > 0$.

Now compare Definition 4.21 with the following result (cf. [132, Theorem 6.1], [13, Corollary 3.27] and [91, pp. 189-190]).

Theorem 4.23. For any partition $(n_1, \dots, n_r)$ of n and a choice of segments so that Δ_i and Δ_{i+1} $(i = 1, \dots, r)$ do not precede each other, there exists a corresponding induced representation, denoted $\mathrm{ind}_{\mathbf{P}}^{\mathbf{G}}(\sigma_1 \dots \otimes \sigma_r)$, whose *unique* irreducible quotient is an irreducible admissible representation of $\mathbf{G}$. Any irreducible admissible representation of $\mathbf{G}$ is equivalent to such a quotient representation. □

Hence, supercuspidal representations can be viewed as the building blocks of admissible representations of $\mathbf{G}$. This concludes the classification of admissible representations of $\mathbf{G}$.

Remark 4.24. Let now $n = 2$, so that $G = \mathrm{GL}_2$ and $\mathbf{G} = \mathrm{GL}_2(K)$. Every infinite-dimensional irreducible admissible representation π which is not supercuspidal is then contained in $\rho(\mu_1, \mu_2)$ for some quasicharacters μ_1, μ_2 of K. If $\mu_1\mu_2^{-1} \neq |\cdot|^{\pm 1}$ then $\rho(\mu_1, \mu_2)$ and $\rho(\mu_2, \mu_1)$ are equivalent and irreducible. We call a representation of this kind a *(non-special) principal series representation.*

If $\rho(\mu_1, \mu_2)$ is reducible, it has a unique finite-dimensional constituent, and a unique infinite-dimensional constituent $\mathscr{B}_s(\mu_1, \mu_2)$, also called a *special representation*. For special representations, there exists a quasicharacter χ such that $\mu_1 = \chi| \cdot |^{-\frac{1}{2}}$ and $\mu_2 = \chi| \cdot |^{\frac{1}{2}}$. Moreover, all special representations are twists of the so-called *Steinberg representation* $\mathrm{St}_{\mathbf{G}}$ of $\mathbf{G}$ by quasicharacters $\chi \circ \det$.

Summarising, any irreducible admissible representation $\pi \colon \mathbf{G} \to V$ satisfies one of the following:

(1): it is absolutely cuspidal;

(2): it is a principal series representation $\pi(\mu_1, \mu_2)$ for some quasicharacters μ_1, μ_2;

(3): it is a special representation $\sigma(\mu_1, \mu_2)$ for some quasicharacters μ_1, μ_2;

(4): it is finite-dimensional and of the form $\pi = \chi \circ \det$ for some quasicharacter χ.

More details on GL_2 can be found in e.g. [50], [23].

Bernstein decomposition

We will introduce the Bernstein decomposition, using [25] and [12] as our main references. Let $\mathbf{G} = \mathrm{GL}_n(K)$ as before.

Definition 4.25. Let $\mathbf{L}$ be a Levi subgroup of some parabolic $\mathbf{P}$ inside $\mathbf{G}$ and let σ be an irreducible cuspidal representation of $\mathbf{L}$. We define the *inertial class* $[\mathbf{L}, \sigma]_{\mathbf{L}}$ of

$(\mathbf{L}, \sigma)$ in $\mathbf{L}$ to be all the cuspidal representations σ' of $\mathbf{L}$ such that $\sigma \cong \sigma'\chi$ for χ an unramified character of $\mathbf{L}$. Similarly, the inertial equivalence class $[\mathbf{L}, \sigma]_{\mathbf{G}}$ consists of all pairs $(\mathbf{L}', \sigma')$ which are $\mathbf{G}$-conjugate to $(\mathbf{L}, \sigma)$, meaning that there exist $g \in \mathbf{G}$ and an unramified character χ of $\mathbf{L}'$ such that $\mathbf{L}' = g^{-1}\ \mathbf{L}\ g$ and $\sigma^g \cong \sigma'\chi$, [25, p. 588]. Let $\mathscr{B}(\mathbf{G})$ be the set of all inertial equivalence classes in $\mathbf{G}$.

We need the following refinement of Theorem 4.23.

Theorem 4.26. For every smooth irreducible representation (π, V) of $\mathbf{G}$ there exists a parabolic $\mathbf{P}$ in $\mathbf{G}$ with Levi subgroup $\mathbf{L}$, and an irreducible supercuspidal representation σ of L, such that (π, V) is equivalent to a subquotient of the parabolic induction $\mathrm{Ind}_{\mathbf{P}}^{\mathbf{G}}(\sigma)$ [49]. The pair $(\mathbf{L}, \sigma)$ is determined up to conjugacy; the corresponding inertial class $s = [\mathbf{L}, \sigma]_{\mathbf{G}}$ is unique ([12, *Le "centre" de Bernstein*, 2.6-2.10], cf. also [29]). □

Definition 4.27. The pair $(\mathbf{L}, \sigma)$ in the previous theorem is called the *cuspidal support* of (π, V); the corresponding inertial class $s = [\mathbf{L}, \sigma]_{\mathbf{G}}$ is called the *inertial support* of (π, V).

Lemma 4.28. [12, *Le "centre" de Bernstein*, Prop. 2.10] Denote by $\mathfrak{R}(\mathbf{G})$ the category of smooth representations (π, V) of $\mathbf{G}$ and by $\mathfrak{R}^s(\mathbf{G})$ the full subcategory, whose objects are such that the inertial support of all their respective irreducible $\mathbf{G}$-subquotients is s. Then there is a direct product decomposition of categories

$$\mathfrak{R}(\mathbf{G}) = \prod_{s \in \mathscr{B}(\mathbf{G})} \mathfrak{R}^s(\mathbf{G}).$$

□

Corollary 4.29. Let $\mathscr{H}_G^s(K)$ be the two-sided ideal of $\mathscr{H}_G(K)$ corresponding to all smooth representations (π, V) of $\mathbf{G}$ of inertial support $s = [\mathbf{L}, \sigma]_{\mathbf{G}}$. That is, $\mathscr{H}_G^s(K)$ is the unique and maximal $\mathbf{G}$-subspace of $\mathscr{H}_G(K)$ lying in $\mathfrak{R}^s(\mathbf{G})$. We call $\mathscr{H}_G^s(K)$ a *Bernstein block.* □

Definition 4.30. The Hecke algebra $\mathscr{H}_G(K)$ has a *Bernstein decomposition*

$$\mathscr{H}_G(K) = \bigoplus_{s \in \mathscr{B}(\mathbf{G})} \mathscr{H}_G^s(K).$$

Definition 4.31. Let (ρ, W) be a smooth representation of a compact open subgroup $\mathbf{K}$ of $\mathbf{G}$, whose contragredient representation is denoted $(\check{\rho}, \check{W})$.
The *ρ-spherical Hecke algebra* $\mathscr{H}(\mathbf{G}, \rho)$ is the unital associative $\mathbf{C}$-algebra of finite type, consisting of compactly supported functions $f\colon \mathbf{G} \to \mathrm{End}_{\mathbf{C}}(\check{W})$ satisfying

$f(k_1 g k_2) = \check{\rho}(k_1) f(g) \check{\rho}(k_2)$ for all $g \in \mathbf{G}, k_1, k_2 \in \mathbf{K}$. It is also called the *intertwining algebra*, since

$$\mathscr{H}(\mathbf{G}, \rho) \cong \mathrm{End}_{\mathbf{G}}(\mathrm{ind}_{\mathbf{K}}^{\mathbf{G}}(\rho))$$

by [25, 2.6], where ind denotes compact induction.

Proposition 4.32. [25, Prop. 5.6] Every $\mathscr{H}_G^s(K)$ is a non-commutative, non-unital, non-finitely generated non-reduced $\mathbf{C}$-algebra, which is Morita equivalent to some intertwining algebra $\mathscr{H}(\mathbf{G}, \rho)$.

Sketch of proof. For every equivalence class s there exist a compact open subgroup $\mathbf{K}$ of $\mathbf{G}$, a smooth representation (ρ, W) of $\mathbf{K}$ and an idempotent element $e_\rho \in \mathscr{H}_G(K)$ (cf. (2.9) of [25]) which satisfies

$$e_\rho(x) = \begin{cases} \frac{\dim(\rho)}{\mu_{\mathbf{G}}(\mathbf{K})} \mathrm{tr}_W(\rho(x^{-1})) & \text{if } x \in \mathbf{K} \\ 0 & \text{if } x \in \mathbf{G}, x \notin \mathbf{K} \end{cases},$$

such that

$$\mathscr{H}_G^s(K) = \mathscr{H}_G(K) * e_\rho * \mathscr{H}_G(K).$$

There is a Morita equivalence (cf. [11, Lemma 2])

$$\mathscr{H}_G(K) * e_\rho * \mathscr{H}_G(K) \sim_M e_\rho * \mathscr{H}_G(K) * e_\rho$$

and the latter is proven in [25, 2.12] to be isomorphic as a unital $\mathbf{C}$-algebra to

$$e_\rho * \mathscr{H}_G(K) * e_\rho \cong \mathscr{H}(\mathbf{G}, \rho) \otimes_{\mathbf{C}} \mathrm{End}_{\mathbf{C}}(W) \tag{4.2}$$

where $\mathscr{H}(\mathbf{G}, \rho)$ is as in Definition 4.31. In particular, there is a Morita equivalence

$$\mathscr{H}_G^s(K) \sim_M \mathscr{H}(\mathbf{G}, \rho), \tag{4.3}$$

i.e., the categories of modules over the left resp. right hand side of (4.3) are equivalent. □

Proof of Theorem 4.11

Definition 4.33. The *(extended) affine Weyl group* of GL_n is $\widetilde{W_n} \cong S_n \ltimes \mathbf{Z}^n$, where the symmetric group S_n acts by permuting the factors of $\mathbf{Z}^n$. We denote its group algebra by

$$\mathbf{C}[\widetilde{W_n}] = \mathbf{C}[S_n \ltimes \mathbf{Z}^n].$$

In this section, we will prove the following result, which immediately implies Theorem 4.11.

Theorem 4.34. Let K be a non-archimedean local field of characteristic zero and $G = \mathrm{GL}_2$. Then up to Morita equivalence, the Bernstein decomposition of $\mathscr{H}_G(K)$ is always of the form

$$\mathscr{H}_{\mathrm{GL}_2}(K) \sim_M \bigoplus_{\mathbf{N}} \left(\mathbf{C}[T, T^{-1}] \oplus \mathbf{C}[X, X^{-1}, Y, Y^{-1}] \oplus \frac{\mathbf{C}[S, T, T^{-1}]}{\langle S^2 - 1, T^2 S - ST^2 \rangle} \right). \tag{4.4}$$

In particular, if K and L are any two non-archimedean local fields of characteristic zero, then

$$\mathscr{H}_G(K) \sim_M \mathscr{H}_G(L).$$

Proof. By Theorem 4.23, every irreducible representation of $\mathbf{G}$ is a subquotient of a parabolically induced representation $\mathrm{ind}_{\mathbf{P}}^{\mathbf{G}}(\sigma_1 \ldots \otimes \sigma_r)$, where the σ_i are irreducible supercuspidal representations of GL_{n_i} and $(n_1, \ldots, n_r)$ is a partition of n, so that consecutive segments do not precede each other. Note that n_i is the multiplicity of σ_i in the tensor product, so that $n_i = 1$ or 2 always.

Proposition 4.32 implies that to determine the corresponding Bernstein blocks $\mathscr{H}_G^s(K)$ of the Hecke algebra up to Morita equivalence, it suffices to determine all intertwining algebras $\mathscr{H}(\mathbf{G}, \rho)$ that occur. To do this, we need the following definition.

Definition 4.35. [24, 5.4.6] Let $m \in \mathbf{Z}_{>0}$ and $r \in \mathbf{C}^\times$. The *affine Hecke algebra* $\mathscr{H}(m, r)$ is the associative unital $\mathbf{C}$-algebra generated by elements S_i (for $1 \leq i \leq m-1$), T, T^{-1}, satisfying the following relations:

1. $(S_i + 1)(S_i - r) = 0$ for $1 \leq i \leq m - 1$,
2. $T^2 S_1 = S_{m-1} T^2$,
3. $TS_i = S_{i-1} T$ for $2 \leq i \leq m - 1$,
4. $S_i S_{i+1} S_i = S_{i+1} S_i S_{i+1}$ for $1 \leq i \leq m - 2$,
5. $S_i S_j = S_j S_i$ for $1 \leq i, j \leq m - 1$ such that $|i - j| \geq 2$.

Note that when $m = 1$, we have $\mathscr{H}(1, r) \cong \mathbf{C}[T, T^{-1}]$ for any value of r. Moreover, note that when $m \leq 2$, relations (3),(4) and (5) are vacuous.

By the Main Theorem of [26], the intertwining algebra corresponding to $\mathrm{ind}_{\mathbf{P}}^{\mathbf{G}}(\sigma_1 \otimes \ldots \otimes \sigma_r)$ is isomorphic to the tensor product $\otimes_{i=1}^{r} \mathscr{H}(n_i, q^{k_i})$ of affine Hecke algebras, where $n_i \leq 2$ since $n = 2$. Here, q is the size of the residue field of K, while k_i is the so-called torsion number of σ_i, cf. [11, p.22]. In particular, $q^{k_i} \neq -1$ always. A priori, the Hecke algebra $\mathscr{H}(2, q^{k_i})$ depends on q^{k_i}. However, we now prove the following.

Lemma 4.36. For any $r \neq -1$, there is an algebra isomorphism $\mathscr{H}(2, r) \cong \mathbf{C}[\widetilde{W}_2]$.

Proof. First let $r = 1$. Let ϖ be a uniformiser of K. Since ϖ is not a root of unity, we may alternatively (cf. [24, pp. 177–178]) write $\widetilde{W}_2 = \langle \Pi \rangle \ltimes W$, where

$$\Pi = \begin{pmatrix} 0 & 1 \\ \varpi & 0 \end{pmatrix},$$

and W is generated by

$$s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We may check that s_1 has order 2 and that sending $S_1 \mapsto s_1$, and $T \mapsto \Pi$ (and $T^{-1} \mapsto \Pi^{-1}$) yields an algebra isomorphism $\mathscr{H}(2, 1) \to \mathbf{C}[\widetilde{W}_2]$.

Now let $r \in \mathbf{C}^\times \setminus \{-1\}$ and let (cf. [128, p. 113])

$$\overline{s}_1 = \left(\frac{q+1}{2} s_1 + \frac{q-1}{2} \right) \in \mathbf{C}[\widetilde{W}_2].$$

Then relation (2),

$$\Pi^2 \overline{s}_1 = \overline{s}_1 \Pi^2$$

still holds. Hence, the map $S_1 \mapsto \overline{s}_1$, and $T \mapsto \Pi$ (and $T^{-1} \mapsto \Pi^{-1}$) determines an algebra isomorphism $\mathscr{H}(2, q) \to \mathbf{C}[\widetilde{W}_2]$, for any r other than $r = -1$. □

It follows that the intertwining algebra for the partition $(n_1, \ldots, n_r)$ of n, corresponding to the representation $\mathrm{ind}_{\mathbf{P}}^{\mathbf{G}}(\sigma_1 \otimes \ldots \otimes \sigma_r)$, is isomorphic to the $\mathbf{C}$-algebra $\otimes_{i=1}^r \mathbf{C}[\widetilde{W}_{n_i}]$.

Finally, we show that any such algebra $\otimes_{i=1}^r \mathbf{C}[\widetilde{W}_{n_i}]$ occurs countably infinitely many times in the Bernstein decomposition. For this, we use the classification of Remark 4.24. The reader may compare this to the explicit description of the intertwining algebras in [98, Example 3.13].

(1): A *supercuspidal representation* (π, V) corresponds to an inertial class $s = [\mathbf{G}, \rho]_{\mathbf{G}}$ where ρ is itself an irreducible supercuspidal representation. The corresponding intertwining algebra is $\mathscr{H}(\mathbf{G}, \rho) \cong \mathscr{H}(1, q) \cong \mathbf{C}[T, T^{-1}]$, for q some power of p. The uncountably infinitely many equivalence classes in

$\mathbf{G}$ of supercuspidal representations are indexed by characters of quadratic extensions of K, cf. [23, Theorem 20.2], so after dividing out by unramified characters, we find uncountably many inertial equivalence classes.

(2): The principal series representations are constituents of representations of the form $\mathrm{ind}_{\mathbf{B}}^{\mathbf{G}}(\chi_1, \chi_2)$ for a choice of Borel subgroup $\mathbf{B}$ of $\mathbf{G}$ and characters χ_1 and χ_2. Therefore, up to inertial equivalence, we find $\rho(\chi_1|\cdot|^z, \chi_2|\cdot|^{z'}) = \mathrm{ind}_B^G(\chi_1|\cdot|^z, \chi_2|\cdot|^{z'})$ for some characters χ_1 and χ_2, and some values z, z'.

Non-special representations then correspond to a choice of χ_1, χ_2 such that $\chi_1\chi_2^{-1} \neq |\cdot|^{\pm 1}$ (i.e. χ_1 and χ_2 are not inertially equivalent), or a choice of χ, z, z' such that $|z - z'| \neq 1$. The corresponding inertial class is $s = [\mathbf{T}, \rho]_{\mathbf{G}}$, where $\mathbf{T}$ is a maximal torus in $\mathbf{B}$. For such ρ, we have $\mathscr{H}(\mathbf{G}, \rho) \cong \mathscr{H}(1, q) \otimes \mathscr{H}(1, q') \cong \mathbf{C}[X, X^{-1}, Y, Y^{-1}]$, for q and q' some powers of p.

We also see that the equivalence classes of these representations are indexed by the characters of $(\mathscr{O}_K^\times)^2$ modulo the action of S_2, which is a countably infinite group.

(3/4): A *special representation* is the infinite-dimensional irreducible subquotient $\mathrm{St}_{\mathbf{G}}\chi|\cdot|^{z+\frac{1}{2}}$ of the reducible representation $\rho = \rho(\chi|\cdot|^{z+1}, \chi|\cdot|^z)$ for some χ and z, and corresponds to $s = [\mathbf{T}, \rho]_{\mathbf{G}}$. The *finite-dimensional representations* appear as the finite-dimensional irreducible subquotients of the same ρ.

Hence, the corresponding inertial equivalence classes s are indexed by the character group of $\mathscr{O}_K^\times$, which is countably infinite. The corresponding intertwining algebras for both special and finite-dimensional representations are

$$\mathscr{H}(2, q) \cong \mathbf{C}[\widetilde{W}_2] \cong \mathbf{C}[S, T, T^{-1}]/\langle S^2 - 1, T^2S - ST^2\rangle.$$

This finishes the proof of Theorem 4.34 and hence of Theorem 4.11. □

Discussion

The results in this section naturally inspire some further questions.

(i) (Generalisations of Theorem 4.11)

1. We have seen that for GL_2, up to Morita equivalence, $\mathscr{H}_G(K)$ does not depend on K. Does the same hold up to algebra isomorphism?
2. An extension of the proof of Theorem 4.34 to GL_n, $n > 2$, is obstructed by the braid relations ((4) of Definition 4.35) among the generators of the affine Hecke algebras. This is pointed out by Xi in [128, 11.7], where

he proves that $\mathscr{H}(3,q) \not\cong \mathbf{C}[\widetilde{W}_3]$ for $q \neq 1$. In fact, Yan proves in [130] that any two affine Hecke algebras $\mathscr{H}(n,q)$ and $\mathscr{H}(n,q')$ of type $\widetilde{A}_2$ are not Morita equivalent when $q' \neq q$ and $q' \neq q^{-1}$.

3. One may still ask whether Theorem 4.34 also holds for other reductive groups G over K. It is known that the Hecke algebras of such groups also admit a Bernstein decomposition. However, it is in general much harder to determine the complex algebras that occur as intertwining algebras and to show that these are independent of K. We would also want to have a similar classification of the representation theory of such G.

(ii) (A global version of Theorem 4.34)
In the proof of Theorem 4.34, we have seen that the residual characteristic p of K does not play a special role. Hence, If K is a number field and $G = \mathrm{GL}_n$, $n \geq 2$, we may consider the (adelic) Hecke algebra $\mathscr{H}_G(K)$ as a restricted tensor product of local Hecke algebras $\mathscr{H}_G(K_v)$, with respect to the maximal open compact subgroups $G(\mathscr{O}_v)$:

$$\mathscr{H}_G(K) = \otimes_v \mathscr{H}_G(K_v),$$

cf. [50, Chapter 9] for $G = \mathrm{GL}_2$ and [21, p.320] for $G = \mathrm{GL}_n$. We know that the module category of any $\mathscr{H}_{\mathrm{GL}_2}(K_v)$ is independent of K_v (so in particular independent of the residual characteristic of K_v). Hence, a natural question would be to ask whether the module category of $\mathscr{H}_{\mathrm{GL}_2}(K)$ is also independent of K. We expect however that the restricted tensor product construction, through the rings of integers $\mathscr{O}_v$, *does* depend on K.

(iii) (An anabelian question)
Exactly which field invariants of K are determined by $\mathscr{H}_G(K)$?

(iv) (The L^1-isomorphism condition in Theorem 7.5)
The condition that the isomorphism $\mathscr{H}_G(K) \cong \mathscr{H}_G(L)$ is an isometry for the L^1-norm is one which we would like to understand from a categorial viewpoint. Does the L^1-isomorphism type of (modules over) a Hecke algebra impose analytic conditions on (certain classes of) the automorphic representations? Or can we relate the L^1-isomorphism type of a Hecke algebra $\mathscr{H}_G(K)$ to the ramification filtration of the absolute Galois group G_K?

Part II

Galois representations

CHAPTER 5

Galois representations for abelian varieties

In this chapter, we present the structure theory of (general) symplectic groups and the general theory of Galois representations attached to the ℓ-torsion of abelian varieties, as well as some results on Galois representations and realisations from the literature, and geometric preliminaries, which will be used in Chapters 6 and 7.

5.1 Structure theory of GSp

Definition 5.1. Let V be an $\mathbf{F}_\ell$-vector space of dimension $2g$, which is endowed with a symplectic (i.e. skew-symmetric, nondegenerate) pairing $\langle\cdot,\cdot\rangle : V \times V \to \mathbf{F}_\ell$. We consider the *symplectic group*

$$\mathrm{Sp}(V, \langle\cdot,\cdot\rangle) := \{M \in \mathrm{GL}(V) : \forall v_1, v_2 \in V, \langle Mv_1, Mv_2\rangle = \langle v_1, v_2\rangle\}$$

and the *general symplectic group*

$$\begin{aligned} \mathrm{GSp}(V, \langle\cdot,\cdot\rangle) := \{M \in \mathrm{GL}(V) :\, &\exists m \in \mathbf{F}_\ell^\times \text{ s.t. } \forall v_1, v_2 \in V, \\ &\langle Mv_1, Mv_2\rangle = m\langle v_1, v_2\rangle\}. \end{aligned}$$

Definition 5.2. Given a finite-dimensional vector space V over $\mathbf{F}_\ell$, endowed with a symplectic pairing $\langle\cdot,\cdot\rangle : V \times V \to \mathbf{F}_\ell$, a *transvection* is an element $T \in \mathrm{GSp}(V, \langle\cdot,\cdot\rangle)$ such that there exists a hyperplane $H \subset V$ satisfying that the restriction $T|_H$ is the identity on H. We say that it is a nontrivial transvection if T is not the identity, but we do call the identity a transvection, so that the set of transvections for a given hyperplane H is a group.

It turns out that the subgroups of $\mathrm{GSp}(V, \langle\cdot,\cdot\rangle)$ that contain a nontrivial transvection can be classified into three categories as follows (for a proof, see e.g. [6, Theorem 1.1]):

This chapter is based on parts of the articles [14] and [4], both joint work with Sara Arias-de-Reyna, Cécile Armana, Marusia Rebolledo, Lara Thomas and Núria Vila.

Theorem 5.3. Let $\ell \geq 5$ be a prime, let V be a finite-dimensional vector space over $\mathbf{F}_\ell$, endowed with a symplectic pairing $\langle \cdot, \cdot \rangle : V \times V \to \mathbf{F}_\ell$ and let $G \subset \mathrm{GSp}(V, \langle \cdot, \cdot \rangle)$ be a subgroup that contains a nontrivial transvection. Then one of the following holds:

1. G is reducible, i.e. there is a proper $\mathbf{F}_\ell$-subspace $S \subset V$ such that $G(S) = S$.
2. There exists a proper decomposition $V = \bigoplus_{i \in I} V_i$ of V into equidimensional nonsingular symplectic subspaces V_i such that, for each $g \in G$ and each $i \in I$, there exists some $j \in I$ with $g(V_i) \subseteq V_j$ and such that the resulting action of G on I is transitive.
3. G contains $\mathrm{Sp}(V, \langle \cdot, \cdot \rangle)$. □

To distinguish between the three cases in Theorem 5.3, we will make use of the following result [8, Corollary 2.2].

Corollary 5.4. Let $\ell \geq 5$ be a prime, let V be a finite-dimensional vector space over $\mathbf{F}_\ell$, endowed with a symplectic pairing $\langle \cdot, \cdot \rangle : V \times V \to \mathbf{F}_\ell$ and let $G \subset \mathrm{GSp}(V, \langle \cdot, \cdot \rangle)$ be a subgroup containing a nontrivial transvection and an element whose characteristic polynomial is irreducible and which has nonzero trace. Then G contains $\mathrm{Sp}(V, \langle \cdot, \cdot \rangle)$. □

5.2 Galois representations attached to the ℓ-torsion of abelian varieties

Let A be an abelian variety of dimension g defined over $\mathbf{Q}$. Fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. The set of $\overline{\mathbf{Q}}$-points of A admits a group structure. Let ℓ be a prime number. Then the subgroup of the $\overline{\mathbf{Q}}$-points of A consisting of all ℓ-torsion points, which is denoted by $A[\ell]$, is isomorphic to $(\mathbf{Z}/\ell\mathbf{Z})^{2g}$ and it is endowed with a natural action of $G_{\mathbf{Q}}$. Therefore, it gives rise to a (continuous) Galois representation

$$\overline{\rho}_{A,\ell} : G_{\mathbf{Q}} \to \mathrm{GL}(A[\ell]) \simeq \mathrm{GL}_{2g}(\mathbf{F}_\ell).$$

Hence, we obtain a realisation of the image of $\overline{\rho}_{A,\ell}$ as a Galois group over $\mathbf{Q}$.

In this section, we will consider principally polarised abelian varieties, i.e. we will consider pairs (A, λ), where A is an abelian variety (defined over $\mathbf{Q}$) and $\lambda : A \to A^\vee$ is an isogeny of degree 1 (that is, an isomorphism between A and the dual abelian variety $A^\vee$), induced from an ample divisor on A. Not every abelian variety A admits a principal polarisation λ and, when it does, this polarisation causes certain restrictions: the image of $\overline{\rho}_{A,\ell}$ then lies inside the general symplectic group of $A[\ell]$

with respect to a certain symplectic pairing. More precisely, let $\mu_\ell(\overline{\mathbf{Q}})$ denote the group of ℓ-th roots of unity inside a fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. Recall that the Weil pairing e_ℓ is a perfect pairing

$$e_\ell : A[\ell] \times A^\vee[\ell] \to \mu_\ell(\overline{\mathbf{Q}}).$$

If (A, λ) is a principally polarised abelian variety, we can consider the pairing

$$\begin{aligned} e_{\ell,\lambda} : A[\ell] \times A[\ell] &\to \mu_\ell(\overline{\mathbf{Q}}) \\ (P, Q) &\mapsto e_\ell(P, \lambda(Q)) \end{aligned}$$

which is a *multiplicative* symplectic pairing, compatible with the action of $G_{\mathbf{Q}}$. This last condition means that, for any $\sigma \in G_{\mathbf{Q}}$,

$$(e_{\ell,\lambda}(P, Q))^\sigma = e_{\ell,\lambda}(P^\sigma, Q^\sigma).$$

Note that $G_{\mathbf{Q}}$ acts on $\mu_\ell(\overline{\mathbf{Q}})$ via the mod ℓ cyclotomic character χ_ℓ, so that $(e_{\ell,\lambda}(P, Q))^\sigma = (e_{\ell,\lambda}(P, Q))^{\chi_\ell(\sigma)}$. If we fix a primitive ℓ-th root of unity ζ_ℓ, we may write the pairing $e_{\ell,\lambda}(\cdot, \cdot)$ additively, i.e. we define

$$\langle \cdot, \cdot \rangle : A[\ell] \times A[\ell] \to \mathbf{F}_\ell$$

as $\langle P, Q \rangle := a$ such that $\zeta^a = e_{\ell,\lambda}(P, Q)$.

In other words, we have a symplectic pairing on the $\mathbf{F}_\ell$-vector space $A[\ell]$ such that, for all $\sigma \in G_{\mathbf{Q}}$, the linear map $\overline{\rho}(\sigma) : A[\ell] \to A[\ell]$ satisfies that there exists a scalar, namely $\chi_\ell(\sigma)$, such that

$$\langle \overline{\rho}(\sigma)(P), \overline{\rho}(\sigma)(Q) \rangle = \chi_\ell(\sigma) \langle P, Q \rangle. \tag{5.1}$$

That is to say, the image of the representation $\overline{\rho}_{A,\ell}$ is contained in the general symplectic group $\mathrm{GSp}(A[\ell], \langle \cdot, \cdot \rangle) \simeq \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$. Therefore, from now on we will consider $\overline{\rho}_{A,\ell}$ as a map into $\mathrm{GSp}(A[\ell], \langle \cdot, \cdot \rangle) \simeq \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ and we will say that it is surjective if $\mathrm{Im}\overline{\rho}_{A,\ell} = \mathrm{GSp}(A[\ell]) \simeq \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$.

Lemma 5.5. Assume that V is the ℓ-torsion group of a principally polarised abelian variety A defined over $\mathbf{Q}$ and $\langle \cdot, \cdot \rangle$ is the symplectic pairing coming from the Weil pairing. If $G = \mathrm{Im}\overline{\rho}_{A,\ell}$ satisfies the third condition in Theorem 5.3, then $G = \mathrm{GSp}(V, \langle \cdot, \cdot \rangle)$.

Proof. We have the following exact sequence

$$1 \to \mathrm{Sp}(V, \langle \cdot, \cdot \rangle) \to \mathrm{GSp}(V, \langle \cdot, \cdot \rangle) \to \mathbf{F}_\ell^\times \to 1,$$

where the map $m : \mathrm{GSp}(A[\ell], \langle \cdot, \cdot \rangle) \to \mathbf{F}_\ell^\times$ associates to M the scalar a satisfying that, for all $u, v \in V$, $\langle Mu, Mv \rangle = a\langle u, v \rangle$. By equation (5.1), the restriction of m to $\mathrm{Im}(\overline{\rho}_{A,\ell})$ coincides with the mod ℓ cyclotomic character χ_ℓ. We can now easily obtain the result, using that χ_ℓ is surjective onto $\mathbf{F}_\ell^\times$.

In other words, $\overline{\rho}_{A,\ell}$ is surjective as soon as $\mathrm{Im}(\overline{\rho}_{A,\ell}) \supset \mathrm{Sp}_{2g}(\mathbf{F}_\ell)$. □

Corollary 5.6. For $\ell \geq 5$, the representation $\overline{\rho}_{A,\ell}$ is surjective if $\mathrm{Im}(\overline{\rho}_{A,\ell})$ contains both a nontrivial transvection and an element whose characteristic polynomial is irreducible and which has nonzero trace.

Proof. This follows from Corollary 5.4 and Lemma 5.5. □

5.3 Surjective Galois representations

The determination of the images of the Galois representations $\overline{\rho}_{A,\ell}$ attached to the ℓ-torsion of abelian varieties is a topic that has received a lot of attention. A remarkable result by Serre quoted in [105, n. 136, Theorem 3] is:

Theorem 5.7 (Serre)**.** Let A be a principally polarised abelian variety of dimension g, defined over a number field K. Assume that $g = 2, 6$ or g is odd and furthermore assume that $\mathrm{End}_{\overline{K}}(A) = \mathbf{Z}$. Then there exists a bound $B_{A,K}$ such that, for all $\ell > B_{A,K}$,

$$\mathrm{Im}\overline{\rho}_{A,\ell} = \mathrm{GSp}(A[\ell]) \simeq \mathrm{GSp}_{2g}(\mathbf{F}_\ell).$$

□

The bound $B_{A,K}$ is not explicit. For arbitrary dimension, the result is not true (see e.g. [77] for a counterexample in dimension 4). However, one eventually obtains a full symplectic image by making some extra assumptions. To state these assumptions, we first give a few definitions.

Definition 5.8. [18, Definition 1.2.1] Let A be an abelian variety over a number field K with ring of integers $\mathscr{O}_K$. The *Néron model* of A/K is a smooth commutative group scheme $\mathscr{A}/\mathscr{O}_K$ satisfying the *Néron mapping property*: for each smooth $\mathscr{O}_K$-scheme B and each K-morphism $u_K \colon B_K \to A$ there is a unique $\mathscr{O}_K$-morphism $u \colon B \to \mathscr{A}$ extending u_K.

This model exists and is unique up to (unique) isomorphism.

For any prime $\mathfrak{p}$ of $\mathscr{O}_K$, we can consider the fibre $A_\mathfrak{p}$ of $\mathscr{A}$. Let $A^0_\mathfrak{p}$ be the connected component of the identity of $A_\mathfrak{p}$.

Definition 5.9. The *group of connected components of* $A_\mathfrak{p}$ is $\Phi_\mathfrak{p} = A_\mathfrak{p}/A^0_\mathfrak{p}$. This is a finite group.

Definition 5.10. When A has semistable (also called semi-abelian) reduction at $\mathfrak{p}$, then $A^0_\mathfrak{p}$ is an extension

$$1 \to T \to A^0_\mathfrak{p} \to A'' \to 1$$

of an abelian variety A'' by a (possibly trivial) affine torus T. The dimension of T (as a group scheme) is the *toric dimension* of the fibre $A_\mathfrak{p}$.

By [18, Theorem 7.4.1], every abelian variety A/K has *potential semi-abelian reduction* at all closed points of $\mathscr{O}_K$; this means that there is a finite Galois extension L/K such that the fibres $A'_{\mathfrak{p}'}$ of the Néron model $\mathscr{A}'$ of A_L have semi-abelian reduction at all primes $\mathfrak{p}'$ of $\mathscr{O}_L$ lying above a closed point $\mathfrak{p}$ of $\mathscr{O}_K$.

Semistable reductions of curves are treated in more detail in Section 5.4.

Now we can state the following result of C. Hall (cf. [38]).

Theorem 5.11 (Hall)**.** Let A be a principally polarised abelian variety of dimension g defined over a number field K, such that $\mathrm{End}_{\overline{K}}(A) = \mathbf{Z}$, and satisfying the following property:

> (T) There is a finite extension L/K so that the Néron model of A/L over the ring of integers of L has a semistable fibre with toric dimension 1.

Then there is an (explicit) finite constant $B_{A,K}$ such that, for all $\ell \geq B_{A,K}$,

$$\mathrm{Im}\overline{\rho}_{A,\ell} = \mathrm{GSp}(A[\ell]) \simeq \mathrm{GSp}_{2g}(\mathbf{F}_\ell).$$

□

Proposition 5.12. [38, p. 704] Suppose that $A = \mathrm{Jac}(C)$ is the Jacobian of a hyperelliptic curve C of genus g, say defined by an equation $Y^2 = f(X)$ with $f(X) \in K[X]$ a polynomial of degree $2g+1$. Then Condition (T) is satisfied at the fibre corresponding to a prime $\mathfrak{p}$ of the ring of integers of K, *if* the coefficients of $f(X)$ have $\mathfrak{p}$-adic valuation greater than or equal to zero and the reduction of $f(X)$ mod $\mathfrak{p}$ has one double zero in a fixed algebraic closure of the residue field, while all the other zeroes are simple. □

As Kowalski points out in [38, Appendix], for every g and any number field K, we can find an abelian variety A over K (which is the Jacobian of a hyperelliptic curve) satisfying the conditions of Theorem 5.11. In particular, applying Theorem 5.11 with $K = \mathbf{Q}$ yields the following partial answer to the Inverse Galois Problem.

Corollary 5.13 (Hall/Kowalski). Let $g \in \mathbf{N}$ be any natural number. Then for *all sufficiently large* primes ℓ, the group $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ can be realised as a Galois group over $\mathbf{Q}$. □

Although it should be possible to find an upper bound for the constant $B_{A,\mathbf{Q}}$, cf. [38, Lemma 4] and [70], it would be far from optimal.

A key point in Theorem 5.11 is the fact that the image under $\overline{\rho}_{A,\ell}$ of the inertia subgroup at the place $\mathfrak{p}$ of L which provides the semistable fibre with toric dimension 1 is generated by a nontrivial transvection (whenever ℓ does not divide $\mathfrak{p}$ nor the cardinality of the group $\Phi_\mathfrak{p}$ of connected components of the special fibre of the Néron model at $\mathfrak{p}$). A detailed proof of this fact can be found in Proposition 1.3 of [60].

Suppose then that we have ensured that A satisfies Condition (T), so that $\mathrm{Im}(\overline{\rho}_{A,\ell})$ contains a nontrivial transvection. In order to apply Corollary 5.6, i.e. in order to find an element of $\mathrm{Im}(\overline{\rho}_{A,\ell})$ whose characteristic polynomial is irreducible and which has nonzero trace, we need some more information on the image of $\overline{\rho}_{A,\ell}$, which we will obtain by looking at the images of the Frobenius elements $Fr_{\mathbf{F}_q}$ (also denoted Fr_q) for primes q of good reduction of A.

More generally, let A be an abelian variety defined over a field K and assume that ℓ is a prime different from the characteristic of K. Any endomorphism α of A induces an endomorphism of $A[\ell]$, in such a way that the characteristic polynomial of α (which is a monic polynomial in $\mathbf{Z}[X]$, cf. e.g. [58, IV.3, Theorem 8]) coincides, after reduction mod ℓ, with the characteristic polynomial of the corresponding endomorphism of $A[\ell]$. In the case when K is a finite field (say of cardinality q), we can consider the (relative) Frobenius endomorphism $\pi_{A/K} \in \mathrm{End}_K(A)$, induced by the action of the (topological) Frobenius element $Fr_q \in \mathrm{Gal}(\overline{K}/K)$. Then the reduction mod ℓ of the characteristic polynomial of $\pi_{A/K}$ coincides with the characteristic polynomial of $\overline{\rho}_{A,\ell}(Fr_q)$ (cf. [58, VII.2, Theorem 3]). This will turn out to be particularly useful in the case when $A = \mathrm{Jac}(C)$ is the Jacobian of a curve C of genus g defined over K, since one can determine the characteristic polynomial of $\overline{\rho}_{\mathrm{Jac}(C),\ell}(Fr_q)$ by counting the $\mathbf{F}_{q^r}$-valued points of C, for $r = 1, \ldots, g$.

In the case of curves C of genus 2, Le Duff has, using the strategy outlined above, studied the image of the Galois representations attached to the ℓ-torsion of $\mathrm{Jac}(C)$, when Condition (T) in Theorem 5.11 is satisfied. The main result in [60] is the following:

Theorem 5.14 (Le Duff)**.** Let C be a genus 2 curve defined over $\mathbf{Q}$, with bad reduction of type (II) or (IV) at a prime p (according to the notation in [63]). Let Φ_p be the group of connected components of the special fibre of the Néron model of $\mathrm{Jac}(C)$ at p. For each prime ℓ and each prime q of good reduction of C, let $P_{q,\ell}(X) = X^4 + aX^3 + bX^2 + qaX + q^2 \in \mathbf{F}_\ell[X]$ be the characteristic polynomial of the image under $\overline{\rho}_{J(C),\ell}$ of the Frobenius element Fr_q at q and let $Q_{q,\ell}(X) = X^2 + aX + b - 2q \in \mathbf{F}_\ell[X]$, with discriminants Δ_P and Δ_Q respectively.

Then for all primes ℓ not dividing $2pq|\Phi_p|$ and such that Δ_P and Δ_Q are not squares in $\mathbf{F}_\ell$, the image of $\overline{\rho}_{J(C),\ell}$ coincides with $\mathrm{GSp}_4(\mathbf{F}_\ell)$. □

Using this result, Le Duff obtains a realisation of $\mathrm{GSp}_4(\mathbf{F}_\ell)$ as Galois group over $\mathbf{Q}$ for all odd primes ℓ smaller than 500000.

In the more general setting of principally polarised g-dimensional abelian varieties, we state the following result, which will be used in the next chapters.

Theorem 5.15. Let A be a principally polarised g-dimensional abelian variety defined over $\mathbf{Q}$. Assume that there exists a prime p such that the following condition holds:

> (T$_p$) The special fibre of the Néron model of A over $\mathbf{Q}_p$ is semistable with toric dimension 1.

Denote by Φ_p the group of connected components of the special fibre of the Néron model at p. Let q be a prime of good reduction of A, let A_q be the special fibre of the Néron model of A over $\mathbf{Q}_q$ and let $P_q(X) = X^{2g} + aX^{2g-1} + \cdots + q^g \in \mathbf{Z}[X]$ be the characteristic polynomial of the Frobenius endomorphism Fr_q acting on A_q.

Then for all primes ℓ which do not divide $6pq|\Phi_p|a$ and such that the reduction of $P_q(X)$ mod ℓ is irreducible in $\mathbf{F}_\ell$, the image of $\overline{\rho}_{A,\ell}$ coincides with $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$.

Proof. Since A satisfies (T) at $p \neq \ell$, and $\ell \nmid |\Phi_p|$, Theorem 5.11 (or alternatively, [60, Proposition 1.3]) implies that $\mathrm{Im}(\overline{\rho}_{A,\ell})$ contains a nontrivial transvection.

From the fact that $\ell \nmid a$ and $P_q(X)$ is irreducible modulo ℓ (and $\ell \neq q$), we see that $\overline{\rho}_{A,\ell}(Fr_q)$ is an element whose characteristic polynomial is irreducible and which has nonzero trace.

Moreover, since $\ell \neq 6$, we must have $\ell \geq 5$. Therefore, we may apply Corollary 5.6 and conclude that $\overline{\rho}_{A,\ell}$ is surjective. □

Remark 5.16. The condition that ℓ does not divide a corresponds to the Frobenius element having nonzero trace modulo ℓ. The theorem is vacuous when $a = 0$.

Remark 5.17. Consider a family of genus g hyperelliptic curves C_t defined over $\mathbf{Q}(t)$ with big monodromy at ℓ, meaning that the image of the Galois representation attached to the ℓ-torsion of a generic point of the family is $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$. Then Hilbert's Irreducibility Theorem provides us with infinitely many specialisations $t = t_0 \in \mathbf{Q}$ such that the Jacobian Jac_{t_0} of the corresponding curve C_{t_0} satisfies that $\mathrm{Im}\overline{\rho}_{\mathrm{Jac}_{t_0},\ell} \simeq \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$. Such families of curves C_{t_0} exist for any odd ℓ (see e.g. [37] or [131]). In particular, for any $g \in \mathbf{N}$ and any odd ℓ, the Inverse Galois Problem has an affirmative answer for the group $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$. Although ensuring the existence of the desired curve, this fact does not tell us how to find such a curve explicitly.

5.4 Semistable curves and their generalised Jacobians

In this section we recall some geometric notions that will be used in Chapter 7.

A curve C over a field k is said to be *semistable* if the curve $C_{\overline{k}} = C \times_k \overline{k}$ is reduced and has at most ordinary double points as singularities. It is said to be *stable* if moreover $C_{\overline{k}}$ is connected, projective of arithmetic genus ≥ 2, and if any irreducible component of $C_{\overline{k}}$ isomorphic to $\mathbf{P}^1_{\overline{k}}$ intersects the other irreducible components in at least three points. A proper flat morphism of schemes $\mathscr{C} \to S$ is said to be *semistable* (resp. *stable*) if it has semistable (resp. stable) geometric fibres.

Let R be a discrete valuation ring with fraction field K and residue field k. Let C be a smooth projective geometrically connected curve over K. A *model* of C over R is a normal scheme $\mathscr{C}/R$ such that $\mathscr{C} \times_R K \cong C$. We say that C has *semistable reduction* (resp. *stable reduction*) if C has a model $\mathscr{C}$ over R which is a semistable (resp. stable) scheme over R. If such a stable model exists, it is unique up to isomorphism and we call it *the stable model of C over R* (cf. [64, Chap.10, Definition 3.27 and Theorem 3.34]). If the curve C has genus $g \geq 1$, then it admits a minimal regular model $\mathscr{C}_{\min}$ over R, unique up to unique isomorphism. Moreover, $\mathscr{C}_{\min}$ is semistable if and only if C has semistable reduction, and if $g \geq 2$, this is equivalent to C having stable reduction (cf. [64, Chap. 10, Theorem 3.34], or [93, Theorem 3.1.1] when R is strictly henselian).

Assume that C is a smooth projective geometrically connected curve of genus $g \geq 2$ over K with semistable reduction. Denote by $\mathscr{C}$ its stable model over R and by $\mathscr{C}_{\min}$ its minimal regular model over R. We know that the Jacobian variety $\mathrm{Jac}(C)$ of C admits a Néron model $\mathscr{J}$ over R and the canonical morphism $\mathrm{Pic}^0_{\mathscr{C}/R} \to \mathscr{J}^0$ is an isomorphism (cf. [18, §9.7, Corollary 2]). Note that since $\mathscr{C}_{\min}$ is also semistable, we have $\mathrm{Pic}^0_{\mathscr{C}_{\min}/R} \cong \mathscr{J}^0$. Moreover, the abelian variety $\mathrm{Jac}(C)$ has semistable reduction, that is to say, $\mathscr{J}^0_k \cong \mathrm{Pic}^0_{\mathscr{C}_k/k}$ is canonically an extension of an abelian variety by a torus T. As we will see, the structure of the algebraic group $\mathscr{J}_k^0$ (by which we mean the toric dimension and the order of the component group of its geometric special fibre) is related to the intersection graphs of $\mathscr{C}_{\overline{k}}$ and $\mathscr{C}_{\min,\overline{k}}$.

Let X be a curve over $\overline{k}$. Consider the *intersection graph* (or *dual graph*) $\Gamma(X)$, defined as the graph whose vertices are the irreducible components of X, where two irreducible components X_i and X_j are connected by as many edges as there are irreducible components in the intersection $X_i \cap X_j$. In particular, if the curve X is semistable, two components X_i and X_j are connected by one edge if there is a singular point lying on both X_i and X_j. Here $X_i = X_j$ is allowed. The *(intersection) graph without loops*, denoted by $\Gamma'(X)$, is the graph obtained by removing from $\Gamma(X)$ the edges corresponding to $X_i = X_j$.

Next, we paraphrase [18, §9.2, Example 8], which gives the toric rank in terms of the cohomology of the graph $\Gamma(\mathscr{C}_{\overline{k}})$.

Proposition 5.18. [18, §9.2, Ex. 8] The Néron model $\mathscr{J}_k^0$ of the Jacobian of the curve $\mathscr{C}_k$ has semistable reduction. More precisely, let $X_1, \ldots, X_r$ be the irreducible components of $\mathscr{C}_k$, and let $\widetilde{X}_1, \ldots, \widetilde{X}_r$ be their respective normalisations. Then the canonical extension associated to $\mathrm{Pic}^0_{\mathscr{C}_k/k}$ is given by the exact sequence

$$1 \longrightarrow T \hookrightarrow \mathrm{Pic}^0_{\mathscr{C}_k/k} \xrightarrow{\pi^*} \prod_{i=1}^{r} \mathrm{Pic}^0_{\widetilde{X}_i/k} \longrightarrow 1$$

where the morphism π^* is induced by the morphisms $\pi_i : \widetilde{X}_i \longrightarrow X_i$. The dimension of the torus T is equal to the rank of the cohomology group $H^1(\Gamma(\mathscr{C}_{\overline{k}}), \mathbf{Z})$. □

We will use the preceding result in Sections 7.3 and 7.4. Note that the toric rank does not change if we replace $\mathscr{C}$ by $\mathscr{C}_{\min}$.

The intersection graph of $\mathscr{C}_{\min,\overline{k}}$ also determines the order of the component group of the geometric special fibre $\mathscr{J}_{\overline{k}}$. Indeed, the scheme $\mathscr{C}_{\min} \times R^{\mathrm{sh}}$, where R^{sh} is the strict henselisation of R, fits the hypotheses of [18, §9.6, Proposition 10] which gives the order of the component group in terms of the graph of $\mathscr{C}_{\min,\overline{k}}$; we will use this result in the proof of Proposition 7.4.

Proposition 5.19. [18, §9.6, Prop. 10] Let X be a proper and flat curve over a strictly henselian discrete valuation ring R with algebraically closed residue field $\overline{k}$. Suppose that X is regular and has a geometrically irreducible generic fibre as well as a geometrically reduced special fibre $X_{\overline{k}}$. Assume that $X_{\overline{k}}$ consists of the irreducible components $X_1, \ldots, X_r$ and that the local intersection numbers of the X_i are 0 or 1 (the latter is the case if different components intersect at ordinary double points). Furthermore, assume that the intersection graph $\Gamma'(X_{\overline{k}})$ consists of l arcs of edges

$\lambda_1, \ldots, \lambda_l$, starting at X_1 and ending at X_r, each arc λ_i consisting of m_i edges, as in the example depicted in Figure 5.1. Then the component group $\mathscr{J}(R^{\mathrm{sh}})/\mathscr{J}^0(R^{\mathrm{sh}})$ has order $\sum_{i=1}^{l} \prod_{j \neq i} m_j$. □

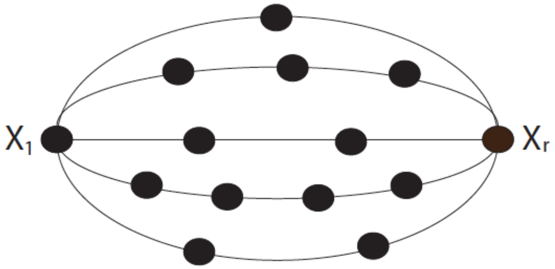


Figure 5.1: Intersection graph $\Gamma'(X_{\overline{k}})$ with 5 arcs and $\{m_i\} = \{2, 3, 3, 4, 5\}$.

CHAPTER 6

Algorithm for Galois realisations of $\mathrm{GSp}_{2n}(\mathbf{F}_\ell)$

Let C be a hyperelliptic curve of genus g over $\mathbf{Q}$, defined by an equation $Y^2 = f(X)$ where $f(X) \in \mathbf{Q}[X]$ is a polynomial of degree $2g+1$. Let $A = \mathrm{Jac}(C)$ be its Jacobian variety. We assume that A satisfies condition (T_p) from Theorem 5.11 for some prime p.

In this chapter we present an algorithm, based on Theorem 5.15, which computes a finite set of prime numbers ℓ for which the Galois representation $\overline{\rho}_{A,\ell}$ has image $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$. We apply this procedure to an example of a genus 3 a curve using a computer algebra system.

6.1 Strategy

First, to apply Theorem 5.15, we restrict ourselves to hyperelliptic curves of genus g whose Jacobian varieties satisfy Condition (T_p) for some p. Namely, we fix a prime number p and then choose $f(X) \in \mathbf{Z}[X]$ monic of degree $2g+1$ such that both of the following conditions hold:

1. The polynomial $f(X)$ only has simple roots over $\overline{\mathbf{Q}}$, so that $Y^2 = f(X)$ is the equation of an hyperelliptic curve C over $\mathbf{Q}$.

2. All coefficients of $f(X)$ have p-adic valuation greater than or equal to zero, and the reduction $f(X) \bmod p$ has one double root in $\overline{\mathbf{F}}_p$, and its other zeroes are simple.

This ensures that $A = \mathrm{Jac}(C)$ satisfies Condition (T_p), by Proposition 5.12.

Any prime of good reduction for C is also a prime of good reduction for its Jacobian A. Primes of good reduction for the hyperelliptic curve can be computed using the discriminant of Weierstrass equations for C (see [66]). In our case, any prime not dividing the discriminant of $f(X)$ is of good reduction for C, hence for A.

This chapter is based on results from the article [14], joint work with Sara Arias-de-Reyna, Cécile Armana, Marusia Rebolledo, Lara Thomas and Núria Vila.

We take such a prime number q of good reduction for A. Recall that $P_q(X) \in \mathbf{Z}[X]$ is the characteristic polynomial of the Frobenius endomorphism acting on the fibre A_q.

Let $\mathscr{S}_q$ denote the set of prime numbers ℓ satisfying the following conditions:

(i) ℓ divides neither $6pq|\Phi_p|$ nor the coefficient of X^{2g-1} in $P_q(X)$,

(ii) the reduction of $P_q(X)$ modulo ℓ is irreducible in $\mathbf{F}_\ell$.

Note that if the coefficient of X^{2g-1} in $P_q(X)$ is nonzero, condition (i) rules out only finitely many prime numbers ℓ, whereas if it vanishes, condition (i) rules out all prime numbers ℓ. By Theorem 5.15, for each $\ell \in \mathscr{S}_q$ the representation $\overline{\rho}_{A,\ell}$ is surjective with image $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$. Also, primes in $\mathscr{S}_q$ can be computed effectively up to a given fixed bound.

Since we want the polynomial $P_q(X)$ (of degree $2g$) to be irreducible modulo ℓ, its Galois group G over $\mathbf{Q}$ must be a transitive subgroup of S_{2g} with a $2g$-cycle. Therefore, by an application of a weaker version of the Chebotarev density theorem due to Frobenius ([111], “Theorem of Frobenius”, p. 32), the density of $\mathscr{S}_q$ is

$$\frac{\#\{\sigma \in G \subset S_{2g} \colon \sigma \text{ is a } 2n\text{-cycle}\}}{\#G}.$$

This estimate is far from what Theorem 5.11 provides us, namely that the density of primes ℓ with $\mathrm{Im}(\overline{\rho}_{A,\ell}) = \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ is 1.

This leads us to discuss the role of the prime q. First of all, we can see that

$$\bigcup_q \mathscr{S}_q = \{\ell \text{ prime} \colon \ell \nmid 6p|\Phi_p| \text{ and } \overline{\rho}_{A,\ell} \text{ surjective}\},$$

where the union is taken over all primes q of good reduction for A. Note that the inclusion $\subset$ follows directly from Theorem 5.15. To show the other inclusion $\supset$, suppose now that $\ell \nmid 6p|\Phi_p|$ and that the representation at ℓ is surjective. Its image $\mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ contains an element with irreducible characteristic polynomial and nonzero trace (see for instance Proposition A.2 of [8]). This element defines a conjugacy class $C \subset \mathrm{GSp}_{2g}(\mathbf{F}_\ell)$ and the Chebotarev density theorem ensures that there exists q such that $\overline{\rho}_{A,\ell}(Fr_q) \in C$, hence $\ell \in \mathscr{S}_q$.

Moreover, if, for some fixed ℓ, the events “ℓ belongs to $\mathscr{S}_q$” are independent as q varies, the density of primes ℓ for which $\overline{\rho}_{A,\ell}$ is surjective will increase when we take several different primes q. A sufficient condition for this density to tend to 1 is that there exists an infinite family of primes q for which the splitting fields of $P_q(X)$ are pairwise linearly disjoint over $\mathbf{Q}$.

Therefore, it seems reasonable to expect that computing the sets $\mathscr{S}_q$ for several values of q increases the density of primes ℓ for which we know the surjectivity of $\overline{\rho}_{A,\ell}$. This is what we observe numerically in the next example.

6.2 A numerical example in genus 3

All computations in this section were done in MAGMA [19].
We consider the hyperelliptic genus 3 curve C over $\mathbf{Q}$ defined by $Y^2 = f(X)$, where

$$f(X) = X^2(X-1)(X+1)(X-2)(X+2)(X-3) + 7(X-28) \in \mathbf{Z}[X].$$

This is a Weierstrass equation, which is minimal at all primes ℓ different from 2 (see [66, Lemma 2.3]), with discriminant $-2^{12} \cdot 7 \cdot 73 \cdot 1069421 \cdot 11735871491$. Thus, C has good reduction away from the primes appearing in this factorization. Clearly, $p = 7$ is a prime for which the reduction of $f(X)$ modulo 7 has one double zero in $\overline{\mathbf{F}}_7$ and otherwise only simple zeroes. Therefore, its Jacobian $\mathrm{Jac}(C)$ satisfies Condition (T_7). The order of the component group Φ_7 is 2. Recall that $P_q(X)$ coincides with the characteristic polynomial of the Frobenius endomorphism of the reduced curve C modulo q over $\mathbf{F}_q$.

Our method provides no significant result for $q \in \{3, 5\}$ because for $q = 3$ the characteristic polynomial $P_q(X)$ is not irreducible in $\mathbf{Z}[X]$ and for $q = 5$ it has zero trace in $\mathbf{Z}$. So in this example, we first take $q = 11$. The curve has $11, 135$ and 1247 points over $\mathbf{F}_{11}$, $\mathbf{F}_{11^2}$ and $\mathbf{F}_{11^3}$, respectively. The characteristic polynomial $P_{11}(X)$ is

$$P_{11}(X) = X^6 - X^5 + 7X^4 - 35X^3 + 77X^2 - 121X + 1331$$

and it is irreducible over $\mathbf{Q}$. Its Galois group G has order 48 and is isomorphic to the wreath product $S_2 \wr S_3$. This group is the direct product of 3 copies of S_2, on which S_3 acts by permutation (see [51, Chapter 4]): an element of $S_2 \wr S_3$ can be written as $((a_1, a_2, a_3), \sigma)$, where (a_1, a_2, a_3) denotes an element of the direct product $S_2 \times S_2 \times S_2$ and σ an element of S_3. The group law is defined as follows:

$$((a_1, a_2, a_3), \sigma)((a_1', a_2', a_3'), \sigma') = ((a_1, a_2, a_3)(a_1', a_2', a_3')^\sigma, \sigma\sigma'),$$

where $(a_1', a_2', a_3')^\sigma = (a_{\sigma(1)}', a_{\sigma(2)}', a_{\sigma(3)}')$. One can also view the wreath product $S_2 \wr S_3$ as the centralizer of $(12)(34)(56)$ in S_6, through an embedding $\psi : S_2 \wr S_3 \to S_6$ whose image is isomorphic to the so-called Weyl group of type B_3 ([51, 4.1.18 and 4.1.33]). More precisely, under ψ, the image of an element $((a_1, a_2, a_3), \sigma) \in S_2 \wr S_3$ is the permutation of S_6 that acts on $\{1, 2, ..., 6\}$ as follows: it first permutes the elements of the sets $E_1 = \{1, 2\}$, $E_2 = \{3, 4\}$ and $E_3 = \{5, 6\}$ separately, according to a_1, a_2 and a_3 respectively (identifying E_2, E_3 with $\{1,2\}$ in an obvious way) and then permutes the pairs E_1, E_2, E_3 according to the action of σ on the indices. For example, denoting $S_2 = \{\mathrm{id}, \tau\}$, the image under ψ of $((\tau, \mathrm{id}, \mathrm{id}), (123))$ is the 6-cycle (135246).

Let us now determine the elements of $S_2 \wr S_3$ which map to 6-cycles in S_6 through the embedding ψ. For an element in $S_2 \wr S_3$ to be of order 6, it has to be of the form $((a_1, a_2, a_3), \gamma)$ with γ a 3-cycle in S_3. Now, ψ sends an element $((a_1, a_2, a_3), \gamma)$ where either one or three a_i's are id, to a product of two disjoint 3-cycles in S_6. So the elements of $S_2 \wr S_3$ which are 6-cycles in S_6 are among the eight elements $((\mathrm{id}, \mathrm{id}, \tau), \gamma)$, $((\mathrm{id}, \tau, \mathrm{id}), \gamma)$, $((\tau, \mathrm{id}, \mathrm{id}), \gamma)$ and $((\tau, \tau, \tau), \gamma)$ with $\gamma = (123)$ or $\gamma = (132)$. Moreover, [51, Theorem 4.2.8] (see also [36, Lemma 3.1] or [116]) ensures that these 8 elements are conjugate. Since $\psi((\tau, \mathrm{id}, \mathrm{id}), (123)) = (135246)$ is a 6-cycle, we deduce that the 8 elements listed above are exactly the elements of $S_2 \wr S_3$ which are 6-cycles in S_6.

To conclude, the Galois group G, viewed as a subgroup of S_6, contains exactly 8 elements that are 6-cycles. Therefore, the density of $\mathscr{S}_{11}$ is $8/48 = 1/6$.

We can compute $P_q(X)$ using efficient algorithms available in MAGMA [19] or SAGE [110], which are based on p-adic methods. We found that there are 6891 prime numbers $11 \leq \ell \leq 500000$ that belong to $\mathscr{S}_{11}$. For these ℓ, we know that the image of $\overline{\rho}_{A,\ell}$ is $\mathrm{GSp}_6(\mathbf{F}_\ell)$, so the groups $\mathrm{GSp}_6(\mathbf{F}_\ell)$ are realised as Galois groups arising from the ℓ-torsion of the Jacobian of the hyperelliptic curve C. For instance, the first ten elements of $\mathscr{S}_{11}$ are

$$47, 71, 79, 83, 101, 113, 137, 251, 269, 271.$$

Also, the proportion of prime numbers $11 \leq \ell \leq 500000$ in $\mathscr{S}_{11}$ is about 0.1659, which is quite in accordance with the density obtained from the Chebotarev density theorem.

By looking at polynomials $P_q(X)$ for several primes q of good reduction, we are able to significantly improve the known proportion of primes ℓ, up to a given bound, for which the Galois representation is surjective. Namely, we computed that

$$\{\ell \text{ prime}, 11 \leq \ell \leq 500000\} \subseteq \bigcup_{11 \leq q \leq 571} \mathscr{S}_q.$$

As a consequence, for any prime $11 \leq \ell \leq 500000$, the group $\mathrm{GSp}_6(\mathbf{F}_\ell)$ is realised as a Galois group arising from the ℓ-torsion of the Jacobian of the hyperelliptic curve C. This is reminiscent of Le Duff's numerical data for $\mathrm{GSp}_4(\mathbf{F}_l)$ (see Theorem 5.14).

Combining all of the above suggests that the single hyperelliptic curve C might provide a positive answer to the inverse Galois problem for $\mathrm{GSp}_6(\mathbf{F}_\ell)$ for any prime $\ell \geq 11$.

CHAPTER 7

Constructing Jacobians with large Galois images

In this chapter, our aim is to find auxiliary primes p and q (depending on ℓ), and explicit congruence conditions on polynomials defining genus 3 curves, which ensure that any curve C, defined by an equation over $\mathbf{Z}$ satisfying these congruences, will have the property that the image of $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ coincides with $\mathrm{GSp}_6(\mathbf{F}_\ell)$. In this way we obtain many realisations of $\mathrm{GSp}_6(\mathbf{F}_\ell)$ as a Galois group over $\mathbf{Q}$.

7.1 Hyperelliptic curves and curves of genus 3

In this chapter, a curve over a field K will be an algebraic variety over K whose irreducible components are of dimension 1. In particular, a curve can be singular. A smooth geometrically connected projective curve C of genus $g \geq 1$ over a field K is *hyperelliptic* if there exists a degree 2 finite separable morphism from $C_{\overline{K}} = C \times_K \overline{K}$ to $\mathbf{P}^1_{\overline{K}}$. If K is algebraically closed or a finite field, then such a curve C has a *hyperelliptic equation* defined over K. (When K is not algebraically closed nor a finite field, the situation can be more complicated,cf. [61, Section 4.1].) That is to say, the function field of C is $K(x)[y]$ under the relation $y^2 + h(x)y = g(x)$ with $g(x), h(x) \in K[x]$, $\deg(g(x)) \in \{2g+1, 2g+2\}$, and $\deg(h(x)) \leq g$. Moreover, if $\mathrm{char}(K) \neq 2$, we can take $h(x) = 0$. Indeed, in that case, the conic defined as the quotient of C by the group generated by the hyperelliptic involution has a K-rational point, hence is isomorphic to $\mathbf{P}^1_K$ (see e.g. [61, Section 1.3] for more details). The curve C is the union of the two affine open schemes

$$\begin{aligned} U &= \mathrm{Spec}\left(K[x,y]/(y^2 + h(x)y - g(x))\right) \quad \text{and} \\ V &= \mathrm{Spec}\left(K[t,w]/(w^2 + t^{g+1}h(1/t)y - t^{2g+2}g(1/t))\right) \end{aligned}$$

glued along $\mathrm{Spec}(K[x,y,1/x]/(y^2 + h(x)y - g(x)))$ via the identifications $x = 1/t, y = t^{-g-1}w$.

If $\mathrm{char}(K) \neq 2$, then any separable polynomial $g(x) \in K[x]$ of degree $2g+1$ or $2g+2$ gives rise to a hyperelliptic curve C of genus g defined over K by glueing

This chapter is based on results from the article [4], joint work with Sara Arias-de-Reyna, Cécile Armana, Marusia Rebolledo, Lara Thomas and Núria Vila.

the open affine schemes U and V (with $h(x) = 0$) as above. We will say that C is *given by the hyperelliptic equation* $y^2 = g(x)$. We will also say that a polynomial in two variables is of *g-hyperelliptic type* if it is of the form $y^2 - g(x)$ with $g(x)$ a polynomial of degree $2g + 1$ or $2g + 2$.

If C is a smooth geometrically connected projective non-hyperelliptic curve of genus 3 defined over a field K, then its canonical embedding $C \hookrightarrow \mathbf{P}^2_K$ identifies C with a smooth plane quartic curve defined over K. This means that the curve C has a model over K given by $\mathrm{Proj}(K[X,Y,Z]/F(X,Y,Z))$ where $F(X,Y,Z)$ is a degree 4 homogeneous polynomial with coefficients in K. Conversely, any smooth plane quartic curve is the image by a canonical embedding of a non-hyperelliptic curve of genus 3. If this curve is $\mathrm{Proj}(K[X,Y,Z]/F(X,Y,Z))$ where $F(X,Y,Z)$ is the homogenisation of a degree 4 polynomial $f(x,y) \in K[x,y]$, we will say that C is the *quartic plane curve defined by the affine equation* $f(x,y) = 0$. We will say that a polynomial in two variables is of *quartic type* if its total degree is 4.

7.2 Statement of main result

We now use the notation from Section 7.1 to state the main theorem of this chapter.

Theorem 7.1. Let $\ell \geq 13$ be a prime number. For all odd distinct prime numbers $p, q \neq \ell$, with $q > 1.82\ell^2$, there exist polynomials $f_p(x,y), f_q(x,y) \in \mathbf{Z}[x,y]$, both of the same type (3-hyperelliptic or quartic), such that for any $f(x,y) \in \mathbf{Z}[x,y]$ of the same type as $f_p(x,y)$ and $f_q(x,y)$ and satisfying

$$f(x,y) \equiv f_q(x,y) \pmod{q} \quad \text{and} \quad f(x,y) \equiv f_p(x,y) \pmod{p^3},$$

the image of the Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the ℓ-torsion points of the Jacobian of the smooth projective genus 3 curve C defined over $\mathbf{Q}$ by the equation $f(x,y) = 0$ is $\mathrm{GSp}_6(\mathbf{F}_\ell)$.

Moreover, for $\ell \in \{5, 7, 11\}$ there exists a prime number $q \neq \ell$ for which the same statement holds for each odd prime number $p \neq q, \ell$.

In Section 7.5 we state and prove a refinement of this Theorem (cf. Theorem 7.12). In fact, the polynomial $f_p(x,y)$ will be of a very specific form. In general we can say little about $f_q(x,y)$, but for any fixed $\ell \geq 13$ and any fixed $q \geq 1.82\ell^2$ we can find suitable polynomials $f_q(x,y)$ by an exhaustive search as follows: there exist only finitely many polynomials $\overline{f}_q(x,y) \in \mathbf{F}_q[x,y]$ of 3-hyperelliptic or quartic type with nonzero discriminant. For each of these, we can compute the characteristic polynomial of the action of the Frobenius endomorphism on the Jacobian of the curve defined by $\overline{f}_q(x,y) = 0$ by counting the $\mathbf{F}_{q^r}$-points of this curve, for $r = 1, 2, 3$, and check whether this polynomial is an ordinary q-Weil polynomial with nonzero middle coefficient, nonzero trace modulo ℓ, and which is irreducible modulo ℓ. Proposition 7.9 ensures that for one of the finitely many $\overline{f}_q(x,y)$ this is indeed the case. Then, any lift of $\overline{f}_q(x,y)$, of the same type (since we lift the coefficients of the polynomial), gives us a suitable polynomial $f_q(x,y) \in \mathbf{Z}[x,y]$.

Note that the above result constitutes an explicit version (for 3-dimensional varieties) of Proposition 4.6 of [8], which proves the existence of a bound ℓ_0 such that for all $\ell \geq \ell_0$ there exists a principally polarised abelian variety with surjective ℓ-torsion Galois representation. We can explicitly give the size of the p-adic and q-adic neighbourhoods where surjectivity of $\overline{\rho}_{A,\ell}$ is preserved; in other words, we can give the powers of the auxiliary primes p and q such that any other curve defined by congruence conditions modulo these powers gives rise to a Jacobian variety with surjective ℓ-torsion representation.

7.3 Local conditions at p

Let $p > 2$ be a prime number.

Definition 7.2. Let $f(x,y) \in \mathbf{Z}_p[x,y]$ be a polynomial with $f(0,0) = 0$ or $v_p(f(0,0)) > 2$. We say that $f(x,y)$ is of type:

(H) if $f(x,y) = y^2 - g(x)$, where $g(x) \in \mathbf{Z}_p[x]$ is of degree 7 or 8 and such that

$$g(x) \equiv x(x-p)m(x) \bmod p^2\mathbf{Z}_p[x],$$

with $m(x) \in \mathbf{Z}_p[x]$ such that its mod p reduction has simple nonzero roots in $\mathbf{F}_p$;

(Q) if $f(x,y)$ is of total degree 4 and such that

$$f(x,y) \equiv px + x^2 - y^2 + x^4 + y^4 \bmod p^2\mathbf{Z}_p[x,y].$$

For $f(x,y) \in \mathbf{Z}_p[x,y]$ a polynomial of type (H) or (Q), we will consider the projective curve C defined by $f(x,y) = 0$ as explained in Section 7.1 and the scheme $\mathscr{C}$ over $\mathbf{Z}_p$ defined, for each case of Definition 7.2 respectively, as follows:

(H) the union of the two affine subschemes

$$U = \mathrm{Spec}(\mathbf{Z}_p[x,y]/(y^2 - g(x))) \text{ and } V = \mathrm{Spec}(\mathbf{Z}_p[t,w]/(w^2 - g(1/t)t^8))$$

glued along $\mathrm{Spec}(\mathbf{Z}_p[x,y,1/x]/(y^2 - g(x)))$ via $x = 1/t, y = t^{-4}w$;

(Q) the scheme $\operatorname{Proj}(\mathbf{Z}_p[X,Y,Z]/(F(X,Y,Z)))$, where $F(X,Y,Z)$ is the homogenisation of $f(x,y)$.

This scheme has generic fibre C.

Proposition 7.3. Let $f(x,y) \in \mathbf{Z}_p[x,y]$ be a polynomial of type (H) or (Q) and let C be the projective curve defined by $f(x,y) = 0$. The curve C is a smooth projective and geometrically connected curve of genus 3 over $\mathbf{Q}_p$ with stable reduction. Moreover, the scheme $\mathscr{C}$ is the stable model of C over $\mathbf{Z}_p$ and the stable reduction is geometrically integral with exactly one singularity, which is an ordinary double point.

Proof. With the description we gave in Section 7.1 of what we called the *projective curve defined by f*, smoothness over $\mathbf{Q}_p$ follows from the Jacobian criterion. This implies that C is a projective curve of genus 3.

The polynomials defining the affine schemes U and V and the quartic polynomial $F(X,Y,Z)$ are all irreducible over $\overline{\mathbf{Q}}_p$, hence over $\mathbf{Z}_p$. So the curve C is geometrically integral (hence geometrically irreducible and geometrically connected) and $\mathscr{C}$ is integral as a scheme over $\mathbf{Z}_p$. It follows in particular that $\mathscr{C}$ is flat over $\mathbf{Z}_p$ (cf. [64, Chap. 4, Corollary 3.10]). Hence, $\mathscr{C}$ is a model of C over $\mathbf{Z}_p$.

We will show that $\mathscr{C}_{\mathbf{F}_p}$ is semistable (i.e. reduced with only ordinary double points as singularities) with exactly one singularity.

Combined with flatness, semistability will imply that the scheme $\mathscr{C}$ is semistable over $\mathbf{Z}_p$. Since C has genus greater than 2, and $C = \mathscr{C}_{\mathbf{Q}_p}$ is smooth and geometrically connected, this is then equivalent to saying that C has stable reduction at p with stable model $\mathscr{C}$, as required (cf. [93, Theorem 3.1.1]).

In what follows, we denote by $\overline{\ }$ the reduction modulo p of any polynomial with coefficient in $\mathbf{Z}_p$. In Case (H), $\mathscr{C}_{\overline{\mathbf{F}}_p}$ is the union of the two affine subschemes

$$U' = \operatorname{Spec}(\overline{\mathbf{F}}_p[x,y]/(y^2 - x^2\overline{m}(x))) \text{ and } V' = \operatorname{Spec}(\overline{\mathbf{F}}_p[t,w]/(w^2 - \overline{m}(1/t)t^6)),$$

glued along $\operatorname{Spec}(\overline{\mathbf{F}}_p[x,y,1/x]/(y^2 - \overline{g}(x))$ via $x = 1/t$ and $y = t^{-4}w$ (cf. [64, Chap. 10, Example 3.5]). In Case (Q), the geometric special fibre is

$$\operatorname{Proj}(\overline{\mathbf{F}}_p[X,Y,Z]/(\overline{F}(X,Y,Z))).$$

In both cases, the defining polynomials are irreducible over $\overline{\mathbf{F}}_p$. Hence, $\mathscr{C}_{\overline{\mathbf{F}}_p}$ is integral, i.e. reduced and irreducible.

Next, we prove that $\mathscr{C}_{\overline{\mathbf{F}}_p}$ has only one ordinary double point as singularity. For Case (H), see e.g. [64, Chap. 10, Examples 3.4, 3.5 and 3.29]. For Case (Q), we proceed analogously: first consider the open affine subscheme of $\mathscr{C}_{\overline{\mathbf{F}}_p}$ defined by $U = \operatorname{Spec}(\overline{\mathbf{F}}_p[x,y]/\overline{f}(x,y))$, where $\overline{f}(x,y) = x^2 - y^2 + x^4 + y^4 \in \mathbf{F}_p[x,y]$. Since

$\mathscr{C}_{\overline{\mathbf{F}}_p} \backslash U$ is smooth, it suffices to prove that U has only ordinary double singularities. Let $u \in U$. The Jacobian criterion shows that U is smooth at $u \neq (0,0)$. So suppose that $u = (0,0)$, and note that $\overline{f}(x,y) = x^2(1+x^2) - y^2(1-y^2)$. Since $2 \in \overline{\mathbf{F}}_p^\times$, there exist $a(x) = 1 + xc(x) \in \overline{\mathbf{F}}_p[[x]]$ and $b(y) = 1 + yd(y) \in \overline{\mathbf{F}}_p[[y]]$ such that $1 + x^2 = a(x)^2$ and $1 - y^2 = b(y)^2$, by ([64, Chap. 1, Exercise 3.9]). Then we have

$$\widehat{\mathscr{O}}_{U,u} \cong \overline{\mathbf{F}}_p[[x,y]]/(xa(x) + yb(y))(xa(x) - yb(y)) \cong \overline{\mathbf{F}}_p[[t,w]]/(tw).$$

It follows that $\mathscr{C}_{\overline{\mathbf{F}}_p}$ has only one singularity (at $[0:0:1]$) which is an ordinary double singularity. We have thus showed that $\mathscr{C}$ is the stable model of C over $\mathbf{Z}_p$ and that its special fibre is geometrically integral and has only one ordinary double singularity. □

Proposition 7.4. Let $f(x,y) \in \mathbf{Z}_p[x,y]$ be a polynomial of type (H) or (Q) and let C be the projective curve defined by $f(x,y) = 0$. The Jacobian variety $\mathrm{Jac}(C)$ of the curve C has a Néron model $\mathscr{J}$ over $\mathbf{Z}_p$ which has semi-abelian reduction of toric rank 1. The component group of the geometric special fibre of $\mathscr{J}$ over $\overline{\mathbf{F}}_p$ has order 2.

Proof. By Proposition 7.3, the curve C is a smooth projective geometrically connected curve of genus 3 over $\mathbf{Q}_p$ with stable reduction and stable model $\mathscr{C}$ over $\mathbf{Z}_p$. Let $\mathscr{C}_{\min}$ be the minimal regular model of C. As recalled in Section 5.4, $\mathrm{Jac}(C)$ admits a Néron model $\mathscr{J}$ over $\mathbf{Z}_p$ and the canonical morphism $\mathrm{Pic}^0_{\mathscr{C}/\mathbf{Z}_p} \to \mathscr{J}^0$ is an isomorphism. In particular, $\mathscr{J}$ has semi-abelian reduction and $\mathscr{J}^0_{\mathbf{F}_p} \cong \mathrm{Pic}^0_{\mathscr{C}_{\mathbf{F}_p}/\mathbf{F}_p}$. Since $\mathscr{C}_{\min}$ is also semistable, we have $\mathrm{Pic}^0_{\mathscr{C}_{\min}/S} \cong \mathscr{J}^0$.

By Proposition 5.18, the toric rank of $\mathscr{J}^0_{\overline{\mathbf{F}}_p}$ is equal to the rank of the cohomology group of the dual graph of $\mathscr{C}_{\overline{\mathbf{F}}_p}$. Since $\mathscr{C}_{\overline{\mathbf{F}}_p}$ is irreducible and has only one ordinary double point, the dual graph consists of one vertex and one loop, so the rank of $\mathscr{J}^0_{\overline{\mathbf{F}}_p}$ is 1.

To determine the order of the component group of the geometric special fibre $\mathscr{J}_{\overline{\mathbf{F}}_p}$, we apply Proposition 5.19 to the minimal regular model $\mathscr{C}_{\min} \times \mathbf{Z}_p^{\mathrm{sh}}$, where $\mathbf{Z}_p^{\mathrm{sh}}$ is the strict henselisation of $\mathbf{Z}_p$. This is still regular and semistable over $\mathbf{Z}_p^{\mathrm{sh}}$ (cf. [64, Chap. 10, Proposition 3.15-(a)]). Let e denote the thickness of the ordinary double point of $\mathscr{C}_{\overline{\mathbf{F}}_p}$ (as defined in [64, Chap. 10, Definition3.23]). Then by [64, Chap. 10, Corollary 3.25], the geometric special fibre $\mathscr{C}_{\min,\overline{\mathbf{F}}_p}$ of $\mathscr{C}_{\min} \times \mathbf{Z}_p^{\mathrm{sh}}$ consists of a chain of $e-1$ projective lines over $\mathbf{F}_p$ and one component of genus 2 (where the latter corresponds to the irreducible component $\mathscr{C}_{\overline{\mathbf{F}}_p}$), which meet transversally at rational points. It follows from Proposition 5.18 that the order of the component group $\mathscr{J}(\mathbf{Z}_p^{\mathrm{sh}})/\mathscr{J}^0(\mathbf{Z}_p^{\mathrm{sh}})$ of the geometric special fibre is equal to the thickness e.

We will now show that in both cases (H) and (Q), the thickness e is equal to 2, which will conclude the proof of Proposition 7.4. For this, in several places, we will use the fact that when $p \neq 2$, every formal power series in $\mathbf{Z}_p[[x]]$ (resp. $\mathbf{Z}_p[[y]]$, $\mathbf{Z}_p[[x,y]]$) with constant term 1 (or more generally a unit square in $\mathbf{Z}_p$) is a square in $\mathbf{Z}_p[[x]]$ (resp. $\mathbf{Z}_p[[y]]$, $\mathbf{Z}_p[[x,y]]$) of some invertible formal power series.

Let U denote the affine subscheme $\mathrm{Spec}(\mathbf{Z}_p[x,y]/(f(x,y)))$ which contains the ordinary double point $P = [0:0:1]$. Firstly, we claim that, possibly after a finite extension of scalars $R/\mathbf{Z}_p$ which splits the singularity, in both cases we may write in $R[[x,y]]$:

$$\pm f(x,y) = x^2 a(x)^2 - y^2 b(y)^2 + p\alpha x + p^2 y g(x,y) + p^r \beta \tag{7.1}$$

where $a(x) \in R[[x]]^\times, b(y) \in R[[y]]^\times, g(x,y) \in \mathbf{Z}_p[x,y], \alpha \in \mathbf{Z}_p^\times, \beta \in \mathbf{Z}_p$. Moreover, from the assumptions on f, it follows that either $\beta = 0$, or $\beta \in \mathbf{Z}_p^\times$ and $r = v_p(f(0,0)) > 2$.

We prove the claim case by case:

(H) We have $f(x,y) = y^2 - g(x) = y^2 - x(x-p)m(x) + p^2 h(x)$ for some $h(x) \in \mathbf{Z}_p[x]$. Since $h(x) = h(0) + xs(x)$ for some $s(x) \in \mathbf{Z}_p[x]$ and $m(x) + ps(x) = m(0) + ps(0) + xt(x)$ for some $t(x) \in \mathbf{Z}_p[x]$, we obtain

$$\begin{aligned} f(x,y) &= y^2 - x^2 m(x) + px(m(x) + ps(x)) + p^2 h(0) \\ &= y^2 - x^2(m(x) - pt(x)) + px(m(0) + ps(0)) + p^2 h(0). \end{aligned}$$

Since $m(0) \not\equiv 0 \pmod p$, we have $m(0) - pt(0) \in \mathbf{Z}_p^\times$, hence if we extend the scalars to some finite extension R over $\mathbf{Z}_p$, in which $m(0) - pt(0)$ is a square, we get that $(m(x) - pt(x))$ is a square of some $a(x)$ in $R[[x]]^\times$. Then $-f(x,y)$ has the expected form. Note that $R/\mathbf{Z}_p$ is unramified because $p \neq 2$ and $m(0) \not\equiv 0 \pmod p$, so we still denote the ideal of R above $p \in \mathbf{Z}_p$ by p.

(Q) We have $f(x,y) = x^4 + y^4 + x^2 - y^2 + px + p^2 h(x,y)$ for some choice of $h(x,y) \in \mathbf{Z}_p[x,y]$. We may write $h(x,y) = \delta + x\gamma + x^2 s(x) + yt(x,y)$ for some $\gamma, \delta \in \mathbf{Z}_p$, $s(x) \in \mathbf{Z}_p[x]$ and $t(x,y) \in \mathbf{Z}_p[x,y]$. We obtain

$$\begin{aligned} f(x,y) &= x^2(1+x^2) - y^2(1-y^2) + px + p^2(\delta + x\gamma + x^2 s(x) + yt(x,y)) \\ &= x^2(1 + x^2 + p^2 s(x)) - y^2(1-y^2) + px(1+p\gamma) + p^2 yt(x,y) \\ &\qquad + p^2\delta. \end{aligned}$$

Since $1 + x^2 + p^2 s(x)$ and $1 - y^2$ have constant terms which are squares in $\mathbf{Z}_p^\times$, the formal power series are squares in $\mathbf{Z}_p[[x]]$, resp. $\mathbf{Z}_p[[y]]$. So $f(x,y)$ again has the desired form.

Next, we show that $e = 2$ for $\pm f(x, y)$ of the form (7.1). In $R[[x, y]]$, we have

$$\pm f(x,y) = \left(xa(x) + p\frac{\alpha}{2a(x)}\right)^2 - \left(yb(y) - p^2\frac{g(x,y)}{2b(y)}\right)^2 + p^2c(x,y),$$

where $c(x, y) = p^{r-2}\beta - \frac{\alpha^2}{4a(x)^2} + p^2\frac{g(x,y)^2}{4b(y)^2}$. Since either $\beta = 0$ or $r > 2$ and $\frac{\alpha^2}{4a(0)^2} \not\equiv 0 \pmod p$, the constant term γ of the formal power series $c(x, y)$ belongs to $R^\times$. It follows that $\gamma^{-1}c(x, y)$ is the square of some other formal power series $d(x, y) \in R[[x, y]]^\times$. Defining the variables

$$u = \frac{xa(x)}{d(x,y)} + p\frac{\alpha}{2a(x)d(x,y)} - \frac{yb(y)}{d(x,y)} + p^2\frac{g(x,y)}{2b(y)d(x,y)}$$

and

$$v = \frac{xa(x)}{d(x,y)} + p\frac{\alpha}{2a(x)d(x,y)} + \frac{yb(y)}{d(x,y)} - p^2\frac{g(x,y)}{2b(y)d(x,y)},$$

we get $\widehat{O}_{U\times R,P} \cong R[[u, v]]/(uv \pm p^2\gamma)$. Since $\gamma \in R^\times$, it follows that $e = 2$. □

7.4 Local conditions at q

This section is devoted to the proof of the following key result. In the statement, the two conditions on the characteristic polynomial, namely nonzero trace and irreducibility modulo ℓ, are the ones appearing in Theorem 5.15 which is used to prove the main Theorem 7.1.

For any integer $g \geq 1$, a g-dimensional abelian variety over a finite field k with q elements is called *ordinary* if its group of $\mathrm{char}(k)$-torsion points has rank g over $\overline{k}$.

Theorem 7.5. Let $\ell \geq 13$ be a prime number. For every prime number $q > 1.82\ell^2$, there exists a smooth geometrically connected curve C_q of genus 3 over $\mathbf{F}_q$ whose Jacobian variety $\mathrm{Jac}(C_q)$ is a 3-dimensional ordinary absolutely simple abelian variety such that the characteristic polynomial of its Frobenius endomorphism is irreducible modulo ℓ and has nonzero trace modulo ℓ.

Moreover, for $\ell \in \{3, 5, 7, 11\}$, there exists a prime number $q > 1.82\ell^2$ such that the same statement holds.

First, let us briefly sketch the strategy for proving Theorem 7.5. Honda-Tate theory relates abelian varieties to Weil polynomials (cf. Definition 7.6). Hence, it suffices to prove the existence of an irreducible ordinary Weil q-polynomial of degree 6 (cf. Proposition 7.9), which gives rise to an isogeny class of simple ordinary abelian varieties of dimension 3. By a result of E. Howe (cf. [45, Theorem 1.2]), such an isogeny class contains a principally polarised abelian variety A over $\mathbf{F}_q$, which is the Jacobian variety of some curve C_q defined over $\overline{\mathbf{F}}_q$ by results due to Oort and Ueno. If this abelian variety A is moreover absolutely simple (cf. Proposition 7.7 and 7.8), the curve is geometrically irreducible and we conclude by a Galois descent argument.

Proof of Theorem 7.5.

Step 1: Weil polynomials and Honda-Tate theory

Definition 7.6. A *Weil q-polynomial*, or simply a *Weil polynomial*, is a monic polynomial $P_q(X) \in \mathbf{Z}[X]$ of even degree $2g$ whose complex roots are all *Weil q-numbers*, i.e., algebraic integers with absolute value $\sqrt{q}$ under all of their complex embeddings. Moreover, a Weil q-polynomial is said to be *ordinary* if its middle coefficient is coprime to q.

In particular, for $g = 3$, every Weil q-polynomial of degree 6 is of the form

$$P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3$$

for some integers a, b and c (cf. [45, Proposition 3.4]). Such a Weil polynomial is ordinary if, moreover, c is coprime to q.

Conversely, not every polynomial of this form is a Weil polynomial. However, we will prove in Proposition 7.14 that for $q > 1.82\ell^2$, every polynomial as above with $|a|, |b|, |c| < \ell$ is a Weil q-polynomial.

As an important example, the characteristic polynomial of the Frobenius endomorphism π_A of an abelian variety A over $\mathbf{F}_q$ is a Weil q-polynomial, by the Riemann hypothesis for abelian varieties as proven by Weil [124], or more generally for varieties over finite fields as proven by Deligne [33].

A variant of the Honda-Tate Theorem (cf. [45, Theorem 3.3]) states that the map which sends an ordinary abelian variety over $\mathbf{F}_q$ to the characteristic polynomial of its Frobenius endomorphism induces a bijection between the set of isogeny classes of ordinary abelian varieties of dimension $g \geq 1$ over $\mathbf{F}_q$ and the set of ordinary Weil q-polynomials of degree $2g$. Moreover, under this bijection, isogeny classes of simple ordinary abelian varieties correspond to irreducible ordinary Weil q-polynomials.

Step 2: Assuring absolute simplicity

We now establish whether the Weil q-polynomial determines if the abelian varieties in the isogeny class are absolutely simple.

In [46], Howe and Zhu give a sufficient condition for an abelian variety over a finite field to be absolutely simple; for ordinary varieties, this condition is also necessary. Let A be a simple abelian variety over a finite field, $\pi = \pi_A$ its Frobenius endomorphism and $m_A(X) \in \mathbf{Z}[X]$ the minimal polynomial of π. Since A is simple, the subalgebra $\mathbf{Q}(\pi)$ of $\mathrm{End}(A) \otimes \mathbf{Q}$ is a field; it contains a filtration of subfields $\mathbf{Q}(\pi^d)$ for $d > 1$. If moreover A is ordinary, then the fields $\mathrm{End}(A) \otimes \mathbf{Q} = \mathbf{Q}(\pi)$ and $\mathbf{Q}(\pi^d)$ $(d > 1)$ are all CM-fields, i.e., totally imaginary quadratic extensions of a totally real field. A slight reformulation of Howe and Zhu's criterion is the following (see [46, Proposition 3 and Lemma 5]):

Proposition 7.7 (Howe-Zhu criterion for absolute simplicity)**.** Let A be a simple abelian variety over a finite field k. If $\mathbf{Q}(\pi^d) = \mathbf{Q}(\pi)$ for all integers $d > 0$, then A is absolutely simple. If A is ordinary, then the converse is also true, and if $\mathbf{Q}(\pi^d) \neq \mathbf{Q}(\pi)$ for some $d > 0$, then A splits over the degree d extension of k. Moreover, if $\mathbf{Q}(\pi^d)$ is a proper subfield of $\mathbf{Q}(\pi)$ such that $\mathbf{Q}(\pi^r) = \mathbf{Q}(\pi)$ for all $r < d$, then either $m_A(X) \in \mathbf{Z}[X^d]$, or $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^d, \zeta_d)$ for a primitive d-th root of unity ζ_d. □

From this criterion, Howe and Zhu give elementary conditions for a simple 2-dimensional abelian variety to be absolutely simple, see [46, Theorem 6]. Elaborating on their criterion and inspired by [46, Theorem 6], we prove the following for dimension 3:

Proposition 7.8. Let A be an ordinary simple abelian variety of dimension 3 over a finite field k of odd cardinality q. Then either A is absolutely simple or the characteristic polynomial of the Frobenius endomorphism of A is of the form $X^6 + cX^3 + q^3$ with c coprime to q and A splits over the degree 3 extension of k.

Proof. Let A be an ordinary simple but not absolutely simple abelian variety of dimension 3 over k. Since A is simple, the characteristic polynomial of π is $m_A(X)$. We apply Proposition 7.7 to A: Let d be the smallest integer such that $\mathbf{Q}(\pi^d) \neq \mathbf{Q}(\pi)$. Either $m_A(X) \in \mathbf{Z}[X^d]$ or there exists a d-th root of unity ζ_d such that $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^d, \zeta_d)$.

Suppose that $m_A(X) \in \mathbf{Z}[X^d]$. Since $m_A(X)$ is ordinary, the coefficient of degree 3 is nonzero, and it will follow that $d = 3$ and that $m_A(X)$ has the form $X^6 + cX^3 + q^3$, proving the proposition.

Suppose instead that $m_A(X) \notin \mathbf{Z}[X^d]$; we will prove that this is impossible. The field $K = \mathbf{Q}(\pi) = \mathbf{Q}(\pi^d, \zeta_d)$ is a CM-field of degree 6 over $\mathbf{Q}$, hence its proper CM-subfield $L = \mathbf{Q}(\pi^d)$ has to be a quadratic imaginary field. It follows that $\phi(d) = 3$ or 6, where ϕ denotes the Euler totient function. However, $\phi(d) = 3$ has no solution, so we must have $\phi(d) = 6$, i.e. $d \in \{7, 9, 14, 18\}$, and $K = \mathbf{Q}(\zeta_d)$. Note that $\mathbf{Q}(\zeta_7) = \mathbf{Q}(\zeta_{14})$ and $\mathbf{Q}(\zeta_9) = \mathbf{Q}(\zeta_{18})$, and they contain only one quadratic imaginary field; namely, $\mathbf{Q}(\sqrt{-7})$ for $d = 7$ (resp. 14), and $\mathbf{Q}(\sqrt{-3})$ for $d = 9$ (resp. $d = 18$) (cf. [119]). Let σ be a generator of the (cyclic) group $\mathrm{Gal}(K/L)$ of order 3. In their proof of [46, Lemma 5], Howe and Zhu show that we can choose ζ_d such that $\pi^\sigma = \zeta_d \pi$. Moreover, $\zeta_d^\sigma = \zeta_d^k$ for some integer k (which can be chosen to lie in $[0, d-1]$). Since σ is of order 3, we have $\pi = \pi^{\sigma^3} = \zeta_d^{(k^2+k+1)}\pi$, which gives $k^2 + k + 1 \equiv 0 \pmod{d}$. This rules out the case $d = 9$ and 18, because -3 is neither a square modulo 9 nor a square modulo 18. So $d = 7$ or 14, $K = \mathbf{Q}(\zeta_7)$ and $\mathbf{Q}(\pi^d) = \mathbf{Q}(\sqrt{-7})$. It follows that the characteristic polynomial of π^d, which is of the form

$$X^6 + \alpha X^5 + \beta X^4 + \gamma X^3 + \beta q^d X^2 + \alpha q^{2d} X + q^{3d} \in \mathbf{Z}[X],$$

is the cube of a quadratic polynomial of discriminant -7. This is true if and only if

$$\alpha^2 - 36q^d + 63 = 0, \quad \alpha^2 - 3\beta + 9q^d = 0 \quad \text{and} \quad \alpha^3 - 27\gamma + 54\alpha q^d = 0,$$

that is,

$$\alpha^2 = 9(4q^d - 7), \quad \beta = 3(5q^d - 7) \quad \text{and} \quad 3\gamma = \alpha(10q^d - 7).$$

However, the first equation has no solution in q. Indeed, suppose that $4q^d - 7$ is a square, say u^2 for some integer u. Then u is odd, say $u = 1 + 2t$ for some integer t, hence $4q^d = 8 + 4t(t+1)$, so 2 divides q, which contradicts the hypothesis.

Hence, we obtain that $m_A(X) \in \mathbf{Z}[X^d]$ and Proposition 7.8 follows. □

Step 3: Existence of an irreducible ordinary Weil polynomial

Finally, the proof of Theorem 7.5 further relies on the following proposition, whose proof consists of counting arguments and is postponed to Section 7.6:

Proposition 7.9. For any prime number $\ell \geq 13$ and any prime number $q > 1.82\ell^2$, there exists an ordinary Weil q-polynomial

$$P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3,$$

with $a \not\equiv 0 \pmod{\ell}$, which is irreducible modulo ℓ. For $\ell \in \{3, 5, 7, 11\}$, there exists some prime number $q > 1.82\ell^2$ and an ordinary Weil q-polynomial as above. Moreover, for all $\ell \geq 3$, the coefficients can be chosen such that

$$\{a, b, c\} \subset \mathbf{Z} \cap [-(\ell-1)/2, (\ell-1)/2].$$

Remark 7.10. Computations (in the range $1.82\ell^2 < q < \ell^2 + 50$) suggest that for $\ell \in \{5, 7, 11\}$ and *any* prime number $q > 1.82\ell^2$, there still exist integers a, b, c such that Proposition 7.9 holds. For $\ell = 3$, this is no longer true: our computations indicate that if q is such that $\left(\frac{q}{\ell}\right) = -1$, then there are no suitable a, b, c, while if q is such that $\left(\frac{q}{\ell}\right) = 1$, they indicate that there are 4 suitable triples (a, b, c).

Step 4: Finishing the proof

Let ℓ and q be two distinct prime numbers as in Proposition 7.9 and let $P_q(X)$ be an ordinary Weil q-polynomial provided by this proposition. Since the polynomial $P_q(X)$ is irreducible modulo ℓ, it is a fortiori irreducible over $\mathbf{Z}$. It is also ordinary and of degree 6. Hence, by Honda-Tate theory, it defines an isogeny class $\mathscr{A}$ of ordinary simple abelian varieties of dimension 3 over $\mathbf{F}_q$. By Proposition 7.8, since $a \neq 0$, the abelian varieties in $\mathscr{A}$ are actually absolutely simple. Moreover, according to Howe (cf. [45, Theorem 1.2]), $\mathscr{A}$ contains a principally polarised abelian variety (A, λ).

Now, by the results of Oort-Ueno (cf. [86, Theorem 4]), there exists a so-called good curve C defined over $\overline{\mathbf{F}}_q$ such that (A, λ) is $\overline{\mathbf{F}}_q$-isomorphic to $(\mathrm{Jac}(C), \mu_0)$, where μ_0 denotes the canonical polarisation on $\mathrm{Jac}(C)$. A curve over $\overline{\mathbf{F}}_q$ is a *good curve* if it is either irreducible and nonsingular or a non-irreducible stable curve whose generalised Jacobian variety is an abelian variety (cf. [45, Definition (13.1)]). In particular, the curve C is stable, and so semistable. Since the generalised Jacobian variety $\mathrm{Jac}(C) \cong \mathrm{Pic}^0_C$ is an abelian variety, the torus appearing in the short exact sequence of Proposition 5.18 is trivial. Hence, there is an isomorphism $\mathrm{Jac}(C) \cong \prod_{i=1}^r \mathrm{Pic}^0_{\widetilde{X_i}}$, where $\widetilde{X_1}, \dots, \widetilde{X_r}$ denote the normalisations of the irreducible component of C over $\overline{\mathbf{F}}_q$. Since $\mathrm{Jac}(C)$ is absolutely simple, we conclude that $r = 1$, i.e., the curve C is irreducible, hence smooth.

We can therefore apply Theorem 9 of the appendix by Serre in [59] (see also the reformulation in [92, Theorem 1.1]) and conclude that the curve C descends to $\mathbf{F}_q$. Indeed, there exists a smooth and geometrically irreducible curve C_q defined over $\mathbf{F}_q$ which is isomorphic to C over $\overline{\mathbf{F}}_q$. Moreover, either (A, λ) or a quadratic twist of (A, λ) is isomorphic to $(\mathrm{Jac}(C_q), \mu)$ over $\mathbf{F}_q$, where μ denotes the canonical polarisation of $\mathrm{Jac}(C_q)$. The characteristic polynomial of the Frobenius endomorphism of $\mathrm{Jac}(C_q)$ is $P_q(X)$ or $P_q(-X)$, since the twist may replace the Frobenius endomorphism with its negative.

Note that the polynomial $P_q(-X)$ is still an ordinary Weil polynomial which is irreducible modulo ℓ with nonzero trace, and $\mathrm{Jac}(C_q)$ is still ordinary and absolutely simple. This proves Theorem 7.5. □

Remark 7.11. In the descent argument above, the existence of a nontrivial quadratic twist may occur in the non-hyperelliptic case only. This obstruction for an abelian variety over $\overline{\mathbf{F}}_q$ to be a Jacobian over $\mathbf{F}_q$ was first stated by Serre in a Harvard course [103]; it was derived from a precise reformulation of Torelli's theorem that Serre attributes to Weil [125]. Note that Sekiguchi investigated the descent of the curve in [99] and [100], but, as Serre pointed out to us, the non-hyperelliptic case was incorrect. According to MathSciNet review MR1002618 (90d:14032), together with Sekino, Sekiguchi corrected this error in the Japanese article [101].

7.5 Proof of the main theorem

The goal of this section is to prove Theorem 7.1, by collecting together the results from Sections 7.3 and 7.4. We keep the notation introduced in Section 7.1; in particular, we will consider genus 3 curves defined by polynomials which are of 3-hyperelliptic or quartic type. We will prove the following more precise version of Theorem 7.1:

Theorem 7.12. Let $\ell \geq 13$ be a prime number. For each prime $q > 1.82\ell^2$, there exists $\overline{f}_q(x,y) \in \mathbf{F}_q[x,y]$ of 3-hyperelliptic or quartic type, for which the following holds: if $f(x,y) \in \mathbf{Z}[x,y]$ is a lift of $\overline{f}_q(x,y)$, of the same type, satisfying the following two conditions for some prime number $p \notin \{2,q,\ell\}$:

1. $f(0,0) = 0$ or $v_p(f(0,0)) > 2$;
2. $f(x,y)$ is congruent modulo p^2 to:

$$\begin{cases} y^2 - x(x-p)m(x) & \text{if } \overline{f}_q(x,y) \text{ is of hyperelliptic type} \\ x^4 + y^4 + x^2 - y^2 + px & \text{if } \overline{f}_q(x,y) \text{ is of quartic type} \end{cases}$$

for some $m(x) \in \mathbf{Z}_p[x]$ of degree 5 or 6 with simple nonzero roots modulo p;

then the projective curve C defined over $\mathbf{Q}$ by the equation $f(x,y) = 0$ is a smooth projective geometrically irreducible genus 3 curve, such that the image of the Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the ℓ-torsion of $\mathrm{Jac}(C)$ coincides with $\mathrm{GSp}_6(\mathbf{F}_\ell)$.

Moreover, if $\ell \in \{5,7,11\}$, the statement is true, replacing "For each prime number q" by "There exists an odd prime number q".

Remark 7.13. Let $\ell \geq 5$ be a prime number. Note that it is easy to construct infinitely many polynomials $f(x,y)$ satisfying the conclusion of Theorem 7.12: choose a polynomial $f_p(x,y)$ satisfying the conditions in Definition 7.2. Then it suffices to choose each coefficient of $f(x,y)$ as a lift of the corresponding coefficient of $\overline{f}_q(x,y)$

to an element of $\mathbf{Z}$, which is congruent mod p^3 to the corresponding coefficient of $f_p(x, y)$. This also proves that Theorem 7.1 follows from Theorem 7.12.

Proof of Theorem 7.12. Fix a prime $\ell \geq 5$. Let q be a prime and let C_q be a genus 3 curve over $\mathbf{F}_q$, provided by Theorem 7.5. The curve C_q is either a plane quartic or a hyperelliptic curve. More precisely, it is defined by an equation $\overline{f}_q(x, y) = 0$, where $\overline{f}_q(x, y) \in \mathbf{F}_q[x, y]$ is a quartic type polynomial in the first case and a 3-hyperelliptic type polynomial otherwise (cf. Section 7.1). Note that if $f(x, y) \in \mathbf{Z}[x, y]$ is a quartic (resp. 3-hyperelliptic type) polynomial which reduces to $\overline{f}_q(x, y)$ modulo q, then it defines a smooth projective genus 3 curve over $\mathbf{Q}$ which is geometrically irreducible.

Let now $p \notin \{2, q, \ell\}$ be a prime. Assume that $f(x, y) \in \mathbf{Z}[x, y]$ is a polynomial of the same type as $\overline{f}_q(x, y)$ which is congruent to $\overline{f}_q(x, y)$ modulo q and also satisfies the two conditions of the statement of Theorem 7.12 for this p. We claim that the curve C defined over $\mathbf{Q}$ by the equation $f(x, y) = 0$ satisfies all the conditions of the explicit surjectivity result of Theorem 5.15. Namely, Proposition 7.3 implies that C is a smooth projective geometrically connected curve of genus 3 with stable reduction. Moreover, according to Proposition 7.4, the Jacobian $\mathrm{Jac}(C)$ is a principally polarised 3-dimensional abelian variety over $\mathbf{Q}$, and its Néron model has semistable reduction at p with toric rank equal to 1. Furthermore, the component group Φ_p of the Néron model of $\mathrm{Jac}(C)$ at p has order 2. Finally, by the choice of q and C_q provided by Theorem 7.5, q is a prime of good reduction of $\mathrm{Jac}(C)$ such that the Frobenius endomorphism of the special fibre at q has Weil polynomial $P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3$, which is irreducible modulo ℓ.

Since the prime ℓ does not divide $6pqa|\Phi_p|$, we conclude from Theorem 5.15 that the image of the Galois representation $\overline{\rho}_{\mathrm{Jac}(C),\ell}$ attached to the ℓ-torsion of $\mathrm{Jac}(C)$ coincides with $\mathrm{GSp}_6(\mathbf{F}_\ell)$. □

7.6 Counting irreducible Weil polynomials of degree 6

In this section, we will prove Proposition 7.9 which was stated in Section 7.4. The proof is based on Proposition 7.14 as well as Lemmas 7.16 and 7.17 below.

Let ℓ and q be distinct prime numbers. Consider a polynomial of the form

$$P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3 \in \mathbf{Z}[X]. \qquad (*)$$

Proposition 7.14 ensures that for $q > 1.82\ell^2$, every polynomial as in $(*)$ with coefficients in $]-\ell, \ell[$ is a Weil polynomial. Because such a polynomial could factor as $P_q(X) = (X - \alpha)(X - \frac{q}{\alpha})Q(X)$ where $Q(X)$ is a degree 4 Weil polynomial, in Proposition 7.14 and below we also study these degree 4 Weil polynomials.

Then Lemmas 7.16 and 7.17 allow us to show that the number of such degree 6 Weil polynomials which are irreducible modulo ℓ is strictly positive.

Proposition 7.14. Let ℓ and q be two prime numbers.

1. Suppose that $q > 1.67\ell^2$. Then every polynomial
$$X^4 + uX^3 + vX^2 + uqX + q^2 \in \mathbf{Z}[X]$$
with integers u, v of absolute value $< \ell$ is a Weil q-polynomial.

2. Suppose that $q > 1.82\ell^2$. Then every polynomial
$$P_q(X) = X^6 + aX^5 + bX^4 + cX^3 + qbX^2 + q^2aX + q^3 \in \mathbf{Z}[X],$$
with integers a, b, c of absolute value $< \ell$, is a Weil q-polynomial.

Remark 7.15. The proof of Proposition 7.14 given in Section 7.6.1 will show that the power in ℓ is optimal, but the constants 1.67 and 1.82 are not.

Let D_6^{*-} be the number of polynomials of form $(*)$ with $a, c \neq 0$, and a, b, c in $[-(\ell-1)/2, (\ell-1)/2]$, and whose discriminant Δ_{P_q} is not a square modulo ℓ. Let R_6 the number of such polynomials which are reducible modulo ℓ. Denoting by $\left(\frac{\cdot}{\ell}\right)$ the Legendre symbol, we have:

Lemma 7.16. Let $\ell > 3$, then
$$D_6^{*-} \geq \frac{1}{2}(\ell-1)^2\left(\ell - 1 - \left(\frac{q}{\ell}\right)\right) + \frac{1}{2}(\ell-1)\left(\frac{q}{\ell}\right)\left(1 - \left(\frac{-1}{\ell}\right)\right) - \ell(\ell-1).$$

Lemma 7.17. Let $\ell > 3$, then
$$R_6 \leq \frac{3}{8}\ell^3 - \frac{5}{8}\ell^2\left(\frac{q}{\ell}\right) - \ell^2 + \frac{3}{2}\ell\left(\frac{q}{\ell}\right) + \frac{5}{8}\ell - \frac{3}{8}\left(\frac{q}{\ell}\right) - \frac{1}{2}.$$

We postpone the proofs of Proposition 7.14 as well as those of Lemmas 7.16 and 7.17 to the following subsections but now use those statements to prove Proposition 7.9. First, let us recall a result of Stickelberger, as proven by Carlitz in [28], which will also be useful for proving Lemmas 7.16 and 7.17: For any monic polynomial $P(X)$ of degree n with coefficients in $\mathbf{Z}$, and any odd prime number ℓ not dividing its discriminant Δ_P, the number s of irreducible factors of $P(X)$ modulo ℓ satisfies
$$\left(\frac{\Delta_P}{\ell}\right) = (-1)^{n-s}.$$

Proof of Proposition 7.9. Let $\ell > 3$ be a prime number. It follows from Stickelberger's result that if $P_q(X)$ as in $(*)$ is irreducible modulo ℓ, then $\left(\frac{\Delta_{P_q}}{\ell}\right) = -1$. Hence by Proposition 7.14, when $q > 1.82\ell^2$, we find that $(D_6^{*-} - R_6)$ is exactly the number of degree 6 ordinary Weil polynomials which have nonzero trace modulo ℓ and are irreducible modulo ℓ.

By Lemmas 7.16 and 7.17, we have

$$D_6^{*-} - R_6 \geq \frac{1}{8}\ell^3 + \frac{1}{8}\ell^2 \left(\frac{q}{\ell}\right) - \frac{1}{2}\ell \left(\frac{-q}{\ell}\right) - \frac{3}{2}\ell^2 + \frac{1}{2}\left(\frac{-q}{\ell}\right) + \frac{15}{8}\ell - \frac{5}{8}\left(\frac{q}{\ell}\right),$$

which is strictly positive for all q, provided that $\ell \geq 13$.

For $\ell = 3, 5, 7$ or 11, direct computations of $(D_6^{*-} - R_6)$ using SAGE [110] show that $q = 19$ for $\ell = 3$, $q = 47$ for $\ell = 5$, $q = 97$ for $\ell = 7$, $q = 223$ for $\ell = 11$ will satisfy the conditions of Proposition 7.9. □

Actually, computations for $1.82\ell^2 < q < \ell^2 + 50$ indicate that for $\ell = 5, 7, 11$, $(D_6^{*-} - R_6)$ should be strictly positive for any prime number q and for $\ell = 3$, it should be strictly positive for all prime numbers q which are not squares modulo ℓ (see Remark 7.10).

7.6.1 Proof of Proposition 7.14

Recall that ℓ and q are two prime numbers.

We first consider degree 4 polynomials. Maisner and Nart prove in [68, Lemma 2.1] that a polynomial $X^4 + uX^3 + vX^2 + uqX + q^2 \in \mathbf{Z}[X]$ is a q-Weil polynomial if and only if the integers u, v satisfy the following inequalities:

(a) $|u| \leq 4\sqrt{q}$,

(b) $2|u|\sqrt{q} - 2q \leq v \leq \frac{u^2}{4} + 2q$.

Let $q > 1.67\ell^2$ and $Q(X) = X^4 + uX^3 + vX^2 + uqX + q^2 \in \mathbf{Z}[X]$ with $|u| < \ell, |v| < \ell$. Then $q \geq \frac{1}{16}\ell^2$ and, since $\ell \geq 2$, we have $q \geq \frac{1}{4}\ell^2 \geq \frac{1}{2}\ell$ so (a) and the right hand side inequality in (b) are satisfied. Finally, $q \geq \left(1 + \frac{1}{2\sqrt{3}}\right)^2 \ell^2$ so $\sqrt{q} \geq \left(1 + \frac{1}{2\sqrt{q}}\right)\ell$ and the left hand side inequality in (b) is satisfied. This proves that $Q(X)$ is a Weil polynomial and the first part of the proposition.

Now we turn to degree 6 polynomials. The proof is similar to the degree 4 case. According to Haloui [39, Theorem 1.1], a degree 6 polynomial of the form $(*)$ is a Weil polynomial if its coefficients satisfy the following inequalities:

(1) $|a| < 6\sqrt{q}$,

(2) $4\sqrt{q}|a| - 9q < b \leq \frac{a^2}{3} + 3q$,

(3) $-\frac{2a^3}{27} + \frac{ab}{3} + qa - \frac{2}{27}(a^2 - 3b^2 + 9q)^{\frac{3}{2}} \leq c \leq -\frac{2a^3}{27} + \frac{ab}{3} + qa + \frac{2}{27}(a^2 - 3b^2 + 9q)^{\frac{3}{2}}$,

(4) $-2qa - 2\sqrt{q}b - 2q\sqrt{q} < c < -2qa + 2\sqrt{q}b + 2q\sqrt{q}$.

Let $q > 1.82\ell^2$ and $P_q(X)$ a polynomial of the form $(*)$ with $|a|, |b|, |c| < \ell$. Then we note:

- We have $q > \frac{1}{36}\ell^2$, so $\ell < 6\sqrt{q}$ and (1) is satisfied.
- The right hand side inequality of (2) is satisfied since $\ell \leq 3q$. Moreover, we have $q > (1 + \sqrt{17/8})\ell^2 \geq 4\ell^2(1 + \sqrt{1 + 9/4\ell})^2/81$. Hence, $9q - 4\,\ell\,\sqrt{q} - \ell > 0$ and the left hand inequality of (2) is satisfied.
- A sufficient condition to have both inequalities in (3) is
$$2\ell^3 + 9\ell^2 + 27q\ell - 2(-3\ell^2 + 9q)^{3/2} + 27\ell \leq 0.$$
A computation shows that this inequality is equivalent to $A \leq B$, with
$$A = \ell^6\left(\frac{28}{729} + \frac{1}{81\ell} + \frac{7}{108\ell^2} + \frac{1}{6\ell^3} + \frac{1}{4\ell^4}\right)$$
and
$$B = q^3\left(1 - \frac{5}{4}\frac{\ell^2}{q} + \frac{\ell^4}{q^2}\left(\frac{8}{27} - \frac{1}{6\ell} - \frac{1}{2\ell^2}\right)\right).$$
Since $\ell \geq 2$, we have $A \leq \frac{4537}{46656}\ell^6$ and $B \geq q^3\left(1 - \frac{5}{4}\frac{\ell^2}{q} + \frac{19}{216}\frac{\ell^4}{q^2}\right)$. Furthermore, since the polynomial
$$\frac{4537}{46656}X^3 - \frac{19}{216}X^2 + \frac{5}{4}X - 1$$
has only one real root with approximate value 0.805, we find that $A \leq B$, because $q \geq 1.243\ell^2$.
- Since $q > 1.82\ell^2$ and $\ell \geq 2$, we have
$$\ell\left(\frac{1}{2q} + \frac{1}{\sqrt{q}} + 1\right) \leq \ell\left(\frac{1}{22} + \frac{1}{\sqrt{11}} + 1\right) < \sqrt{q}.$$
Hence, $-2q\ell - 2\sqrt{q}\ell + 2q\sqrt{q} - \ell > 0$ and (4) is satisfied.

This proves that $P_q(X)$ is a Weil polynomial and the second part of the proposition. □

7.6.2 Proofs of Lemmas 7.16 and 7.17

In this section, $\ell > 2$, $q \neq \ell$ are prime numbers and we, somewhat abusively, denote with the same letter an integer in $[-(\ell-1)/2, (\ell-1)/2]$ and its image in $\mathbf{F}_\ell$.

We will use the following elementary lemma.

Lemma 7.18. Let $D \in \mathbf{F}_\ell^*$ and $\varepsilon \in \{-1, 1\}$. We have

$$\left|\left\{x \in \mathbf{F}_\ell \colon \left(\frac{x^2 - D}{\ell}\right) = \varepsilon\right\}\right| = \frac{1}{2}\left(\ell - 1 - \varepsilon - \left(\frac{D}{\ell}\right)\right);$$

and

$$\left|\left\{(x,y) \in \mathbf{F}_\ell^2 \colon \left(\frac{x^2 - Dy^2}{\ell}\right) = \varepsilon\right\}\right| = \frac{1}{2}(\ell - 1)\left(\ell - \left(\frac{D}{\ell}\right)\right).$$

□

Estimates on the number of degree 4 Weil polynomials modulo ℓ

Proposition 7.19.

1. For $\varepsilon \in \{-1, 1\}$, we denote by D_4^ε the number of degree 4 polynomials of the form $X^4 + uX^3 + vX^2 + uqX + q^2 \in \mathbf{F}_\ell[X]$ with discriminant Δ such that $\left(\frac{\Delta}{\ell}\right) = \varepsilon$. Then

$$D_4^- = \frac{1}{2}(\ell - 1)\left(\ell - \left(\frac{q}{\ell}\right)\right) \quad \text{and} \quad D_4^+ = \frac{1}{2}(\ell - 3)\left(\ell - \left(\frac{q}{\ell}\right)\right) + 1.$$

2. The number N_4 of degree 4 Weil polynomials with coefficients in $[-(\ell-1)/2, (\ell-1)/2]$ which are irreducible modulo ℓ satisfies

$$N_4 \leq \frac{1}{4}(\ell + 1)(\ell - 1). \tag{7.2}$$

3. The number T_4 of degree 4 Weil polynomials with coefficients in $[-(\ell-1)/2, (\ell-1)/2]$ with exactly two irreducible factors modulo ℓ satisfies

$$T_4 \leq \frac{1}{4}(\ell - 3)\left(\ell - \left(\frac{q}{\ell}\right)\right) + \frac{1}{8}(\ell - 1)(\ell + 1). \tag{7.3}$$

Moreover, if $q > 1.67\ell^2$, inequalities (7.2) and (7.3) are equalities.

Proof. First, we compute D_4^ε. The polynomial $Q(X) = X^4+uX^3+vX^2+uqX+q^2$ has discriminant

$$\Delta = q^2\kappa^2\delta \quad \text{where} \quad \kappa = -u^2 - 8q + 4v \quad \text{and} \quad \delta = (v+2q)^2 - 4qu^2.$$

So, since $q \in \mathbf{F}_\ell^*$, we have $\left(\frac{\Delta}{\ell}\right) = \left(\frac{\kappa}{\ell}\right)^2 \left(\frac{\delta}{\ell}\right)$. Moreover, notice that if $\kappa = 0$ then $\delta = (v-6q)^2$. Hence the set $\mathscr{D}_4^\varepsilon$ of $(u,v) \in \mathbf{F}_\ell^2$ such that $\left(\frac{\Delta}{\ell}\right) = \varepsilon$ is equal to

$$\begin{aligned}\mathscr{D}_4^\varepsilon &= \left\{(u,v) \in \mathbf{F}_\ell^2 \colon \left(\frac{\delta}{\ell}\right) = \varepsilon\right\} \setminus \left\{(u,v) \in \mathbf{F}_\ell^2 \colon \left(\frac{\delta}{\ell}\right) = \varepsilon \text{ and } \kappa = 0\right\} \\ &= \left\{(u,v) \in \mathbf{F}_\ell^2 \colon \left(\frac{\delta}{\ell}\right) = \varepsilon\right\} \setminus \left\{(u,v) \in \mathbf{F}_\ell^2 \colon \left(\frac{v-6q}{\ell}\right)^2 = \varepsilon \right. \\ &\qquad\qquad\qquad\qquad\qquad\qquad \left. \text{and } u^2 = 4(v-2q)\right\}.\end{aligned}$$

It follows that

$$D_4^- = |\mathscr{D}_4^-| = \left|\left\{(u,v) \in \mathbf{F}_\ell^2 \colon \left(\frac{\delta}{\ell}\right) = -1\right\}\right|$$

and

$$\begin{aligned}D_4^+ &= |\mathscr{D}_4^+| = \left|\left\{(u,v) \in \mathbf{F}_\ell^2 \colon \left(\frac{\delta}{\ell}\right) = 1\right\}\right| \\ &\quad - \left|\left\{(u,v) \in \mathbf{F}_\ell^2 \colon v \neq 6q \text{ and } u^2 = 4(v-2q)\right\}\right|.\end{aligned}$$

Since the map $(u,v) \mapsto (v+2q, 2u)$ is a bijection on $\mathbf{F}_\ell^2$ (because $\ell \neq 2$), by Lemma 7.18 we have

$$\begin{aligned}\left|\left\{(u,v) \in \mathbf{F}_\ell^2 \colon \left(\frac{\delta}{\ell}\right) = \varepsilon\right\}\right| &= \left|\left\{(x,y) \in \mathbf{F}_\ell^2 \colon \left(\frac{x^2-qy^2}{\ell}\right) = \varepsilon\right\}\right| \\ &= \frac{(\ell-1)}{2}\left(\ell - \left(\frac{q}{\ell}\right)\right)\end{aligned}$$

for any $\varepsilon \in \{\pm 1\}$. This gives the result for D_4^-. Moreover

$$\begin{aligned}&\left|\left\{(u,v) \colon v \neq 6q \text{ and } u^2 = 4(v-2q)\right\}\right| \\ =\ &\left|\left\{(u,v) \colon u^2 = 4(v-2q)\right\}\right| - \left|\left\{u \in \mathbf{F}_\ell \colon u^2 = 16q\right\}\right| \\ =\ &\ell - 1 - \left(\frac{q}{\ell}\right).\end{aligned}$$

This gives the result for D_4^+.

Next, we bound the quantity N_4. By Stickelberger's result recalled at the beginning of the section, if a monic polynomial of degree 4 in $\mathbf{Z}[X]$ is irreducible modulo ℓ then it has non-square discriminant modulo ℓ. Conversely, if a monic degree 4 polynomial in $\mathbf{Z}[X]$ has non-square discriminant modulo ℓ, then it has one or three distinct irreducible factors in $\mathbf{F}_\ell[X]$. If the reduction of a degree 4 Weil polynomial with non-square discriminant modulo ℓ has three distinct irreducible factors in $\mathbf{F}_\ell[X]$, then it has the form

$$(X-\alpha')(X-\frac{q}{\alpha'})(X^2-B'X+q)$$

with $X^2-B'X+q$ irreducible in $\mathbf{F}_\ell[X]$ and $\alpha' \neq q/\alpha'$ in $\mathbf{F}_\ell^*$. By Lemma 7.18, there are

$$\frac{1}{4}\left(\ell-2-\left(\frac{q}{\ell}\right)\right)\left(\ell-\left(\frac{q}{\ell}\right)\right)$$

such polynomials with three irreducible factors. It follows that

$$N_4 \leq D_4^- - \frac{1}{4}\left(\ell-2-\left(\frac{q}{\ell}\right)\right)\left(\ell-\left(\frac{q}{\ell}\right)\right) \leq \frac{1}{4}(\ell-1)(\ell+1).$$

Finally, we bound the quantity T_4. As in the paragraph above, Stickelberger's result implies that a degree 4 Weil polynomial $Q(X)$ in $\mathbf{Z}[X]$ has exactly two distinct irreducible factors modulo ℓ if and only if $\left(\frac{\Delta_Q}{\ell}\right)=1$ and $Q(X) \pmod{\ell}$ does not have four distinct roots in $\mathbf{F}_\ell$. By Lemma 7.18, there are

$$\frac{1}{8}\left(\ell-\left(\frac{q}{\ell}\right)-2\right)\left(\ell-\left(\frac{q}{\ell}\right)-4\right)$$

Weil polynomials with coefficients in $[-(\ell-1)/2,(\ell-1)/2]$ whose reduction modulo ℓ has four distinct roots in $\mathbf{F}_\ell$. It follows that

$$\begin{aligned} T_4 &\leq D_4^+ - \frac{1}{8}\left(\ell-\left(\frac{q}{\ell}\right)-2\right)\left(\ell-\left(\frac{q}{\ell}\right)-4\right) \\ &\leq \frac{1}{4}(\ell-3)\left(\ell-\left(\frac{q}{\ell}\right)\right)+\frac{1}{8}(\ell-1)(\ell+1). \end{aligned}$$

When $q > 1.67\ell^2$, these upper bounds for N_4 and T_4 are equalities, since in this case, by Proposition 7.14, every polynomial of the form $X^4+uX^3+vX^2+uqX+q^2$ with $|u|,|v|<\ell$ is a Weil polynomial. □

Proof of Lemma 7.17

Let $P_q(X)$ be a degree 6 Weil polynomial with coefficients in $[-(\ell-1)/2,(\ell-1)/2]$ and non-square discriminant modulo ℓ. We may drop the conditions $a\neq 0, c\neq 0$ to simplify computations for finding an upper bound for R_6. By Stickelberger's result, $P_q(X)$ has $1,\ 3$ or 5 distinct irreducible factors in $\mathbf{F}_\ell[X]$. Note that a root α of $P_q(X)$ in $\overline{\mathbf{F}}_\ell$ is in $\mathbf{F}_\ell$ if and only q/α is also in $\mathbf{F}_\ell$. So a degree 6 Weil polynomial $P_q(X)$ with non-square discriminant modulo ℓ is reducible modulo ℓ if and only if its factorisation in $\mathbf{F}_\ell[X]$ is of one of the following types:

1. $P_q(X)\equiv(X-\alpha)(X-\frac{q}{\alpha})(X-\beta)(X-\frac{q}{\beta})(X^2-CX+q)$, with C^2-4q non-square modulo ℓ and $\alpha\neq q/\alpha$, $\beta\neq q/\beta$ and $\{\alpha,q/\alpha\}\neq\{\beta,q/\beta\}$; equivalently $P_q(X)\equiv(X^2-AX+q)(X^2-BX+q)(X^2-CX+q)$ where the first two quadratic polynomials are distinct and both reducible and the third one is irreducible;

2. $P_q(X)\equiv(X-\alpha)(X-\frac{q}{\alpha})Q(X)$, where $\alpha\neq q/\alpha$ and the irreducible factor $Q(X)$ is the reduction of a degree 4 Weil polynomial;

3. $P_q(X)$ is the product of three distinct irreducible quadratic polynomials, i.e., $P_q(X)\equiv(X^2-CX+q)Q(X)$ where X^2-CX+q is irreducible and $Q(X)$ is the reduction of a degree 4 Weil polynomial which has two distinct irreducible factors, both of which are distinct from X^2-CX+q.

We will count the number of polynomials of each type.

Type 1. By Lemma 7.18, there are $\frac{1}{2}\left(\ell-\left(\frac{q}{\ell}\right)\right)$ irreducible quadratic polynomials X^2-CX+q. Also by Lemma 7.18, there are $\frac{1}{2}\left(\ell-2-\left(\frac{q}{\ell}\right)\right)$ choices for reducible X^2-AX+q without a double root and then there are $\frac{1}{2}\left(\ell-2-\left(\frac{q}{\ell}\right)\right)-1$ choices for reducible X^2-BX+q without a double root and distinct from X^2-AX+q. It follows that there are $\frac{1}{16}\left(\ell-\left(\frac{q}{\ell}\right)\right)\left(\ell-\left(\frac{q}{\ell}\right)-2\right)\left(\ell-\left(\frac{q}{\ell}\right)-4\right)$ such polynomials.

Type 2. By Proposition 7.19 and Lemma 7.18, the number of polynomials with decomposition of this type is

$$\frac{1}{2}\left(\ell-\left(\frac{q}{\ell}\right)-2\right)N_4\le\frac{1}{8}(\ell+1)(\ell-1)\left(\ell-\left(\frac{q}{\ell}\right)-2\right).$$

Type 3. Proposition 7.19 and Lemma 7.18 imply that there are

$$\le\frac{1}{2}\left(\ell-\left(\frac{q}{\ell}\right)\right)T_4\le\frac{1}{8}\left(\ell-\left(\frac{q}{\ell}\right)\right)^2(\ell-3)+\frac{1}{16}(\ell-1)(\ell+1)\left(\ell-\left(\frac{q}{\ell}\right)\right)$$

polynomials of this type. The first inequality is due to the fact that we do not take into account that X^2-CX+q has to be distinct from the factors of $Q(X)$.

Summing these three upper bounds yields the lemma. □

Proof of Lemma 7.16

The discriminant of $P_q(X)$ is $\Delta_{P_q} = q^6\Gamma^2\delta$, where

$$\Gamma = 8qa^4 + 9q^2a^2 - 42qa^2b + a^2b^2 - 4a^3c + 108q^3 - 108q^2b + 36qb^2 - 4b^3 \\ +54qac + 18abc - 27c^2$$

and $\delta = (c+2aq)^2 - 4q(b+q)^2$. Hence, we have

$$\begin{aligned} D_6^{*-} &= \left|\left\{(a,b,c)\colon a,c \neq 0, \Gamma \not\equiv 0 \bmod \ell \text{ and } \left(\frac{\delta}{\ell}\right) = -1\right\}\right| \\ &= \left|\left\{(a,b,c)\colon a,c \neq 0, \left(\frac{\delta}{\ell}\right) = -1\right\}\right| \\ &- \left|\left\{(a,b,c)\colon a,c \neq 0, \Gamma \equiv 0 \bmod \ell \text{ and } \left(\frac{\delta}{\ell}\right) = -1\right\}\right| \\ &\geq M - W, \end{aligned}$$

for $M = \left|\left\{(a,b,c)\colon a,c \neq 0, \left(\frac{\delta}{\ell}\right) = -1\right\}\right|$ and
$W = |\{(a,b,c)\colon a \neq 0, \Gamma \equiv 0 \bmod \ell\}|$.

Computation of M. Since $\ell > 2$ and $q \in \mathbf{F}_\ell^*$, for any fixed $c \in \mathbf{F}_\ell^\times$, the map $(a,b) \mapsto (c+2aq, b+q)$ is a bijection from $\mathbf{F}_\ell^* \times \mathbf{F}_\ell$ to $\mathbf{F}_\ell \backslash \{c\} \times \mathbf{F}_\ell$. From this and Lemma 7.18 we deduce that

$$\begin{aligned} M &= \sum_{c \in \mathbf{F}_\ell^*} \left|\left\{(x,y) \in \mathbf{F}_\ell^2\colon x \neq c, \left(\frac{x^2-4qy^2}{\ell}\right) = -1\right\}\right| \\ &= \sum_{c \in \mathbf{F}_\ell^*} \left|\left\{(x,y) \in \mathbf{F}_\ell^2\colon \left(\frac{x^2-4qy^2}{\ell}\right) = -1\right\}\right| \\ &- \sum_{c \in \mathbf{F}_\ell^*} \left|\left\{y \in \mathbf{F}_\ell\colon \left(\frac{c^2-4qy^2}{\ell}\right) = -1\right\}\right| \\ &= \frac{1}{2}(\ell-1)^2\left(\ell - \left(\frac{q}{\ell}\right)\right) - \sum_{c \in \mathbf{F}_\ell^*} M_c', \end{aligned}$$

where

$$\begin{aligned} M_c' &= \left|\left\{y \in \mathbf{F}_\ell\colon \left(\frac{c^2-4qy^2}{\ell}\right) = -1\right\}\right| \\ &= \left|\left\{y \in \mathbf{F}_\ell\colon \left(\frac{y^2-(c^2/4q)}{\ell}\right) = -\left(\frac{-q}{\ell}\right)\right\}\right|. \end{aligned}$$

By Lemma 7.18, if $\left(\frac{-q}{\ell}\right) = -1$, then

$$M'_c = \left|\left\{y \in \mathbf{F}_\ell \colon \left(\frac{y^2 - (c^2/4q)}{\ell}\right) = 1\right\}\right| = \frac{1}{2}\left(\ell - 2 - \left(\frac{q}{\ell}\right)\right)$$

and if $\left(\frac{-q}{\ell}\right) = 1$, then

$$M'_c = \left|\left\{y \in \mathbf{F}_\ell \colon \left(\frac{y^2 - (c^2/4q)}{\ell}\right) = -1\right\}\right| = \frac{1}{2}\left(\ell - \left(\frac{q}{\ell}\right)\right).$$

This can be rewritten, for all q and ℓ, as $M'_c = \frac{1}{2}\left(\ell - 1 - \left(\frac{q}{\ell}\right) + \left(\frac{-q}{\ell}\right)\right)$. We obtain

$$M = \frac{1}{2}(\ell-1)^2\left(\ell - 1 - \left(\frac{q}{\ell}\right)\right) + \frac{1}{2}(\ell-1)\left(\frac{q}{\ell}\right)\left(1 - \left(\frac{-1}{\ell}\right)\right).$$

Computation of W. Note that Γ can be viewed as a degree 2 polynomial in c over $\mathbf{F}_\ell[a,b]$:

$$\Gamma = -27c^2 + G_1 c + G_0, \quad \text{where} \quad G_1(a,b) = -2a(2a^2 - 27q - 9b)$$

and

$$G_0(a,b) = 8qa^4 + 9q^2a^2 - 42qa^2b + a^2b^2 + 108q^3 - 108q^2b + 36qb^2 - 4b^3.$$

The discriminant of Γ as a polynomial in c is $\gamma = 16(a^2+9q-3b)^3$. So $\Gamma \equiv 0 \bmod \ell$ if and only if

$$\left(\left(\frac{\gamma}{\ell}\right) = 1 \text{ and } c = \frac{-1}{54}(-G_1 \pm \sqrt{\gamma})\right) \text{ or } \left(\gamma = 0 \text{ and } c = \frac{1}{54}G_1\right),$$

where $\sqrt{\gamma}$ denotes a square root of γ in $\mathbf{F}_\ell$. It follows that

$$\begin{aligned} W &= 2 \cdot \left|\left\{(a,b) \in \mathbf{F}_\ell^2 \colon a \neq 0, \left(\frac{\gamma}{\ell}\right) = 1\right\}\right| + \left|\left\{(a,b) \in \mathbf{F}_\ell^2 \colon a \neq 0, \gamma = 0\right\}\right| \\ &= 2 \cdot \left|\left\{(a,b) \in \mathbf{F}_\ell^2 \colon a \neq 0, \left(\frac{a^2 - 3(b-3q)}{\ell}\right) = 1\right\}\right| \\ &+ \left|\left\{(a,b) \in \mathbf{F}_\ell^2 \colon a \neq 0, a^2 = 3(b-3q)\right\}\right|. \end{aligned}$$

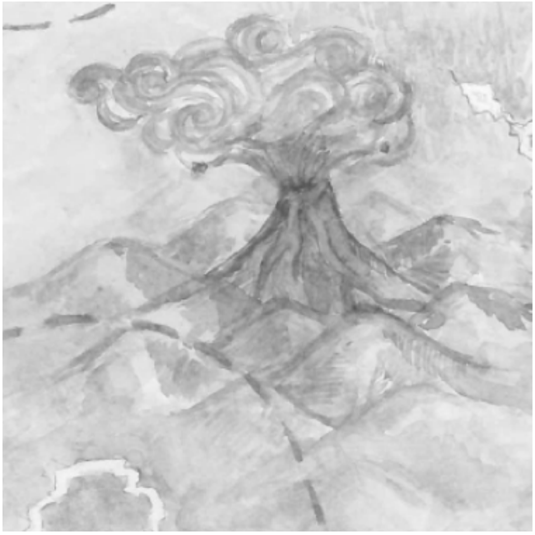
Since $\ell > 3$, the map $b \mapsto 3(b-3q)$ is a bijection on $\mathbf{F}_\ell$, so we have

$$\begin{aligned}
W &= 2\cdot\left|\left\{(x,y)\in\mathbf{F}_\ell^2\colon x\neq 0, \left(\frac{x^2-y}{\ell}\right)=1\right\}\right| \\
&+ \left|\left\{(x,y)\in\mathbf{F}_\ell^2\colon x\neq 0, x^2=y\right\}\right| \\
&= 2\cdot\sum_{y\in\mathbf{F}_\ell}\left|\left\{x\in\mathbf{F}_\ell\colon \left(\frac{x^2-y}{\ell}\right)=1\right\}\right| - 2\cdot\left|\left\{y\in\mathbf{F}_\ell\colon \left(\frac{-y}{\ell}\right)=1\right\}\right| \\
&+ \sum_{y\in\mathbf{F}_\ell^*}\left|\{x\in\mathbf{F}_\ell^*\colon x^2=y\}\right| \\
&= \sum_{y\in\mathbf{F}_\ell^*}\left(\ell-2-\left(\frac{y}{\ell}\right)\right)+2(\ell-1)-(\ell-1)+(\ell-1),
\end{aligned}$$

using Lemma 7.18 (the second term is the contribution of $y=0$). This yields $W=\ell(\ell-1)$ and computing $M-W$ concludes the proof. □

Part III

Abelian varieties



CHAPTER 8

Abelian varieties over finite fields and twists

In this chapter, we present some background material on supsersingular abelian varieties over finite fields and their twists, which will be used in subsequent chapters.

Let $K = \mathbf{F}_q$ be a finite field of cardinality $q = p^r$, for p a prime number, and let $k = \overline{\mathbf{F}}_p$.

8.1 L-polynomials and supersingular abelian varieties

Field of definition

Definition 8.1. Consider the isomorphism class of an abelian variety A over k. Let $K \subset k$ be a finite field. We say that A is *defined over* K if it has a model over K, i.e., if there exists a K-variety A' such that $A' \times_K k \cong A$. The field K is then a *field of definition* for A.

Definition 8.1 may be adapted to define the field of definition of a (smooth projective connected) curve X/k.

In this and subsequent chapters, we will assume that the field of definition of an abelian variety A or a curve X is a finite field K.

The results in this chapter are joint work with Rachel Pries.

Supersingular abelian varieties

Let A be an abelian variety of dimension g defined over K.

Definition 8.2. An abelian variety A/K is a projective group scheme. Consider an open affine subscheme $U = \mathrm{Spec}(R)$ for some K-algebra R; the map which sends $x \mapsto x^q$ for all $x \in R$ induces a Frobenius map f_U on U. The *absolute Frobenius endomorphism* $f_A \colon A \times_K k \to A \times_K k$ of an abelian variety A/K is defined to be the glueing of these Frobenius endomorphisms f_U over all open subschemes U of A.

The *relative Frobenius endomorphism* $\pi = \pi_A \colon A \times_K k \to A \times_K k$ of A is defined as the factorisation of f_A over the fibre product of $A \to \mathrm{Spec}(k) \leftarrow \mathrm{Spec}(k)$, where the second map is the absolute Frobenius $f_{\mathrm{Spec}(k)}$ [85, 21.2].

Recall that G_K denotes the absolute Galois group $\mathrm{Gal}(k/K)$ of K. Fix a topological generator Fr_K (Frobenius) of G_K; it is also called the *topological Frobenius endomorphism* of K.

These three Frobenius maps are related via

$$\pi_A = f_A \otimes Fr_K^{-1}. \tag{8.1}$$

Compare Definition 8.2 to the discussion on p. 62 and to Definition 7.6.

The characteristic polynomial $P(A/K,T)$ of the relative Frobenius endomorphism π_A of A is a monic polynomial in $\mathbf{Z}[T]$ of degree $2g$. Writing

$$P(A/K,T) = \prod_{i=1}^{2g}(T - \alpha_i),$$

the roots $\alpha_i \in \overline{\mathbf{Q}}$ all satisfy $|\alpha_i| = \sqrt{q}$, by the Riemann hypothesis for abelian varieties as proven by Weil [124].

Definition 8.3. The roots $\{\alpha_1, \ldots, \alpha_{2g}\}$ of $P(A/K,T)$ are the *Weil numbers* of A. The *normalised Weil numbers* of A/K are $\{\alpha_1/\sqrt{q}, \ldots, \alpha_{2g}/\sqrt{q}\} = \{z_1, \ldots, z_{2g}\}$.

Theorem 8.4. [73, Chapter II, Theorem 1.1],

1. The number of K-points of A is

$$|A(K)| = \deg(\pi_{A/K} - \mathrm{id}) = P(A/K,1) = \prod_{i=1}^{2g}(1 - \alpha_i). \tag{8.2}$$

2. Also,

$$||A(K)| - q^g| \leq 2gq^{(g-\frac{1}{2})} + (2^{2g} - 2g - 1)q^{(g-1)}.$$

□

Definition 8.5. [73, Chapter II, Section 1] The *zeta function* of A over $K = \mathbf{F}_q$ is

$$Z(A/K, T) = \exp\left(\sum_{m\geq 1} |A(\mathbf{F}_{q^m})|\frac{t^m}{m}\right).$$

Theorem 8.6. [33, Theorem 1.6],[124, §IX, 71] The zeta function of A over $K = \mathbf{F}_q$ from Definition 8.5 satisfies

$$Z(A/K, T) = \frac{P_1(T) \cdot \ldots \cdot P_{2g-1}(T)}{P_0(T)P_2(T) \cdot \ldots \cdot P_{2g-2}(T)P_{2g}(T)},$$

with

$$P_s(T) = \prod (1 - \alpha_{i,s}T),$$

where the $\alpha_{i,s}$ for a fixed s range over all products of s Weil numbers of A/K, i.e.,

$$\alpha_{i,s} = \alpha_{i_1}\alpha_{i_2} \cdot \ldots \cdot \alpha_{i_s}\ ,\ 0 < i_1 < \ldots < i_s \leq 2g.$$

□

Note that $P(A/K, T) = T^{2g}P_1(\frac{1}{T})$. The polynomials P_i describe the action of Frobenius on the i-th (ℓ-adic) cohomology of A. By [115, Theorem 1], two abelian varieties A_1 and A_2 over K have the same zeta function if and only if $P(A_1/K, T) = P(A_2/K, T)$ if and only if A_1 and A_2 are isogenous over K.

Definition 8.7. [85, Section 21] Recall that $K = \mathbf{F}_q$ for $q = p^r$. We may write $P(A/K, T) = \sum_{j=1}^{2g} b_j T^{2g-j}$. Then its *Newton polygon* is defined as the lower convex hull of the set of points

$$\left\{\left(j, \frac{v_p(b_j)}{r}\right) : 0 \leq j \leq 2g\right\}.$$

Definition 8.8. If the Newton polygon of $P_1(T)$ is a line segment of slope $1/2$ then A is *supersingular.*

Definition 8.9. An elliptic curve E/K is *supersingular* if $E[p](k) = \{0\}$. For such an elliptic curve, we denote the p-divisible group $E[p^\infty]$ by $G_{1,1}$.

There are many equivalent formulations of the supersingular property:

Theorem 8.10. Suppose A/K is an abelian variety of dimension g. The following properties are equivalent:

1. A is supersingular;

2. A is geometrically isogenous to a product of supersingular elliptic curves [84, Theorem 4.2], i.e., $A \times_K k \sim E^g$ for an elliptic curve E satisfying $E[p](k) = \{0\}$, cf. Definition 8.9;

3. the formal group of A is geometrically isogenous to $(G_{1,1})^g$ ([62, Section 1.4], cf. Definition 8.9);

4. the only slope of the p-divisible group $A[p^\infty]$ is $\frac{1}{2}$;

5. the complex roots of $P(A/K, T)$ can be written as $\zeta\sqrt{q}$ where ζ is a root of unity [69, Theorem 4.1], [84, p. 116]. □

Definition 8.11. The abelian variety A/K is *maximal* (resp. *minimal*) if its normalised Weil numbers all equal -1 (resp. 1). Since $|A(K)|$ is an integer, equation (8.2) implies that q is a square (i.e. $r = \log_p q$ is even) if A/K is maximal (resp. minimal).

Supersingular curves

Let X be a smooth projective connected curve of genus g defined over K. The curve X is *supersingular* if its Jacobian $\mathrm{Jac}(X)$ is supersingular.

Theorem 8.12. [123, §IV, 22],[124, §IX, 69] The zeta function of X/K can be written as

$$Z(X/K, T) = \frac{L(X/K, T)}{(1-T)(1-qT)},$$

where the *L-polynomial* $L(X/K, T) \in \mathbf{Z}[T]$ of X/K has degree $2g$ and factors as

$$L(X/K, T) = \prod_{i=1}^{2g}(1 - \alpha_i T).$$

□

Then $P(X/K, T) = T^{2g}L(X/K, T^{-1})$ is the characteristic polynomial of the relative Frobenius endomorphism of Jac(X). The roots $\{\alpha_1, \ldots, \alpha_{2g}\}$ of $P(X/K, T)$ are the *Weil numbers* of X. The *normalised Weil numbers* of X/K are

$$\{\alpha_1/\sqrt{q}, \ldots, \alpha_{2g}/\sqrt{q}\} = \{z_1, \ldots, z_{2g}\}$$

(note that $|\alpha_i/\sqrt{q}| = 1$).

Corollary 8.13 (Hasse-Weil Bound)**.** The number of K-points of X satisfies

$$|X(K) - (q+1)| \leq 2g\sqrt{q}. \tag{8.3}$$

□

Definition 8.14. Let X/K be a curve of genus g.

1. The curve X/K is *maximal* if $|X(K)| = q + 1 + 2g\sqrt{q}$. Equivalently, $L(X/K, T) = (1 + \sqrt{q}T)^{2g}$, or the normalised Weil numbers are all -1.
2. The curve X/K is *minimal* if $|X(K)| = q + 1 - 2g\sqrt{q}$. Equivalently, X has $L(X/K, T) = (1 - \sqrt{q}T)^{2g}$, or its normalised Weil numbers are all 1.

Note that if X/K is maximal or minimal, then q is a square (r is even).

Basic properties

The following facts are well-known, follow from the previous results, and hold for curves as well, cf. [118, Theorem 1.9] and [112, Theorem V.1.15(f)].

Lemma 8.15. If $P(A/K, T) = \prod_{i=1}^{2g}(T - \alpha_i)$, then

$$P(A/\mathbf{F}_{q^m}, T) = \prod_{i=1}^{2g}(T - \alpha_i^m).$$

□

Corollary 8.16. If A/K is minimal or maximal, then it is supersingular. Conversely, if A/K is supersingular, then it is minimal over some finite extension $\mathbf{F}_{q^m}$. □

Corollary 8.17.

1. If A/K is maximal, then $A/\mathbf{F}_{q^m}$ is maximal for odd m and minimal for even m.
2. If A/K is minimal, then $A/\mathbf{F}_{q^m}$ is minimal for all m. □

8.2 Twists

Let A/K be an abelian variety of dimension g and let X/K be a smooth projective connected curve of genus g, where we take K to be the minimal field of definition of A or X.

Review of twists

We follow the reference [104, Chapter III, §1], which treats the theory of twists (or *forms*) of general algebraic varieties.

Definition 8.18. A *twist* of A/K is an abelian variety A'/K such that A and A' are geometrically isomorphic, meaning that there is an isomorphism

$$\phi : A \times_K k \xrightarrow{\sim} A' \times_K k. \tag{8.4}$$

The *order* of a twist A'/K is the degree of the minimal field of definition K' of ϕ over K. In particular, a twist A'/K is *trivial* if $A \cong_K A'$.

Definition 8.19. Let $\Theta(A/K)$ denote the set of twists of A/K, modulo K-isomorphisms (i.e., modulo trivial twists). For K'/K a field extension, let $\Theta(A, K'/K) \subset \Theta(A/K)$ denote the set of twists A'/K of A/K such that $A \times_K K' \cong A' \times_K K'$, modulo K'-isomorphisms.

Proposition 8.20. [104, Proposition III.5] For every finite Galois extension K'/K, there is a bijection

$$\theta\colon \Theta(A, K'/K) \to H^1(\mathrm{Gal}(K'/K), \mathrm{Aut}_{K'}(A)). \tag{8.5}$$

There is an induced bijection

$$\theta\colon \Theta(A/K) \to H^1(G_K, \mathrm{Aut}_k(A)). \tag{8.6}$$

□

We give the definition of θ as in equation (8.6) from the proof in [104]. Given $\sigma \in G_K$ and a twist A'/K for ϕ an isomorphism as above, let ${}^{\sigma}\phi : A \times_K k \to A' \times_K k$ be the twisted isomorphism satisfying, for all $x \in A \times_K k$, that

$${}^{\sigma}\phi(x) = {}^{\sigma}(\phi({}^{\sigma^{-1}}x)). \tag{8.7}$$

This defines a cocycle $\xi_\phi\colon G_K \to \mathrm{Aut}_k(A)$ by

$$\xi_\phi(\sigma) = \phi^{-1} \circ^{\sigma} \phi. \tag{8.8}$$

Then $\theta(A'/K)$ is the equivalence class of ξ_ϕ in $H^1(G_K, \mathrm{Aut}_k(A))$, so we write $A' = A_{\xi_\phi}$.

Given $\tau \in \mathrm{Aut}_k(A)$, let ${}^{Fr_K}\tau$ be the twisted automorphism by the topological Frobenius Fr_K, satisfying

$${}^{Fr_K}\tau(x) =^{Fr_K} (\tau({}^{Fr_K^{-1}}x))$$

for all $x \in A \times_K k$.

Definition 8.21 and Proposition 8.22 are adaptations of [72, Definition 7 and Proposition 9].

Definition 8.21. Two elements $g, h \in \mathrm{Aut}_k(A)$ are *K-Frobenius conjugate* if there is an element $\tau \in \mathrm{Aut}_k(A)$ such that

$$\tau g = h({}^{Fr_K}\tau).$$

Proposition 8.22. There is a bijection

$$H^1(G_K, \mathrm{Aut}_k(A)) \to \{K\text{-Frobenius conjugacy classes of } \mathrm{Aut}_k(A)\}.$$

In particular, the number of twists of A/K is equal to the number of K- Frobenius conjugacy classes of $\mathrm{Aut}_k(A)$.

Proof. Each cocycle is uniquely determined by its value at Fr_K. Two cocycles ξ and ψ are equivalent in $H^1(G_K, \mathrm{Aut}_k(A))$ if there exists an element $\tau \in \mathrm{Aut}_k(A)$ such that $\xi(Fr_K) \circ ({}^{Fr_K}\tau) = \tau \circ \psi(Fr_K)$. By Definition 8.21, this is the same as saying that $\xi(Fr_K)$ and $\psi(Fr_K)$ are K-Frobenius conjugate. □

Thus, there are one-to-one correspondences between a twist A'/K of A/K and a cocycle ξ_ϕ such that $\xi_\phi(Fr_K) = g$ for some $g \in \mathrm{Aut}_k(A)$ (so that $A' = A_{\xi_\phi}$), as well as between a cocycle ξ_ϕ such that $\xi_\phi(Fr_K) = g$ and the K-Frobenius conjugacy class $[g]_{\mathrm{Frob}}$.

Now, we look at the effect of finite extensions on twists, as in [35, Section 2] for curves.

Remark 8.23. Let K' be a finite extension of K of degree $[K' \colon K] = n$. Then $Fr_{K'} = Fr_K^n$. There is a natural map $\Theta(A/K) \to \Theta(A/K')$ which sends the K-isomorphism class of a twist A_{ξ_ϕ}/K to the K'-isomorphism class of A_{ξ_ϕ}/K'. The equivalent map on cocycles is

$$H^1(G_K, \mathrm{Aut}_k(A)) \to H^1(\mathrm{Gal}(k/K'), \mathrm{Aut}_k(A)),\ \xi_\phi \mapsto \xi_\phi|_{\mathrm{Gal}(k/K')}.$$

Taking $g \in \mathrm{Aut}_k(A)$ to be such that $\xi_\phi(Fr_K) = g$, this yields

$$\xi_\phi|_{\mathrm{Gal}(k/K')} \colon Fr_{K'} \mapsto g({}^{Fr_K}g)({}^{Fr_K^2}g)\dots({}^{Fr_K^{n-1}}g).$$

Remark 8.24. The field over which the elements $\mathrm{Aut}_k(A)$ are defined plays an important role, as is made explicit in [27]. Most importantly, if all automorphisms of A are defined over a finite field K, then G_K acts trivially on $\mathrm{Aut}_k(A)$, so that Frobenius conjugacy classes are the same as standard conjugacy classes. In this case, if a twist A_{ξ_ϕ}/K corresponds to the conjugacy class of $g \in \mathrm{Aut}_K(A)$, then its base change A_{ξ_ϕ}/K' corresponds to the conjugacy class of g^n. By [115, Theorem 2(d)], an abelian variety over K is maximal or minimal if and only if all its endomorphisms are defined over K.

Effect of twists on Frobenius endomorphisms

Recall that $\pi = \pi_A \in \mathrm{End}_K(A)$ denotes the relative Frobenius endomorphism of A. By a famous result due to Tate [115], there is a bijection

$$\mathbf{Q}_\ell \otimes \mathrm{End}_K(A) \to \mathrm{End}_{G_K}(T_\ell(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell) \tag{8.9}$$

for any $\ell \neq p$, where $T_\ell(A)$ denotes the ℓ-adic Tate module of A. This bijection allows us to consider endomorphisms like π_A as linear operators on the vector space $T_\ell(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. Moreover, the characteristic polynomial of an endomorphism (in the sense of [58, p. 110]) coincides with that of its corresponding linear operator, by e.g. [58, Chapter VII, Theorem 3].

In this section, we investigate how twisting A affects π and its $2g$ eigenvalues. Let $[-1] \in \mathrm{End}_K(A)$ be the multiplication-by-(-1) map on A. The eigenvalues of $[-1]$, i.e. of the corresponding linear operator in $\mathrm{End}_{G_K}(T_\ell(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell)$, are then all -1.

Since π is semisimple (cf. [115, p. 138]), the corresponding linear operator is diagonalisable over $\overline{\mathbf{Q}}_\ell$. When A is maximal (resp. minimal) over K, this operator is already diagonalisable over $\mathbf{Q}_\ell$, and all its eigenvalues equal -1 (resp. 1). Thus, π is conjugate, hence equal to, the central element $[-1]$ (resp. $[1]$) of $\mathbf{Q}_\ell \otimes \mathrm{End}_K(A)$.

That is, A is maximal over K if and only if $\pi = [-1]$, and A is minimal over K if and only if $\pi = [1] = \mathrm{id}$.

Proposition 8.25. Let A_{ξ_ϕ}/K be a twist of A/K and consider the corresponding cocycle ξ_ϕ. Then its relative Frobenius endomorphism $\pi' = \pi_{A_{\xi_\phi}}$ satisfies

$$\phi^{-1} \circ \pi' \circ \phi = \pi \circ (\xi_\phi(Fr_K))^{-1}.$$

Proof. By equation (8.1), $\pi = \pi_A$ satisfies $\pi_A = f_A \otimes Fr_K^{-1}$, where $f = f_A$ is the absolute Frobenius endomorphism of A, cf. Definition 8.2. Similarly, by writing $f' = f_{A_{\xi_\phi}}$, we have $\pi' = f' \otimes Fr_K^{-1}$. Moreover, the geometric isomorphism $\phi\colon A \times_K k \xrightarrow{\sim} A_{\xi_\phi} \times_K k$ has the property that

$$f = \phi^{-1} \circ f' \circ \phi.$$

Furthermore, by equation (8.8), we have

$$(\xi_\phi(Fr_K))^{-1} = (\mathrm{id}_A \otimes Fr_K) \circ \phi^{-1} \circ (\mathrm{id}_A \otimes Fr_K^{-1}) \circ \phi.$$

Hence, adapting the proof of [72, Proposition 11], we find that the endomorphism π' on $A^{\phi} \times_K k$ satisfies

$$\begin{aligned}\phi^{-1} \circ \pi' \circ \phi &= \phi^{-1} \circ \left(f' \otimes Fr_K^{-1}\right) \circ \phi \\ &= \phi^{-1} \circ \left(\left(\phi \circ f \circ \phi^{-1}\right) \otimes Fr_K^{-1}\right) \circ \phi \\ &= \left(f \otimes Fr_K^{-1}\right) \circ (\mathrm{id}_A \otimes Fr_K) \circ \phi^{-1} \circ \left(\mathrm{id}_A \otimes Fr_K^{-1}\right) \circ \phi \\ &= \pi \circ \left(\xi_\phi(Fr_K)\right)^{-1}\end{aligned} \tag{8.10}$$

as required. □

Corollary 8.26. Suppose that A is maximal over K. A twist A_{ξ_ϕ}/K of A is minimal over K if and only if $g = \xi_\phi(Fr_K) = [-1]$. If this happens, A_{ξ_ϕ} is a nontrivial quadratic twist of A. The same holds with "maximal" and "minimal" interchanged.

Proof. By Proposition 8.25, if A/K is maximal, then there exists a twist A_{ξ_ϕ}/K which is minimal if and only if $\pi_A = -\pi_{A_{\xi_\phi}}$. So the first statement follows from the fact that $\pi_A \left(= g \circ \pi_{A_{\xi_\phi}}\right) = -\pi_{A_{\xi_\phi}}$ if and only if $g = [-1]$.

For the second part, since A is maximal over K, we have $\mathrm{Aut}_k(A) = \mathrm{Aut}_K(A)$, by [115, Theorem 2(d)]. In particular, ${}^{Fr_K}g = g$ for all $g \in \mathrm{Aut}_k(A)$. By Remark 8.23, a nontrivial quadratic twist corresponds precisely to a cocycle ξ_ϕ which satisfies $\xi_\phi(Fr_K) = g \neq \mathrm{id}$ and $\xi_\phi|_{\mathrm{Gal}(k/K')}(Fr_{K'}) = g({}^{Fr_K}g) = \mathrm{id}$ for the (unique) quadratic extension K'/K. So if A is maximal, a nontrivial quadratic twist A_{ξ_ϕ} corresponds precisely to a nontrivial $g \in \mathrm{Aut}_k(A)$ such that $g^2 = \mathrm{id}$. Then, $g = [-1]$ is a nontrivial automorphism which satisfies $g^2 = \mathrm{id}$, so the result follows. □

Twists of Jacobians

Suppose that $A = \mathrm{Jac}(X)$ for a curve X/K; then A is canonically principally polarised. Let X_{ξ_ϕ}/K be a twist of X. Then the isomorphism $\phi\colon X \times_K k \xrightarrow{\sim} X_{\xi_\phi} \times_K k$ induces an isomorphism

$$\mathrm{Jac}(\phi)\colon \mathrm{Jac}(X_{\xi_\phi}) \times_K k = \mathrm{Jac}(X_{\xi_\phi} \times_K k) \xrightarrow{\sim} \mathrm{Jac}(X \times_K k) = \mathrm{Jac}(X) \times_K k.$$

Let $f = f_X\colon X \times_K k \to X \times_K k$ be the absolute Frobenius morphism of X, let $F = F_X\colon X \times_K k \to X \times_K k$ be the relative Frobenius morphism (cf. Definition 8.2), and let $\pi\colon \mathrm{Jac}(X \times_K k) \to \mathrm{Jac}(X \times_K k)$ be the endomorphism induced by F. Then the characteristic polynomial of π is equal to $L(X/K, T)$. Also, $\xi_\phi(\sigma) \in \mathrm{Aut}_k(X)$ induces an automorphism, denoted by $\mathrm{Jac}(\xi_\phi(\sigma))$, on $\mathrm{Jac}(X \times_K k)$.

The analogue of Proposition 8.25 is the following result.

Proposition 8.27. ([72, Proposition 11]) The relative Frobenius endomorphism π' of $\mathrm{Jac}(X_{\xi_\phi} \times_K k)$ satisfies

$$\mathrm{Jac}(\phi) \circ \pi' \circ \mathrm{Jac}(\phi^{-1}) = \pi \circ \mathrm{Jac}(\xi_\phi(Fr_K)).$$

□

Now let X/K be a (smooth projective connected) supersingular curve of genus g. Let $\Theta(X/K)$ denote the set of twists of X/K modulo K-isomorphisms. The normalised Weil numbers $\{z_i\}_{1 \le i \le 2g}$ of X are the same as for $\mathrm{Jac}(X)$. However, the respective automorphism groups of X and $\mathrm{Jac}(X)$ (as a polarised abelian variety), and hence the respective sets of their twists, can be different; as a corollary of the arithmetic Torelli theorem (cf. [125]), Serre [59, Appendice] shows that

$$\mathrm{Aut}_k(\mathrm{Jac}(X)) \cong \begin{cases} \mathrm{Aut}_k(X) & \text{if } X \text{ is hyperelliptic,} \\ \{\pm 1\} \times \mathrm{Aut}_k(X) & \text{if } X \text{ is not hyperelliptic.} \end{cases}$$

We obtain that there exists an automorphism g of X that acts as $[-1]$ on $\mathrm{Jac}(X)$ if and only if X is hyperelliptic.

As a corollary, we find the analogue of Corollary 8.26 for curves.

Corollary 8.28. Suppose that a curve X is maximal (resp. minimal) over K. There exists a twist X_{ξ_ϕ}/K of X which is minimal (resp. maximal) over K if and only if X is hyperelliptic, in which case X_{ξ_ϕ} is the nontrivial quadratic twist associated with the cocycle taking Fr_K to the unique hyperelliptic involution of X.

Proof. By Corollary 8.26, there exists a twist X_{ξ_ϕ}/K with $\pi' = -\pi$, if and only if $\mathrm{Jac}(g) = \mathrm{Jac}(\xi_\phi(Fr_K)) = [-1]$, for some $g \in \mathrm{Aut}_k(X)$. Such g exists if and only if X is hyperelliptic, by the arithmetic Torelli theorem. Moreover, by choosing the base point of the Abel-Jacobi map $X \to \mathrm{Jac}(X)$ to be a hyperelliptic Weierstrass point (i.e. a ramification point of the hyperelliptic involution), we ensure that the restriction g of $\mathrm{Jac}(g) = [-1]$ to X coincides with the unique hyperelliptic involution of X. In particular, g has order 2 and X_{ξ_ϕ} is a nontrivial quadratic twist of X. □

Examples

Elliptic curves with j-invariant 1728

Lemma 8.29. If $p \equiv 3 \bmod 4$, then the elliptic curve $E : y^2 = x^3 - x$ (defined over $K = \mathbf{F}_p$) is supersingular and has j-invariant 1728.

1. If $p > 3$, then the only nontrivial twist E_{ξ_ϕ} of E has order 2 and the corresponding cocycle satisfies $\xi_\phi(Fr_K) = [-1]$.

2. If $p = 3$, then E has three nontrivial twists, one quadratic twist for which $\xi_\phi(Fr_K) = [-1]$ and two twists of order 3.

Proof. For all $p \equiv 3 \bmod 4$, consider the twist $E' : -y_1^2 = x_1^3 - x_1$, also defined over $\mathbf{F}_p$, for which the geometric isomorphism $\phi : E \to E'$ is given by $\phi(x, y) = (x, iy)$. This twist has order 2, since E and E' are isomorphic over $\mathbf{F}_{p^2}$, where -1 is a square. The corresponding cocycle ξ_ϕ sends Fr_K to the hyperelliptic involution:

$$\begin{aligned} \xi_\phi(Fr_K)(x,y) &= \phi^{-1}(Fr_K(\phi(Fr_K^{-1}(x,y)))) = \phi^{-1}(Fr_K(\phi(x^{1/p}, y^{1/p}))) \\ &= \phi^{-1}(Fr_K(x^{1/p}, iy^{1/p})) = \phi^{-1}(x, i^p y) = (x, i^{p-1}y). \end{aligned}$$

Since $p \equiv 3 \bmod 4$, then $\xi_\phi(Fr_K)(x, y) = (x, -y)$ is the hyperelliptic involution. Thus $\xi_\phi(Fr_K) = [-1]$.

1. If $p > 3$, then $\mathrm{Aut}_k(A) \simeq \mathbf{Z}/4\mathbf{Z}$. One computes that the $\mathbf{F}_p$-Frobenius conjugacy classes are

   - $\{\mathrm{id}, (x \mapsto x, y \mapsto -y)\}$
   - $\{(x \mapsto -x, y \mapsto -iy), (x \mapsto -x, y \mapsto iy)\}$.

   Thus $E/\mathbf{F}_p$ has only one nontrivial twist, which is quadratic by Remark 8.23.

2. If $p = 3$, then $|\mathrm{Aut}_k(A)| = 12$ by [107, Appendix A, Proposition 1.2]. The $\mathbf{F}_p$-Frobenius conjugacy classes are as follows:

   - $\{\mathrm{id}, (x \mapsto x, y \mapsto -y)\}$
   - $\{(x \mapsto x - 1, y \mapsto y), (x \mapsto x + 1, y \mapsto -y)\}$
   - $\{(x \mapsto x - 1, y \mapsto -y), (x \mapsto x + 1, y \mapsto y)\}$
   - $\{(x \mapsto -x, y \mapsto -iy), (x \mapsto -x, y \mapsto iy), (x \mapsto -x - 1, y \mapsto -iy),$ $(x \mapsto -x-1, y \mapsto iy), (x \mapsto -x+1, y \mapsto -iy), (x \mapsto -x+1, y \mapsto iy)\}$

   The first of these classes corresponds to the trivial twist, and the last class corresponds to the quadratic twist E' already described.

   Now let $\alpha \in \mathbf{F}_{27}$ be an element such that $\alpha^3 - \alpha = 1$. The other two $\mathbf{F}_p$-Frobenius conjugacy classes then correspond to the twists $E'' : y^2 + 1 = x^3 - x$ and $E''' : y^2 + 2 = x^3 - x$ respectively, where $\phi'' : E \to E''$ takes

$(x, y) \mapsto (x - \alpha, y)$ and $\phi''' : E \to E'''$ takes $(x, y) \mapsto (x + \alpha, y)$. One computes that

$$\begin{aligned}
\xi_{\phi'}(Fr_K)(x,y) &= (\phi')^{-1}(Fr_K(\phi'(Fr_K^{-1}(x,y)))) \\
&= (\phi')^{-1}(Fr_K(\phi'(x^{1/p}, y^{1/p}))) \\
&= (\phi')^{-1}(Fr_K(x^{1/p} \pm \alpha, y^{1/p})) \\
&= (\phi')^{-1}(x \pm \alpha^p, y) \\
&= (x \pm (\alpha^p - \alpha), y) \\
&= (x \pm 1, y).
\end{aligned}$$

Since the automorphisms g taking $(x, y) \mapsto (x \pm 1, y)$ are defined over $\mathbf{F}_p$ and have order 3, the last two twists have order 3 by Remark 8.23. □

Elliptic curves with j-invariant 0

Lemma 8.30. If $p \equiv 2 \bmod 3$ is odd, then the elliptic curve $E : y^2 = x^3 + 1$ (defined over $K = \mathbf{F}_p$) is supersingular and has j-invariant 0. The only nontrivial twist E_{ξ_ϕ} of E has order 2 and the corresponding cocycle satisfies $\xi_\phi(Fr_K) = [-1]$.

Proof. Note that $\mathrm{Aut}_k(E) \simeq \mathbf{Z}/6\mathbf{Z}$, again by [107, Appendix A, Proposition 1.2]. The automorphisms are $(x \mapsto \zeta_6^{2k} x, y \mapsto \zeta_6^{3k} y)$, $0 \leq k \leq 5$. The $\mathbf{F}_p$-Frobenius conjugacy classes are:

- $\{\mathrm{id}, (x \mapsto \overline{\zeta}_3 x, y \mapsto y), (x \mapsto \zeta_3 x, y \mapsto y)\}$
- $\{(x \mapsto x, y \mapsto -y), (x \mapsto \overline{\zeta}_3 x, y \mapsto -y), (x \mapsto \zeta_3 x, y \mapsto -y)\}$

Choose $a \in \mathbf{F}_p^*$ to be a quadratic non-residue. The nontrivial quadratic twist is $E' : ay^2 = x^3 + 1$, with $\phi : E \to E'$ given by $\phi(x, y) = (x, y/\sqrt{a})$. The corresponding cocycle ξ_ϕ sends Fr_K to the hyperelliptic involution:

$$\begin{aligned}
\xi_\phi(Fr_K)(x,y) &= \phi^{-1}(Fr_K(\phi(Fr_K^{-1}(x,y)))) = \phi^{-1}(Fr_K(\phi(x^{1/p}, y^{1/p}))) \\
&= \phi^{-1}(Fr_K(x^{1/p}, y^{1/p}/\sqrt{a})) = \phi^{-1}(x, y/\sqrt{a}^p) \\
&= (x, y/a^{(p-1)/2}).
\end{aligned}$$

Since a is not a square mod p, then $a^{(p-1)/2} \equiv -1 \bmod p$ and then $\xi_\phi(Fr_K)(x, y) = (x, -y)$ is the hyperelliptic involution. Thus $\xi_\phi(Fr_K) = [-1]$. □

CHAPTER 9

The period and the parity

In this chapter, we define the period and the parity of a supersingular abelian variety, and study their properties. We introduce the notion of a *type* of such a variety and investigate the relation between the type and the normalised Weil numbers. For elliptic curves and abelian surfaces, we look at these notions in great detail.

9.1 Definitions and properties of period and parity

In this section, let A denote a supersingular principally polarised abelian variety of dimension g over $K = \mathbf{F}_q$, and let $z_1, \ldots, z_{2g}$ denote its normalised Weil numbers, which are roots of unity. As before, let $q = p^r$ and $k = \overline{\mathbf{F}}_p = \overline{\mathbf{F}}_q$.

Throughout, one may replace A by a smooth projective connected supersingular curve X/K of genus g and consider the relative Frobenius endomorphism π of its Jacobian $\mathrm{Jac}(X)$.

Arithmetic definition of the period and parity

Definition 9.1.

1. The *K-period* $\mu(A)$ of A is the smallest natural number m such that q^m is square (i.e. rm is even) and

   (i) $z_i^m = -1$ for all $1 \leq i \leq 2g$, or

   (ii) $z_i^m = 1$ for all $1 \leq i \leq 2g$.

2. The *K-parity* $\delta(A)$ is 1 in case (i) and is -1 in case (ii), for $m = \mu(A)$.

These same notions are also (and equivalently) defined in the literature as follows.

Definition 9.2. [113, p. 144] Write $P(A/K, T) = \prod f_i^{d_i}$ where the f_i are pairwise relatively prime.

The results in this chapter are joint work with Rachel Pries.

1. The *K-period* of A/K is

   $$\mu(A) = \min\{n \in \mathbf{N} \mid q^{n/2} \in \mathbf{Z} \mid \prod f_i \text{ divides } (T^n + q^{n/2}) \text{ or } (T^n - q^{n/2})\}.$$

2. The *K-parity* of A/K is

   $$\delta(A) = \begin{cases} 1 & \text{if } \prod f_i \text{ divides } (T^{\mu(A)} + q^{\mu(A)/2}) \\ -1 & \text{if } \prod f_i \text{ divides } (T^{\mu(A)} - q^{\mu(A)/2}) \end{cases}.$$

It is clear that A is maximal (resp. minimal) over K if and only if $\mu(A) = 1$ and $\delta(A) = 1$ (resp. $\delta(A) = -1$). In Chapter 10 we study how $\mu(A)$ and $\dim(A)$ are related, and in Section 9.2 we compute $\mu(A)$ and $\delta(A)$ when $\dim(A)$ is 1 or 2.

Geometric definition of maximal and minimal types

Suppose that $K(= \mathbf{F}_q)$ is the field of definition of A. As in Definition 8.19, let $\Theta(A/K)$ denote the set of abelian varieties A_0/K such that $A_0 \times_K k \simeq_k A \times_K k$, modulo K-isomorphisms, so that $\Theta(A/K)$ consists of all the K-twists of A, modulo trivial twists.

Definition 9.3. A supersingular abelian variety A with field of definition K is of one of the following *types*:

1. *fundamentally maximal* if A_0/K has K-parity $\delta = 1$ for all $A_0 \in \Theta(A/K)$;
2. *fundamentally minimal* if A_0/K has K-parity $\delta = -1$ for all $A_0 \in \Theta(A/K)$;
3. *partially maximal* if there exist $A_0, A_0' \in \Theta(A/K)$ with K-parities $\delta(A_0) = 1$ and $\delta(A_0') = -1$.

Some observations about the period and the parity

Suppose from now on that $A_0/K \in \Theta(A/K)$ is a K-twist of A. Let t be the order of the twist; the possibilities for t are determined by $\mathrm{Aut}_k(A)$. Let K_t be the (unique up to isomorphism) field extension of K of degree t. Then $A \times_K K_t \cong_{K_t} A_0 \times_K K_t$. Denote the normalised Weil numbers of A/K by $\{z_i\}$ and those of A_0/K by $\{w_i\}$. After possibly reordering, we have $z_i^t = w_i^t$ and without loss of generality,

$$z_i = w_i y_i \tag{9.1}$$

for some (not necessarily primitive) t-th root of unity y_i, for every i, such that the least common multiple of the orders of the y_i is t.

In Lemma 9.4 up to Proposition 9.7, we assume the following hypothesis holds:

Hypothesis: The abelian variety A/K has K-period M and K-parity 1, and its K-twist A_0/K has K-period N and K-parity -1.

Lemma 9.4. If $M = N$, then t is even.

Proof. This follows immediately from the fact that $y_i^M \neq -1$ if t is odd. □

In general, A and A_0 need not have the same period. However, there is the following relation between their periods.

Proposition 9.5. Suppose that m and n are the smallest positive numbers such that $\{z_i\} \subset \mu_m$ and $\{w_i\} \subset \mu_n$. (This implies that $M \in \{m, m/2\}$ and $N \in \{m, m/2\}$). Then either $\gcd(t, n) > 1$ or $\gcd(t, m) > 1$.

Proof. By equation (9.1), we can write $z_1 = \zeta_m$, $w_1 = \zeta_n$ and $y_1 = \zeta_{t'}$ as primitive roots of unity, where $t'|t$. Hence,

$$\zeta_m = \zeta_{nt'}^{t'+n}, \tag{9.2}$$

where the right hand side is in lowest terms if and only if $(t', n) = 1$. It $(t', n) > 1$, then since $t = t'u$ for some u, also $(t, n) > 1$ and we are done. If $(t', n) = 1$, it follows that $m = nt'$, so $(t', m) > 1$, hence $(t, m) > 1$, and we are also done. □

If A and A_0 have the same period but different parities, we obtain the following result.

Proposition 9.6. Suppose that $M = N$. Fix a primitive t-th root of unity ζ_t. Let $g \in \mathrm{Aut}_k(A)$ be the automorphism corresponding to this twist, determined up to Frobenius conjugacy, and denote by the same letter g its image under the bijection from Equation (8.9). Now consider the decomposition of $T_\ell(A) \otimes \mathbf{Q}_\ell$ into eigenspaces L_j where g acts such that the normalised Weil numbers are multiplied by ζ_t^j, for some $0 \leq j \leq t-1$. Let $\ell_j = \dim(L_j)$. Then the 2-adic valuation $v_2(j)$ of j is constant over all j for which $\ell_j \neq 0$.

Proof. By definition, $z_i^N = -1$ and $w_i^N = 1$ for all i and $w_i = \zeta_t^j z_i$ for exactly ℓ_j choices of i. Hence, $\zeta_t^{jN} = -1$ for all j such that $\ell_j \neq 0$. In particular, $\ell_0 = 0$ since $\zeta_t^0 \neq -1$.

From now on, suppose j is such that $\ell_j \neq 0$. From Lemma 9.4 it follows that t is even. Write $t = 2^a t_1$ and $N = 2^b N_1$ where t_1, N_1 are odd and $a \geq 1$. Then

$$-1 = \zeta_t^{jN} = \zeta_{2^a t_1}^{j2^bN_1} = (\zeta_{2^a}^U \zeta_{t_1}^V)^{j2^bN_1} = \zeta_{2^a}^{Uj2^bN_1} \cdot \zeta_{t_1}^{Vj2^bN_1},$$

where U and V are such that $Ut_1 + V2^a = 1$. Note that $\zeta_{t_1}^{Vj2^bN_1} \neq -1$ since t_1 is odd, so

$$\zeta_{t_1}^{Vj2^bN_1} = 1$$

for each j. Therefore, $t_1 | VN_1$.

Now consider the term $\zeta_{2^a}^{Uj2^bN_1}$. If $b \geq a$, then $\zeta_{2^a}^{Uj2^bN_1} = 1$. So $b < a$. For each j, write $Uj = 2^{c_j} j_1$ where j_1 odd. Then

$$\zeta_{2^a}^{Uj2^bN_1} = (\zeta_{2^a}^{2^{b+c_j}})^{j_1N_1} = -1$$

so

$$\zeta_{2^a}^{2^{b+c_j}} = -1,$$

which implies that $c_j + b \equiv a - 1 \bmod a$. That is,

$$c_j \equiv -(1 + b) \bmod a$$

for all j such that $\ell_j \neq 0$, where the right hand side is constant as j varies. Since $c_j < a$, and $c_j = v_2(Uj) = v_2(U) + v_2(j)$ with $v_2(U)$ also constant, the result follows. □

Proposition 9.7. Fix a primitive t-th root of unity ζ_t. For each $1 \leq i \leq 2g$, there exists a $0 \leq j \leq t - 1$ such that $w_i = \zeta_t^j z_i$.

1. If $M > N$, then $j \neq 0$, t is even, and $t | 2jM$.
2. If $M < N$ and $M \equiv N \bmod 2$, then $\zeta_t^{jN} = 1$, so $t | jN$.
3. If $M < N$ and $M \not\equiv N \bmod 2$, then $t | 2jN$.

Proof. This follows from the formula $w_i = \zeta_t^j z_i$, with the relations $w_i^N = 1$ and $z_i^M = -1$ for all i. In cases 1. and 3., note that $t = 2$ implies that jM is odd for all j. Moreover, when $t \neq 2$, either $\gcd(t, jN) > 1$ or $\gcd(t, jM) > 1$, cf. Proposition 9.5. □

Arithmetic definition of maximal and minimal types

The previous section indicates that there is a relation between the type (cf. Definition 9.3) of an abelian variety and arithmetic properties of its normalised Weil numbers. This will be made explicit below.

As before, let K be the minimal field of definition of A and let $\{z_1, \ldots, z_{2g}\}$ denote the normalised Weil numbers of A/K. Fix an embedding $\overline{\mathbf{Q}} \subset \mathbf{C}$. For each

z_i, write $z_i = \zeta_{N_i}^{j_i}$, where $\gcd(N_i, j_i) = 1$, and where we view ζ_N as a (fixed) primitive root of unity. Furthermore, write $N_i = 2^{e_i} o_i$ where o_i is odd. Then e_i is the *binary value* of z_i, and we write $[z_i]_2 = v_2(N_i) = e_i$.

Remark 9.8. If $\zeta_n^k = -1$, then n is even. More generally, there exists an integer a such that $z_i^a = (\zeta_{N_i}^{j_i})^a = -1$ if and only if $2aj_i \equiv N_i \bmod 2N_i$.

From this, we see that A has K-parity $+1$ if and only if all $e_i = e \geq 1$ for all i, and K-parity -1 if and only if either $e_i = 0$ for all i, or not all e_i are the same.

Remark 9.9. By writing the normalised Weil numbers $z_i = \zeta_{N_i}^{j_i}$ as above, we ensure that the binary value of z_i is well-defined. Note however that we may also write a set of Weil numbers as $\{\sqrt{q}\zeta_n^{j_1}, \ldots, \sqrt{q}\zeta_n^{j_{2g}}\}$ for the same integer n, where the $\zeta_n^{j_i}$ might no longer be in lowest terms.

The following lemma summarises the relation between $[z]_2$ and $[-z]_2$.

Lemma 9.10. Let $z = \zeta_N^j$ be a normalised Weil number, with $0 < j < N$ coprime to N. Then $[z]_2 = 0$ if and only if $[-z]_2 = 1$. If $[z]_2 \geq 2$, then $[-z]_2 = [z]_2$.

Proof. If $[z]_2 = 0$, then N is odd and $-z = -\zeta_N^j = \zeta_{2N}^{N+2j}$, so $[-z]_2 = 1$.

If $[z]_2 = 1$, then $N = 2M$ where $M = 2\ell + 1$ is odd. Then j must be odd; write $j = 2d + 1$. Hence,

$$-z = -\zeta_N^j = \zeta_{2M}^{M+j} = \zeta_M^{\ell+d+1},$$

so $[-z]_2 = 0$.

Finally, if $[z]_2 \geq 2$, then $N = 2M$ where $M = 2\ell$ is even. Again $j = 2d + 1$ must be odd. Then

$$-z = -\zeta_N^j = \zeta_{2M}^{M+j} = \zeta_{4\ell}^{2(\ell+d)+1},$$

so $[-z]_2 = [z]_2$. □

Note that a quadratic twist is precisely a twist which negates some of the (normalised) Weil numbers, and recall that the automorphism $[-1]$ corresponds the only quadratic twist which negates all (normalised) Weil numbers simultaneously.

Proposition 9.11.

1. If A/K is fundamentally maximal, then all e_i equal the same value $e \geq 2$.

2. If A/K is fundamentally minimal, then not all e_i are the same.

Proof. 1. Suppose that A/K is fundamentally maximal. Then in particular it has parity $+1$, so by Remark 9.8, its e_i are all the same and ≥ 1. However, if $e_i = 1$ for all i, the nontrivial quadratic twist $[-1]$ will make sure that all $e_i = 0$, by Lemma 9.10; this twist has parity -1, so this cannot happen. (In fact, any twist negating some of the Weil numbers will have parity -1.) Therefore, all e_i are equal and ≥ 2.

2. Suppose now that A/K is fundamentally minimal. Then it has parity -1, so Remark 9.8 implies that either all e_i are zero, or the e_i are not all the same. But when all e_i are zero, the same twist by $[-1]$ (and no other twist negating some of the Weil numbers) will have parity $+1$, contradiction. Therefore, not all e_i are the same. □

Proposition 9.12.

1. If $e_i = 0$ for all i, or $e_i = 1$ for all i, then A/K is partially maximal.

2. If all $e_i \geq 2$ are the same, the parity of A/K is not affected by quadratic twists.

3. If not all e_i are the same, the twist by $[-1]$ does not affect the parity of A/K.

Proof. 1. follows from the proof of Proposition 9.11 and 2. follows from Proposition 9.10, since negation does not affect any $e_i \geq 2$. For 3., note that the twisted e_i will still not be all the same, so the parity of this twist is still -1. □

Types for Jacobians

Let X/K be a (smooth projective connected) supersingular curve of genus g. Recall that $\Theta(X/K)$ denotes the set of twists of X/K modulo K-isomorphisms.

The arithmetic Torelli theorem (see the discussion following Proposition 8.27) implies that when X is hyperelliptic, then $\Theta(\mathrm{Jac}(X)/K) = \Theta(X/K)$, in particular X and its Jacobian $\mathrm{Jac}(X)$ have the same type. When X is not hyperelliptic, any twist of the curve still induces a twist of its Jacobian, but the converse no longer holds. For any curve, we still define the type as follows.

Definition 9.13. A supersingular curve X with field of definition K is of one of the following *types*:

1. fundamentally maximal if X/K has K-parity $\delta = 1$ for all $X \in \Theta(X/K)$;

2. fundamentally minimal if X/K has K-parity $\delta = -1$ for all $X \in \Theta(X/K)$;

3. partially maximal if there exist $X, X' \in \Theta(X/K)$ with K-parities $\delta(X) = 1$ and $\delta(X') = -1$.

Proposition 9.14.

1. If X/K is fundamentally maximal and X has a nontrivial quadratic twist, then all e_i have the same value $e \geq 2$.

2. If X/K is fundamentally minimal and not hyperelliptic, then either all e_i are zero, or not all e_i are the same.

3. If X/K is partially maximal, then $\mathrm{Jac}(X)$ is partially maximal.

4. If all $e_i \geq 2$ are the same, then the parity of X/K is not affected by quadratic twists.

5. If X is hyperelliptic and not all e_i are the same, the twist by $[-1]$ does not affect the parity of X/K.

Proof. The proof is largely the same as for Propositions 9.11 and 9.12. For 3., note that if two curves in $\Theta(X/K)$ have different parities, then their Jacobians are in $\Theta(\mathrm{Jac}(X)/K)$ and have different parities. □

If X is not hyperelliptic, then partially maximal behaviour can still occur, despite Corollary 8.28, as seen in the example below.

Example of a partially maximal curve

Suppose q is odd and $a \in K = \mathbf{F}_q$. Consider the following plane quartic (introduced by Ciani in 1899 , and studied in [72, Section 4])

$$C_a : x^4 + y^4 + z^4 = (a+1)(x^2y^2 + y^2z^2 + x^2z^2),$$

which is nonsingular of genus 3 when $a \notin \{1, 0, -3\}$. The points of C_a in the hyperplane $z = 0$ are the points $[x' : y : 0]$ where x' is a root of $x^4 - (a+1)x^2 + 1$.

Meagher and Top show in [72] that $\mathrm{Jac}(C_a) \sim_K E_a^3$, where

$$E_a : (a+3)y^2 = x(x-1)(x-a).$$

As a result, C_a is maximal over K if and only if E_a is maximal over K and C_a is minimal over K if and only if E_a is minimal over K. Choose a such that C_a is maximal over K (i.e., it has K-period 1 and K-parity 1).

If $a \neq -1$ and $a^2 - a + 16 \neq 0$, then $\mathrm{Aut}_{\overline{K}}(C_a) \simeq S_4$. Since the automorphisms are defined over K, the twists of C_a are in bijection with conjugacy classes in S_4. So there are 5 twists of C_a, each corresponding to a specific cycle type in S_4. By discussing each of these twists, Meagher and Top show that none of the nontrivial twists of C_a are maximal over K.

We compute the periods and parities of all twists of C_a. In particular, we see that some of the nontrivial twists of C_a are not maximal over any field extension of K.

- One 3-cycle corresponds to the automorphism ϕ taking $x \mapsto z \mapsto y \mapsto x$. It acts on $\mathrm{Jac}(C_a)$ with eigenvalues ζ_3, ζ_3^2, 1. Note that if $p > 3$, then ϕ has 2 fixed points $[1 : \zeta_3 : \zeta_3^2]$ and $[1 : \zeta_3^2 : \zeta_3]$ and the quotient of C_a by ϕ has genus 1. The twist has period 3 and parity 1.

- One 4-cycle corresponds to the automorphism ψ taking $x \mapsto -y$ and $y \mapsto x$ and $z \mapsto z$. It acts on $\mathrm{Jac}(C_a)$ with eigenvalues i, $-i$, 1. The twist has period 4 and parity -1.

- The 2-cycle $\tau_1 = \psi\phi$ acts on $\mathrm{Jac}(C_a)$ with eigenvalues -1, -1, 1. We see that if $[x : y : z] = \tau_1[x : y : z] = [z : -y : x]$ then $y \neq 0$ and $z = -x$. There are typically 4 points of this form, so the quotient of C_a by τ_2 has genus 1. The twist has period 2 and parity -1.

- The $2-2$ cycle $\tau_2 = \psi^2$ acts on $\mathrm{Jac}(C_a)$ with eigenvalues -1, -1, 1. If $[x : y : z] = \tau_2[x : y : z] = [-x : -y : z]$, then $z = 0$. Moreover, τ_2 fixes the 4 points with $z = 0$, so the quotient of C_a by τ_2 has genus 1. The twist has period 2 and parity -1.

The last two cases provide examples of quadratic (i.e. degree 2) twists which act on part, but not all, of the Jacobian as multiplication by -1.

Note that C_a is partially maximal, since it has twists with parity -1. Hence, $\mathrm{Jac}(C_a)$ is also partially maximal.

9.2 Analysis in low genus

As before, we fix a finite field $K = \mathbf{F}_q$ of characteristic p. In this section, we fix a dimension g and consider all g-dimensional (simple) supersingular abelian varieties A/K. We ask the following question.

Question 9.15. What are the relative probabilities for A/K being partially maximal, fundamentally maximal, and fundamentally minimal, respectively?

However, these probabilities do not behave well for simple supersingular abelian varieties as g tends to infinity. To see this, we make the following observations. When A is simple, all its Weil numbers are conjugates of $\sqrt{\pm q}\zeta_n$ for some n, cf. Remark 9.9. Lemmas 10.4 and 10.5 imply that, depending on $q = p^r$, the possible values of n that occur are those in $\widetilde{A}(g) = \{n \colon \phi(n) \in \{g, 2g, 4g\}\}$. In particular, $v_2(g) \leq v_2(\phi(n)) \leq v_2(g) + 2$, where v_2 denotes the 2-adic valuation. As is observed in [108, Theorem 13.6], there are infinitely many values of g for which these sets are empty, in which case no g-dimensional simple A/K exists. Thus, there is no well-defined limiting behaviour as $g \to \infty$. Furthermore, the value of $v_2(\phi(n))$ does not completely determine the value of $v_2(n)$.

In this section, we instead analyse the simple supersingular abelian varieties "by hand", for small g.

Remark 9.16. The number of isogeny classes of g-dimensional simple supersingular abelian varieties A/K has been worked out in [108, Theorems 13.7 and 13.8]. Their answer is necessarily dependent on $|\widetilde{A}(m)| = |\{x\colon \phi(x) = m\}|$ for $m = 2g$ or g.

Elliptic curves ($g = 1$)

If E/K is an elliptic curve, then its L-polynomial is of the form

$$L(E/K,T) = T^2 - \beta T + q,$$

for some rational integer β. Note that E is supersingular if and only if $p \mid \beta$. The L-polynomial is either irreducible over $\mathbf{Z}$ or of the form $(T-b)^2$ for some $b \in \mathbf{Z}$.

By the Honda-Tate theorem, the K-isogeny class of E is determined by the conjugacy class of the Weil numbers, i.e., the roots of $L(E/K,T)$, and hence by β. Waterhouse [120] determined the possible values of $\pm\beta$. In the next result, we list the normalised Weil numbers ("NWN's"), (K-)periods and (K-)parities for each isogeny class. The normalised Weil numbers are (primitive) n-th roots of unity for some n; we also list the 2-adic valuations $v_2(n)$, i.e., the binary values $[z]_2$.

Proposition 9.17. Let $q = p^r$. A supersingular elliptic curve E over $K = \mathbf{F}_q$ with L-polynomial $L(E/K,T) = T^2 - \beta T + q$ is in one of the following cases.

Case	Conditions on (r,p)	β	NWN's	$[z]_2$	Period	Parity
1a	r even	$2\sqrt{q}$	$(1,1)$	0	1	-1
1b	r even	$-2\sqrt{q}$	$(-1,-1)$	1	1	1
2a	r even, $p \not\equiv 1 \pmod 3$	$\sqrt{q}$	$(-\zeta_3, -\overline{\zeta}_3)$	1	3	1
2b	r even, $p \not\equiv 1 \pmod 3$	$-\sqrt{q}$	$(\zeta_3, \overline{\zeta}_3)$	0	3	-1
3	r even, $p \equiv 3 \pmod 4$ or r odd	0	$(i,-i)$	2	2	1
4a	r odd, $p = 2$	$\sqrt{2q}$	$(\zeta_8, \overline{\zeta}_8)$	3	4	1
4b	r odd, $p = 2$	$-\sqrt{2q}$	$(\zeta_8^5, \overline{\zeta}_8^5)$	3	4	1
4c	r odd, $p = 3$	$\sqrt{3q}$	$(\zeta_{12}, \overline{\zeta}_{12})$	2	6	1
4d	r odd, $p = 3$	$-\sqrt{3q}$	$(\zeta_{12}^7, \overline{\zeta}_{12}^7)$	2	6	1

□

Using Proposition 9.17 and [107, Appendix A, Proposition 1.1], we further analyse the situation for $p = 2$ and 3. In both cases, there is a unique supersingular curve over $k = \overline{\mathbf{F}}_p$.

Lemma 9.18.

1. If $p = 2$, the supersingular elliptic curve over k is fundamentally maximal.
2. If $p = 3$, the supersingular elliptic curve over k is fundamentally maximal.

Proof. 1. Let E denote the unique supersingular elliptic curve in characteristic 2. It is defined over $\mathbf{F}_2$, with equation $y^2 + y = x^3$. We find $|E(\mathbf{F}_2)| = 3$, so $\beta = 0$, and E is in case 3 of Proposition 9.17. Since all its $\mathbf{F}_2$-twists are by construction also defined over $\mathbf{F}_2$, they are necessarily in one of the cases 3, 4a and 4b, which all have parity $+1$. Thus, E is fundamentally maximal.

2. Let E denote the unique supersingular elliptic curve in characteristic 3. It is defined over $\mathbf{F}_3$, with equation $y^2 = x^3 - x$. Then $|E(\mathbf{F}_3)| = 4$, so $\beta = 0$, and E is in case 3 of Proposition 9.17. By Example 8.29, the only nontrivial twist (of even order) acts as $[-1]$. Thus, E is fundamentally maximal. □

From now on, we suppose $p \geq 5$; then, by [107, Chapter V, Theorem 4.1(c)], the number of isomorphism classes of supersingular elliptic curves is

$$\lfloor \frac{p}{12} \rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \bmod 12 \\ 1 & \text{if } p \equiv 5 \bmod 12 \\ 1 & \text{if } p \equiv 7 \bmod 12 \\ 2 & \text{if } p \equiv 11 \bmod 12. \end{cases}$$

All the supersingular j-invariants are in $\mathbf{F}_{p^2}$. Of these $\frac{p}{12} + O(1)$ supersingular j - invariants, $O(\sqrt{p})$ lie in $\mathbf{F}_p$ [114, p. 3]. Moreover, the field of definition of the j-invariant is the field of definition of the elliptic curve.

We now analyse the supersingular elliptic curves with extra automorphisms.

Lemma 9.19. Let $p \geq 5$.

1. If $p \equiv 3 \bmod 4$, the unique supersingular elliptic curve E over k, for which $\mathrm{Aut}_k(E) \simeq \mathbf{Z}/4\mathbf{Z}$, is fundamentally maximal.
2. If $p \equiv 2 \bmod 3$, the unique supersingular elliptic curve E over k, for which $\mathrm{Aut}_k(E) \simeq \mathbf{Z}/6\mathbf{Z}$, is fundamentally maximal.

Proof. 1. The elliptic curve E is defined over $\mathbf{F}_p$ with equation $y^2 = x^3 - x$. It is in case 3 of Proposition 9.17, with normalised Weil numbers $\{i, -i\}$. By Example 8.29, the nontrivial twist acts as $[-1]$. Hence, this curve is fundamentally maximal.

2. The elliptic curve E is defined over $\mathbf{F}_p$ with equation $y^2 = x^3 + 1$. It is in case 3 of Proposition 9.17, with normalised Weil numbers $\{i, -i\}$. By Example 8.30, its nontrivial twist is $ay^2 = x^3 + 1$ for $a \in \mathbf{F}_p^*$ a quadratic non-residue. This twist is also in case 3. Thus, E is fundamentally maximal. □

Lemma 9.20. Let $p \geq 5$. Suppose E/k is a supersingular elliptic curve with $\mathrm{Aut}_k(E) \simeq \mathbf{Z}/2\mathbf{Z}$. Let K be the field of definition of E.

1. If $K = \mathbf{F}_p$, then E is fundamentally maximal.

2. If $K = \mathbf{F}_{p^2}$, then E is partially maximal.

Proof. The hyperelliptic involution ι acts as $[-1]$ and hence negates the normalised Weil numbers. If $K = \mathbf{F}_p$, then E and its twist by ι are both in case 3, thus E is fundamentally maximal. If $K = \mathbf{F}_{p^2}$, then E and its twist by ι are both in case 1, or both in case 2, thus E is partially maximal. □

In conclusion, for $g = 1$, we have proved that no supersingular elliptic curve is fundamentally minimal. This also follows from Proposition 9.11(2): an isogeny class of elliptic curves is determined by two normalised Weil numbers z and $\overline{z}$, which satisfy $[z]_2 = [\overline{z}]_2$, so all e_i are necessarily the same.

Instead, if E has normalised Weil numbers $\{z, \overline{z}\}$, we proved that E is fundamentally maximal if $[z]_2 \geq 2$ and is partially maximal if $[z]_2 \in \{0, 1\}$.

For a given finite field $\mathbf{F}_q$, applying [96, Theorem 4.6], we can count the number $N(\beta)$ of $\mathbf{F}_q$-isomorphism classes of elliptic curves in the $\mathbf{F}_q$-isogeny class determined by β. Since $N(\beta)$ is independent of the sign of β, it suffices to compute them simultaneously for the respective subcases of (1) to (3) of Proposition 9.17, as summarised in the table below.

	$\pm\beta$	$N(\beta)$
1	$\pm 2\sqrt{q}$	$\frac{1}{12}\left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right)\right)$
2	$\pm\sqrt{q}$	$1 - \left(\frac{-3}{p}\right)$
3 (r odd)	0	$H(-4p)$
3 (r even)	0	$1 - \left(\frac{-4}{p}\right)$

Here, H denotes the Kronecker class function, which is defined as a sum of class numbers (cf. [96, Proposition 2.2]), and some of whose values are tabulated in [96, page 208]. The function H grows very slowly with p. The number $N(\beta)$ depends only on p and not on q. When r is even, almost all of the isomorphism classes belong to case (1) of Proposition 9.17, since the number of isomorphism classes in the other isogeny classes is either 0, 1 or 2.

Combining this table with the data from Proposition 9.17, we draw the following conclusion.

Lemma 9.21. Let $p \geq 5$ and $q = p^r$.

1. When r is odd, there are $H(-4p)$ isomorphism classes of supersingular elliptic curves over $\mathbf{F}_q$ and they are all fundamentally maximal.

2. Suppose r is even. When $p \equiv 3 \bmod 4$ then, among the isomorphism classes of supersingular elliptic curves over $\mathbf{F}_q$, there are 2 isomorphism classes which are fundamentally maximal, and the rest are partially maximal.

   When $p \not\equiv 3 \bmod 4$, all of the isomorphism classes of supersingular elliptic curves over $\mathbf{F}_q$ are partially maximal. □

Abelian surfaces ($g = 2$)

Let A be a supersingular abelian surface over K. Its K-isogeny class is determined by the conjugacy class of its Weil numbers, or equivalently by (the Galois orbit of) the coefficients (a_1, a_2) of the characteristic polynomial of its Frobenius endomorphism,

$$P(A/K, T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2 \in \mathbf{Z}[T].$$

If A is simple, then $P(A/K,T) = h_A(T)^e$ for some irreducible $h_A(T) \in \mathbf{Z}[T]$. We want to classify the isogeny classes of supersingular abelian surfaces. But Corollary 2.8 of [68] shows that there exists a simple abelian surface over $K = \mathbf{F}_{p^r}$ with $h_A(T) = T^2 - \beta T + q$ if and only if r is even and either $\beta = \pm\sqrt{q}$ (for $p \equiv 1 \pmod 3$) or $\beta = 0$ (for $p \equiv 1 \pmod 4$), which are not supersingular by Proposition 9.17. Hence, it suffices to focus on irreducible quartic Weil polynomials.

Proposition 9.22. Let A be a simple supersingular abelian surface defined over $K = \mathbf{F}_q = \mathbf{F}_{p^r}$, with $P(A/K,T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2$.

Let $L = \mathbf{F}_{q^{t_0}}$ be the minimal field of decomposition of A, meaning that there is an L-isogeny $A \sim_L E \times E$, for some supersingular elliptic curve E. Let n_E denote the case from the first column of Table 9.17 in which E appears. The normalised Weil numbers of A over L will be of the form $(z, \overline{z}, z, \overline{z})$, so we only need to give z

(denoted by z/L). We can also compute the normalised Weil numbers $(z_1, \overline{z}_1, z_2, \overline{z}_2)$ of A over K, of which we show (z_1, z_2), as well as the K-period (denoted by P) and the K-parity (denoted by δ). The following cases occur.

	(a_1, a_2)	Conditions on (r, p)	t_0	n_E	z/L	(z_1, z_2)	P	δ
1a	$(0, 0)$	r odd, $p \equiv 3\ (4)$ or r even, $p \not\equiv 1\ (4)$	2	3	i	(ζ_8, ζ_8^3)	4	1
1b	$(0, 0)$	r odd, $p \equiv 1\ (4)$ or r even, $p \equiv 5\ (8)$	4	1	-1	(ζ_8, ζ_8^3)	4	1
2a	$(0, q)$	r odd, $p \not\equiv 1\ (3)$	2	2	ζ_3	(ζ_6, ζ_3)	6	-1
2b	$(0, q)$	r odd, $p \equiv 1\ (3)$	6	1	-1	$(\zeta_{12}, \zeta_{12}^5)$	6	1
3a	$(0, -q)$	r odd, $p \neq 3$ or r even, $p \not\equiv 1\ (3)$	2	2	$-\zeta_3$	$(\zeta_{12}, \zeta_{12}^5)$	6	1
3b	$(0, -q)$	r odd, $p \equiv 1\ (3)$ or r even, $p \equiv 4, 7, 10\ (12)$	3	3	i	$(\zeta_{12}, \zeta_{12}^5)$	6	1
4a	$(\sqrt{q}, q)$	r even, $p \not\equiv 1\ (5)$	5	1	1	(ζ_5, ζ_5^2)	5	-1
4b	$(-\sqrt{q}, q)$	r even, $p \not\equiv 1\ (5)$	5	1	-1	$(\zeta_{10}, \zeta_{10}^3)$	5	1
5a	$(\sqrt{5q}, 3q)$	r odd, $p = 5$	5	1	± 1	$(\zeta_{10}^3, \zeta_5^2)$	10	-1
5b	$(-\sqrt{5q}, 3q)$	r odd, $p = 5$	5	1	± 1	(ζ_{10}, ζ_5)	10	-1
6a	$(\sqrt{2q}, q)$	r odd, $p = 2$	4	2	$-\zeta_3$	$(\zeta_{24}^{13}, \zeta_{24}^{19})$	12	1
6b	$(-\sqrt{2q}, q)$	r odd, $p = 2$	4	2	$-\zeta_3$	$(\zeta_{24}, \zeta_{24}^7)$	12	1
7a	$(0, -2q)$	r odd	2	1	1	$(1, -1)$	2	-1
7b	$(0, 2q)$	r even, $p \equiv 1\ (4)$	2	2	-1	(i, i)	2	1
8a	$(2\sqrt{q}, 3q)$	r even, $p \equiv 1\ (3)$	3	1	1	(ζ_3, ζ_3)	3	-1
8b	$(-2\sqrt{q}, 3q)$	r even, $p \equiv 1\ (3)$	3	1	-1	(ζ_6, ζ_6)	3	1

Proof. We make use of the computations of Maisner and Nart [68]. In particular, the first three columns form Table 1 on p. 325 of [68]. We also use their Lemma 2.13, together with the observation at the end of the statement of their Theorem 2.9, to compute the coefficients of the L-polynomial of A over the extension $L = \mathbf{F}_{q^{t_0}}$ of $\mathbf{F}_q$, and hence to determine n_E. From this, z/L can be read off from Table 9.17. This in turn determines the period P, since P is the product of t_0 and the period of the elliptic curves, while the parity of the surface $A \sim E \times E$ is the same as the parity of E; both the period and the parity of the elliptic curves are taken from Table 9.17.

To determine the normalised Weil numbers of A over $\mathbf{F}_q$, denoted $(z_1, \overline{z}_1, z_2, \overline{z}_2)$ or (b_1, b_2, b_3, b_4), we first computed all the t_0-th roots of the normalised Weil numbers over L and found the possible conjugate pairs $z + \overline{z}$ of these. Then, we checked whether a combination of two such pairs $(z_1, \overline{z}_1)$ and $(z_2, \overline{z}_2)$ satisfied the relations

$z_1 + \overline{z}_1 + z_2 + \overline{z}_2 = -a_1$ and $\sum_{1 \le i < j \le 4} b_i b_j = a_2$; the unique solution to this provided the normalised Weil numbers over $\mathbf{F}_q$. Alternatively, we found the roots of the L-polynomial $T^4 + a_1 T^3 + a_2 T^2 + q a_1 T + q^2 = 0$ directly, using MATHEMATICA.

Case 5 is an interesting one. Maisner and Nart show that A first decomposes over $\mathbf{F}_{q^5}$. We used MATHEMATICA to find the roots of the corresponding Weil polynomial $T^4 + \sqrt{5q}T^3 + 3qT^2 + \sqrt{5q}qT + q^2$ over $\mathbf{F}_q$. Raising these normalised $\mathbf{F}_q$-Weil numbers to the fifth power, we obtain $(-1, -1, 1, 1)$ for the normalised Weil numbers over $L = \mathbf{F}_{q^5}$. This is what the ± 1 table entry for z/L in this case signifies. We conclude that A is L-isogenous to $E_1 \times E_2$, where E_1 has normalised Weil numbers $(-1, -1)$ and E_2 has normalised Weil numbers $(1, 1)$. Note that E_1 is in case 1b and E_2 in case 1a of Proposition 9.17. Over $\mathbf{F}_{q^{10}}$, both E_1 and E_2 become minimal; therefore, A has parity -1. □

Remark 9.23. It follows from Proposition 9.12 that Cases (4) and (8) of Proposition 9.22 are partially maximal. To determine the types of the other surfaces, we would need to know their automorphism groups explicitly.

Chapter 10

Arithmetic statistics of dimension

Let us fix a finite field $K = \mathbf{F}_q$ of characteristic p. In this chapter, we use (normalised) Weil numbers to determine the expected dimension of a "randomly chosen" supersingular abelian variety over K.

Given a root of unity z, the Honda-Tate theorem guarantees that there exists a simple supersingular abelian variety A_z over K, unique up to K-isogeny, whose Weil numbers are $\sqrt{q}z$ and its Galois conjugates.

Question 10.1. Suppose $z_1, \ldots, z_s$ are s randomly chosen roots of unity. That is, all z_i are independently picked from a set μ_{ℓ^N} of ℓ^N-th roots of unity, for some prime number ℓ and integer N, equipped with the uniform distribution. Consider the supersingular abelian variety $A = A_{z_1} \times \cdots \times A_{z_s}$. What is the probability that A has dimension g?

In Proposition 10.7, we answer this question for $\ell = 2$.

The probabilities

Fix a prime number ℓ and an integer N. The set μ_{ℓ^N} of ℓ^N-th roots of unity has cardinality ℓ^N. Assuming that we are equally likely to pick any element of μ_{ℓ^N}, we can compute the following probabilities as relative proportions.

Lemma 10.2. Pick $z \in \mu_{\ell^N}$ at random. Then

- $\mathbf{P}(z = 1) = \frac{1}{\ell^N}$,
- $\mathbf{P}(z \in \mu_{\ell^{N-1}}) = \frac{1}{\ell}$,
- $\mathbf{P}(z \in \mu_{\ell^i} \setminus \mu_{\ell^{i-1}}) = \frac{\ell - 1}{\ell^{N+1-i}}$ for any $1 \leq i \leq N$.

□

The results in this chapter are joint work with Rachel Pries.

Expected dimension

Recall that $\pi_A \in \mathrm{End}(A)$ is the relative Frobenius endomorphism of A.

Let $\mathscr{E} = \mathrm{End}_K(A) \otimes \mathbf{Q}$ and let $\Psi = \mathbf{Q}(\pi_A)$ be the subalgebra of $\mathscr{E}$ generated by π_A. Since $\mathscr{E}$ is a division algebra and Ψ is the centre of $\mathscr{E}$, Ψ is a field [121, Theorem 8.2]. For $\mathfrak{p}$ a prime of $\mathscr{O}_\Psi$, consider the local invariant $\mathrm{inv}_\mathfrak{p}(\mathscr{E})$, which satisfies $||\pi_A||_\mathfrak{p} = q^{-\mathrm{inv}_\mathfrak{p}(\mathscr{E})}$. By [121, Theorem 8.4], we have

$$\mathrm{inv}_\mathfrak{p}(\mathscr{E}) \equiv \begin{cases} \frac{1}{2} & \text{if } \mathfrak{p} \text{ is real} \\ 0 & \text{if } \mathfrak{p} \text{ lies above } l \neq p \\ \frac{v_\mathfrak{p}(\pi_A)}{v_\mathfrak{p}(q)}[\Psi_\mathfrak{p} \colon \mathbf{Q}_p] & \text{if } \mathfrak{p} \text{ lies above } p. \end{cases}$$

Let e be the smallest positive integer such that $e \cdot \mathrm{inv}_\mathfrak{p}(\mathscr{E}) \in \mathbf{Z}$ for all $\mathfrak{p} \in \mathscr{O}_\Psi$. The characteristic polynomial $P(A/K, T)$ of π_A satisfies $P(A/K, T) = h_A^e$ for some irreducible monic $h_A \in \mathbf{Z}[T]$.

The relation between the dimension $g = \dim(A)$ and the Weil numbers is given by the following equation, cf. [121, Theorem 8.3]:

$$2\mathrm{dim}(A) = [\mathscr{E} \colon \Psi]^{\frac{1}{2}}[\Psi \colon \mathbf{Q}] = e[\Psi \colon \mathbf{Q}]. \tag{10.1}$$

Now consider the factorisation of $P(A/K, T)$ in $\mathbf{Q}_p[T]$ into a product $\prod_i f_i(T)$ of irreducible polynomials. There is a bijection between the irreducible factors f_i and the primes $\mathfrak{p}_i$ above p. By [108, pp. 2 – 3], since A is supersingular,

$$\mathrm{inv}_{\mathfrak{p}_i}(E) \equiv \begin{cases} 0 & \text{if } \deg(f_i) \text{ is even} \\ \frac{1}{2} & \text{if } \deg(f_i) \text{ is odd} \end{cases} \pmod{\mathbf{Z}}. \tag{10.2}$$

In particular, $e = 1$ if $\deg(f_i)$ is even for all i and $e = 2$ if either $\deg(f_i)$ is odd for some i, or $\pi_A = \pm\sqrt{q}$ (since then $P(A/K, T)$ has only real roots, cf. Lemma 10.3).

Below, let us write a normalised Weil number $z = \zeta_n$ as a primitive n-th root of unity and a Weil number as $\alpha = \sqrt{q}z = \sqrt{q}\zeta_n$. We will consider the simple supersingular abelian variety denoted A or A_z over K.

Let $\Phi_m(T)$ denote the m-th cyclotomic polynomial of degree $\phi(m)$ and let $\Phi_m^{[\sqrt{q}]}(T) = (\sqrt{q})^{\phi(m)}\Phi(\frac{T}{\sqrt{q}})$. Moreover, for any prime number p and integer m, let

$$u = \begin{cases} \text{order of } p \text{ in } (\mathbf{Z}/m\mathbf{Z})^* & \text{if } (p, m) = 1 \\ f(p^k - p^{k-1}) \text{ where } f \text{ is the order of } p \text{ in } (\mathbf{Z}/s\mathbf{Z})^* & \text{if } m = p^k s \end{cases}. \tag{10.3}$$

Lemma 10.3. Let $K = \mathbf{F}_q = \mathbf{F}_{p^r}$ and suppose that $\pi_A = \pm\sqrt{q}$. Then we have $\alpha = \pm\sqrt{q}$, so $\zeta_n = \pm 1$, i.e. $n = 1$ or 2.

- When r is odd, $\Psi = \mathbf{Q}(\pi_A) = \mathbf{Q}(\pm\sqrt{q})$, so $[\Psi \colon \mathbf{Q}] = 2$ and $e = 2$. Hence, $\dim(A) = 2$, the normalised Weil numbers are $(1, 1, -1, -1)$, and $P(A/K, T) = (T^2 - q)^2$.
- When r is even, $\Psi = \mathbf{Q}$ and $u = 1$ is odd, so $e = 2$ and $\dim(A) = 1$. Hence, A is a minimal or maximal elliptic curve with normalised Weil numbers $(1, 1)$ or $(-1, -1)$. We have $P(A/K, T) = (T \pm \sqrt{q})^2$.

In particular, $\pi_A = \pm\sqrt{q}$ is equivalent to $P(A/K, T)$ having only real roots. □

The first case of Lemma 10.3 occurs in Case 5 of Proposition 9.22.

Lemma 10.4 (Theorems 3.1 and 11.1 of [108])**.** Let $K = \mathbf{F}_q = \mathbf{F}_{p^r}$ and suppose that $\pi_A \neq \pm\sqrt{q}$.

- Suppose r is odd. Then $P(A/K, T)$ is irreducible for any simple supersingular abelian variety A/K, so $e = 1$ and $2\dim(A) = [\Psi \colon \mathbf{Q}]$.
- Suppose r is even. Then $P(A/K, T)$ for any simple supersingular abelian variety A/K is of the form $(\Phi_m^{[\sqrt{q}]}(T))^e$ where $\phi(m) = 2g$ for some integer g. If u is even for m and p, then $e = 1$, so $\dim(A) = g$; if u is odd, then $e = 2$ so $\dim(A) = 2g$. □

Having determined e for any simple supersingular A_z/K, it remains to determine the possible values for $[\Psi \colon \mathbf{Q}]$ that occur. We note that $[\Psi \colon \mathbf{Q}] = \deg(h_A)$ is the degree of the minimal polynomial of $\sqrt{q}z = \sqrt{q}\zeta_n$. As such, $[\Psi \colon \mathbf{Q}]$ is completely determined by $q = p^r$ (i.e. by p and r) and n. We have the following result (cf. also [108, Theorem 3.3 and Remark 3.4(1)]).

Lemma 10.5. Consider a Weil number $\alpha = \sqrt{q}\zeta_n$, where $q = p^r$ and $n \neq 1, 2$. If r is even, then α is a primitive n-th root of unity and $[\Psi \colon \mathbf{Q}] = \phi(n)$.

Let r be odd.

1. Suppose that $p \nmid n$. Then

$$[\Psi \colon \mathbf{Q}] = \begin{cases} \phi(n) & \text{if } v_2(n) \geq 2, \\ 2\phi(n) & \text{if } v_2(n) \leq 1. \end{cases}$$

2. Suppose that $p | n$ and $p \equiv 1 \bmod 4$. Then

$$[\Psi \colon \mathbf{Q}] = \phi(n).$$

3. Suppose that $p|n$ and $p \equiv 3 \bmod 4$. Then
$$[\Psi\colon \mathbf{Q}] = \begin{cases} \phi(n) & \text{if } v_2(n) \geq 3, \\ \frac{1}{2}\phi(n) & \text{if } v_2(n) = 2, \\ 2\phi(n) & \text{if } v_2(n) \leq 1. \end{cases}$$

4. Suppose that $p|n$ and $p = 2$. Then
$$[\Psi\colon \mathbf{Q}] = \begin{cases} \phi(n) & \text{if } v_2(n) \geq 4, \\ \frac{1}{2}\phi(n) & \text{if } v_2(n) = 3, \\ \phi(n) & \text{if } v_2(n) = 2, \\ 2\phi(n) & \text{if } v_2(n) = 1. \end{cases}$$

Proof. We give the conjugates of α in all cases; some cases were taken from [108, pp. 5-6].

- When r is even, $\sqrt{q} \in \mathbf{Q}$, so the conjugates of α are $\sqrt{q}\zeta_n^j$ for $j \in (\mathbf{Z}/n\mathbf{Z})^*$, of which there are $\phi(n)$.
  So from now on, we will assume r is odd.

- First suppose that $p \nmid n$ so that $\sqrt{q} \notin \mathbf{Q}(\zeta_n)$. When $v_2(n) \geq 2$, the conjugates of α are $\sqrt{q}\zeta_n^j$ for $j \in (\mathbf{Z}/n\mathbf{Z})^*$ again. This follows from the fact that $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ has index 2 in $\mathrm{Gal}(\mathbf{Q}(\zeta_n, \sqrt{q})/\mathbf{Q})$, since $-\zeta_n = \zeta_n^{1+n/2}$ is primitive and hence the automorphism $\sqrt{q} \mapsto -\sqrt{q}$, $\zeta_n \mapsto -\zeta_n$ fixes α. When $v_2(n) \leq 1$ however, $-\zeta_n$ is no longer a primitive n-th root of unity, so the conjugates of α are $\pm\sqrt{q}\zeta_n^j$, for $j \in (\mathbf{Z}/n\mathbf{Z})^*$, and $[\Psi\colon \mathbf{Q}] = 2\phi(n)$.

- Now suppose $p|n$ and $p > 2$. When $p \equiv q \equiv 1 \bmod 4$, $\sqrt{q} \in \mathbf{Q}(\zeta_n)$, so the conjugates of α are
  $$\left(\frac{j}{p}\right)\sqrt{q}\zeta_n^j,$$
  for $j \in (\mathbf{Z}/n\mathbf{Z})^*$, hence $[\Psi\colon \mathbf{Q}] = \phi(n)$.
  When $p \equiv q \equiv 3 \bmod 4$ and $v_2(n) \geq 3$, the conjugates of α are
  $$(j \bmod 4)\left(\frac{j}{p}\right)\sqrt{q}\zeta_n^j,$$
  for $j \in (\mathbf{Z}/n\mathbf{Z})^*$. When $v_2(n) = 2$, $n = 4t$ for t odd, and the conjugates are $(j \bmod 4)\left(\frac{j}{p}\right)\sqrt{q}\zeta_n^j$, for $j \in (\mathbf{Z}/t\mathbf{Z})^*$, since $j = 1 + 2t$ leaves α fixed. When $v_2(n) \leq 1$, $\sqrt{q} \notin \mathbf{Q}(\zeta_n)$ and we again find conjugates $\pm\sqrt{q}\zeta_n^j$, for $j \in (\mathbf{Z}/n\mathbf{Z})^*$.

- Finally, suppose that $p = 2$. When $v_2(n) \geq 4$, the conjugates of α are $\chi(j)\sqrt{q}\zeta_n^j$, for $j \in (\mathbf{Z}/n\mathbf{Z})^*$, where $\chi\colon (\mathbf{Z}/8\mathbf{Z})^* \to (\mathbf{Z}/4\mathbf{Z})^*$ is a character satisfying $\chi(\pm 1) = 1$ and $\chi(\pm 3) = -1$. When $v_2(n) = 3$ so $n = 8s$ for s odd, they are $\sqrt{q}\zeta_8^{\pm 1}\zeta_s^b$, for $b \in (\mathbf{Z}/s\mathbf{Z})^*$, of which there are $2\phi(s) = \frac{1}{2}\phi(n)$. When $v_2(n) = 2$, they are $\sqrt{q}\zeta_n^j$ for $j \in (\mathbf{Z}/n\mathbf{Z})^*$, since $\sqrt{2} \notin \mathbf{Q}(\zeta_n)$. When $v_2(n) = 1$, $-\zeta_n$ is not primitive, so the conjugates are $\pm\sqrt{q}\zeta_n^j$, for $j \in (\mathbf{Z}/n\mathbf{Z})^*$; the same is true when $v_2(n) = 0$, which was included in the $p \nmid n$ case above. □

Corollary 10.6. A simple supersingular abelian variety A/K is not fundamentally minimal when r is even.

Proof. This follows from Lemma 10.5, since the binary values of the normalised Weil numbers of A are always all the same. □

Finally, recall that an integer $n = 2^k p_1^{k_1} \dots p_r^{k_r}$ (where p_i are distinct odd primes) satisfies

$$\phi(n) = 2^{k-1} p_1^{k_1 - 1}(p_1 - 1) \cdot \dots \cdot p_r^{k_r - 1}(p_r - 1), \tag{10.4}$$

so that

$$v_2(\phi(n)) \geq k - 1 + r. \tag{10.5}$$

Now we study the expected dimension of an abelian variety that arises in the random way explained in Lemma 10.2. We make the simplifying assumption that $z \in \mu_{2^N}$. That is, we pick $z \in \mu_{2^N}$ at random and write $z = \zeta_{2^m}^j$ (and $\alpha = \sqrt{q}z$), where $\gcd(2^m, j) = 1$. Recall that $\phi(2^m) = 2^{m-1}$.

Proposition 10.7. Let $q = p^r$. Pick $z = \zeta_{2^m}^j \in \mu_{2^N}$ at random.

1. Let r be odd and $p > 2$. Then

$$\dim(A) = \begin{cases} 1 \\ 2 \\ 2^{m-2} \text{ for } 4 \leq m \leq N \end{cases} \quad \text{with probability} \begin{cases} \frac{1}{2^{N-1}} \\ \frac{6}{2^N} \\ \frac{1}{2^{N+1-m}} \end{cases}.$$

2. Let r be odd and $p = 2$. Then

$$\dim(A) = \begin{cases} 1 \\ 2 \\ 2^{m-2} \text{ for } 4 \leq m \leq N \end{cases} \quad \text{with probability} \begin{cases} \frac{3}{2^{N-1}} \\ \frac{1}{2^{N-1}} \\ \frac{1}{2^{N+1-m}} \end{cases}.$$

3. Let r be even and $p > 2$. Then u (cf. Lemma 10.4) is odd, so
$$\dim(A) = \begin{cases} 1 \\ 2^{m-1} \text{ for } 2 \leq m \leq N \end{cases} \quad \text{with probability } \begin{cases} \frac{1}{2^{N-1}} \\ \frac{1}{2^{N+1-m}} \end{cases}.$$

4. Let r be even and $p = 2$. Then u (cf. Lemma 10.4) is even, so
$$\dim(A) = \begin{cases} 1 \\ 2^{m-2} \text{ for } 3 \leq m \leq N \end{cases} \quad \text{with probability } \begin{cases} \frac{1}{2^{N-2}} \\ \frac{1}{2^{N+1-m}} \end{cases}.$$

Proof. Suppose that r is odd and $p > 2$. Lemma 10.3 implies that $\dim(A) = 2$ when $[z]_2 = m \leq 1$. When instead $m \geq 2$, Lemmas 10.4 and 10.5 show that $2\dim(A) = [\Psi\colon \mathbf{Q}] = \phi(2^m) = 2^{m-1}$, i.e. $\dim(A) = 2^{m-2}$. Thus, $\dim(A) = 1$ if and only if $m = 2$, which happens with probability $1/2^{N-1}$ by Lemma 10.2. Also, $\dim(A) = 2$ if $m = 0, 1$ or 3, with probability
$$\frac{1}{2^N} + \frac{1}{2^N} + \frac{1}{2^{N-2}} = \frac{6}{2^N}.$$
Finally, $\dim(A) = 2^{m-2}$ for $m \geq 4$ with probability $1/2^{N+1-m}$.

The other cases are proven similarly. □

Remark 10.8. Using Proposition 10.7, it is straightforward to compute the probabilities for $\dim(A)$ when $A = A_{z_1} \times \ldots \times A_{z_s}$ corresponds to a choice of several $z_1, \ldots, z_s$, since we may consider the probabilities for the $\dim(A_{z_i})$ as independent.

Remark 10.9. The simplifying assumption that $n = 2^m$ implies we can only obtain abelian varieties whose dimension is a power of 2. However, Proposition 10.7 shows that every such dimension is obtained with nonzero probability, if we let N tend to infinity. Moreover, for any choice of N, a random abelian variety will have the maximal dimension 2^{N-2} (or 2^{N-1}) with probability $\frac{1}{2}$.

Remark 10.10. It is an interesting question to ask whether one can put a meaningful probability distribution on all isogeny classes of simple supersingular abelian varieties, in order to study the distribution of dimensions that occur. In particular, we would like to understand whether some (normalised) Weil numbers are more likely to occur than others. At this stage, it is not clear to us which probability distribution would be most natural.

HOOFDSTUK 11

Samenvatting

In dit hoofdstuk zullen de resultaten van het tweede deel van dit proefschrift (met de titel “Galois representations”), worden uitgelegd voor niet-wiskundigen.

Sommige voorwerpen zijn symmetrisch: een wit vel papier bijvoorbeeld, of een glas, of een frisbee. We kunnen symmetrieën opvatten als handelingen, namelijk, als dingen die je kunt doen met een voorwerp zonder wezenlijk te veranderen hoe het eruit ziet. Zo kunnen we het vel papier bijvoorbeeld omdraaien, maar niet opvouwen of scheuren. In het bijzonder telt “niks doen” ook als een symmetrie. Alle symmetrieën van één object vormen een zogeheten *groep*, omdat we symmetrieën ongedaan kunnen maken en kunnen samenstellen (dat wil zeggen, de ene symmetrie na de andere uitvoeren).

Niet alleen fysieke objecten hebben symmetrieën; vergelijkingen kunnen ook symmetrisch zijn. Als voorbeeld nemen we de vergelijking

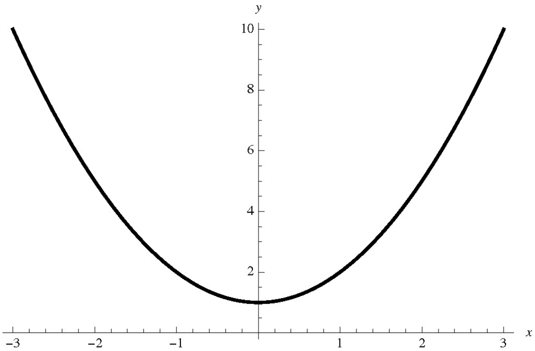
$$x^2 + 1 = 0. \tag{11.1}$$

Aangezien geen enkel *reëel* getal (dat wil zeggen, een getal dat we op een getallenlijn kunnen zetten, zoals 23 of π of $\sqrt{2}$) een kwadraat heeft dat negatief is, lijkt het erop dat vergelijking (11.1) geen oplossing heeft. Maar hiervoor hebben wiskundigen de *complexe* getallen bedacht; we gebruiken de letter i voor een (*“imaginair”*) getal dat voldoet aan $i^2 = -1$. Omdat dan ook $i^2 + 1 = -1 + 1 = 0$, is i dus een oplossing voor onze vergelijking. Dan zien we meteen dat $-i$ ook een oplossing is, want ook $(-i)^2 = i^2 = -1$. Merk nu op dat we net zo goed het eerste getal $-i$ hadden kunnen noemen en het tweede getal i; zolang de *symmetrie* tussen de oplossingen, die zegt dat de ene oplossing de negatieve versie van de andere is, maar is behouden.

Door een vergelijking op te vatten als een functie en daar de grafiek van te tekenen, vinden we een verband tussen vergelijkingen en fysieke, geometrische objecten. De grafiek van vergelijking (11.1) zou eruit zien als twee punten (eentje voor i, en eentje voor $-i$). Maar nemen we bijvoorbeeld de vergelijking

$$y = x^2 + 1, \tag{11.2}$$

dan vinden we een zogenaamde parabool; dit is een één-dimensionaal object, zie Figuur 11.1. Hierbij tekenen we de reële oplossingen; we zien dus dat $y \neq 0$, omdat bij $y = 0$ de complexe waarden $x = i, -i$ horen.



Figuur 11.1: De grafiek van de parabool $y = x^2 + 1$.

Beschouwen we meerdere vergelijkingen tegelijk, met meer variabelen dan alleen x en y, dan vinden we hoger-dimensionale objecten. Hieruit kunnen we concluderen dat er een nauw verband is tussen het bestuderen van geometrische objecten en vergelijkingen. Een geometrisch object dat wordt beschreven door vergelijkingen als hierboven heet een *algebraïsche variëteit*.

Als iemand je een object of een verzameling vergelijkingen geeft, dan is het een interessant probleem om te bepalen welke symmetrieën het allemaal heeft. De technieken die wiskundigen hiervoor gebruiken, zijn geïntroduceerd door Évariste Galois (1811-1832).

Maar het is ook mogelijk om de tegenovergestelde vraag te stellen: als iemand je een groep symmetrieën geeft, kun je dan een object bedenken, beschreven door vergelijkingen, wat precies die symmetrieën heeft? Dit heet het Inverse Galois Probleem. Als een symmetriegroep inderdaad een bijbehorende algebraïsche variëteit heeft, zeggen we dat die groep *realiseerbaar* is ("als een Galoisgroep").

Het Inverse Galois Probleem werd voor het eerste geformuleerd door David Hilbert (1862-1943). In 1892 bewees hij dat de zogenaamde permutatiegroepen S_n en A_n realiseerbaar zijn (voor alle waarden van n). In 1954 bewees Igor Shafarevich hetzelfde voor een andere soort symmetriegroepen: de eindige oplosbare groepen.

Of daadwerkelijk *alle* groepen realiseerbaar zijn, is nog niet opgelost. Tijdens mijn promotieonderzoek heb ik bewezen dat een bepaalde oneindige familie van groepen, namelijk de zes-dimensionale *symplectische* groepen, realiseerbaar zijn. Hiervóór was realiseerbaarheid alleen bewezen voor vier-dimensionale symplectische groepen.

Het idee van het bewijs is als volgt: binnen een zes-dimensionale symplectische groep vinden we twee symmetrieën die de groep *voortbrengen*. Dat wil zeggen dat als we deze twee symmetrieën (en hun *inverses*, die ze ongedaan maken) maar vaak genoeg samenstellen, we uiteindelijk alle elementen van de groep zullen vinden.

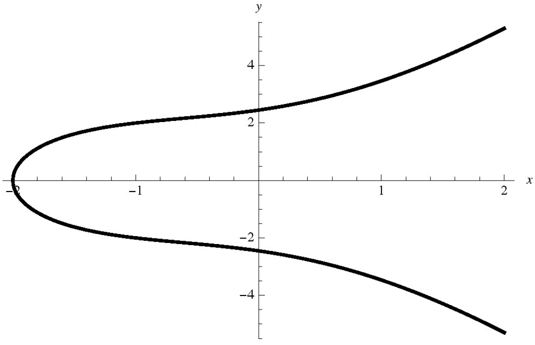
Nu construeren we twee *krommen*, laten we ze C_p en C_q noemen. Een kromme is een één-dimensionale algebraïsche variëteit, zoals de parabool $y = x^2 + 1$. We doen het zo, dat C_p de ene voortbrengende symmetrie van de symplectische groep heeft en C_q de andere.

Vervolgens maken we een nieuwe kromme, genaamd C, die informatie onthoudt over allebei de vorige krommen, en daardoor allebei de symmetrieën heeft. (In wiskundetaal: C_p en C_q zijn *reducties* van C.)

We bekijken een voorbeeld van een kromme en twee van haar reducties. Stel dat de kromme C wordt beschreven door de vergelijking

$$y^2 = x^3 + 2x^2 + 3x + 6. \tag{11.3}$$

De grafiek van de (reële) oplossingen van deze vergelijking ziet er zo uit:

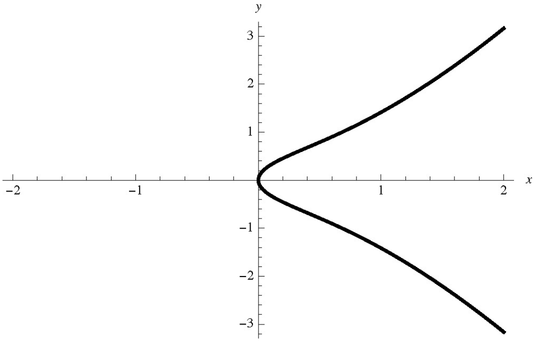


Figuur 11.2: De grafiek van de kromme C: $y^2 = x^3 + 2x^2 + 3x + 6$.

Nu vormen we de eerste reductie van C, als volgt: de *coëfficiënten* aan de rechterkant van vergelijking (11.3) zijn 1, 2, 3 en 6. We rekenen uit wat de waarde van deze coëfficiënten is, *modulo* 2. Dat wil zeggen: we delen de getallen door 2, en kijken wat de rest van deze deling is. We vinden achtereenvolgens 1, 0, 1 en 0. Door de coëfficiënten van C te vervangen door deze nieuwe getallen, vinden we een nieuwe vergelijking:

$$y^2 = x^3 + x. \tag{11.4}$$

Dit beschrijft ook een kromme, die we C_2 noemen. We zeggen dat C_2 de *reductie bij* 2 is van C. Deze kromme ziet er als volgt uit.

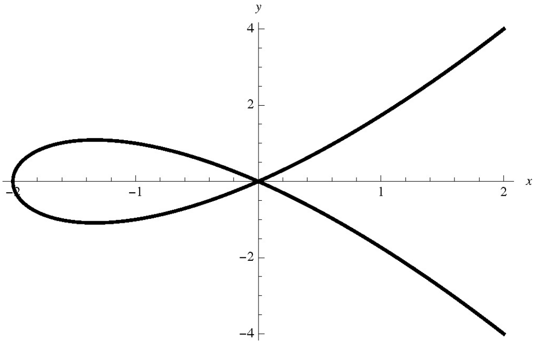


Figuur 11.3: De grafiek van de kromme $C_2\colon\, y^2 = x^3 + x$.

We kunnen hetzelfde trucje uitvoeren door niet modulo 2, maar modulo 3 te rekenen. De coëfficiënten 1, 2, 3 en 6 van C_1 worden nu 1, 2, 0 en 0. Vergelijking (11.3) wordt dan:

$$y^2 = x^3 + 2x^2. \tag{11.5}$$

De grafiek van vergelijking (11.5) geeft ons een derde kromme C_3, die de reductie van C bij 3 is:



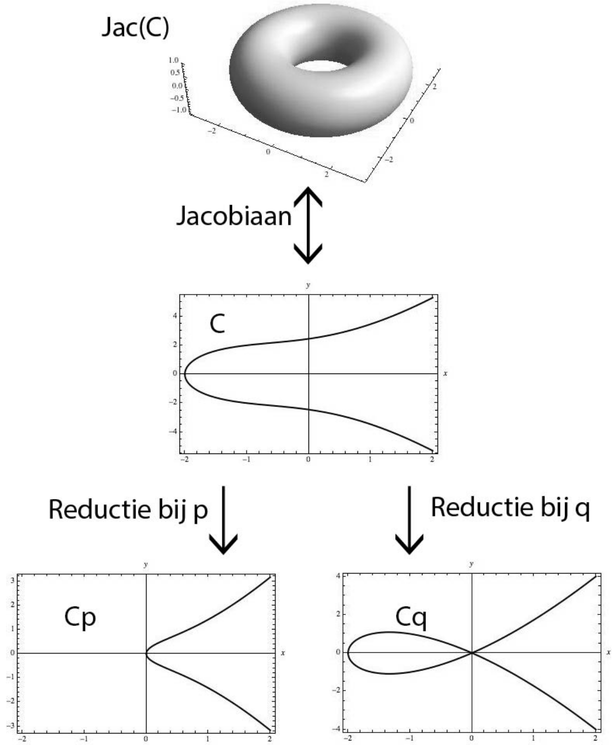
Figuur 11.4: De grafiek van de kromme $C_3\colon\, y^2 = x^3 + 2x^2$.

Voor ieder getal n kunnen we de reductie van C bij n op eenzelfde manier maken. Het grappige is, dat iedere reductie er weer heel anders uit kan zien, zoals we ook in de bovenstaande plaatjes zien.

Wiskundige opmerking: we laten in Figuren 11.3 en 11.4 weer de reële oplossingen zien, terwijl de krommen eigenlijk gedefinieerd zijn over $\mathbf{Z}/2\mathbf{Z}$, resp. $\mathbf{Z}/3\mathbf{Z}$.

Terug naar het bewijs van de stelling: stel nu dat we een kromme C hebben, die twee reducties heeft, C_p en C_q, die zo gekozen zijn, dat ze elk een voortbrengende symmetrie hebben. We vormen dan de *Jacobiaan* van deze kromme C; hoe dit in zijn werk gaat, zou helaas te lang duren om uit te leggen. Terwijl een kromme ééndimensionaal is, heeft onze Jacobiaan dimensie drie. Daarnaast heeft de Jacobiaan de eigenschap dat hij niet alleen de twee bijzondere symmetrieën heeft die de kromme heeft, maar ook alle symmetrieën die daar weer combinaties van zijn. Doordat de twee bijzondere symmetrieën *voortbrengers* zijn, vormen deze combinaties precies de symplectische groep die we wilden realiseren!

De Jacobiaan van C, afgekort tot $\mathrm{Jac}(C)$, is dus het object waarmee we de symplectische groep realiseren. In Figuur 11.5 vatten we de constructie nog een keer samen.



Figuur 11.5: Overzicht van de bewijsconstructie.

Disclaimer voor wiskundigen: C, C_p en C_q uit het voorbeeld en Figuur 11.5 zijn elliptische krommen, terwijl de krommen die in het bewijs gebruikt worden, geslacht 3 hebben.

CHAPTER 12

Acknowledgements

First of all, I would like to thank my supervisor, Gunther Cornelissen, for his guidance during the past four years, and for everything he has taught me about mathematics, academia, and other things.

I am indebted to the members of the thesis committee, Frits Beukers, Julia Hartmann, Elena Mantovan, Bart de Smit, and Maarten Solleveld, for carefully reading this thesis and sending me valuable feedback.

Working with Sara Arias-de-Reyna, Cécile Armana, Marusia Rebolledo, Lara Thomas, and Núria Vila has been a great experience from which I have learned a lot. Thanks to Marie-José Bertin, Alina Bucur, Brooke Feigon, and Leila Schneps for organising the Women in Numbers Europe conference in 2013 that inititated this collaboration.

I would like to thank Rachel Pries for inviting me to Colorado, and for the wonderful time spent discussing supersingular abelian varieties and many other things. Thanks to Douglas Ortego and Katherine Zaunbrecher for being such wonderful and welcoming hosts, and to Jeffrey Achter, Ryan Becker, Anne Ho and others at CSU; your friendliness made my visits even more enjoyable.

To Frans Oort, I am grateful for the numerous times he either explained things to me, or listened to my ideas and gave me useful feedback, also on parts of this thesis.

I gratefully acknowledge the interesting and helpful discussions I have had with various other people at Utrecht University, including Frits Beukers, Carel Faber, and Wilberd van der Kallen.The other PhD students and colleagues in Utrecht I would like to thank for the pleasant working conditions at the department. In particular, thanks to Jean Arthur, Ria Bekkering-Bosboom, Helga Hoiting, and Cécile Lemette, for taking such good care of everything.

It has been a pleasure to discuss Hecke algebras with Maarten Solleveld, who kindly shared his knowledge on this topic. I thank other colleagues from outside Utrecht for their interest in my work and helpful discussions.

I am grateful to Ariane Mézard for hosting me in Paris, to Marie-France Vignéras for her warm hospitality and the interesting conversations, and to Jan Nekovář for useful discussions on Galois representations.

Het eerste jaar in kamer 600 met Janne verdient een torenkamer in mijn geheugenpaleis. De daaropvolgende jaren als kamergenote van KaYin hadden niet beter kunnen zijn, dankzij alle thee- en chocoladepauzes, ansichtkaarten en gezelligheid, zowel op als buiten het werk. Ook bedankt voor de fijne samenwerking voor EWM-NL en de LATEX-hulp.

Ik voel me bevoorrecht zoveel mensen te mogen bedanken voor hun vriendschap en steun. In het bijzonder wil ik de volgende mensen noemen: Anna, die de beste huisgenote is geweest die ik me kon wensen; Tessa, die ook de prachtige omslag van dit proefschrift heeft gemaakt; Cecilia en Tamar, al zo lang een constante factor; Boris en Yvette, voor veel gezellige en culturele avondjes; Jeltsje en Justine en Sanne, voor het zingen, kletsen en koffie- of theedrinken; Adam, Arne, Chris, Claire, Eddy, Hannah, Jenny, Julius, Lily, Margaret, Mike, Olli, Pri, and Rob, close friends despite the distance. Daarnaast ben ik Anna, Elijah, Eva, Ino en Yvette erkentelijk voor hun commentaar op de Nederlandse samenvatting.

Zonder al mijn teamgenoten, bij UFO en het Nederlands Damesteam, waren deze vier jaar maar een kale bedoening geweest. Samen met jullie op een frisbeeveld staan was niet alleen de perfecte tegenhanger van een dag in mijn eentje over wiskunde nadenken, maar ook een eer en een geweldige ervaring op zichzelf. Dank jullie wel daarvoor.

Cilia, bedankt voor je goede zorgen, aanmoediging, interesse, en al het andere. Mijn familie, met name Eva en Dirk, wil ik bedanken voor hun onvoorwaardelijke steun.

Tenslotte is het niet meer dan terecht dat Ino en Eva, die in het leven het dichtst bij mij staan, dat ook tijdens de verdediging van dit proefschrift zullen doen. Jullie zijn mijn klankbord, mijn lievelingsmensen met wie ik alles kan delen; jullie zijn de besten!

Curriculum Vitae

Valentijn Zoë Karemaker was born on 13 April 1990 in Utrecht, the Netherlands. In 2007, she graduated from both Christelijk Gymnasium Utrecht and Junior College Utrecht. She subsequently studied mathematics, physics and astronomy at Utrecht University for a year. From 2008 until 2012 she studied mathematics at Cambridge University (UK), where she wrote her Part III essay on p-adic uniformisation under the supervision of Professor Anthony Scholl and obtained her MMath degree with distinction.

In September 2012, she started her PhD project under the supervision of Professor Gunther Cornelissen, which has led to two scientific articles that constitute the first part of this thesis. Between 2012 and 2016, she attended several international schools and conferences, including the Arizona Winter School in Tucson (in 2014 and 2015), and the Women in Numbers Europe conference in Luminy (in 2013). This conference led to a collaboration resulting in two research articles, forming the second part of this thesis. In February 2014, she visited Professor Ariane Mézard at Jussieu, Paris. In October 2014 and September 2015, she visited Professor Rachel Pries at Colorado State University, Fort Collins; this collaboration resulted in the third part of this thesis.

During these years, she also taught various undergraduate and master's courses at Utrecht University. Together with KaYin Leung, she was the local coordinator for European Women in Mathematics (EWM), and founder of the Dutch platform EWM-NL, for which she organised several national events.

From August 2016, she will be a postdoctoral fellow at the University of Pennsylvania in Philadelphia.

Bibliography

[1] Victor Abrashkin, *On a local analogue of the Grothendieck conjecture*, Internat. J. Math. **11** (2000), no. 2, 133–175.

[2] ______, *Modified proof of a local analogue of the Grothendieck conjecture*, J. Théor. Nombres Bordeaux **22** (2010), no. 1, 1–50.

[3] Athanasios Angelakis and Peter Stevenhagen, *Imaginary quadratic fields with isomorphic abelian Galois groups*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 21–39.

[4] Sara Arias-de-Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, and Núria Vila, *Large galois images for jacobian varieties of genus 3 curves*, Preprint, arXiv:1507.05913 (2015).

[5] Sara Arias-de-Reyna, Luis Dieulefait, Sug Woo Shin, and Gabor Wiese, *Compatible systems of symplectic Galois representations and the inverse Galois problem III. Automorphic construction of compatible systems with suitable local properties*, Math. Ann. **361** (2015), no. 3-4, 909–925.

[6] Sara Arias-de-Reyna, Luis Dieulefait, and Gabor Wiese, *Classification of subgroups of symplectic groups over finite fields containing a transvection*, Demonstratio Mathematica, to appear (2015).

[7] Sara Arias-de Reyna, Wojciech Gajda, and Sebastian Petersen, *Big monodromy theorem for abelian varieties over finitely generated fields*, J. Pure Appl. Algebra **217** (2013), no. 2, 218–229.

[8] Sara Arias-de-Reyna and Christian Kappen, *Abelian varieties over number fields, tame ramification and big Galois image*, Math. Res. Lett. **20** (2013), no. 1, 1–17.

[9] Sara Arias-de-Reyna and Núria Vila, *Tame Galois realizations of* $\mathrm{GL}_2(\mathbb{F}_l)$ *over* $\mathbb{Q}$, J. Number Theory **129** (2009), no. 5, 1056–1065.

[10] ______, *Tame Galois realizations of* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *over* $\mathbb{Q}$, Int. Math. Res. Not. IMRN (2011), no. 9, 2028–2046.

[11] Anne-Marie Aubert, Paul Baum, and Roger Plymen, *The Hecke algebra of a reductive p-adic group: a geometric conjecture*, Noncommutative geometry and number theory, Aspects Math., E37, Vieweg, Wiesbaden, 2006, pp. 1–34.

[12] Joseph Bernstein, Pierre Deligne, David Kazhdan, and Marie-France Vignéras (eds.), *Représentations des groupes réductifs sur un corps local*, Travaux en Cours. [Works in Progress], Hermann, Paris, 1984.

[13] Joseph Bernstein and Andrei Zelevinskiĭ, *Representations of the group $GL(n, F)$, where F is a local non-Archimedean field*, Uspehi Mat. Nauk **31** (1976), no. 3(189), 5–70.

[14] Marie José Bertin, Alina Bucur, Brooke Feigon, and Leila Schneps (eds.), *Women in Numbers Europe: research directions in number theory*, Association for Women in Mathematics Series, vol. 2, Springer, 2015.

[15] Corinne Blondel, *Quelques propriétés des paires couvrantes*, Math. Ann. **331** (2005), no. 2, 243–257.

[16] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[17] Armand Borel and Jacques Tits, *Groupes réductifs*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 27, 55–150.

[18] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[19] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[20] Glen Bredon, *Topology and geometry*, Graduate Texts in Mathematics, vol. 139, Springer-Verlag, New York, 1993.

[21] Daniel Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, vol. 55, Cambridge University Press, Cambridge, 1997.

[22] Daniel Bump, James Cogdell, Ehud de Shalit, Dennis Gaitsgory, Emmanuel Kowalski, and Stephen Kudla, *An introduction to the Langlands program*, Birkhäuser Boston, Inc., Boston, MA, 2003, Lectures presented at the Hebrew University of Jerusalem, Jerusalem, March 12–16, 2001, Edited by Joseph Bernstein and Stephen Gelbart.

[23] Colin Bushnell and Guy Henniart, *The local Langlands conjecture for* $\mathrm{GL}(2)$, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 335, Springer-Verlag, Berlin, 2006.

[24] Colin Bushnell and Philip Kutzko, *The admissible dual of* $\mathrm{GL}(N)$ *via compact open subgroups*, Annals of Mathematics Studies, vol. 129, Princeton University Press, Princeton, NJ, 1993.

[25] ______, *Smooth representations of reductive* p*-adic groups: structure theory via types*, Proc. London Math. Soc. (3) **77** (1998), no. 3, 582–634.

[26] ______, *Semisimple types in* GL_n, Compositio Math. **119** (1999), no. 1, 53–97.

[27] Gabriel Cardona, *On the number of curves of genus 2 over a finite field*, Finite Fields Appl. **9** (2003), no. 4, 505–526.

[28] Leonard Carlitz, *A theorem of Stickelberger*, Math. Scand. **1** (1953), 82–84.

[29] William Casselman, *Introduction to the theory of admissible representations of* p*-adic reductive groups*, 1995, Available at https://www.math.ubc.ca/~cass/research/pdf/p-adic-book.pdf.

[30] John Cassels, *Local fields*, London Mathematical Society Student Texts, vol. 3, Cambridge University Press, Cambridge, 1986.

[31] Yu Chen, *Isomorphisms of adjoint Chevalley groups over integral domains*, Trans. Amer. Math. Soc. **348** (1996), no. 2, 521–541.

[32] Gunther Cornelissen and Valentijn Karemaker, *Hecke algebra isomorphisms and adelic points on algebraic groups*, Preprint, arXiv:1409.1385 (2014).

[33] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307.

[34] Michael Dettweiler, Ulf Kühn, and Stefan Reiter, *On Galois representations via Siegel modular forms of genus two*, Math. Res. Lett. **8** (2001), no. 4, 577–588.

[35] Daniel Goldstein, Robert Guralnick, Everett Howe, and Michael Zieve, *Nonisomorphic curves that become isomorphic over extensions of coprime degrees*, J. Algebra **320** (2008), no. 6, 2526–2558.

[36] Jean-Baptiste Gramain, *On defect groups for generalized blocks of the symmetric group*, J. Lond. Math. Soc. (2) **78** (2008), no. 1, 155–171.

[37] Chris Hall, *Big symplectic or orthogonal monodromy modulo l*, Duke Math. J. **141** (2008), no. 1, 179–203.

[38] ______, *An open-image theorem for a general class of abelian varieties*, Bull. Lond. Math. Soc. **43** (2011), no. 4, 703–711, With an appendix by Emmanuel Kowalski.

[39] Safia Haloui, *The characteristic polynomials of abelian varieties of dimensions 3 over finite fields*, J. Number Theory **130** (2010), no. 12, 2745–2752.

[40] Michael Harris and Richard Taylor, *The geometry and cohomology of some simple Shimura varieties*, Annals of Mathematics Studies, vol. 151, Princeton University Press, Princeton, NJ, 2001, With an appendix by Vladimir G. Berkovich.

[41] Helmut Hasse, *Zahlentheorie*, Dritte berichtigte Auflage, Akademie-Verlag, Berlin, 1969.

[42] Guy Henniart, *Une preuve simple des conjectures de Langlands pour* $\mathrm{GL}(n)$ *sur un corps p-adique*, Invent. Math. **139** (2000), no. 2, 439–455.

[43] Edwin Hewitt and Karl Stromberg, *Real and abstract analysis*, Springer-Verlag, New York-Heidelberg, 1975, A modern treatment of the theory of functions of a real variable, Third printing, Graduate Texts in Mathematics, No. 25.

[44] David Hilbert, *Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. **110** (1892), 104–129.

[45] Everett Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401.

[46] Everett Howe and Hui June Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory **92** (2002), no. 1, 139–163.

[47] Masatoshi Ikeda, *Completeness of the absolute Galois group of the rational number field*, J. Reine Angew. Math. **291** (1977), 1–22.

[48] Kenkichi Iwasawa, *On the rings of valuation vectors*, Ann. of Math. (2) **57** (1953), 331–356.

[49] Hervé Jacquet, *Représentations des groupes linéaires p-adiques*, Theory of group representations and Fourier analysis (Centro Internaz. Mat. Estivo (C.I.M.E.), II Ciclo, Montecatini Terme, 1970), Edizioni Cremonese, Rome, 1971, pp. 119–220.

[50] Hervé Jacquet and Robert Langlands, *Automorphic forms on* $\mathrm{GL}(2)$, Lecture Notes in Mathematics, Vol. 114, Springer-Verlag, Berlin-New York, 1970.

[51] Gordon James and Adalbert Kerber, *The representation theory of the symmetric group*, Encyclopedia of Mathematics and its Applications, vol. 16, Addison-Wesley Publishing Co., Reading, Mass., 1981, With a foreword by P. M. Cohn, With an introduction by Gilbert de B. Robinson.

[52] Moshe Jarden and Jürgen Ritter, *On the characterization of local fields by their absolute Galois groups*, J. Number Theory **11** (1979), no. 1, 1–13.

[53] Christian Jensen, Arne Ledet, and Noriko Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002, Constructive aspects of the inverse Galois problem.

[54] Valentijn Karemaker, *Hecke algebras for* GL_n *over local fields*, Preprint, arXiv:1510.06606 (2015).

[55] Yukiyosi Kawada, *On the group ring of a topological group*, Math. Japonicae **1** (1948), 1–5.

[56] Chandrashekhar Khare, Michael Larsen, and Gordan Savin, *Functoriality and the inverse Galois problem*, Compos. Math. **144** (2008), no. 3, 541–564.

[57] Norbert Klingen, *Arithmetical similarities*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1998, Prime decomposition and finite group theory, Oxford Science Publications.

[58] Serge Lang, *Abelian varieties*, Interscience Tracts in Pure and Applied Mathematics. No. 7, Interscience Publishers, Inc., New York; Interscience Publishers Ltd., London, 1959.

[59] Kristin Lauter, *Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields*, J. Algebraic Geom. **10** (2001), no. 1, 19–36, With an appendix in French by J.-P. Serre.

[60] Pierre Le Duff, *Représentations galoisiennes associées aux points d'ordre ℓ des jacobiennes de certaines courbes de genre* 2, Bull. Soc. Math. France **126** (1998), no. 4, 507–524.

[61] Reynald Lercier and Christophe Ritzenthaler, *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects*, J. Algebra **372** (2012), 595–636.

[62] Ke-Zheng Li and Frans Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Mathematics, vol. 1680, Springer-Verlag, Berlin, 1998.

[63] Qing Liu, *Courbes stables de genre* 2 *et leur schéma de modules*, Math. Ann. **295** (1993), no. 2, 201–222.

[64] ______, *Algebraic geometry and arithmetic curves (second edition, 2006)*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[65] Manfred Lochter, *Arithmetische Ähnlichkeiten zwischen globalen Körpern positiver Characteristik*, Diplomarbeit Universität Köln (1989).

[66] Paul Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342** (1994), no. 2, 729–752.

[67] Oliver Lorscheid and Cecília Salgado, *Schemes as functors on topological rings*, J. Number Theory **159** (2016), 193–201.

[68] Daniel Maisner and Enric Nart, *Abelian surfaces over finite fields as Jacobians*, Experiment. Math. **11** (2002), no. 3, 321–337, With an appendix by Everett W. Howe.

[69] Yuri Manin, *Theory of commutative formal groups over fields of finite characteristic*, Uspehi Mat. Nauk **18** (1963), no. 6 (114), 3–90.

[70] David Masser and Gisbert Wüstholz, *Isogeny estimates for abelian varieties, and finiteness theorems*, Ann. of Math. (2) **137** (1993), no. 3, 459–472.

[71] William Massey, *Singular homology theory*, Graduate Texts in Mathematics, vol. 70, Springer-Verlag, New York-Berlin, 1980.

[72] Stephen Meagher and Jaap Top, *Twists of genus three curves over finite fields*, Finite Fields Appl. **16** (2010), no. 5, 347–368.

[73] James Milne, *Abelian varieties (v2.00)*, 2008, Available at www.jmilne.org/math/.

[74] ———, *Basic theory of affine group schemes*, 2012, Available at www.jmilne.org/math/.

[75] ———, *Lie algebras, algebraic groups, and lie groups*, 2013, Available at www.jmilne.org/math/.

[76] Shinichi Mochizuki, *A version of the Grothendieck conjecture for p-adic local fields*, Internat. J. Math. **8** (1997), no. 4, 499–506.

[77] David Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*, Math. Ann. **181** (1969), 345–351.

[78] Jürgen Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. Math. **6** (1969), 296–314.

[79] ———, *Über die absoluten Galoisgruppen algebraischer Zahlkörper*, Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976), Soc. Math. France, Paris, 1977, pp. 67–79. Astérisque, No. 41–42.

[80] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[81] Joseph Oesterlé, *Nombres de Tamagawa et groupes unipotents en caractéristique p*, Invent. Math. **78** (1984), no. 1, 13–88.

[82] Timothy O'Meara, *Lectures on linear groups*, American Mathematical Society, Providence, R.I., 1974, Expository Lectures from the CBMS Regional Conference held at Arizona State University, Tempe, Ariz., March 26–30, 1973, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 22.

[83] Midori Onabe, *On the isomorphisms of the Galois groups of the maximal Abelian extensions of imaginary quadratic fields*, Natur. Sci. Rep. Ochanomizu Univ. **27** (1976), no. 2, 155–161.

[84] Frans Oort, *Subvarieties of moduli spaces*, Invent. Math. **24** (1974), 95–119.

[85] ———, *Abelian varieties over finite fields*, Higher-dimensional geometry over finite fields, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16, IOS, Amsterdam, 2008, pp. 123–188.

[86] Frans Oort and Kenji Ueno, *Principally polarized abelian varieties of dimension two or three are Jacobian varieties*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **20** (1973), 377–381.

[87] Robert Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), no. 3, 342–360.

[88] Vasyl' Petechuk, *Automorphisms of matrix groups over commutative rings*, Mat. Sb. (N.S.) **117(159)** (1982), no. 4, 534–547, 560.

[89] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen.

[90] Bjorn Poonen, *Rational points on varieties*, 2016, Available at http://math.mit.edu/~poonen/.

[91] Dipendra Prasad and Anantharam Raghuram, *Representation theory of* $\mathrm{GL}(n)$ *over non-Archimedean local fields*, School on Automorphic Forms on $\mathrm{GL}(n)$, ICTP Lect. Notes, vol. 21, Abdus Salam Int. Cent. Theoret. Phys., Trieste, 2008, pp. 159–205.

[92] Christophe Ritzenthaler, *Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves*, LMS J. Comput. Math. **13** (2010), 192–207.

[93] Matthieu Romagny, *Models of curves*, Arithmetic and geometry around Galois theory. Based on two summer schools, Istanbul, Turkey, 2008 and 2009, Basel: Birkhäuser, 2013, pp. 149–170.

[94] Igor Šafarevič, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR. Ser. Mat. **18** (1954), 525–578.

[95] Helmut Salzmann, Theo Grundhöfer, Hermann Hähl, and Rainer Löwen, *The classical fields*, Encyclopedia of Mathematics and its Applications, vol. 112, Cambridge University Press, Cambridge, 2007, Structural features of the real and rational numbers.

[96] René Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211.

[97] Otto Schreier and Bartel van der Waerden, *Die Automorphismon der projektiven Gruppen*, Abh. Math. Sem. Univ. Hamburg **6** (1928), no. 1, 303–322.

[98] Vincent Sécherre, *The Bernstein decomposition for smooth complex representations of GL(n,F)*, Science Press (2013), Available at http://lmv.math.cnrs.fr/annuaire/vincent-secherre/.

[99] Tsutomu Sekiguchi, *The coincidence of fields of moduli for nonhyperelliptic curves and for their Jacobian varieties*, Nagoya Math. J. **82** (1981), 57–82.

[100] ______, *Erratum: "The coincidence of fields of moduli for nonhyperelliptic curves and for their Jacobian varieties"* [*Nagoya Math. J.* **82** *(1981), 57–82*], Nagoya Math. J. **103** (1986), 161.

[101] Kaoru Sekino and Tsutomu Sekiguchi, *On the fields of definition for a curve and its Jacobian variety*, Bull. Fac. Sci. Engrg. Chuo Univ. Ser. I Math. **31** (1988), 29–31 (1989).

[102] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[103] ______, *Rational points on curves over finite fields*, Lectures given at Harvard University. Notes by F. Q. Gouvêa (1985).

[104] ______, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.

[105] ______, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000, 1985–1998.

[106] Carl Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math. **66** (1944), 122–136.

[107] Joseph Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[108] Vijaykumar Singh, Gary McGuire, and Alexey Zaytsev, *Characteristic polynomial of supersingular abelian varieties over finite fields*, Preprint, arXiv: 1110.1116 (2011).

[109] Tonny Springer, *Linear algebraic groups*, second ed., Progress in Mathematics, vol. 9, Birkhäuser Boston, Inc., Boston, MA, 1998.

[110] William Stein et al., *Sage Mathematics Software (Version 6.0)*, The Sage Development Team, 2014, http://www.sagemath.org.

[111] Peter Stevenhagen and Hendrik Lenstra Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37.

[112] Henning Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[113] Henning Stichtenoth and Chao Ping Xing, *On the structure of the divisor class group of a class of curves over finite fields*, Arch. Math. (Basel) **65** (1995), no. 2, 141–150.

[114] Andrew Sutherland, *Identifying supersingular elliptic curves*, (2012), Available at https://math.mit.edu/~drew/AMS2012.pdf.

[115] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[116] Jay Taylor, *Families of irreducible representations of* $s_2 \wr s_3$, 2012, Available at https://documents.epfl.ch/users/j/jt/jtaylor/www/PDF/representations_of_S2-wrS3.pdf.

[117] Kôji Uchida, *Isomorphisms of Galois groups*, J. Math. Soc. Japan **28** (1976), no. 4, 617–620.

[118] Paulo Viana and Jaime Rodriguez, *Eventually minimal curves*, Bull. Braz. Math. Soc. (N.S.) **36** (2005), no. 1, 39–58.

[119] Lawrence Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[120] William Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

[121] William Waterhouse and James Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64.

[122] Torsten Wedhorn, *The local Langlands correspondence for* $\mathrm{GL}(n)$ *over* p*-adic fields*, School on Automorphic Forms on $\mathrm{GL}(n)$, ICTP Lect. Notes, vol. 21, Abdus Salam Int. Cent. Theoret. Phys., Trieste, 2008, pp. 237–320.

[123] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.

[124] ———, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946), Hermann & Cie., Paris, 1948.

[125] ———, *Zum Beweis des Torellischen Satzes*, Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. **1957** (1957), 33–53.

[126] Steven Weintraub, *Fundamentals of algebraic topology*, Graduate Texts in Mathematics, vol. 270, Springer, New York, 2014.

[127] James Wendel, *On isometric isomorphism of group algebras*, Pacific J. Math. **1** (1951), 305–311.

[128] Nan Hua Xi, *Representations of affine Hecke algebras*, Lecture Notes in Mathematics, vol. 1587, Springer-Verlag, Berlin, 1994.

[129] Shuji Yamagata, *A counterexample for the local analogy of a theorem by Iwasawa and Uchida*, Proc. Japan Acad. **52** (1976), no. 6, 276–278.

[130] Rong Yan, *Isomorphisms between affine Hecke algebras of type* $\widetilde{A}_2$, J. Algebra **324** (2010), no. 5, 984–999.

[131] Yuri Zarhin, *Two-dimensional families of hyperelliptic jacobians with big monodromy*, Preprint, arXiv:1310.6532 (2014).

[132] Andrei Zelevinskiĭ, *Induced representations of reductive* $\mathfrak{p}$*-adic groups. II. On irreducible representations of* $\mathrm{GL}(n)$, Ann. Sci. École Norm. Sup. (4) **13** (1980), no. 2, 165–210.