École Polytechnique Fédérale de Lausanne

Master's Thesis in Mathematics

Associating abelian varieties to weight-2 modular forms: the Eichler-Shimura construction

Author:
Corentin Perret-Gentil

Supervisors:

Prof. Akshay Venkatesh
Stanford University

Prof. Philippe Michel
EPF Lausanne

Spring 2014

Abstract

This document is the final report for the author's Master's project, whose goal was to study the Eichler-Shimura construction associating abelian varieties to weight-2 modular forms for $\Gamma_0(N)$. The starting points and main resources were the survey article by Fred Diamond and John Im [DI95], the book by Goro Shimura [Shi71], and the book by Fred Diamond and Jerry Shurman [DS06]. The latter is a very good first reference about this subject, but interesting points are sometimes eluded. In particular, although most statements are given in the general setting, the book mainly deals with the particular case of elliptic curves (i.e. with forms having rational Fourier coefficients), with little details about abelian varieties. On the other hand, Chapter 7 of Shimura's book is difficult, according to the author himself, and the article by Diamond and Im skims rapidly through the subject, being a survey. The goal of this document is therefore to give an account of the theory with intermediate difficulty, accessible to someone having read a first text on modular forms – such as [Zag08] – and with basic knowledge in the theory of compact Riemann surfaces (see e.g. [Mir95]) and algebraic geometry (see e.g. [Har77]).

This report begins with an account of the theory of abelian varieties needed for what follows. The main goal is to explain why the Jacobian (resp. Picard group) of a compact Riemann surface (resp. nonsingular algebraic curve) are abelian varieties, and to explain when quotients of abelian varieties can be formed. Then, we summarize the construction of modular curves as compact Riemann surfaces and their relationship with modular forms. Moreover, we introduce moduli spaces of enhanced elliptic curves and show how they relate to modular curves as well. The next step is to introduce the Hecke algebra, and its action on modular forms, moduli spaces, and on modular curves and their Jacobians, through the Hecke ring. As soon as we have studied the number field associated to an eigenform and the action of its complex embeddings on newforms, we can define and study the abelian variety associated to a newform: its dimension and alternative expressions, the action of Hecke operators and the decomposition of the Jacobian. The last two chapters are devoted to proving the relationships through L-functions between a modular form and its associated abelian variety. To do that, the main step is to prove the *Eichler-Shimura relation*, computing the reduction of Hecke operators on Jacobians of modular curves in terms of the Frobenius. It remains then to transfer this relation to the abelian varieties to be able to conclude. At the end of the text, two appendices give respectively numerical examples in the genus 1 case, and a summary of the basic theory of modular forms to fix notations and serve as a reference.

Acknowledgements

I would like to express my sincere gratitude to Professor Akshay Venkatesh, who accepted to supervise my learning on this subject at Stanford, and who patiently spent time to shed light on my questions in extremely interesting ways.

I am equally grateful to Professor Philippe Michel and the Chair of Analytic Number Theory at EPFL, who made my coming to Stanford possible and from whom I have learnt so much during the past two years.

Finally, I would not have been able to take this wonderful opportunity without a fellowship from the EPFL; I thank them and the Section de Mathématiques.

Contents

Introduction

The famous *modularity theorem*, whose proof was recently established by Wiles, Breuil, Conrad, Diamond and Taylor, can be stated as follows:

Theorem. *Any elliptic curve E defined over $\mathbb{Q}$ with conductor N is* modular*: there exists a newform $f \in S_2(\Gamma_0(N))$ such that $L(s, E) = L(s, f)$. Equivalently, $a_p(E) = a_p(f)$ for all primes p.*

Previously known as the *Taniyama-Shimura-Weil conjecture*, this result arose as a converse of the following construction of Eichler and Shimura: *If $f \in S_2(\Gamma_0(N))$ is a newform with rational Fourier coefficients, there exists an elliptic curve E defined over $\mathbb{Q}$ such that $a_p(E) = a_p(f)$ for almost all primes p.*

For example, we will see that the unique newform in $\Gamma_0(11)$, whose Fourier expansion begins with

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + \dots$$

corresponds to the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

This construction can be generalized by the following theorem, whose study will be the goal of this document:

Theorem (Eichler-Shimura, Carayol, Langlands, Deligne)**.** *Let $f \in S_2(\Gamma_0(N))$ be a newform. There exists an abelian variety A_f such that*

1. *A_f is defined over $\mathbb{Q}$.*
2. *A_f has dimension $[K_f : \mathbb{Q}]$, where $K_f = \mathbb{Q}(\{a_n(f) : n \geq 0\})$ is the number field of f. In particular, if the Fourier coefficients of f are all rational, then A_f is an elliptic curve.*
3. *A_f and f are related by their L-functions: we have*

   $$L(A_f, s) = \prod_{\tau} L(f_\tau, s),$$

   where the product is over the complex embeddings $\tau : K_f \to \mathbb{C}$. Alternatively, $a_p(A_f) = \sum_\tau a_p(f_\tau)$ for all primes p.

The idea is the following: we consider *modular curves*, which are compact Riemann surfaces strongly related to modular forms. By the general theory of compact Riemann surfaces, their Jacobians are complex abelian varieties. The *Hecke algebra* acts on modular forms, modular curves, and the Jacobians of the latter. Moreover, the set of newforms is composed of simultaneous eigenvectors for the Hecke operators, and the eigenvalues are the Fourier coefficients. By quotienting the Jacobian of a modular curve by the action of a well-chosen subgroup of the Hecke algebra, we obtain the desired abelian variety.

By analyzing their function fields, we see that these modular curves, as algebraic curves, can in fact be defined over $\mathbb{Q}$. Moreover, the same holds true for their

Jacobians and the Hecke operators, leading to the fact that the abelian varieties can be defined over $\mathbb{Q}$ as well.

The key property, equality of L-functions, comes from a relationship between Hecke operators on a modular curve and the Frobenius maps on its reductions: the *Eichler-Shimura relation.* From the latter, we obtain the relationship between local factors of the L-function of the abelian variety (which are related to the Frobenius maps) and local factors of L-functions of modular forms (which are related to eigenvalues of Hecke operators).

The modular curves we are interested in also correspond to moduli spaces of enhanced elliptic curves (elliptic curves with additional torsion information). The Hecke operators transfer in this setting, where their action can easily be described explicitly.

By an important result of Igusa (later generalized by Deligne-Rapoport and Katz-Mazur), these modular curves admit a model compatible with the moduli space in a functorial way. The Eichler-Shimura relation is proven in the moduli space, and can then be transferred back to the modular curves.

The restriction to all but finitely many primes corresponds to the primes of bad reduction for the modular curve and its Jacobian. However, a result of Carayol shows that the equality also holds at these primes.

Something fascinating in the Eichler-Shimura construction is the interplay between algebraic geometry, analytic geometry, and arithmetic. The following are some of these relationships:

- the fact that every compact Riemann surface is a complex algebraic curve. This allows us to consider modular curves as algebraic curves.
- the algebraization of complex tori with a polarization. This shows that the Jacobian of a compact Riemann surface is an abelian variety. Moreover, this will let us show that quotients of complex abelian varieties exist.
- the interpretation of modular curves as moduli spaces for enhanced elliptic curves, which gives good models for modular curves compatible with the moduli space interpretation.
- a relationship between modular forms (resp. cusp forms) and meromorphic (resp. holomorphic) differential forms on modular curves.

By Faltings' isogeny theorem, the modularity theorem actually means that the Eichler-Shimura construction gives all elliptic curves defined over $\mathbb{Q}$, up to isogeny. More generally, we can use the ideas of this construction to give equivalent formulations of the modularity theorem.

For example, it can be shown that an elliptic curve over $\mathbb{Q}$ with conductor N is modular if and only if there exists a nonconstant holomorphic mapping from a modular curve $X_1(N)$ (or its Jacobian) to the elliptic curve. Alternatively, the Eichler-Shimura construction can be used to define 2-dimensional ℓ-adic Galois representations $\rho_{f,\ell}$ associated to a newform $f \in S_2(\Gamma_0(N))$, and it can be shown that an elliptic curve over $\mathbb{Q}$ is modular if and only if there exists a newform $f \in S_2(\Gamma_0(N))$ such that

$$\rho_{f,\ell} \cong \rho_{E,\ell},$$

where $\rho_{E,\ell}$ is the 2-dimensional ℓ-adic representation associated to E, obtained from the Tate module.

Chapter 1

Abelian varieties

In this first chapter, we study *abelian varieties*, groups in the category of projective algebraic varieties. As we mentioned in the introduction, these generalize elliptic curves and are the objects which we will try to associate to modular forms.

Besides studying their basic properties, the main goals are to show that the Jacobian (resp. Picard group) of a compact Riemann surface (resp. nonsingular algebraic curve) are abelian varieties and to explain when quotients of abelian varieties can be formed. These are three fundamental facts for what follows. At the end of the chapter, we explain what are Néron models and define L-functions of abelian varieties.

After some point, we will mostly focus on *complex* abelian varieties, the case in which we will be mainly interested. While all the results we will see in this context can be generalized over an arbitrary field, we will not need these generalizations; moreover, results are more easily given and motivated in the complex case. In particular, we will see that the structure of complex abelian varieties can easily be described.

The references for this chapter are:

- For the theory of abelian varieties over arbitrary fields: [Mil08] and [Mum08];
- For the theory of complex abelian varieties: [BL04], [KM93] and [RS11];
- For the theory of compact Riemann surfaces: [Mir95].

1. Abelian varieties over an arbitrary field

First, we define abelian varieties over an arbitrary field and study their first properties.

Definition 1.1. An *abelian variety* defined over an algebraically closed field K is a projective algebraic variety A with morphisms

$$\begin{array}{rccc} m: & A \times A & \to & A \\ u: & A & \to & A \end{array}$$

along with an element $e \in A$, that induce a group structure on A. The *dimension* of A is its dimension as a variety. We say that A is *defined over* a subfield $k \subset K$ if A, m, u are defined over k and $e \in A(k)$.

In other words, an abelian variety is a group in the category of projective algebraic varieties. The notions of *morphisms* and *subvarieties* of abelian varieties are defined in the natural way.

Remarks 1.2. We will only consider abelian varieties defined over $\mathbb{C}$, $\mathbb{Q}$ or finite fields. The hypothesis *projective* is important; the affine theory is that of *linear algebraic groups.*

Example 1.3. An elliptic curve defined over any field is an abelian variety, motivating this generalization. We will see another important family of examples later on, in particular generalizing elliptic curves.

1.1. Abelian varieties are nonsingular and commutative

Proposition 1.4. *An abelian variety is nonsingular.*

Proof. By [Har77, I.5.3], any variety has a dense nonsingular subset. Since translation by any point is an isomorphism, this shows that every point is nonsingular. □

Theorem 1.5 (Rigidity)**.** *Let V, W, U be projective varieties defined over an algebraically closed field k and $f : V \times W \to U$ be a regular map. If there exist $v_0 \in v(k), w_0 \in W(k), u_0 \in U(k)$ such that*

$$f(V \times \{w_0\}) = f(\{v_0\} \times W) = \{u_0\},$$

then f is constant, equal to u_0.

Proof. Let U_0 be an affine neighborhood of u_0 in U. Since V is projective (hence complete), the projection $\pi : V \times W \to W$ is closed. Therefore, the set $W_0 = \pi(f^{-1}(U - U_0)) \subset W$ is closed as well. Note that

$$W - W_0 = \{w \in W : f(V \times \{w\}) \subset U_0\};$$

in particular, $w_0 \in W - W_0$. Since it is a morphism between a projective and an affine variety, the (co)restriction $f : V \times (W - W_0) \to U_0$ is constant by [Har77, I.3.2-3.5,], with image equal to u_0 since $f(v_0, w_0) = u_0$. Hence, $f : V \times W \to U_0$ is constant equal to u_0, by [Har77, I.4.1]. □

Corollary 1.6. *Any regular map between abelian varieties is the composition of a homomorphism followed by a translation.*

Proof. Let $f : A \to B$ be a regular map between abelian varieties. Composing with a translation reduces to the case $f(1_A) = 1_B$. Let $\alpha : A \times A \to B$ be the map

$$(a, a') \mapsto f(aa')f(a)^{-1}f(a')^{-1}.$$

Note that α verifies the hypotheses of Theorem 1.5, with $v_0 = w_0 = 1_A$ and $u_0 = 1_B$. Hence $\alpha = 1_B$, which implies that f is a homomorphism. □

Corollary 1.7. *An abelian variety is commutative.*

Proof. If A is an abelian variety, the previous Corollary shows that the regular map $a \mapsto a^{-1}$ is a homomorphism, since it sends the identity element to itself. Hence, A is commutative. □

1.2. Images and sums

Proposition 1.8. *If $f : A \to B$ is a morphism of abelian varieties, then $f(A)$ is an abelian subvariety of B.*

Proof. Since A is projective, it is complete and therefore $f(A)$ is closed in B. □

Remark 1.9. We see here that the projectivity is important: the image of a morphism of varieties may not be a subvariety in general.

Corollary 1.10. *Let A, B be abelian varieties over a field k. Then $A \times B$ is an abelian variety. If A and B are subvarieties of an abelian variety C, then $A + B$ is a subvariety of C.*

Proof. It suffices to recall that the product of projective varieties is projective. The second point follows from Proposition 1.8, since $A+B$ is the image of $A \times B$ by the natural morphism $A \times B \to C$. □

1.3. Isogenies

Definition 1.11. Let A, B be two abelian varieties. An *isogeny* is a surjective morphism $f : A \to B$ with finite kernel.

Proposition 1.12. *If $f : A \to B$ is a morphism of abelian varieties, the following conditions are equivalent:*

- *f is an isogeny;*
- *$\dim A = \dim B$ and f is surjective;*
- *$\dim A = \dim B$ and $\ker f$ is finite;*

Proof. By [Har77, II.3.22], if f is dominant, there exists an open set U in B such that

$$\dim f^{-1}(b) = \dim A - \dim f(A)$$

for all $b \in U$. Since all the fibers have the same dimension (they are isomorphic through translation), this equality holds for all $b \in B$. Hence, the first two conditions are equivalent. By applying this to the corestriction $f : A \to f(A)$, we get that the three conditions are equivalent by [Har77, Ex. 1.10(d)]. □

We could say much more about isogenies in the general case (see [Mil08, I.7]), but as announced, we will restrict to isogenies of complex abelian varieties in what follows. Most of the results we will see can be generalized over an arbitrary field, and they also generalize the theory of isogenies of elliptic curves (see [Sil09, III.5]).

1.4. Reducibility

Definition 1.13. An abelian variety is *simple* if it does not have a nontrivial abelian subvariety.

Proposition 1.14 (Poincaré reducibility)**.** *Let A be an abelian variety defined over a field k. If B is an abelian subvariety defined over k, there exists an abelian subvariety C of A defined over k such that the natural morphism $B \times C \to A$ is an isogeny defined over k.*

Remark 1.15. We will not prove this result over an arbitrary field here (see [Mil08, I.10.1]), but we will do it over $\mathbb{C}$ in the next section. However, we will still need this general case later on.

Corollary 1.16. *Let A be an abelian variety defined over a field k. There exist simple abelian subvarieties $A_1, \dots, A_n$ defined over k such that*

$$A_1 \times \cdots \times A_n \to A$$

is an isogeny defined over K.

Proof. By [Har77, Ex. 1.10(d)], dimension for closed subvarieties is strictly decreasing, so the result follows from Proposition 1.14 by induction. □

2. Algebraic geometry and analytic geometry

As explained in the introduction, important points in what follows will be the relationships between algebraic geometry and analytic geometry. In this section, we give the relationships between three algebraic/analytic objects: smooth complex algebraic varieties/complex analytic manifolds, complex abelian varieties/complex Lie groups and complex algebraic curves/compact Riemann surfaces.

2.1. Smooth algebraic varieties and analytic manifolds

Any smooth complex algebraic variety can be viewed as a complex manifold, since smoothness is equivalent to the condition on a Jacobian matrix that allows one to use the inverse function theorem to find local coordinates. More precisely, we have the following result:

Proposition 1.17. *There is a functor $\cdot\ (\mathbb{C}) : \mathrm{SmthVar}_{\mathbb{C}} \to \mathrm{Man}_{\mathbb{C}}$, from the category of smooth varieties over $\mathbb{C}$ to the category of complex analytic manifolds, such that:*

- *The diagram*

$$\begin{tikzcd}
\mathrm{SmthVar}_{\mathbb{C}} \arrow[rr, "\cdot\ (\mathbb{C})"] \arrow[dr] & & \mathrm{Man}_{\mathbb{C}} \arrow[dl] \\
& \mathrm{Set} &
\end{tikzcd}$$

  commutes, where the vertical arrows are the forgetful functors.

- *Irreducible varieties are mapped to connected complex manifolds.*

- *If X is a smooth variety over $\mathbb{C}$, the first point indicates that X and $X(\mathbb{C})$ are equal as sets. Then, the topology of $X(\mathbb{C})$ is stronger than the Zariski topology of X.*

- *If X is projective, then $X(\mathbb{C})$ is compact.*

– *The dimension of a smooth complex variety X is equal to the dimension of $X(\mathbb{C})$ as a complex manifold. In particular, smooth curves are mapped to Riemann surfaces.*

Proof (Sketch). Since the irreducible components of a smooth variety are disjoint, we can consider only irreducible varieties without loss of generality. If X is a smooth affine variety in $\mathbb{A}^n$ of dimension d, let $f_1, \dots, f_d$ be generators of $I(X) \subset \mathbb{C}[X_1, \dots, X_n]$, and let $P \in V$. By hypothesis, $(\partial f_i/\partial x_j)$ has rank $n-d$, so we can suppose without loss of generality that $(\partial f_i/\partial x_j)_{i,j=d+1,\dots,n}$ is invertible. By the implicit function theorem, there exist open sets $U \subset \mathbb{C}^d$, $V \subset \mathbb{C}^{n-d}$, and a holomorphic function $\varphi : U \to V$ such that

$$\{(x, \varphi(x)) : x \in U\} = X \cap (U \times V),$$

i.e. a local coordinate for X near P. We check that this gives a well-defined complex manifold structure to X. If X is a smooth projective variety in $\mathbb{P}^n$, it suffices to choose an open cover by irreducible affine subvarieties. For the details and generalizations[1], see [Wer11]. □

The topologies on $X(\mathbb{C})$ and X are in general not equal. However, we have the following fundamental theorem that we will use extensively:

Theorem 1.18 (Chow)**.** *Let X be a projective algebraic variety and Y be a closed analytic subset of $X(\mathbb{C})$. Then Y is Zariski-closed in X and smooth.*

Proof. See [Fri02, Theorem 5.13]. □

Remark 1.19. The hypothesis *projective* is needed: $\{x \in \mathbb{C} : \sin(x) = 0\}$ is a closed analytic subset of $\mathbb{C}$, but it is not algebraic, since all proper algebraic subsets of $\mathbb{C}$ are finite.

Corollary 1.20. *Let X, Y be projective algebraic varieties and $f : X(\mathbb{C}) \to Y(\mathbb{C})$ be a holomorphic map. By Proposition 1.17, we can consider f as a map from X to Y. Then $f : X \to Y$ is an algebraic morphism. Conversely, if $f : X \to Y$ is an algebraic morphism, then $f : X(\mathbb{C}) \to Y(\mathbb{C})$ is a holomorphic map.*

Proof. If U is closed in Y, then it is closed in $Y(\mathbb{C})$, since the topology of $Y(\mathbb{C})$ is stronger than the Zariski topology. Hence $f^{-1}(U)$ is closed in $X(\mathbb{C})$, whence closed in X by Theorem 1.18. Therefore, $f : X \to Y$ is continuous. See [Mum08, p. 33] for the proof that $f : X \to Y$ is a morphism. The last assertion follows from Proposition 1.17. □

2.2. Complex abelian varieties and complex Lie groups

Let A be a complex abelian variety. By Proposition 1.17, there is a functorially-associated connected compact manifold $A(\mathbb{C})$ such that $A \cong A(\mathbb{C})$ as topological spaces. By functoriality and Corollary 1.20, $A(\mathbb{C})$ has a group structure given by holomorphic maps, thus it is a *connected compact complex Lie group.*

[1] Serre's GAGA gives a functor from the whole category of algebraic varieties over $\mathbb{C}$ to the category of "analytic spaces", generalizing complex manifolds by allowing singularities. This functor restricts to the functor given above for *smooth* projective varieties.

Proposition 1.21. *Let A, B be complex abelian varieties. If $f : A \to B$ is a morphism of complex Lie groups, then $f : A(\mathbb{C}) \to B(\mathbb{C})$ is a morphism of abelian varieties, and conversely.*

Proof. Follows from Proposition 1.17 and Corollary 1.20. □

However, we will see that the categories of complex abelian varieties and complex compact connected Lie groups are not equivalent.

2.3. Compact Riemann surfaces are algebraic curves

A fundamental result from the theory of compact Riemann surfaces is the following (see [Mir95, VI-VII]):

Theorem 1.22. *If X is a compact Riemann surface, then X is isomorphic to a compact Riemann surface Y that is* holomorphically embedded in $\mathbb{P}^n$ *for some $n \geq 1$, i.e. $Y \subset \mathbb{P}^n$ and for every $p = [p_0, \dots, p_n] \in Y$, there exists some $0 \leq i \leq n$ such that*

1. *$p_i \neq 0$;*
2. *For all $0 \leq j \leq n$, the function z_j/z_i is holomorphic on Y near p;*
3. *There exists $0 \leq j \leq n$ such that z_j/z_i is a local coordinate near p.*

Since Y is compact in $\mathbb{P}^n$ with respect to the strong topology, it is closed. By Theorem 1.18, there is therefore a smooth projective algebraic curve X_{alg}, such that $X_{\text{alg}}(\mathbb{C}) \cong Y \cong X$. Moreover, the function field of X_{alg} (as an algebraic curve) is isomorphic to the function field of X (as a Riemann surface). Hence, *compact Riemann surfaces are nonsingular algebraic curves.*

Example 1.23. Note that smooth projective plane curves and (local) complete intersection curves are indeed compact Riemann surfaces holomorphically embedded in a projective space (see [Mir95, II.2]).

3. Complex abelian varieties

In this section, we study the structure and properties of complex abelian varieties as commutative compact connected complex Lie groups.

Given an elliptic curve E defined over $\mathbb{Q}$, it is a fundamental fact that E corresponds to a complex torus of dimension one: there exists a lattice Λ in $\mathbb{C}$ (i.e. a discrete subgroup of rank 2) such that

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda$$

as Lie groups[2]. We will see that this result generalizes to complex abelian varieties: as Lie groups, they are isomorphic to complex tori of higher dimensions.

Recall that a *lattice* in $\mathbb{C}^g$ is a discrete subgroup of maximal rank $2g$. Equivalently, it is a free abelian group in $\mathbb{C}^g$ containing a $\mathbb{R}$-basis of $\mathbb{C}^g$. If Λ is a lattice in $\mathbb{C}^g$, note that the quotient $\mathbb{C}^g/\Lambda$ is a compact connected complex Lie group of dimension g.

[2] More precisely, the isomorphism is given by $(\wp_\Lambda, \wp'_\Lambda) : \mathbb{C}/\Lambda \to E(\mathbb{C})$, where $\wp_\Lambda$ is the Weierstrass elliptic function associated to Λ.

Definition 1.24. A Lie group isomorphic to $\mathbb{C}^g/\Lambda$ for some integer $g \geq 1$ and a lattice Λ in $\mathbb{C}^g$ is called a *complex torus*.

3.1. Complex abelian varieties are complex tori

Using basic tools of the theory of Lie groups, we now determine the Lie group structure of complex abelian varieties.

Theorem 1.25. *A commutative connected compact complex Lie group is a complex torus.*

Proof. Recall that if V is the Lie algebra of a compact complex Lie group G, then (see [Var84, 2.7,2.10]):

- For all $v \in V$, there exists a unique holomorphic integral curve $\varphi_v : \mathbb{C} \to G$ for v, i.e. $(d\varphi_v)_e : \mathbb{C} \to V$ is $t \mapsto tv$.
- The *flow* $\varphi : V \times \mathbb{C} \to G$ defined by $(v, t) \mapsto \varphi_v(t)$ is holomorphic.
- The *exponential map* $\exp : V \to G$ is defined by $\exp(v) = \varphi_v(1)$ for all $v \in V$. By the unicity of integral curves, we have $\exp(tv) = \varphi_v(t)$ for all $v \in V, t \in \mathbb{C}$. Moreover, $(d \exp)_e = \mathrm{id}$.

Now, let us note that:

- exp is a homomorphism: indeed, let $v, w \in V$ and consider the map $\psi : \mathbb{C} \to G$ given by $t \mapsto \exp(tx)\exp(ty)$. If G is commutative, we have $(d\psi)_e(t) = t(x + y)$, so $\psi = \varphi_{x+y}$ by unicity of integral curves. Evaluating at $t = 1$ gives
$$\exp(x + y) = \exp(x)\exp(y).$$
- exp is surjective: by the above, the image $\exp(V)$ is a subgroup of G. Since $(d \exp)_e = \mathrm{id}$, the exponential map is a diffeomorphism in a neighborhood of 0, so $\exp(V)$ contains an open neighborhood of e. But any neighborhood of the identity in a compact connected Lie group generates the whole group, so that $\exp(V) = G$.
- $\ker \exp$ is a lattice in V: since $G \cong V/\ker \exp$ is compact, it suffices to prove that $\ker \exp$ is a discrete subgroup of V, which is clear since exp is a diffeomorphism in a neighborhood of e.
- exp is holomorphic since the flow φ is holomorphic.

Hence, $A \cong V/\ker \exp$ as complex Lie groups, where $V/\ker \exp$ is a complex torus. □

Corollary 1.26. *Complex abelian varieties are complex tori.*

Remark 1.27. Actually, the hypothesis "commutative" in Theorem 1.25 is unnecessary: using similar ideas, we could have simply shown that a compact connected complex Lie group is commutative (see [KM93, 12.1.22]).

4. Complex tori

In the previous section, we saw that complex abelian varieties are complex tori. In this section, we study these and answer the following question: Are all complex tori complex abelian varieties (i.e. given a complex torus, does there exist a complex abelian variety isomorphic to it as Lie group)? This will allow us to consider quotients of abelian varieties later.

4.1. Morphisms

Definition 1.28. A *morphism* of complex tori is a morphism of the underlying complex Lie groups.

Proposition 1.29. *Let $f : V/\Lambda \to V'/\Lambda'$ be a morphism of complex tori. Then there exists a unique $\mathbb{C}$-linear map $\hat{f} : V \to V'$ with $\hat{f}(\Lambda) \subset \Lambda'$ such that the diagram*

$$\begin{tikzcd}
0 \arrow[r] & \Lambda \arrow[r] \arrow[d, "\hat{f}|_\Lambda"] & V \arrow[r] \arrow[d, "\hat{f}"] & V/\Lambda \arrow[r] \arrow[d, "f"] & 0 \\
0 \arrow[r] & \Lambda' \arrow[r] & V' \arrow[r] & V'/\Lambda' \arrow[r] & 0
\end{tikzcd}$$

commutes.

Proof. The tangent spaces at 0 of V/Λ and V'/Λ' are V, V' respectively. We have isomorphisms $V/\Lambda \cong V/\ker\exp$ and $V'/\Lambda' \cong V'/\ker\exp'$ induced by the exponential maps. By the properties of the latter, the diagram

$$\begin{tikzcd}
V \arrow[r, "(df)_0"] \arrow[d, "\exp"'] & V' \arrow[d, "\exp"'] \\
V/\ker\exp \arrow[r, "f"] & V'/\ker\exp' .
\end{tikzcd}$$

commutes, giving the result since $(df)_0$ is $\mathbb{C}$-linear, and clearly takes $\ker\exp$ to $\ker\exp'$ by the diagram. The unicity is clear. □

Therefore, we get injective homomorphisms of abelian groups

$$\begin{aligned}
\rho_{\mathbb{C}} : \mathrm{Hom}(V/\Lambda, V'/\Lambda') &\to \mathrm{Hom}_{\mathbb{C}}(V, V') \\
\rho_{\mathbb{Z}} : \mathrm{Hom}(V/\Lambda, V'/\Lambda') &\to \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda').
\end{aligned}$$

Indeed, since Λ (resp. Λ') generates V (resp. V') as a $\mathbb{R}$-vector space, an element of $\mathrm{Hom}(V/\Lambda, V'/\Lambda')$ is determined by its image in $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda')$.

Proposition 1.30. *If X, X' are complex tori of dimensions g, g', we have* $\mathrm{Hom}(X, X') \cong \mathbb{Z}^m$ *for some $m \leq 4gg'$.*

Proof. Since the homomorphism $\rho_{\mathbb{Z}}$ is injective, we can view $\mathrm{Hom}(X, X')$ as a subgroup of the free abelian group $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda')$ of rank $(2g)(2g') = 4gg'$. □

4.2. Subtori and quotients

Definition 1.31. A *subtorus* of a complex torus X is a Lie subgroup of X which is also a complex torus.

Proposition 1.32. *The subtori of a complex torus are its compact connected Lie subgroups.*

Proof. Let H be a Lie subgroup of a complex torus G. If H is compact and connected, then H is a complex torus by Theorem 1.25, thus a subtorus of G. Conversely, if H is a complex torus, then it is compact and connected. □

More explicitly, we have the following description:

Proposition 1.33. *Let $X = V/\Lambda$ be a complex torus. Then the subtori of X are the tori*

$$(V' + \Lambda)/\Lambda \cong V'/(\Lambda \cap V'),$$

where V' is a subspace of V such that $\Lambda \cap V'$ is a lattice in V'.

Proof. Clearly, the given spaces are subtori of X. Conversely, let X' be a subtorus of X and write $X' = V'/\Lambda'$ for V' a complex vector space and Λ' a lattice of V'. By Proposition 1.29, we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \Lambda' \arrow[r] \arrow[d] & V' \arrow[r] \arrow[d, "\hat{\iota}"] & V'/\Lambda' \arrow[r] \arrow[d, "\iota"] & 0 \\
0 \arrow[r] & \Lambda \arrow[r] & V \arrow[r] & V/\Lambda \arrow[r] & 0.
\end{tikzcd}$$

Since ι is injective, we get that $\ker \hat{\iota} \subset \Lambda'$. Hence, $\ker \hat{\iota} = 0$ because Λ' is discrete, showing that we can view V' as a vector subspace of V. Moreover, the diagram shows that $V' \cap \Lambda = \Lambda'$. Hence, $X' = V'/\Lambda' = V'/(V' \cap \Lambda) \cong (V' + \Lambda)/\Lambda$. □

Proposition 1.34. *If Γ is a finite subgroup of a complex torus X, then X/Γ is also a complex torus of the same dimension.*

Proof. Let $X = V/\Lambda$ for V a complex vector space and Λ a lattice in V. There exists a subgroup Λ' of V containing Λ such that $\Gamma = \Lambda'/\Lambda$, so

$$X/\Gamma \cong V/\Lambda'.$$

Since $\Lambda \subset \Lambda'$, we have that Λ' contains a $\mathbb{R}$-basis of V. Moreover, since Γ is finite, there exist $v_1, \dots, v_r \in \Lambda'$ such that $\Lambda' = \coprod_{i=1}^{r}(v_i + \Lambda)$. Thus, Λ' is a discrete subgroup of V because Λ is. □

Proposition 1.35. *Let $f : X \to X'$ be a morphism of complex tori. Then* $\operatorname{im} f$ *is a subtorus of X' and the connected component of* $\ker f$ *containing* 0 *is a subtorus of X.*

Proof.

1. The image $\operatorname{im} f$ is a compact connected Lie subgroup of X', so it is a subtorus by Proposition 1.32.
2. The kernel $\ker f$ is a closed Lie subgroup of X. Since the connected component $(\ker f)_0$ is closed (thus compact) and connected, it is a subtorus as well by Proposition 1.32.

□

4.3. Isogenies

Definition 1.36. An *isogeny* of complex tori $f : X \to Y$ is a surjective morphism with finite kernel. We write $X \sim Y$ if there is an isogeny $f : X \to Y$. The *degree* of the isogeny is $\deg f = |\ker f|$.

Example 1.37. If $f : A \to B$ is an isogeny of complex abelian varieties, then $f : A(\mathbb{C}) \to B(\mathbb{C})$ is an isogeny of complex tori.

We have the following analogue of Proposition 1.12:

Proposition 1.38. *Let $f : X \to Y$ be a morphism of complex tori. The following are equivalent:*

1. *f is an isogeny.*
2. *f is surjective and* $\dim X = \dim Y$*.*
3. *f has finite kernel and* $\dim X = \dim Y$*.*

Proof. By [Lee12, 7.10,7.15], when f is surjective, we have an isomorphism of Lie groups $X/\ker f \cong Y$, with $\dim X - \dim\ker f = \dim Y$. Since $\dim\ker f = 0$ as a manifold if and only if it is finite, we obtain the equivalence of the first two points. For the third one, it suffices to apply this to the corestriction $f : X \to f(Y)$ and use that the dimension of a proper connected Lie subgroup is strictly smaller than the dimension of the ambient Lie group[3]. □

Proposition 1.39. *Let $f : V/\Lambda \to V'/\Lambda'$ an isogeny between complex tori. Then the induced map $\hat{f} : V \to V'$ of Proposition 1.29 is an isomorphism.*

Proof. First of all, we note that $\ker \hat{f} \subset \Lambda$. Indeed, an element $v \in \ker \hat{f} - \Lambda$ would generate an infinite subgroup of $\ker f$ since $\mathbb{C}v \cap \Lambda$ is discrete. Hence, we must have $\ker \hat{f} = 0$ because Λ is discrete. By Proposition 1.38, $\dim V = \dim V'$, so f is an isomorphism. □

Proposition 1.40. *The composition of two isogenies is an isogeny.*

Proof. Clear, since the composition of two surjective homomorphisms is a surjective homomorphism, and if $f : X \to Y$, $g : Y \to Z$ have finite kernel, then $|\ker(g \circ f)| = |\ker(g)||\ker(f)|$. □

Example 1.41. Let X be a complex torus and Γ be a finite subgroup of X. By Proposition 1.34, the quotient X/Γ is a complex torus. The projection $p : X \to X/\Gamma$ is an isogeny.

Example 1.42. Let X be a complex torus of dimension g. For $n \in \mathbb{Z}$, the multiplication $[n] : X \to X$ is an isogeny of degree n^{2g}. Indeed, if $X = V/\Lambda$,

$$X[n] = \ker[n] = \frac{1}{n}\Lambda/\Lambda \cong \Lambda/n\Lambda \cong (\mathbb{Z}/n)^{2g},$$

since $\Lambda \cong \mathbb{Z}^{2g}$.

[3] Using the correspondence between connected Lie subgroups and subalgebras of the Lie algebra, see [Lee12, Theorem 15.31].

4.4. Dual isogenies

Proposition 1.43. *If $f : X \to Y$ is an isogeny of complex tori with $\deg f = n$, then there exists a unique isogeny $\tilde{f} : Y \to X$ such that*

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "{[n]_X}"'] & Y \arrow[d, "{[n]_Y}"] \arrow[dl, "\tilde{f}"'] \\
X \arrow[r, "f"] & Y
\end{tikzcd} \qquad f \circ \tilde{f} = [n]_Y \textit{ and } \tilde{f} \circ f = [n]_X$$

Moreover, $\tilde{f}$ has degree n^{2g-1}.

Proof. By definition of the degree, we have that $\ker f \subset \ker([n]_X)$. Therefore, there exists a homomorphism $\hat{f} : Y \to X$ such that $\hat{f} \circ f = [n]_X$. Moreover,

$$(f \circ \hat{f}) \circ f = f \circ (\hat{f} \circ f) = f \circ [n]_X = [n]_X \circ f,$$

thus $f \circ \hat{f} = [n]_X$ since f is surjective. From the relation $\hat{f} \circ f = [n]_X$, we deduce that $\hat{f}$ is surjective and has finite kernel. By Proposition 1.29, $\hat{f}$ is in fact given by $[x] \mapsto [n\varphi(x)]$, where $\varphi : \mathbb{C}^{\dim X} \to \mathbb{C}^{\dim Y}$ is a linear isomorphism. Hence, $\hat{f}$ is holomorphic as well. Finally, the relation $\hat{f} \circ f = [n]_X$ implies that $\deg \hat{f} \cdot n = n^{2g}/n = n^{2g-1}$, using Example 1.42. The unicity is clear, since if g verifies the same properties as $\hat{f}$, then $(\hat{f} - g) \circ f = 0$, thus $g = \hat{f}$ because f is surjective. □

Definition 1.44. The unique isogeny $\tilde{f}$ of Proposition 1.43 is called the *dual isogeny* of f.

Example 1.45. If X is a complex tori of dimension g, then $\widetilde{[n]} = [n^{2g-1}]$.

Corollary 1.46. *Isogeny of complex tori is an equivalence relation.*

If there exists an isogeny between two complex tori, we say that they are *isogenous.*

4.5. Complex tori as abelian varieties

In the previous section, we saw that complex abelian varieties are complex tori (as Lie groups). In this paragraph, we analyze the converse problem: when is a complex torus isomorphic to a complex abelian variety (as Lie groups) ?

Proposition 1.47. *There exists at most one (up to isomorphism) structure of complex abelian variety on a complex torus.*

Proof. Follows directly from Proposition 1.21. □

By abuse of language, we will say that the torus *is an abelian variety* if it can be endowed with such a structure.

In dimension one, we know that *all complex tori are abelian varieties* (as Lie groups): if Λ is a lattice in $\mathbb{C}$, there exists an elliptic curve defined over $\mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ as Lie groups. In higher dimensions, the answer is not always positive, and we can give the following criterion:

Definition 1.48. Let $\mathbb{C}^g/\Lambda$ be a complex torus. A positive-definite Hermitian form $H = H_1 + iH_2$ on $\mathbb{C}^g$ such that $H_2(\Lambda \times \Lambda) \subset \mathbb{Z}$ is called a *Riemann form* (or *polarization*) on $\mathbb{C}^g/\Lambda$ (or, on $\mathbb{C}^g$ with respect to Λ).

Theorem 1.49. *A complex torus is a complex abelian variety if and only if it admits a Riemann form.*

Proof. See the book [KM93], which is focused on proving this result. □

Example 1.50. A 1-dimensional complex torus is an abelian variety, since it is isomorphic to an elliptic curve. Any 1-dimensional complex torus is isomorphic to $\mathbb{C}/\Lambda_z$ for some $z \in \mathbb{H}$, where $\Lambda_z = \mathbb{Z} + z\mathbb{Z}$. A Riemann form on $\mathbb{C}/\Lambda_z$ is given by $H(u, v) = u\overline{v}/\operatorname{Im}(z)$ for $u, v \in \mathbb{C}$.

Example 1.51. An example of a complex torus which is *not* an abelian variety can be given as follows: if $H = H_1 + iH_2$ is a Riemann form on a complex torus $\mathbb{C}^g/\Lambda$, we easily see that $H_2(iu, iv) = H_2(u, v)$ for all $u, v \in \mathbb{C}^g$. Let us denote again $H_i \in M_{2g}(\mathbb{R})$ the matrix of H_i in the canonical basis and $\Lambda \in M_{2\times 2g}(\mathbb{C})$ the matrix of a basis of Λ in the canonical basis. Then, $\Lambda H_2^{-1}\Lambda^t = 0$ (see the following proofs or [BL04, Theorem 4.2.1]). Hence, if $\lambda_1, \dots, \lambda_{2g}$ is a real basis of $\mathbb{C}^g$ with algebraically independent coordinates, there cannot exist a Riemann form on $\mathbb{C}^g/\Lambda$.

We see that the property of a complex torus to be an abelian variety is preserved by taking subtori and through isogenies:

Proposition 1.52. *If a complex torus admits a Riemann form, then any subtorus also has a Riemann form.*

Proof. Clearly, the restriction of any Riemann form on X to any subtorus is again a Riemann form. □

Proposition 1.53. *If a complex torus X has a Riemann form and $f : X \to X'$ is an isogeny of complex tori, then X' also has a Riemann form.*

Proof. Let us write $X = V/\Lambda$ and $X' = V'/\Lambda'$ as before. By Proposition 1.29, the isogeny f is induced by an isomorphism of vector spaces $f : V \to V'$ such that $f(\Lambda) \subset \Lambda'$. Let $H : V \times V \to \mathbb{C}$ be a Riemann form on X. Composing with f^{-1}, we obtain a Hermitian form

$$H' = H \circ (f^{-1} \times f^{-1}) : V' \times V' \to \mathbb{C}.$$

However, H' restricted to $\Lambda' \times \Lambda'$ is not necessarily integer-valued. To correct this, we note that since $\ker f \cong \Lambda'/f(\Lambda)$ is finite, there exists an integer $n \geq 1$ such that $n\Lambda' \subset f(\Lambda)$. Letting $\hat{H} = n^2 H' = \hat{H}_1 + i\hat{H}_2$, we obtain a Riemann form on X'. Indeed, for all $\lambda_1, \lambda_2 \in \Lambda'$, we have

$$\hat{H}_2(\lambda_1, \lambda_2) = H'(n\lambda_1, n\lambda_2) \in \mathbb{Z}.$$

□

5. Quotients of complex abelian varieties

In this paragraph, we use the results obtained above concerning complex tori and their polarizations to study the construction of quotients of complex abelian varieties.

5.1. Reducibility and decomposition

We can now prove Proposition 1.14 for complex abelian varieties.

Proposition 1.54 (Poincaré reducibility)**.** *Let A' be a subvariety of a complex abelian variety A. Then there exists an subvariety A'' of A such that $A = A' + A''$ and $A' \cap A''$ is finite. In other words, the map $A' \times A'' \to A$ is an isogeny.*

Proof. Let $A(\mathbb{C}) = V/\Lambda$ for V a complex vector space and Λ a lattice in V. By Theorem 1.49, there exists a Riemann form $H : V \times V \to \mathbb{C}$ with respect to Λ. Since $A'(\mathbb{C})$ is a subtorus of $A(\mathbb{C})$, we can suppose by Proposition 1.33 that $A'(\mathbb{C}) = V'/(\Lambda \cap V')$ for V' a vector subspace of V. Let V'' be the orthogonal complement to V' with respect to H, $\Lambda'' = \Lambda \cap V''$ and $X'' = V''/\Lambda''$. Note that:

- *X'' is a complex torus:* Since Λ is discrete in V, the set Λ'' is also discrete in V''. We need to show that X'' is compact, i.e. that Λ'' has maximal rank in V''. By hypothesis, $H = H_1 + iH_2$ induces an antisymmetric positive-definite pairing
$$I = H_2 \mid_\Lambda : \Lambda \times \Lambda \to \mathbb{Z}.$$
  Let us prove that Λ'' is the orthogonal complement of Λ' in Λ with respect to I. On one hand, Λ'' is clearly included in the orthogonal complement. On the other hand, let $v \in \Lambda$ such that $I(v', v) = 0$ for all $v' \in \Lambda'$. Since $V' = \Lambda' \otimes \mathbb{R}$, it follows that $H_2(v, v') = 0$ for all $v' \in V'$, whence $H_1(v, v') = H_2(u, iv') = 0$ for all $v' \in V'$. Therefore, $v \in \Lambda \cap V'' = \Lambda''$.

  Let us now consider $\hat{\Lambda} = \Lambda \otimes \mathbb{Q}$, and $\hat{\Lambda}'$, $\hat{\Lambda}''$ defined in the same way. The pairing I induces a bilinear antisymmetric positive-definite pairing $\hat{I} : \hat{\Lambda} \times \hat{\Lambda} \to \mathbb{Q}$ such that $\hat{\Lambda}''$ is the orthogonal complement of $\hat{\Lambda}'$ in $\hat{\Lambda}$. Thus, we get that $\hat{\Lambda} = \hat{\Lambda}' \oplus \hat{\Lambda}''$, which implies that
$$\begin{aligned} \operatorname{rank} \Lambda'' &= \dim_{\mathbb{Q}} \hat{\Lambda}'' \\ &= \dim_{\mathbb{Q}} \hat{\Lambda} - \dim_{\mathbb{Q}} \hat{\Lambda}' \\ &= \operatorname{rank} \Lambda - \operatorname{rank} \Lambda' \\ &= 2(\dim_{\mathbb{C}} V - \dim_{\mathbb{C}} V') \\ &= 2 \dim_{\mathbb{C}} V'' = \dim_{\mathbb{R}} V''. \end{aligned}$$

- *X'' is an abelian variety:* This is a subtorus of $A(\mathbb{C})$, so we can conclude by Proposition 1.52: there exists an abelian variety A'' such that $A''(\mathbb{C}) = X''$.

- *We have $A = A' + A''$:* Indeed, $A' + A'' = A'(\mathbb{C}) + A''(\mathbb{C}) = A'(\mathbb{C}) + X'' = V'/\Lambda' + V''/\Lambda'' = A(\mathbb{C})$.

- *The set $A' \cap A''$ is finite:* Since this set is a subset of the compact A, it is sufficient to prove that it is discrete. Let $x \in A' \cap A''$, i.e. $x = \pi(v')$ with $v' \in V' \cap V''$ and $\pi : V \to A$ the projection. Let $U \subset V$ be a neighborhood of v' such that $U \cap (U + \lambda) = \varnothing$ for all nonzero $\lambda \in \Lambda$. Then $\pi(U)$ is a neighborhood of $[v']_\Lambda$ such that $\pi(U) \cap (A \cap A') = \{[v']_\Lambda\}$.

□

Corollary 1.55. *Every complex abelian variety is isogenous to a product of simple abelian varieties.*

Proof. We can proceed as in Corollary 1.16, since dimension of subgroups of a connected Lie group is strictly decreasing. □

5.2. Quotients

Proposition 1.56. *Let A' be a subvariety of a complex abelian variety A. Then there exists an abelian variety B and a surjective morphism $f : A \to B$ with kernel A' such that for every morphism of abelian varieties $g : A \to C$ with $A' \subset \ker g$, there exists a morphism $\hat{g} : B \to C$ such that*

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

commutes. Moreover B has dimension $\dim A - \dim A'$ and $B \cong A/A'$ as groups.

Proof. By Proposition 1.54, there exists an abelian subvariety A'' of A such that $A = A' + A''$ and $A' \cap A''$ is finite. Thus,

$$A/A' \cong A(\mathbb{C})/A'(\mathbb{C}) \cong (A'(\mathbb{C}) + A''(\mathbb{C}))/A'(\mathbb{C}) \cong A''(\mathbb{C})/(A'(\mathbb{C}) \cap A''(\mathbb{C}))$$

as abelian groups. But $A''(\mathbb{C})/(A'(\mathbb{C}) \cap A''(\mathbb{C}))$ is a complex torus by Proposition 1.34, the set $A'(\mathbb{C}) \cap A''(\mathbb{C})$ being finite. By Proposition 1.53, there is an abelian variety B such that $A''(\mathbb{C})/(A'(\mathbb{C}) \cap A''(\mathbb{C})) \cong B(\mathbb{C})$ as Lie groups, and $B \cong B(\mathbb{C}) \cong A/A'$ as groups. The dimension of the complex torus $B(\mathbb{C})$ is equal to $\dim A''(\mathbb{C}) = \dim V'' = \dim V - \dim V' = \dim A(\mathbb{C}) - \dim A'(\mathbb{C}) = \dim A - \dim A'$. By Corollary 1.20, the surjective morphism of Lie groups $A(\mathbb{C}) \to B(\mathbb{C})$ with kernel $A'(\mathbb{C})$ gives a surjective morphism of abelian varieties $f : A \to B$ with kernel A'.

Let us now show the universal property. Let $g : A \to C$ be a morphism of abelian varieties such that $A' \subset \ker g$. From the definition of B, there exists a morphism $\hat{g} : B(\mathbb{C}) \to C(\mathbb{C})$ such that the diagram

$$\begin{tikzcd} A(\mathbb{C}) \arrow[r, "g"] \arrow[d, "f"'] & C(\mathbb{C}) \\ B(\mathbb{C}) \arrow[ur, "\hat{g}"'] & \end{tikzcd}$$

commutes. By Corollary 1.20, these maps (co)restrict to give the commutative diagram in the statement. □

Definition 1.57. Let A' be an abelian subvariety of a complex abelian variety A. The *quotient* A/A' is the unique abelian variety (up to isomorphism) given by Proposition 1.56.

Remark 1.58. More generally, Proposition 1.56 holds over any field of characteristic zero. Poincaré reducibility still holds (Proposition 1.14) and the result follows from considerations about quotient of varieties by actions of finite groups (see [Mil08, I.8]). See [CCP] for an interesting discussion.

6. Jacobians of compact Riemann surfaces

In this section, we recall the definition of the Jacobian of a compact Riemann surface, and we prove that it is an abelian variety. This is probably the most important class of examples of abelian varieties, and they also generalize the case of elliptic curves, which are isomorphic to their Jacobian.

6.1. The Jacobian of a compact Riemann surface

Let X be a compact Riemann surface of genus g and denote by $\Omega^1_{\mathrm{hol}}(X)$ the space of holomorphic 1-forms on X.

Since $\pi_1(X)$ is the free group on $2g$ generator, it follows that

$$H_1(X,\mathbb{Z}) = \pi_1(X)_{\mathrm{ab}} = \pi_1(X)/[\pi_1(X),\pi_1(X)] \cong \mathrm{CLCH}(X)/\mathrm{BCH}(X)$$

is a free abelian group of rank $2g$.

Let us fix $p \in X$. For any $\gamma \in \pi_1(X,p)$, we can define a linear map

$$\int_\gamma : \Omega^1_{\mathrm{hol}}(X) \to \mathbb{C}$$

and since $\mathbb{C}$ is commutative, this gives a map

$$\int_{[\gamma]} : \Omega^1_{\mathrm{hol}}(X) \to \mathbb{C}$$

where $[\gamma]$ is the class of γ in $H_1(X,\mathbb{Z})$. Alternatively, from the equivalent point of view $H_1(X,\mathbb{Z}) \cong \mathrm{CLCH}(X)/\mathrm{BCH}(X)$, this follows from the fact that integration over boundary chains is zero.

Definition 1.59. A *period* is an element of $\Omega^1_{\mathrm{hol}}(X)^*$ that is of the form $\int_{[c]}$ for some homology class $[c] \in H_1(X)$. If Λ is the subgroup of periods, we define the *Jacobian* of X as the abelian group

$$\mathrm{Jac}(X) = \Omega^1_{\mathrm{hol}}(X)^*/\Lambda.$$

As a corollary of the Riemann-Roch theorem, the complex vector space $\Omega^1_{\mathrm{hol}}(X)$ has dimension g (i.e. the topological genus is equal to the analytic genus, see [Mir95, pp. 191-192]). Thus,

$$\mathrm{Jac}(X) \cong \mathbb{C}^g/\Lambda$$

for Λ the subgroup of $\mathbb{C}^g$ corresponding to periods.

Example 1.60. The Jacobian of the Riemann sphere is the trivial group. The Jacobian of a complex torus $X = \mathbb{C}/\Lambda$ is isomorphic to X. Indeed, we have $\Omega^1_{\mathrm{hol}}(X) \cong \mathbb{C}$, and letting $\omega_1, \omega_2 \in \mathbb{C}$ be a $\mathbb{Z}$-basis of Λ, the group of periods is homothetic to Λ (or equal to if we choose dz as a basis for $\Omega^1_{\mathrm{hol}}(X)$).

6.2. Jacobians are complex tori

For $p_0 \in X$ an arbitrary base point, recall the *Abel-Jacobi map*

$$A : \mathrm{Div}(X) \to \mathrm{Jac}(X)$$

defined by $p \mapsto \int_{[\gamma_p]}$, where γ_p is any path between p_0 and p in X. We then have the following alternative interpretation of the Jacobian:

Theorem 1.61 (Abel-Jacobi)**.** *Let us consider the map* $A_0 : \mathrm{Div}^0(X) \to \mathrm{Jac}(X)$ *obtained by restricting* A*. Then:*

- *(Abel) The kernel of* A_0 *is equal to the set of principal divisors in* $\mathrm{Div}^0(X)$*.*
- *(Jacobi) The map* $\mathrm{Div}^0(X) \to \mathrm{Jac}(X)$ *is surjective.*

Hence, $\mathrm{Jac}(X) \cong \mathrm{Pic}^0(X)$*.*

Recall the following part of the proof of Abel's theorem (see [Mir95, Chapter VIII]): let a_i, b_i $(1 \leq i \leq g)$ be a basis of the free abelian group $H_1(X)$, so that the subgroup of periods Λ is generated by:

$$A_i = \int_{a_i} \text{ and } B_i = \int_{b_i} \text{ for } 1 \leq i \leq g.$$

Let $\omega_1, \dots, \omega_g$ be a basis of $\Omega^1_{\mathrm{hol}}(X)$ and let A, B be the $g \times g$ *period matrices* defined by $(A)_{ij} = A_i(\omega_j)$ and $(B)_{ij} = B_i(\omega_j)$. To prove Abel's theorem, recall that we show that (see [Mir95, Chapter VIII, Lemmas 4.4,4.5,4.8]):

Lemma 1.62. *Under the above notations, we have:*

a) A *and* B *are nonsingular.*

b) $A^tB = B^tA$*.*

c) The $2g$ *columns of* A *and* B *are* $\mathbb{R}$*-linearly independent.*

Corollary 1.63. *The subgroup of periods* Λ *is a lattice in* $\mathbb{C}^g$*.*

Proof. Indeed, Λ is a free abelian group in $\mathbb{C}^g$ containing the basis $\{A_i, B_i\}$ of $\mathbb{C}^g$ as a $\mathbb{R}$-vector space. □

Corollary 1.64. *The Jacobian of a compact Riemann surface is a complex torus of dimension equal to the genus of the surface*

6.3. Jacobians are abelian varieties

We now show the fundamental fact that the Jacobian of a compact Riemann surface X of genus g is an abelian variety. To do this, we need to define a polarization on

$$\mathrm{Jac}(X) \cong \Omega^1_{\mathrm{hol}}(X)^*/\Lambda \cong \mathbb{C}^g/\Lambda$$

by Theorem 1.49, where Λ is the lattice corresponding to periods.

Note that since the period matrix A is nonsingular, we can choose the basis (ω_i) of $\Omega^1_{\mathrm{hol}}(X)$ such that $A = I$. Then B is called *normalized* and we have the following result (see [Mir95, Lemma VII.4.7]):

Lemma 1.65. *The normalized period matrix* B *is symmetric and has positive-definite imaginary part (i.e.* $\operatorname{im} B$ *is a positive-definite real matrix).*

Proposition 1.66. *Let* X *be a compact Riemann surface of genus* g *and* Λ *its lattice of periods. Then there exists a Riemann form for* $\mathbb{C}^g/\Lambda \cong \mathrm{Jac}(X)$*.*

Proof. Let $\delta_1, \dots, \delta_g, B_1, \dots, B_g$ be the $\mathbb{Z}$-basis of Λ corresponding to A, B as above, and let $x_1, \dots, x_g, y_1, \dots, y_g$ be the corresponding real dual basis in $(\mathbb{C}^g)^*$

(since $\mathbb{C}^g = \Lambda \otimes \mathbb{R}$). Let $E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ be the pairing defined by

$$E = \sum_{j=1}^{g} y_j \wedge x_j.$$

By definition, E is a $\mathbb{R}$-bilinear antisymmetric real form such that the image of $\Lambda \times \Lambda$ lies in $\mathbb{Z}$. Moreover, note that $E(iu, iv) = E(u, v)$ for all $u, v \in \mathbb{C}^g$. Indeed, if we let $B = B_1 + iB_2$ with B_1, B_2 real matrices and B_2 positive-definite, we get that if $v = v_1 + iv_2 \in \mathbb{C}^g$, then

$$v_2 = B_2^{-1} \operatorname{Im}(v) \text{ and } v_1 = \operatorname{Re}(v) - B_1 B_2^{-1} v_2,$$

which implies that

$$E(u, v) = \langle B_2^{-1} \operatorname{Im}(u), \operatorname{Re}(v) - B_1 B_2^{-1} \operatorname{Im}(u)\rangle - \langle B_2^{-1} \operatorname{Im}(v), \operatorname{Re}(u) - B_1 B_2^{-1} \operatorname{Im}(v)\rangle$$

for $u, v \in \mathbb{C}^g$, where $\langle \cdot \rangle$ denotes the standard inner product on $\mathbb{R}$. Hence, $E(iu, iv)$ is equal to

$$\begin{aligned} & \langle B_2^{-1} \operatorname{Im}(iu), \operatorname{Re}(iv) - B_1 B_2^{-1} \operatorname{Im}(iu)\rangle - \langle B_2^{-1} \operatorname{Im}(iv), \operatorname{Re}(iu) - B_1 B_2^{-1} \operatorname{Im}(iv)\rangle \\ = \; & \langle B_2^{-1} \operatorname{Re}(u), -\operatorname{Im}(v) - B_1 B_2^{-1} \operatorname{Re}(u)\rangle - \langle B_2^{-1} \operatorname{Re}(v), -\operatorname{Im}(u) - B_1 B_2^{-1} \operatorname{Re}(v)\rangle \end{aligned}$$

which is equal to $E(u, v)$ since B_1, B_2 are symmetric real matrices. Similarly, we see that $E(iu, v) = E(iv, u)$ and $E(iv, v) > 0$ if $v \neq 0$ by Lemma 1.62. Now, define a pairing $H : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ by $H(u, v) = E(iu, v) + iE(u, v)$. This is a Riemann form for $\mathbb{C}^g/\Lambda$ since:

- it is sesquilinear;
- it is antisymmetric since E is antisymmetric and $(u, v) \mapsto E(iu, v)$ is symmetric;
- its imaginary part is E, which is integer-valued on $\Lambda \times \Lambda$;
- it is positive-definite. Indeed, for all nonzero $v \in V$, $H(v, v) = E(iv, v) + iE(v, v)$. But $E(v, v) = E(iv, iv) = E(i(iv), v) = -E(v, v)$, so that $H(v, v) = E(iv, v) > 0$.

□

Corollary 1.67. *The Jacobian of a compact Riemann surface is an abelian variety.*

Example 1.68. Let E be a compact Riemann surface of genus 1 (i.e. a complex torus by [Mir95, VII.1.9]). By Example 1.60, $\operatorname{Jac}(E) \cong E$ as compact Riemann surfaces, so that E is an abelian variety. This is the elliptic curve corresponding to this torus. Similarly, a smooth projective plane cubic curve (of genus 1 by Plücker's formula) is an abelian variety.

Finally, we note the following universal property:

Proposition 1.69. *Let X be a compact Riemann surface with genus $g \geq 1$ and a chosen base point P_0, giving an injection $\iota : X \hookrightarrow \operatorname{Jac}(X)$ defined by $P \mapsto [P - P_0]$. Then for any complex abelian variety B with a morphism of complex manifolds $X \to B(\mathbb{C})$ such that P_0 is mapped to 0, there exists a unique morphism of complex*

Lie groups $\mathrm{Jac}(X) \to B(\mathbb{C})$ *such that the diagram*

$$\begin{tikzcd}
X \arrow[r] \arrow[d] & \mathrm{Jac}(X) \arrow[dl] \\
B(\mathbb{C}) &
\end{tikzcd}$$

commutes.

Proof. Let B be a complex abelian variety with $f : X \to B(\mathbb{C})$ a morphism of complex manifolds such that $f(P_0) = 0$. Note that we can extend f to a function $f : \mathrm{Div}(X) \to B(\mathbb{C})$, since $B(\mathbb{C})$ is an abelian variety. First, let us suppose that there exists a morphism $\hat{f} : \mathrm{Jac}(X) \to B(\mathbb{C})$ such that $\hat{f} \circ \iota = f$. By Riemann-Roch, we have $\dim L(D+gP_0) \geq 1$, so that for any element in $D \in \mathrm{Div}^0(X)$, there exists an effective divisor $E \in \mathrm{Div}(X)$ of degree g such such that $[E - gP_0] = [D]$. Hence, $\hat{f}([D]) = f(E)$, which proves that $\hat{f}$ is uniquely determined.

To prove that it exists, it suffices to show that $f(\mathrm{div}(\varphi)) = 0$ for all $\varphi \in \mathbb{C}(X)$. To do so, we generalize what is done in [Mir95, V.2.8]. Let us write $B(\mathbb{C}) \cong \mathbb{C}^d/\Lambda$ for Λ a lattice in $\mathbb{C}^d$ and let $\mathcal{P}$ be the standard identified polygon of X (see [Mir95, VIII.1]). By the general lifting lemma ([Mun00, 79.1]), f (resp. φ) lifts to a map $\tilde{f} : D \to \mathbb{C}^d$ (resp. to a map $\tilde{\varphi} : \mathcal{P} \to \mathbb{C}$). By Cauchy's argument principle,

$$\frac{1}{2\pi i} \int_{\partial \mathcal{P}} \tilde{\varphi}(z) \mathrm{dlog} f(z) = \mathrm{div}(\tilde{\varphi}) \pmod{\Lambda}.$$

On the other hand, this integral belongs to Λ as in [Mir95, V.2.8], which implies the assertion. □

7. Jacobians of algebraic curves

Given a compact Riemann surface X, we have just seen that there exists an abelian variety isomorphic to $\mathrm{Jac}(X)$ as complex Lie groups. In particular, by Theorem 1.61, there exists an abelian variety isomorphic to $\mathrm{Pic}^0(X)$ (as groups).

Since compact Riemann surfaces are algebraic curves, we can go on to wonder whether we can generalize this: being given an algebraic curve C defined over a field k, does there exist an abelian variety $\mathrm{Jac}(C)$ (defined over k ?) such that

$$\mathrm{Pic}^0(C) \cong \mathrm{Jac}(C)$$

as groups ? More precisely, since Pic^0 is a functor from the category of algebraic curves to the category of groups, we would like this association to have functorial properties. Alternatively, we could also want to generalize the universal property of Proposition 1.69.

In this section, we give a brief survey of the answer, given by A. Weil during his proof of the Riemann hypothesis for function fields and his work on Abelian and Jacobian varieties between 1940 and 1950. At first, he constructed the Jacobian of a curve over an extension of the base field. Around 1950, Chow showed that an extension of the base field was not needed, and Weil showed in 1955 that his construction did not need an extension of the base field either. The details of the construction can be found in [Mil08, Part III].

The result is the following:

Theorem 1.70. *Let C be a nonsingular algebraic curve of genus g defined over a field k, and such that $C(k) \neq \varnothing$. There exists an abelian variety $\mathrm{Jac}(C)$ defined over k such that:*

1. *The dimension of $\mathrm{Jac}(C)$ is g.*
2. *There is a functorial isomorphism $\mathrm{Pic}^0(C_L) \cong \mathrm{Jac}(C_L)$ for any field extension L/k.*
3. *$\mathrm{Jac}(C)$ is the unique abelian variety that is birationally equivalent to the variety $C^{(g)} = C^g/S_g$, where the symmetric group S_g acts on the product C^g.*
4. *(Universal property) Let $P \in C(k)$. There is an injective morphism $f : C \to \mathrm{Jac}(C)$ such that $f(P) = 0$, with the following universal property: if A is an abelian variety and $g : C \to A$ is a morphism such that $g(P) = 0$, then there exists a unique morphism of abelian varieties $\hat{g} : \mathrm{Jac}(C) \to A$ such that the diagram*

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "g"'] & \mathrm{Jac}(C) \arrow[dl, "\hat{g}"] \\ A & \end{tikzcd}$$

commutes.

Remarks 1.71.

- For the third point, it can indeed be shown that $C^{(g)}$, as the quotient of a variety by the action of a finite group, is a nonsingular variety.
- The fourth property defines the Jacobian up to isomorphism of abelian varieties.
- As we explained above, the fact that the Jacobian can be defined over the same base field as the curve is important. It is actually what we will need later.

7.1. Construction of the Jacobian

The starting point for the construction of the Jacobian is the following: let us pick a base point $P_0 \in C$; for any integer $r \geq 0$, there is a map

$$C^r \to \mathrm{Pic}^0(C)$$

given by $(P_1, \dots, P_r) \mapsto [P_1 + \cdots + P_r - rP_0]$. Since $\mathrm{Pic}^0(C)$ is abelian, this induces a map $C^{(r)} \to \mathrm{Pic}^0(C)$.

Proposition 1.72. *If $r = g$, this map is surjective.*

Proof. Note that the set $C^{(g)}$ can be identified with the set of effective divisors of degree g on C, and the map is given by $E \mapsto [E - gP_0]$. Let D be a divisor of degree 0. By Riemann-Roch,

$$\begin{aligned} \ell(D + gP_o) &= \ell(K - D - gP_0) + \deg(D + gP_0) + 1 - g \\ &= \ell(K - D - gP_0) + 1 \geq 1, \end{aligned}$$

thus there exists an effective divisor, of degree g, such that $[D] = [E - gP_0]$, whence the surjectivity. □

The idea of Weil's construction is then:

- Make $C^{(g)}$ into a "birational group", a variety with a group multiplication that is a rational map. Indeed, using the surjection $C^{(g)} \to \mathrm{Pic}^0(C)$, we can define the sum of two elements of $C^{(g)}$ modulo linear equivalence. Then, we can prove that there exist an open set $U \subset C^{(g)} \times C^{(g)}$ such that $\ell(D + D' - gP_0) = 1$ for all $(D, D') \in U$. By the proof of Proposition 1.72, multiplication is well-defined on U.
- A general result about birational groups shows that there exists a unique group variety J defined over k and a birational map $f : C^{(g)} \to J$ that is a homomorphism where products are defined, i.e. $f(ab) = f(a)f(b)$ when ab is defined in $C^{(g)}$. The group variety J is defined by "gluing" copies of translates of U.
- Prove that J is complete (so projective by his later work) and that the rational map $f : C^{(g)} \to J$ is a birational equivalence and a morphism. Moreover, if $D, D' \in C^{(g)}$ (as effective divisors of degree g) are linearly equivalent, then $f(D) = f(D')$.
- Therefore, we get an abelian variety J with a morphism $f : C^{(g)} \to J$ that is a birational equivalence. Moreover, $\mathrm{Pic}^0(C) \cong J$ as groups.

A posteriori, this is motivated by point 3 of Theorem 1.70.

7.2. Compatibility of the two Jacobians

Let X be a compact Riemann surface. By Theorem 1.22, there exists a non-singular algebraic curve X_{alg} defined over $\mathbb{C}$ such that $X \cong X_{\mathrm{alg}}(\mathbb{C})$ as compact Riemann surfaces. We can wonder about the relationship between the two Jacobians $\mathrm{Jac}(X)$ and $\mathrm{Jac}(X_{\mathrm{alg}})$.

Proposition 1.73. *The Jacobian of the compact Riemann surface X is the Jacobian of the algebraic curve X_{alg}, i.e.* $\mathrm{Jac}(X) \cong \mathrm{Jac}(X_{alg})$ *as abelian varieties over* $\mathbb{C}$*.*

Proof. Note that we have $\mathrm{Jac}(X) \cong \mathrm{Jac}(X_{\mathrm{alg}}(\mathbb{C}))$, so that we need to show that $\mathrm{Jac}(X_{\mathrm{alg}}(\mathbb{C})) \cong \mathrm{Jac}(X_{\mathrm{alg}})$. We use the universal properties from Proposition 1.69 and Theorem 1.70, along with Chow's theorem (Corollary 1.20). To simplify the notations, let A be an abelian variety such that $A(\mathbb{C}) \cong \mathrm{Jac}(X)$ as complex Lie groups. We prove that A satisfies the universal property of Theorem 1.70. The injective morphism $X_{\mathrm{alg}}(\mathbb{C}) \hookrightarrow \mathrm{Jac}(X_{\mathrm{alg}}(\mathbb{C})) \cong A(\mathbb{C})$ gives an injective morphism $X \to A$ by Corollary 1.20. Let B be an abelian variety with a morphism $g : X_{\mathrm{alg}} \to B$. By Proposition 1.69, this gives a morphism $g : X_{\mathrm{alg}}(\mathbb{C}) \to B(\mathbb{C})$, hence a morphism of complex Lie groups $\mathrm{Jac}(X_{\mathrm{alg}}(\mathbb{C})) \to B(\mathbb{C})$ such that the diagram

$$\begin{tikzcd}
X_{\mathrm{alg}}(\mathbb{C}) \arrow[r] \arrow[d] & \mathrm{Jac}(X_{\mathrm{alg}}(\mathbb{C})) \cong A(\mathbb{C}) \arrow[dl] \\
B(\mathbb{C}) &
\end{tikzcd}$$

commutes. Again, by Corollary 1.20, this gives a morphism of abelian varieties $A \to B$ such that

$$\begin{tikzcd}
X_{\mathrm{alg}} \arrow[r] \arrow[d] & A \arrow[dl] \\
B &
\end{tikzcd}$$

commutes, whence the result.

□

8. Néron models

An outstanding fact of the arithmetic of abelian varieties is the existence of *Néron models*, in particular generalizing the results we had about reduction of elliptic curves:

Theorem 1.74. *Let R be a Dedekind domain with field of fractions K and let A be an abelian variety over K. There exists a smooth commutative group scheme $\mathcal{A}$ over R such that for any smooth scheme $\mathcal{X}$ over R, the map*

$$\mathrm{Hom}_R(\mathcal{X}, \mathcal{A}) \to \mathrm{Hom}_K(\mathcal{X}_K, A)$$

is surjective, i.e. $\mathcal{A}(\mathcal{X}) \cong A(\mathcal{X}_K)$.

We call $\mathcal{A}$ the *Néron model* of A (defined up to isomorphism by this universal property).

By taking $\mathcal{X} = R$, we find in particular that $\mathcal{A}(R) \cong A(K)$, so that $\mathcal{A}$ is indeed a model for A.

In other words, the Néron model of A is a model over R such that morphisms to A can be extended[4] to morphism to $\mathcal{A}$. In particular, let X be a variety over K with a model $\mathcal{X}$ over R (in the sense of [Liu06, Chapter 10]) and let $f : X \to A$ be a morphism. Then f extends to a morphism $\hat{f} : \mathcal{X} \to \mathcal{A}$ and if $\mathfrak{p}$ is a prime ideal of R, we have a commutative diagram

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d] & A \arrow[d] \\
\mathcal{X}_{\mathfrak{p}} \arrow[r, "f_{\mathfrak{p}}"] & \mathcal{A}_{\mathfrak{p}},
\end{tikzcd}$$

where the vertical maps are reduction modulo $\mathfrak{p}$.

Definition 1.75. Let A be an abelian variety defined over the field of fractions K of a Dedekind domain R. We say that A has good reduction modulo a prime ideal $\mathfrak{p}$ of R if the fiber $A_{\mathfrak{p}} := \mathcal{A}_{\mathfrak{p}}$ is an abelian variety over $R/\mathfrak{p}$.

We will also use the fact that Néron models of Picard groups can be given "explicitly" in terms of the Picard functor (see [BLR90, 9.5]), but we shall explain this in given time.

The canonical reference about Néron models is the book [BLR90]. The case of elliptic curves is explained in great detail in [Sil94] and [Liu06].

9. L-functions

In this section, we summarize the definition of the L-function of an abelian variety[5]. The main resource about this subject is [Mil08, I.9]. The particular case of

[4] In some (weak) sense, it extends the fact that we can reduce morphisms between curves, which can be seen as follows: if $f : C \to C'$ is a morphism between two curves C, C' defined over $\mathbb{Q}$, then there exists a rational map $f_p : C_p \to C'_p$, which extends to a morphism.

[5] At the places of good reduction only for the sake of simplicity, since we do not treat the cases of bad reduction here. This is also what Shimura does in [Shi71]. In [Per13], we studied the factors at bad reduction as well.

elliptic curve is detailed in [Sil09, III.8.6]. As this subject was already studied by the author in [Per13], we go through this rather quickly.

9.1. Tate module and ℓ-adic representations

Let A be an abelian variety of dimension d defined over a field K. Recall that if K has characteristic zero or if the characteristic of K does not divide an integer m, then $A[m] \cong (\mathbb{Z}/m)^{2d}$. If ℓ is a prime distinct from the characteristic of K, we have the *Tate module*

$$T_\ell A = \varprojlim_{n\geq 0} A[\ell^n] \cong (\mathbb{Z}_\ell)^{2d}$$

as $\mathbb{Z}_\ell$-modules. Moreover, we have a natural map

$$\operatorname{End}(A) \to \operatorname{End}(T_\ell A) \cong M_{2d}(\mathbb{Z}_\ell),$$

which can be extended to a ℓ-adic representation

$$\rho_\ell : \operatorname{End}_{\mathbb{Q}}(A) \to M_{2d}(\mathbb{Q}_\ell),$$

where $\operatorname{End}_{\mathbb{Q}}(A) = \operatorname{End}(A) \otimes \mathbb{Q}$. A surprising result is the following:

Theorem 1.76. *If $\alpha \in \operatorname{End}_{\mathbb{Q}}(A)$, let $P_{\alpha,\ell} \in \mathbb{Q}_\ell[X]$ be the characteristic polynomial of $\rho_\ell(\alpha)$. Then*

1. *$P_{\alpha,\ell} \in \mathbb{Q}[X]$ (resp. $\mathbb{Z}[X]$ if $\alpha \in \operatorname{End}(A)$).*
2. *In particular, $P_{\alpha,\ell}$ does not depend on ℓ.*
3. *$P_{\alpha,\ell}$ has the form*

   $$X^{2d} - \operatorname{tr}(\alpha)X^{2d-1} + \cdots + \deg(\alpha),$$

   where $\operatorname{tr}(\alpha) = 1 + \deg(\alpha) - \deg(\operatorname{id} - \alpha)$.
4. *For all $x \in \mathbb{Z}$, we have $P_{\alpha,\ell}(x) = \deg(\alpha - x)$.*

Proof. See [Mil08, I.9]. The particular case of elliptic curves is done in [Sil09, III.8.6], where it is proven that $\det(\rho(\alpha)) = \deg(\alpha) \in \mathbb{Z}$ and $\operatorname{tr}(\rho(\alpha)) = 1 + \deg(\alpha) - \deg(\operatorname{id} - \alpha)$ using the Weil pairing, which is enough to conclude when $d = 1$. □

9.2. L-functions of abelian varieties

Suppose now that A is an abelian variety over a Galois number field K with ring of integers $\mathcal{O}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ of good reduction for A. If $\mathfrak{p}$ lies above the rational prime p, we have the Frobenius morphism $\sigma_{\mathfrak{p}} : A_{\mathfrak{p}} \to A_{\mathfrak{p}}$, along with representations

$$\begin{aligned} \rho : \operatorname{End}_{\mathbb{Q}}(A) &\to M_{2d}(\mathbb{Q}_\ell) \\ \rho_p : \operatorname{End}_{\mathbb{Q}}(A_p) &\to M_{2d}(\mathbb{Q}_\ell) \end{aligned}$$

such that

$$\begin{tikzcd} \operatorname{End}_{\mathbb{Q}}(A) \arrow[r, "\rho"] \arrow[d] & M_{2d}(\mathbb{Q}_\ell) \\ \operatorname{End}_{\mathbb{Q}}(A_p) \arrow[ur, "\rho_p"'] & \end{tikzcd}$$

commutes, where ℓ is any prime distinct from p. Hence, we have an operator $\rho_p(\sigma_p) \in M_{2d}(\mathbb{Q}_\ell)$, whose characteristic polynomial $\det(XI - \rho_p(\sigma_p))$ belongs to $\mathbb{Z}[X]$ by Theorem 1.76.

Definition 1.77. The *local factor at* $\mathfrak{p}$ is

$$L_{\mathfrak{p}}(A,s) = \det(1 - \rho_p(\sigma_p)X)(N(\mathfrak{p})^{-s})^{-1}$$

and the *L-function associated to A* is (up to the local factors at places of bad reduction)

$$L(A,s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(A,s),$$

where the product is over all prime ideals $\mathfrak{p}$ of $\mathcal{O}$.

Let $a_{\mathfrak{p}}(A) = |A_{\mathfrak{p}}|$. As in the case of elliptic curves, we compute that $\sigma_p + \hat{\sigma}_p = [a_{\mathfrak{p}}(A)]$, $\deg(\sigma_p) = p$ and $\mathrm{tr}(\sigma_p) = a_{\mathfrak{p}}(A)$. Hence, Theorem 1.76 shows that:

Proposition 1.78. *The local factor at a prime* $\mathfrak{p}$ *of good reduction has for form*

$$L_{\mathfrak{p}}(A,s) = 1 - a_{\mathfrak{p}}(A)N(\mathfrak{p})^{-s} + \cdots + pN(\mathfrak{p})^{-2ds},$$

where $a_{\mathfrak{p}}(A) = |A_{\mathfrak{p}}|$.

Example 1.79. If E is an elliptic curve, the characteristic polynomial of $\rho(\sigma_p)$ is $X^2 - \mathrm{tr}(\sigma_p) + \deg(\sigma_p)$ by Theorem 1.76. This gives the classical local factor $1 - a_p(E)p^{-s} + p^{1-2s}$ if p is a prime of good reduction for E.

Remark 1.80. For the places of bad reduction, we consider the action of an "algebraic" Frobenius in $\mathrm{Gal}(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}})$ (defined up to conjugation and to the choice of a lift) on $(T_\ell A \otimes \mathbb{Q}_\ell)^{I_{\mathfrak{p}}}$, where $I_{\mathfrak{p}} \subset \mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ is the inertia at $\mathfrak{p}$. When A has good reduction at $\mathfrak{p}$, the criterion of Néron-Ogg-Safarevich asserts that $T_\ell A$ is unramified at $\mathfrak{p}$ and the actions of the two Frobenius ("algebraic" and "geometric") are the same. Hence, the definitions agree in this case. See [Mil08, I.9], or [Per13] for an elementary account in the case of elliptic curves (or more generally representations of compact groups).

Chapter 2

Modular curves

In this chapter, we examine *modular curves* associated to congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and study their properties, in particular their structure of compact Riemann surfaces as well as their connections with moduli spaces of elliptic curves and modular forms. As explained in the introduction, modular curves and their Jacobians will be the starting point for associating abelian varieties to modular forms, thanks to the relationships between these objects.

The first part of the chapter, which gives the construction of modular curves, is not fully detailed, and is instead used as to remind of what, to fix notations, and to give references and recall elements that will be used in the second part. This subject is fully developed in [Miy06] and [DS06].

1. Congruence subgroups and their action on the upper half-plane

Let us first begin by recalling some facts about congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and their action on the upper half-plane $\mathbb{H}$.

1.1. Congruence subgroups

Definition 2.1. For an integer $N \geq 1$, the *principal congruence subgroup* of level N is

$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv I_2 \pmod{N}\}.$$

A *congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup containing $\Gamma(N)$ for some $N \geq 1$.

Example 2.2. In what follows, we will mainly consider the congruence subgroups $\Gamma(N)$,

$$\begin{aligned}\Gamma_0(N) &= \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N}\} \text{ and} \\ \Gamma_1(N) &= \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\}.\end{aligned}$$

Note that $\Gamma(N) \trianglelefteq \Gamma_1(N) \trianglelefteq \Gamma_0(N) \trianglelefteq \mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$.

Proposition 2.3. *Any congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *has finite index.*

Proof. It suffices to prove that $\Gamma(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$ for all $N \geq 1$. By definition, $\Gamma(N)$ is the kernel of the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N)$, which surjects. Indeed, let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ be the lift of an element in $\mathrm{SL}_2(\mathbb{Z})$. Without loss of generality, suppose that $c \neq 0$. Since $(c, d, N) = 1$, the integer $d' = d + N \prod_{p \mid c, p \nmid d} p$ satisfies $(c, d') = 1$. Letting $u, v \in \mathbb{Z}$ be such that $uc + vd' = 1$, we find that $\left(\begin{smallmatrix} a+vN & b-uN \\ c & d' \end{smallmatrix}\right)$ is another lift of the element, in $\mathrm{SL}_2(\mathbb{Z})$. Hence $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N)$, which is finite. □

Proposition 2.4. *If* Γ *is a congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *and* $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, *then* $\alpha\Gamma\alpha^{-1} \cap \mathrm{SL}_2(\mathbb{Z})$ *is a congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$.

Proof. Since $\alpha\Gamma(N)\alpha^{-1} = (M\alpha)\Gamma(N)(M\alpha)^{-1}$ for all $M \in \mathbb{Q}^*$, we can suppose that α has integral entries. If $D = \det\alpha$, then $\alpha^{-1}\Gamma(ND)\alpha \subset \mathrm{SL}_2(\mathbb{Z}) \cap \Gamma(N)$. □

1.2. Action on the upper half-plane

Recall that the topological group $\mathrm{SL}_2(\mathbb{R})$ acts properly on the upper half-plane $\mathbb{H}$ by restricting the action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$ by fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d} \; (z \in \mathbb{H}).$$

We will consider the restriction of this action for $\mathrm{SL}_2(\mathbb{Z})$ and its congruence subgroups. Since the action is proper and $\mathrm{SL}_2(\mathbb{Z})$ is discrete, we obtain[1]:

Proposition 2.5. *For any compacts $K, K' \subset \mathbb{H}$, the set*

$$\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma K \cap K' \neq \varnothing\}$$

is finite.

Corollary 2.6. *For any $z, z' \in \mathbb{H}$, there exist neighborhoods U, U' of z, respectively z', such that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$*

$$\gamma(U) \cap U' \neq \varnothing \Rightarrow \gamma(z) = z'.$$

Proof. By Proposition 2.5, the set $\{\gamma \in \Gamma : \gamma\overline{B}(z,1) \cap \overline{B}(z',1) \neq \varnothing\}$ is finite. Let $\gamma_1, \dots, \gamma_r$ be its elements. Since $\mathbb{H}$ is separated, let U_i and U_i' be disjoint neighborhoods in $\mathbb{H}$ of $\gamma_i z$, respectively z', for $1 \le i \le r$. Letting

$$U = B(z,1) \cap \left(\bigcap_{i=1}^{r} \gamma^{-1} U_i\right), \quad U' = B(z',1) \cap \left(\bigcap_{i=1}^{r} U_i'\right)$$

yields the result. □

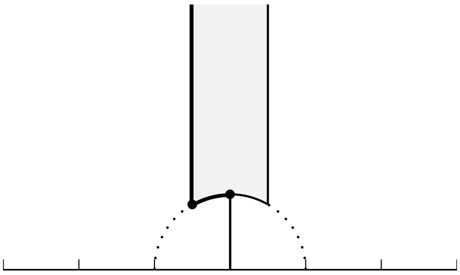

Figure 2.1: The fundamental domain $\{z \in \mathbb{H} : |\mathrm{Re}(z)| < 1/2,\ |z| > 1\}$ for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

Note that the action of $\{\pm I\}$ is trivial, so we will often consider the action of $\mathrm{PSL}_2(\mathbb{Z})$ instead of $\mathrm{SL}_2(\mathbb{Z})$. If Γ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ we will denote $\overline{\Gamma}$ to denote its image by the projection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$.

[1] Refer to the first chapter of [tD87], in particular section 3.

1.3. Stabilizers and elliptic points

Again, let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Proposition 2.7. *The stabilizers Γ_z ($z \in \mathbb{H}$) are finite cyclic groups.*

Proof. Let $z \in \mathbb{H}$. By Proposition 2.5, Γ_z is finite. Moreover, since $\mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathbb{H}$, we find that $\mathrm{SL}_2(\mathbb{R})_z$ is conjugate to $\mathrm{SL}_2(\mathbb{R})_i = \mathrm{SO}_2(\mathbb{R}) \cong S^1$. The result follows from the fact that any finite subgroup of S^1 is cyclic. □

Definition 2.8. The *period* of a point $z \in \mathbb{H}$ (with respect to Γ) is equal to the order of the group $\overline{\Gamma}_z \subset \mathrm{PSL}_2(\mathbb{Z})$. If z has order 1, we say that it is *elliptic*.

Remark 2.9. Note that the period is invariant with respect to the action of Γ, so we can also define the *period* of an element of $\Gamma\backslash\mathbb{H}$. An element of period 1 in $\Gamma\backslash\mathbb{H}$ will again be called *elliptic*.

2. Modular curves

We can now define the main objects of study for this chapter.

Definition 2.10. The *modular curve* $Y(\Gamma)$ associated to a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is the set $\Gamma\backslash\mathbb{H}$.

Notation 2.11. For any integer $N \geq 1$, we define $Y(N) = Y(\Gamma(N))$, $Y_0(N) = Y(\Gamma_0(N))$ and $Y_1(N) = Y(\Gamma_1(N))$, where $\Gamma(N), \Gamma_0(N)$ and $\Gamma_1(N)$ are as defined in Example 2.2.

We will now show that we can endow any modular curve with the structure of a Riemann surface, which we will then compactify.

For the remainder of this section, let us fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$.

2.1. Topological space structure

Let us give $Y(\Gamma)$ the quotient topology, making the projection $\pi : \mathbb{H} \to Y(\Gamma)$ continuous and open. Moreover, we have:

Proposition 2.12. *The topological space $Y(\Gamma)$ is separated.*

Proof. This follows from the more general fact that the quotient of a locally compact separated space by a proper group action is separated[2]. Alternatively, we can also use Corollary 2.6: let $z, z' \in \mathbb{H}$ with distinct images in $Y(\Gamma)$ and U, U' be neighborhoods as in the corollary. Then $\pi(U), \pi(U')$ are disjoint neighborhoods of $\pi(z)$, respectively $\pi(z')$. □

2.2. Riemann surface structure

Let $z \in \mathbb{H}$. By Corollary 2.6, there exists a neighborhood U of z such that for all $\gamma \in \Gamma$,

$$\gamma U \cap U \neq \varnothing \Rightarrow \gamma \in \Gamma_z. \tag{2.1}$$

[2] See [tD87, I.3.18] or [Miy06, Chapter I].

Charts around non-elliptic points Suppose that $\pi(z)$ is not elliptic. Then, Equation (2.1) shows that $\pi : U \to Y(\Gamma)$ is injective. Since it is continuous and open, it induces a isomorphism onto its image and gives a chart around $\pi(z)$.

Charts around elliptic points Suppose now that $\pi(z)$ is elliptic of order n. For any $z_1, z_2 \in U$,

$$\pi(z_1) = \pi(z_2) \Leftrightarrow z_1 \in \Gamma_z z_2.$$

Let $\delta_z = \left(\begin{smallmatrix} 1 & -z \\ 1 & -\overline{z} \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{C})$ be the Cayley transformation, mapping z to 0 and $\overline{z}$ to ∞. The conjugate $(\delta_z \Gamma \delta_z^{-1})_0 = \delta_z \Gamma_z \delta_z^{-1} \subset \mathrm{GL}_2^+(\mathbb{C})$ is cyclic and fixes the points $0, \infty$. As a group of fractional linear transformations of $\mathbb{P}^1(\mathbb{C})$, it is therefore generated by the multiplication by $e(1/n) = e^{2i\pi/n}$. Thus, we get that

$$\begin{aligned} \pi(z_1) = \pi(z_2) \quad &\Leftrightarrow \quad \delta_z z_1 = (\delta_z \Gamma_z \delta_z^{-1}) \delta_z z_2 \\ &\Leftrightarrow \quad \delta_z z_1 = e(d/n) \delta_z z_2 \text{ (for some } d \in \mathbb{Z}) \end{aligned}$$

Hence

$$\pi(z_1) = \pi(z_2) \Leftrightarrow (\delta_z z_1)^n = (\delta_z z_2)^n.$$

Therefore, defining $\psi : U \to \mathbb{C}$ as $\psi(w) = (\delta_z(w))^n$, we get that $\pi(z_1) = \pi(z_2)$ if and only if $\psi(z_1) = \psi(z_2)$. Thus, ψ induces an injection $\hat{\psi} : \pi(U) \to \mathbb{C}$. In other words, we have the commutative diagram

$$\begin{tikzcd}
U \arrow[r, "\delta"'] \arrow[rr, bend left, "\psi"] \arrow[d, "\pi"'] & \mathbb{C} \arrow[r, "\rho"'] & \mathbb{C} \\
\pi(U) \arrow[urr, dashed, "\hat{\psi}"'] & &
\end{tikzcd}$$

where $\rho : \mathbb{C} \to \mathbb{C}$ is defined by $\rho(w) = w^n$. By the open mapping theorem, $\psi(U)$ is an open subset of $\mathbb{C}$, so we finally obtain a isomorphism $\hat{\psi} : \pi(U) \to \psi(U)$ that we can use as a chart around z.

Compatibility of the charts It now remains to show that the charts defined above are compatible.

Proposition 2.13. *For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, the charts above endow the modular curve $Y(\Gamma)$ with the structure of a Riemann surface.*

Proof. See [DS06, Ch. 2] or [Miy06, Ch. 1] for this computation. □

3. Compactification

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The goal of this section is to compactify the modular curve $Y(\Gamma)$ by adding points to it, the *cusps*, to obtain a compact Riemann surface $X(\Gamma)$.

3.1. Cusps

Since $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, we can make the following definition:

Definition 2.14. An equivalence class of $\mathbb{P}^1(\mathbb{Q})$ under the action of Γ is called a *cusp* with respect to Γ.

Example 2.15. The full modular group $\mathrm{SL}_2(\mathbb{Z})$ has only one cusp, since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$.

Proposition 2.16. *There are finitely many cusps with respect to* Γ.

Proof. Since any congruence subgroup has finite index in $\mathrm{SL}_2\,\mathbb{Z}$, it suffices to prove that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{P}^1(\mathbb{Q})$ is finite, which is shown in Example 2.15. □

Width of a cusp Just as we defined the period of an elliptic point earlier, we will now define the *width* of a cusp. Let $s \in \mathbb{P}^1(\mathbb{Q})$ and choose $\delta \in \mathrm{SL}_2(\mathbb{Z})$ such that $\delta s = \infty$. Note that $\overline{\mathrm{SL}_2(\mathbb{Z})_\infty}$ is cyclic, generated by the translation $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{Z})$. Moreover,

$$\begin{aligned} h_s := [\overline{\mathrm{SL}_2(\mathbb{Z})_\infty} : \overline{\delta\Gamma_s\delta^{-1}}] = [\delta^{-1}\,\mathrm{SL}_2(\mathbb{Z})_\infty\delta : \Gamma_s] &= [(\delta^{-1}\,\mathrm{SL}_2(\mathbb{R})\delta)_s : \Gamma_s] \\ &= [\mathrm{SL}_2(\mathbb{Z})_s : \Gamma_s], \end{aligned}$$

which is finite by Proposition 2.3, so that $\overline{\delta\Gamma_s\delta^{-1}} = \langle\left(\begin{smallmatrix}1&h_s\\0&1\end{smallmatrix}\right)\rangle \subset \mathrm{PSL}_2(\mathbb{Z})$. Note that the integer h_s

1. is independent of δ;
2. does not depend on the image of s in $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$;
3. satisfies the equation $\pm\delta\Gamma_s\delta^{-1} = \pm\langle\left(\begin{smallmatrix}1&h_s\\0&1\end{smallmatrix}\right)\rangle$.

Hence, we can make the following definition:

Definition 2.17. Let $s \in \mathbb{P}^1(\mathbb{Q})$ and $\pi : \mathbb{P}^1(\mathbb{Q}) \to \Gamma\backslash\mathbb{P}^1(\mathbb{Q})$ be the natural projection. The *width* of the cusp $\pi(s)$ is the index $h_s = [\mathrm{SL}_2(\mathbb{Z})_s : \Gamma_s]$.

3.2. The modular curve $X(\Gamma)$

We define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ and we remark that $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}^* \subset \mathbb{P}^1(\mathbb{C})$.

Definition 2.18. The *modular curve* $X(\Gamma)$ is the quotient $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$.

Note that $X(\Gamma) = Y(\Gamma) \cup \Gamma\backslash\mathbb{P}^1(\mathbb{Q})$. That is, the modular curve $X(\Gamma)$ is equal to $Y(\Gamma)$ with finitely many points added, the cusps.

Notation 2.19. For all $N \geq 1$, we define $X(N), X_1(N)$ and $X_0(N)$ as in Notation 2.11.

3.3. The topology on $X(\Gamma)$

First of all, we define a topology on $\mathbb{H}^*$. The subspace topology with respect to the Riemann sphere $\mathbb{P}^1(\mathbb{C})$ would be too fine to have the quotient $X(\Gamma)$ separated. Rather, we define the topology of $X(\Gamma)$ as the one generated by:

1. the open sets of $\mathbb{H}$;
2. the sets

$$\alpha(N_M \cup \{\infty\})$$

for all $M > 0$ and $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, where $N_M = \{z \in \mathbb{H} : \operatorname{Im} z > M\}$. These give neighborhoods of the cusps, which are in fact[3] disks tangent to the real line at the rational cusps, and half-planes $N_{M'} \cup \{\infty\}$ at ∞, for $M' > 0$.

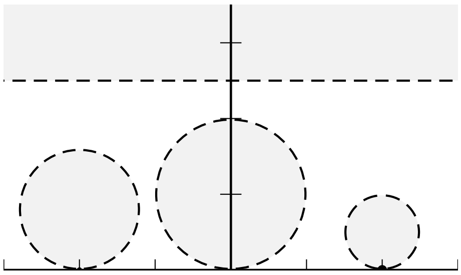

Figure 2.2: Open neighborhoods of cusps.

The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}^*$ is not proper[4], but we nonetheless have:

Proposition 2.20. *The modular curve $X(\Gamma)$ with the quotient topology induced by $\pi : \mathbb{H}^* \to X(\Gamma)$ is separated, compact and connected.*

Proof. See [DS06, Proposition 2.4.5] or [Miy06, Ch. 1]. □

3.4. Charts around the cusps

Let us now give $X(\Gamma) \supset Y(\Gamma)$ the structure of a Riemann surface. To do so, we need to find charts around the cusps. We will need the following Lemma, which is an easy computation:

Lemma 2.21. *Let $U = N_2 \cup \{\infty\}$. If $\gamma U \cap U \neq \varnothing$ for some $\gamma \in \mathrm{SL}_2(\mathbb{C})$, then γ is a translation.*

Let $s \in \mathbb{Q} \cup \{\infty\}$ be a cusp of width h in $X(\Gamma)$. First, let us choose $\delta \in \mathrm{SL}_2(\mathbb{Z})$ such that $\delta s = \infty$. Let U be as in Lemma 2.21 and let $U' = \delta^{-1}(U)$. Since U is a neighborhood of ∞ and δ_s is a homeomorphism, we get that U' is a neighborhood of s. Then, for $z_1, z_2 \in U$,

$$\begin{aligned}\pi(z_1) = \pi(z_2) \quad &\Leftrightarrow \quad z_1 = \gamma z_2 \text{ for some } \gamma \in \Gamma \\ &\Leftrightarrow \quad \delta(z_1) = (\delta\gamma\delta^{-1})(\delta z_2) \text{ for some } \gamma \in \Gamma\end{aligned}$$

In this case, Lemma 2.21 shows that $\delta\gamma\delta^{-1}$ is a translation. But

$$\delta\Gamma\delta^{-1} \cap \mathrm{SL}_2(\mathbb{Z})_\infty = (\delta\Gamma\delta^{-1})_\infty \subset \pm\langle\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)\rangle.$$

So $\delta(z_1) = \delta(z_2) + mh$ for some $m \in \mathbb{Z}$. Conversely, this condition implies that $z_1 = \gamma z_2$ for some $\gamma \in \Gamma$, since $\{\pm I\}(\delta\Gamma\delta^{-1})_\infty = \{\pm I\}\langle\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)\rangle$.

Therefore, if we define $\psi : U' \to \mathbb{C}$ by $\psi(z) = e(\delta z/h)$, we obtain that $\psi(z_1) = \psi(z_2)$ if and only if $\pi(z_1) = \pi(z_2)$. Hence, as before, ψ induces a map $\hat{\psi} : \pi(U) \to$

[3] Recall that fractional linear transformation preserve *lines*, i.e. subsets of the form $L \cup \{\infty\}$ for L a line in $\mathbb{C} \cong$, and circles in $\mathbb{C}$.

[4] For example, the stabilizer of ∞ in $X(1)$ is infinite.

$\mathbb{C}$, and finally a chart $\hat{\psi} : \pi(U) \to \psi(U)$ around s:

$$\begin{tikzcd} U \arrow[r, "\delta"'] \arrow[rr, bend left, "\psi"] \arrow[d, "\pi"'] & \mathbb{C} \arrow[r, "\rho"'] & \mathbb{C} \\ \pi(U) \arrow[urr, dashed, "\hat{\psi}"'] & & \end{tikzcd} \tag{2.2}$$

Note that $\psi = \rho \circ \delta$, where $\rho : \mathbb{C} \to \mathbb{C}$ is the map $z \mapsto e(z/h)$.

Summary of the charts on $X(\Gamma)$ We can summarize the charts of $X(\Gamma)$ by the following: for any $z \in \mathbb{H}^*$, there exists a neighborhood $U \subset \mathbb{H}^*$ of z such that for all $\gamma \in \Gamma$, the condition $\gamma U \cap U \neq \varnothing$ implies $\gamma \in \Gamma_z$. Let $\rho : \mathbb{C} \to \mathbb{C}$ and $\delta : U \to U$ be defined by

	ρ	δ
$z \in \mathbb{H}$	$z \mapsto z^h$, for h the period of z.	$\begin{pmatrix} 1 & -z \\ 1 & -\bar{z} \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{C})$
$z \in \mathbb{P}^1(\mathbb{Q})$	$z \mapsto e(z/h)$, for h the width of z	any $\delta \in \mathrm{SL}_2(\mathbb{Z})$ such that $\delta z = \infty$.

Then the chart around $\pi(z)$ is

$$\hat{\psi} : \pi(U) \to V$$

where $\hat{\psi}$ is such that $\hat{\psi} \circ \pi = \psi$, i.e. Diagram (2.2) commutes, where $\psi = \rho \circ \delta$. It now remains to check that these charts are compatible.

Theorem 2.22. *If* Γ *is a congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$*, the modular curve* $X(\Gamma)$ *is a compact Riemann surface.*

Proof. See [DS06, II.4] or [Miy06, Ch. 1]. □

Corollary 2.23. *If* Γ *is a congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$*, the modular curve* $X(\Gamma)$ *has only finitely many elliptic points.*

Proof. By Corollary 2.6, the set of elliptic points is discrete. □

4. Modular curves algebraically

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. By Section 1.2.3, the modular curve $X(\Gamma)$ is a complex algebraic curve. More precisely, there exists a complex algebraic curve $X(\Gamma)_{\mathrm{alg}}$ such that $X(\Gamma) \cong X(\Gamma)_{\mathrm{alg}}(\mathbb{C})$.

4.1. Planar model for $X_1(N)_{\mathrm{alg}}$

In Chapter 5, we will determine the function fields of $X(N)$ and $X_1(N)$ (as compact Riemann surfaces or algebraic curves) for any $N \geq 1$ as

$$\mathbb{C}(X(N)) = \mathbb{C}(j, \{f^v : v \in \mathbb{Z}^2 - 0\}) \text{ and } \mathbb{C}(X_1(N)) = \mathbb{C}(j, f_1),$$

where $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ is the modular j-invariant, $\{f^v \in \mathbb{C}(X(N)) : v \in \mathbb{Z}^2 - 0\}$ is a family of functions on $X(N)$, and f_1 is the composition of $f^{(0,1)^t}$ with the surjection $X_1(N) \to X(N)$.

Using this, we can give a planar model of $X_1(N)_{\mathrm{alg}}$ that will be used later. Indeed, let $p_1 \in \mathbb{C}(j)[X]$ be the minimal polynomial of f_1 over $\mathbb{C}(j)$, and let $\hat{p}_1 \in \mathbb{C}[j, X]$ be the polynomial obtained from clearing the denominators of p_1. Let

$$X_1(N)^{\mathrm{planar}} = \{(x, y) \in \mathbb{C}^2 : \hat{p}_1(x, y) = 0\}.$$

By the correspondence between function fields and curves (see [Har77, I.6] and [Ful08, Ch. 7] for the explicit construction), there is a birational map

$$(j, f_1) : X_1(N)_{\mathrm{alg}} \to X_1(N)^{\mathrm{planar}}.$$

More precisely, $X_1(N)_{\mathrm{alg}}$ can be obtained by resolving the singularities of the curve $X_1(N)^{\mathrm{planar}}$.

5. Jacobians varieties

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. As shown in the previous chapter, the Jacobian of the modular curve $X(\Gamma)$ (as a compact Riemann surface or as an algebraic curve) is a complex abelian variety of dimension equal to the genus of the curve. We will come back to these fundamental objects in the next chapters.

6. Moduli spaces

Let us now show how modular curves associated to the congruence subgroups $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$ can be seen as *moduli spaces* for *enhanced elliptic curves*. This point of view will be used in an important way later.

6.1. Enhanced elliptic curve and moduli spaces

An *enhanced elliptic curve* is an elliptic curve with additional torsion information. More precisely, we define the following spaces:

Definition 2.24. Let $N \geq 1$ be an integer.

- $S(\mathrm{SL}_2(\mathbb{Z}))$ is the moduli space of complex elliptic curves, i.e. the set of isomorphism classes of such objects.
- $S_1(N)$ is the moduli space of couples (E, Q), where E is an elliptic curve defined over $\mathbb{C}$ and $Q \in E$ a point of order N. Two such couples (E, Q) and (E', Q') are isomorphic if there is an isomorphism $E \cong E'$ mapping Q to Q'.
- $S_0(N)$ is the moduli space of couples (E, C), where E is an elliptic curve defined over $\mathbb{C}$ and $C \subset E$ is a subgroup of order N. Two such couples (E, C) and (E', C') are isomorphic if there is an isomorphism $E \cong E'$ mapping C to C'.
- $S(N)$ is the moduli space of couples $(E, (P, Q))$, where E is an elliptic curve defined over $\mathbb{C}$ and $(P, Q) \in E \times E$ is a pair of points of E generating $E[N]$. Two such couples $(E, (P, Q))$ and $(E', (P', Q'))$ are isomorphic if there exists an isomorphism $E \cong E'$ such that P (resp. Q) is mapped to P' (resp. Q').

We will denote the moduli classes of such couples with square brackets. Note that if $N = 1$, the three last objects reduce to the first one (the set of isomorphism classes of complex elliptic curves), and $Y(1) = Y_1(1) = Y_0(1)$ as well.

Proposition 2.25. *There are bijections $S(\mathrm{SL}_2(\mathbb{Z})) \equiv Y(\mathrm{SL}_2(\mathbb{Z}))$, $S_1(N) \equiv Y_1(N)$, $S_0(N) \equiv Y_0(N)$ and $S(N) = Y(N)$ given respectively by*

$$\begin{array}{rcl}
[\mathbb{C}/\Lambda_z] & \mapsto & [z]_{\mathrm{SL}_2(\mathbb{Z})} \\
[\mathbb{C}/\Lambda_z, [1/N]_{\Lambda_z}] & \mapsto & [z]_{\Gamma_1(N)} \\
[\mathbb{C}/\Lambda_z, \langle [1/N]_{\Lambda_z} \rangle] & \mapsto & [z]_{\Gamma_0(N)} \\
[\mathbb{C}/\Lambda_z, ([z/N]_{\Lambda_z}, [1/N]_{\Lambda_z})] & \mapsto & [z]_{\Gamma(N)}
\end{array}$$

where we identify complex elliptic curves and complex tori, and for $z \in \mathbb{H}$, Λ_z is the lattice $\mathbb{Z} + z\mathbb{Z}$.

Proof.

1. We know (see page 6) that any complex elliptic curve is isomorphic to a complex torus of dimension 1 (as complex Lie group). Since any lattice in $\mathbb{C}$ is homothetic to Λ_z for some $z \in \mathbb{H}$, this implies that any complex elliptic curve is isomorphic to $\mathbb{C}/\Lambda_z$ for some $z \in \mathbb{H}$. Moreover, if $z, z' \in \mathbb{H}$, then $\mathbb{C}/\Lambda_z \cong \mathbb{C}/\Lambda_{z'}$ if and only if $[z] = [z']$ in $Y(\mathrm{SL}_2(\mathbb{Z}))$. Indeed, by Proposition 1.29, $\mathbb{C}/\Lambda_z \cong \mathbb{C}/\Lambda_{z'}$ if and only if there exists $\alpha \in \mathbb{C}^*$ such that $\Lambda_z = \alpha\Lambda_{z'} = \alpha\mathbb{Z} \oplus \alpha z'\mathbb{Z}$, and the isomorphism $\mathbb{C}/\Lambda_z \mapsto \mathbb{C}/\Lambda_{z'}$ is given by $w \mapsto \alpha^{-1}w$. This condition holds if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(z,1)^t = (\alpha z', \alpha)^t$, i.e. $z' = \gamma z$.
2. Let $\mathbb{C}/\Lambda_z$ be an elliptic curve with a point Q of order N. Equivalently, there exist $c, d \in \mathbb{Z}$ such that $Q = [(c + dz)/N]$ and $(c, d, N) = 1$. Let $a, b, e \in \mathbb{Z}$ such that $ac - bd - eN = 1$ and consider the matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$. Since $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N)$ surjects, we can suppose that a, b, c, d are such that $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. By the above, the map $w \mapsto (cz+d)^{-1}w$ gives an isomorphism $\mathbb{C}/\Lambda_z \to \mathbb{C}/\Lambda_{\gamma z}$, sending Q to $[1/N]_{\Lambda_{\gamma z}}$. Hence, $[\mathbb{C}/\Lambda_z, Q] = [\mathbb{C}/\Lambda_{\gamma z}, [1/N]]$.

   If $z \in \mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, then the isomorphism $\mathbb{C}/\Lambda_{\gamma z} \to \mathbb{C}/\Lambda_z$ given by $w \mapsto (cz+d)w$ sends $[1/N]$ to $[1/N]$, since $(c, d) \equiv (0, 1) \pmod N$. Thus, the map $[z] \mapsto [\mathbb{C}/\Lambda_z, [1/N]]$ is well-defined.

   Finally, suppose that $z, z' \in \mathbb{H}$ are such that $[\mathbb{C}/\Lambda_z, [1/N]] = [\mathbb{C}/\Lambda_{z'}, [1/N]]$. By 1., there exists $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $z' = \gamma z$, and the isomorphism $\mathbb{C}/\Lambda_{z'} \to \mathbb{C}/\Lambda_z$ is given by $w \mapsto (cz + d)w$. Since $[(cz + d)/N]_{\Lambda_z} = [1/N]_{\Lambda_z}$, this gives $(c, d) \equiv (0, 1) \pmod N$, i.e. $\gamma \in \Gamma_1(N)$, so that $[z] = [z']$ in $Y_1(N)$.

3-4. The method is similar to the previous cases

□

6.2. Modular forms and functions on lattices

As a consequence of the moduli space interpretation of the modular curves $Y(\Gamma)$ of Proposition 2.25 ($\Gamma = \mathrm{SL}_2(\mathbb{Z}), \Gamma_1(N), \Gamma_0(N), \Gamma(N)$), we get the following natural interpretation of weight-k invariant functions on $\mathbb{H}$ with respect to these subgroups:

Definition 2.26. Let Γ be as above and let $k \in \mathbb{Z}$. A complex-valued function F on the set of enhanced elliptic curves with respect to Γ is called *k-homogeneous* if for all $\lambda \in \mathbb{C}^*$

$$\begin{cases} F(\mathbb{C}/\lambda\Lambda) = \lambda^{-k}F(\mathbb{C}/\Lambda) & \text{if } \Gamma = \mathrm{SL}_2(\mathbb{Z}) \\ F(\mathbb{C}/\lambda\Lambda, \lambda Q) = \lambda^{-k}F(\mathbb{C}/\Lambda, Q) & \text{if } \Gamma = \Gamma_1(N) \\ F(\mathbb{C}/\lambda\Lambda, \langle\lambda Q\rangle) = \lambda^{-k}F(\mathbb{C}/\Lambda, \langle Q\rangle) & \text{if } \Gamma = \Gamma_0(N) \\ F(\mathbb{C}/\lambda\Lambda, (\lambda P, \lambda Q)) = \lambda^{-k}F(\mathbb{C}/\Lambda, (P, Q)) & \text{if } \Gamma = \Gamma(N). \end{cases}$$

Proposition 2.27. *Let Γ be as above. There is a bijection between weight-k invariant functions $f : \mathbb{H} \to \mathbb{C}$ with respect to Γ and k-homogeneous complex-valued functions F on the set of enhanced elliptic curves with respect to Γ, given by*

$$f(z) = \begin{cases} F(\mathbb{C}/\Lambda_z) & \textit{if } \Gamma = \mathrm{SL}_2(\mathbb{Z}) \\ F(\mathbb{C}/\Lambda_z, [1/N]) & \textit{if } \Gamma = \Gamma_1(N) \\ F(\mathbb{C}/\Lambda_z, \langle[1/N]\rangle) & \textit{if } \Gamma = \Gamma_0(N) \\ F(\mathbb{C}/\Lambda_z, ([z/N], [1/N])) & \textit{if } \Gamma = \Gamma(N). \end{cases}$$

Proof. We only prove the first case, the three others being similar calculations. First of all, note that the formula in the statement defines F from f uniquely. Indeed, if $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ with $z = \omega_1/\omega_2 \in \mathbb{H}$, then $\Lambda = \omega_2\Lambda_z$ and

$$F(\mathbb{C}/\Lambda) = F(\mathbb{C}/\omega_2\Lambda_z) = \omega_2^{-k}F(\mathbb{C}/\Lambda_z) = \omega_2^{-k}f(z).$$

Moreover, if $\omega_1'\mathbb{Z} + \omega_2'\mathbb{Z} = \Lambda$ with $z' = \omega_1'/\omega_2' \in \mathbb{H}$, then there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\omega_1, \omega_2)^t = (\omega_1', \omega_2')^t$ and $z' = \gamma z$, thus

$$\omega_2' f(z') = (c\omega_1 + d\omega_2)^{-k} f(\gamma z) = \omega_2^{-k} f(z).$$

Finally, let us show the transfer of invariance properties. Suppose that F is a k-homogeneous function on the set of complex tori. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$f(\gamma z) = F(\mathbb{C}/\Lambda_{\gamma z}) = F(\mathbb{C}/(cz+d)^{-1}\Lambda_z) = (cz+d)^k F(\mathbb{C}/\Lambda_z) = (cz+d)^k f(z),$$

using that $\Lambda_{\gamma z} = (cz+d)^{-1}\Lambda_z$ as in the proof of Proposition 2.25. On the other hand, suppose that f is a weight-k invariant function on $\mathbb{H}$ with respect to $\mathrm{SL}_2(\mathbb{Z})$. If $\lambda \in \mathbb{C}^*$ and $\omega_1, \omega_2 \in \mathbb{C}$ are such that $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ and $z = \omega_1/\omega_2 \in \mathbb{H}$, then $F(\mathbb{C}/\lambda\Lambda) = (\lambda\omega_2)^{-k} f(z) = \lambda^{-k} F(\mathbb{C}/\Lambda_z)$.

□

Example 2.28 (Eisenstein series). If $k > 1$, the function on lattices $\Lambda \mapsto \sum_{z \in \Lambda - 0} \frac{1}{z^{2k}}$ is homogeneous of degree $2k$ and corresponds to the Eisenstein series G_{2k}, a modular form of weight $2k$ with respect to $\mathrm{SL}_2(\mathbb{Z})$. Recall that we define $g_2 = 60G_4$ and $g_3 = 140G_6$.

Example 2.29. The following is an example that we will use later on: For $v = (v_1, v_2) \in \mathbb{Z}^2 - 0$, define a function F^v on the set of enhanced elliptic curves with respect to $\Gamma(N)$ by

$$F^v(\mathbb{C}/\Lambda, (P, Q)) = \frac{g_2(\Lambda)}{g_3(\Lambda)} \wp_\Lambda(v_1 P + v_2 Q),$$

where $\wp$ is the Weierstrass elliptic function. Since F^v is 0-homogeneous, the corresponding function $f^v : \mathbb{H} \to \mathbb{C}$ given by

$$f^v(z) = \frac{g_2(\Lambda_z)}{g_3(\Lambda_z)} \wp_{\Lambda_z}\left(\frac{v_1 z + v_2}{N}\right)$$

is $\Gamma(N)$-invariant, so it defines a function $f^v : Y(N) \to \mathbb{C}$.

7. Relationship with modular forms

Finally, we investigate the relationship between modular curves and modular forms. Appendix B recalls the definition, notations, and basic properties of the latter.

The following is the key result:

Proposition 2.30. *For any even integer k, there is an isomorphism of complex vector spaces*

$$A_k(\Gamma) \cong \Omega^{k/2}(X(\Gamma)),$$

which (co)restricts to an isomorphism $\Omega^1_{hol}(X(\Gamma)) \cong S_2(\Gamma)$.

This comes from the fact that meromorphic modular forms are Γ-invariants meromorphic objects, and so are meromorphic forms on $X(\Gamma)$.

7.1. Pushbacks of differential forms

Let us consider the projection $\pi : \mathbb{H} \to X(\Gamma)$. It is a morphism of compact Riemann surfaces, which induces a linear map

$$\pi^* : \Omega^k(X(\Gamma)) \to \Omega^k(\mathbb{H}).$$

Let $\omega \in \Omega^k(X(\Gamma))$. Since $\mathbb{H}$ has a global chart, there exists a meromorphic function $f \in \mathbb{C}(\mathbb{H})$ such that $\pi^*(\omega) = f(z)(dz)^k$. This will give the bijection of Proposition 2.30.

In the following technical lemma, we begin by determining explicitly f in terms of ω, locally.

Lemma 2.31. *Let $\omega \in \Omega^k(X(\Gamma))$. For $w \in X(\Gamma)$, let $\hat{\psi} : \pi(U) \to \psi(U)$ be a coordinate near w defined as in Section 2.3. If ω is given locally by $g(z)(dz)^k \in \Omega^k(\psi(U))$, then $\pi^*(\omega) \in \Omega^k(\mathbb{H})$ is given locally by*

1. *if $w \in Y(\Gamma)$ has period h,*

$$g(\psi(z)) \left(\frac{\delta(z)^{h-1} h \det(\delta)}{(z - \overline{w})^2} \right)^k (dz)^k \in \Omega^k(U);$$

2. *if w is a cusp with width h,*

$$g(\psi(z)) \left(\frac{2\pi i \psi(z)}{h} \right)^k j(\delta, z)^{-2k} (dz)^k \in \Omega^k(U).$$

Proof. Recall that the coordinate near w is such that

- $U \subset \mathbb{H}^*$ is a neighborhood of w such that for all $\gamma \in \Gamma$, the condition $\gamma U \cap U \neq \varnothing$ implies $\gamma \in \Gamma_z$.
- $\psi : U \to \mathbb{C}$ is defined by a composition $\rho \circ \delta$ for some functions $\delta \in \mathrm{GL}_2(\mathbb{C})$ and $\rho : \mathbb{C} \to \mathbb{C}$.
- $\hat{\psi}$ is such that $\hat{\psi} \circ \pi = \psi$.

On the other hand, a chart around w in $\mathbb{H}$ is given by $\mathrm{id} : U \to U$. The map $\pi : \mathbb{H} \to X(\Gamma)$ in local coordinates is $\hat{\psi} \circ \pi = \psi = \rho \circ \delta : U \to \psi(U)$.

1. If w is not a cusp, then $\rho(z) = z^h$ and $\delta = \left(\begin{smallmatrix} 1 & -w \\ 1 & -\overline{w} \end{smallmatrix}\right)$. Note that
$$\frac{d\psi}{dz}(z) = \frac{d\rho}{dz}(\delta z)\frac{d\delta}{dz}(z) = \delta(z)^{h-1}\frac{h\det(\delta)}{(z-\overline{w})^2},$$
which gives the expression above for $\pi^*(\omega)$ locally in $\Omega^k(U)$.
2. If w is a cusp of width h, then $\rho(z) = e(z/h)$ and $\delta \in \mathrm{SL}_2(\mathbb{Z})$ is such that $\delta w = \infty$. Again, note that
$$\frac{d\psi}{dz}(z) = \frac{d\rho}{dz}(\delta z)\frac{d\delta}{dz}(z) = \frac{2\pi i\psi(z)}{h}j(\delta, z)^{-2},$$
which gives the expression above for $\pi^*(\omega)$ locally in $\Omega^k(U)$.

□

7.2. Differential forms to meromorphic modular forms

Lemma 2.32. *For $\omega \in \Omega^k(X(\Gamma))$, the function $f \in \mathbb{C}(\mathbb{H})$ such that $\pi^*(\omega) = f(z)(dz)^k$ is a meromorphic modular form of weight $2k$ with respect to Γ.*

Proof. First, let us prove that $f[\gamma]_{2k} = f$ for all $\gamma \in \Gamma$. For $\pi : \mathbb{H} \to X(\Gamma)$ the projection, the meromorphic map $\gamma : \mathbb{H} \to \mathbb{H}$ is such that $\pi \circ \gamma = \pi$. Hence, $\gamma^* \circ \pi^* = \pi^*$, so that
$$f(z)(dz)^k = \pi^*(\omega) = \gamma^*(\pi^*(\omega)) = \gamma^*(f(z)(dz)^n) = f(\gamma z)j(\gamma, z)^{-2k}(dz)^n,$$
where we used that $\frac{d\gamma(z)}{dz} = j(\gamma, z)^{-2}$. This shows that $f[\gamma]_{2k} = f$. We now need to prove that f is meromorphic at the cusps. For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we compute a local expression for $f[\gamma]_{2k}$ around ∞. Let $w = \gamma\infty$. By Lemma 2.31,
$$f(z)(dz)^k = \pi^*(\omega)(z) = g(\psi(z))\left(\frac{2\pi i\psi(z)}{h}\right)^k j(\gamma^{-1}, z)^{-2k}(dz)^k$$
for z in some neighborhood $U \subset \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ of w. Let $z' = \gamma^{-1}z$. Using that $j(\gamma^{-1}, z')j(\gamma, z) = 1$, we find that
$$f[\gamma]_{2k}(z') = g(\rho(z'))\left(\frac{2\pi i\rho(z')}{h}\right)^k \tag{2.3}$$
for $z' \in \gamma^{-1}U$, a neighborhood of ∞. This shows that f is meromorphic at the cusp w, for the weight $2k$. □

7.3. Differential forms to meromorphic modular forms

Lemma 2.33. *If $f \in A_{2k}(\Gamma)$, there exists $\omega \in \Omega^k(X(\Gamma))$ such that $\pi^*(\omega) = f(z)(dz)^k$.*

Proof. Let $(\pi(U_i), \hat{\psi}_i)$ be the atlas of $X(\Gamma)$ defined in this chapter. It suffices to find elements $\omega_i \in \Omega^k(\hat{\psi}_i(U_i))$ such that $(\hat{\psi})^*(\omega_i) = f(z)(dz)^k$ locally, since these would then be compatible, inducing $\omega \in \Omega^k(X(\Gamma))$ such that $\pi^*(\omega) = f(z)(dz)^k$.

Let $\pi(w) \in X(\Gamma)$ and let $\hat{\psi} : \pi(U) \to \psi(U)$ be the local coordinate around w as in Section 2.3. By Lemma 2.31, we need to find a meromorphic function $g : \psi(U) \to \mathbb{C}$ such that

- if $\pi(w)$ is a cusp of width h, let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $z = \gamma\infty$. By Equation (2.3), we find that we must have

$$g(\rho(z')) = f[\gamma]_{2k}(z') \left(\frac{2\pi i \rho(z')}{h}\right)^{-k}$$

for $z' \in \gamma^{-1}U$. Recall that $\rho(z') = e(z'/h)$. Since f is meromorphic at the cusp z, there exists a complex function k meromorphic around 0 such that $f[\gamma]_{2k}(z') = k(\rho(z'))$. Thus, around 0, we can define

$$g(z) = k(z) \left(\frac{2\pi i z}{h}\right)^{-k}. \tag{2.4}$$

- if $w \in \mathbb{H}$ has period h, we must have

$$f(z) = g(\psi(z)) \left(\frac{\delta(z)^{h-1} h \det(\delta)}{(z-\overline{w})^2}\right)^{k}$$

for $z \in U$. Letting $z' = \delta z$ with δ as in the definition of the chart, we find that this is equivalent to

$$g(\rho(z')) = \left[f[\delta^{-1}]_{2k}(z')(z')^k\right] \rho(z')^{-k} \det(\delta)^{k-1} h^{-k}$$

for $z' \in \delta U$. To conclude as was done above, it suffices to prove that there exists a function $\hat{k} : \mathbb{H} \to \mathbb{C}$ meromorphic at the origin such that $k(z') = \hat{k}(\rho(z'))$ for z' near 0, where $k : \mathbb{H} \to \mathbb{C}$ is the meromorphic function between square brackets above. Indeed, we can then define

$$g(z) = \hat{k}(z)(zh)^{-k} \det(\gamma)^{k-1}. \tag{2.5}$$

To do that, it is enough to show that k is invariant under the transformation $z' \mapsto e(1/h)z'$. Recall that $\delta\Gamma_z\delta^{-1}$ as a group of fractional linear transformations of $\mathbb{P}^1(\mathbb{C})$ is cyclic of order h generated by multiplication by $e(1/h)$. Let $\gamma \in \Gamma_z$ such that $\delta\gamma\delta^{-1}$ corresponds to multiplication by $e(1/h)$. Then

$$k(e(1/h)z') = k[\delta\gamma\delta^{-1}]_{2k}(z') = f[\gamma\delta^{-1}]_{2k}(z')(\delta\gamma\delta^{-1}z')^k = k(z').$$

□

7.4. Proof of Proposition 2.30

Proof of Proposition 2.30. Let us consider the map $\Phi : \Omega^{k/2}(X(\Gamma)) \to A_k(\Gamma)$ defined by

$$\pi^*(\omega)(z) = \Phi(\omega)(z)(dz)^n$$

for $\omega \in \Omega^{k/2}(X(\Gamma))$. This is well-defined by Lemma 2.33. By Lemma 2.32, this map is surjective. Finally, Φ is clearly $\mathbb{C}$-linear and injective. For $w \in \mathbb{H}^*$, Equations (2.4) and (2.5) show that

- if $w \in \mathbb{P}^1(\mathbb{Q})$,

$$v_{\pi(w)}(\omega) = v_0(k) - \frac{k}{2} = \mathrm{ord}_w(f) - \frac{k}{2}.$$

If $k = 2$, this gives that f vanishes at the cusp $\pi(w)$ if and only if ω is holomorphic at $\pi(w)$.

– if $w \in \mathbb{H}$,

$$v_{\pi(w)}(\omega) = \mathrm{ord}_0(\hat{k}) - \frac{k}{2} = \frac{\mathrm{ord}_w(f)}{h} - \frac{k}{2}\left(1 - \frac{1}{h}\right).$$

If $k = 2$, it follows that $v_{\pi(w)}(\omega) = (\mathrm{ord}_w(f) - h + 1)/h$ or $\mathrm{ord}_w(f) = hv_{\pi(w)}(\omega) + h - 1$. Since these two numbers are integers, it follows that f is holomorphic at w if and only if ω is holomorphic at $\pi(w)$.

Consequently, $\omega \in \Omega^1_{\mathrm{hol}}(X(\Gamma))$ if and only if $\Phi(\omega) \in S_2(\Gamma)$.

□

7.5. Dimensions of spaces of modular forms

Through the isomorphism of Proposition 2.30, a lot of information about spaces of modular forms can be obtained by studying spaces of meromorphic differentials on modular curves.

In particular, using the Riemann-Roch theorem, we obtain dimension formulas for spaces of modular forms and cusp forms (and finite-dimensionality!) in terms of the number of elliptic points and cusps. The restriction "k even" can be lifted to obtain results about spaces of modular forms of any weight.

It is not our goal to study these arguments here; the reader can refer to [DS06, Ch. 3] and [Miy06, Ch. 2]. However, we still note the following basic case, which will be useful later:

Corollary 2.34. *For any even integer $k \geq 0$, the dimension of the $\mathbb{C}$-vector space of cusp forms $S_2(\Gamma)$ is equal to the genus of the modular form $X(\Gamma)$.*

Proof. By Proposition 2.30, $S_2(\Gamma) \cong \Omega^1_{\mathrm{hol}}(X(\Gamma))$. As a corollary of Riemann-Roch (see [Mir95, p. 192]), the dimension of $\Omega^1_{\mathrm{hol}}(X(\Gamma))$ ("analytic genus" of $X(\Gamma)$) is equal to the (topological) genus of $X(\Gamma)$. □

7.6. Jacobians and cusp forms

By Proposition 2.30, we have $S_2(\Gamma_1(N)) \cong \Omega^1_{\mathrm{hol}}(X_1(N))$. Since $\mathrm{Jac}(X_1(N)) = \Omega^1_{\mathrm{hol}}(X_1(N))^*/H_1(X_1(N))$, there exists a lattice $\Lambda \subset S_2(\Gamma_1(N))^*$ such that

$$S_2(\Gamma_1(N))^*/\Lambda \cong \mathrm{Jac}(X)$$

as complex tori. We will also call Λ the *lattice of periods.*

Chapter 3

Hecke operators, modular curves and modular forms

In this chapter, we will study *Hecke operators* on modular forms, moduli spaces, and on modular curves and their Jacobians. They will be the tools used to "cut" the Jacobian of a modular curve into abelian varieties related to particular modular forms.

The main references for this chapter are [DS06, Chapter 5], [Miy06, 2.7-2.8] and [Shi71, Chapter 3]. In [DS06], the Hecke ring is not introduced and properties such as commutativity of Hecke operators on modular forms are proved by using explicit formulas. The two other books introduce the Hecke ring and its properties in great generality. Here, we take an intermediate approach.

1. Double cosets

A way to define operators on modular forms, moduli spaces and modular curves and their Jacobians is by using *double cosets* of congruence subgroups.

Definition 3.1. Let Γ_1 and Γ_2 be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. For any $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, we can consider the *double coset* $\Gamma_1\alpha\Gamma_2$. We denote the free abelian group on the set of such double cosets by $A(\Gamma_1, \Gamma_2)$.

Proposition 3.2. *If Γ_1 and Γ_2 are congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, the set $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is finite for all $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$.*

Proof. Let $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 \subset \Gamma_2$. Then, there is a bijection between $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ and $\Gamma_3\backslash\Gamma_2$, given by $[\alpha\gamma_2] \mapsto [\gamma_2]$. Since Γ_2 and Γ_3 are congruence subgroups (by Lemma 2.4 for the second one), the quotient $\Gamma_3\backslash\Gamma_2$ is finite. □

Hence, we can write

$$\Gamma_1\alpha\Gamma_2 = \bigsqcup_{j=1}^{n} \Gamma_1\beta_j(\alpha) \tag{3.1}$$

for some $\beta_j(\alpha) \in \Gamma_1\alpha\Gamma_2$ $(1 \leq j \leq n)$. Using this decomposition, we can define actions of $A(\Gamma_1, \Gamma_2)$ on abelian groups with a right action of $\mathrm{GL}_2^+(\mathbb{Q})$ that is Γ_1 invariant:

Proposition 3.3. *Let Γ_1, Γ_2 be as above, and let M be an abelian group with a right-action of $\mathrm{GL}_2^+(\mathbb{Q})$. There is then a right action of $A(\Gamma_1, \Gamma_2)$ on M^{Γ_1} given by*

$$m(\Gamma_1\alpha\Gamma_2) = \sum_{j=1}^{n} m\beta_j(\alpha)$$

for $m \in M$ and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, where $\beta_j(\alpha)$ are as in (3.1).

Proof. We need to show that the definition above does not depend on the chosen decomposition. Suppose that $\Gamma_1\alpha\Gamma_2 = \sqcup_{j=1}^{n}\Gamma_1\beta_j'$ for some $\beta_j' \in \Gamma_1\alpha\Gamma_2$. Then, there exist $\sigma \in S_k$ and $\gamma^{(1)}, \dots, \gamma^{(n)} \in \Gamma_1$ such that $\beta'_j = \gamma^{(j)}\beta_{\sigma(j)}$, so that

$$\sum_{j=1}^{n} m\beta'_j = \sum_{j=1}^{n} m\beta_{\sigma(j)} = \sum_{j=1}^{n} m\beta_j$$

for all $m \in M^{\Gamma_1}$. □

2. The Hecke ring

Let us now consider the case $\Gamma_1 = \Gamma_2$.

Definition 3.4. For Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and Δ a semigroup in $M_2^+(\mathbb{Z}) = \{\delta \in M_2(\mathbb{Z}) : \det(\delta) > 0\}$ containing Γ, we let the *Hecke ring* $R(\Gamma, \Delta)$ be the subgroup $\{\Gamma\alpha\Gamma : \alpha \in \Delta\}$ of $A(\Gamma, \Gamma)$.

We define a composition law on $R(\Gamma, \Delta)$ as follows: if

$$\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{n} \Gamma\alpha_i, \ \Gamma\beta\Gamma = \bigsqcup_{j=1}^{m} \Gamma\beta_j \in R(\Gamma, \Delta),$$

then we set

$$(\Gamma\alpha\Gamma)(\Gamma\beta\Gamma) = \sum_{i=1}^{n}\sum_{j=1}^{m} \Gamma\alpha_i\beta_j = \sum c_\gamma \Gamma\gamma\Gamma \in R(\Gamma, \Delta),$$

where the second sum is over all (distinct) double cosets $\Gamma\gamma\Gamma \in R(\Gamma, \Delta)$ and

$$c_\gamma = |\{(i,j) : \Gamma\gamma = \Gamma\alpha_i\beta_j\}| = |\{(i,j) : \Gamma\gamma\Gamma = \Gamma\alpha_i\beta_j\Gamma\}|/|\Gamma\backslash\Gamma\gamma\Gamma|. \qquad (3.2)$$

Proposition 3.5. *Let* Γ *and* Δ *be as above. Then the composition law on* $R(\Gamma, \Delta)$ *is well-defined and associative.*

Proof. Let us consider the free abelian group A on the set $\Gamma\backslash\Delta$. Then A is a right Γ-module and we have a homomorphism $R(\Gamma, \Delta) \hookrightarrow A$ given by $\Gamma\alpha\Gamma = \bigsqcup_i \Gamma\alpha_i \mapsto \sum_i \Gamma\alpha_i$. It is injective since if $\Gamma\alpha\Gamma = \bigsqcup_i \Gamma\alpha_i \neq \bigsqcup_j \Gamma\alpha'_j = \Gamma\alpha'\Gamma$, then $\Gamma\alpha_i \neq \Gamma\alpha'_j$ for all i, j. Moreover, we see that $R(\Gamma, \Delta) = A^\Gamma$. By Proposition 3.3, there is a right action of $A(\Gamma, \Gamma)$ on $R(\Gamma, \Delta)$ given by

$$(\Gamma\alpha\Gamma).(\Gamma\beta\Gamma) = \sum_{i=1}^{n} (\Gamma\alpha\Gamma)\beta_i = \sum_{i=1}^{n}\sum_{j=1}^{m} \Gamma\alpha_j\beta_i$$

for all $\alpha \in \Delta, \beta \in \mathrm{GL}_2^+(\mathbb{Q})$, where $\Gamma\beta\Gamma = \bigsqcup_{i=1}^{n} \Gamma\beta_i$ and $\Gamma\alpha\Gamma = \bigsqcup_{j=1}^{m} \Gamma\alpha_j$. This is equal to the multiplication $(\Gamma\alpha\Gamma)(\Gamma\beta\Gamma)$, so the composition law on $R(\Gamma, \Delta)$ is well-defined and associative. □

Proposition 3.6. *Let* Γ *and* Δ *be as above.*

1. *If there exists an anti-involution*[1] $\varphi : \Delta \to \Delta$ *such that* $\varphi(\Gamma) = \Gamma$ *and* $\Gamma\alpha\Gamma = \Gamma\varphi(\alpha)\Gamma$ *for all* $\alpha \in \Delta$, *then* $R(\Gamma, \Delta)$ *is a commutative ring with unit* $\Gamma 1 \Gamma = \Gamma$.

[1] This is, $\varphi \circ \varphi = \mathrm{id}$ and φ is an antihomomorphism.

2. *In this case, if M is an abelian group with a right action of Δ, then M^Γ is a right $R(\Gamma, \Delta)$-module.*

Proof. First, we prove that if $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ is such that $|\Gamma\backslash\Gamma\alpha\Gamma| = |\Gamma\alpha\Gamma/\Gamma|$, then there exists $\beta_i \in \Gamma\alpha\Gamma$ $(1 \leq i \leq n)$ such that

$$\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{n} \Gamma\beta_i = \bigsqcup_{i=1}^{n} \beta_i\Gamma.$$

Indeed, let α_i and α_i' $(1 \leq i \leq n)$ such that $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{n} \Gamma\alpha_i = \bigsqcup_{i=1}^{n} \alpha_i'\Gamma$. It suffices to show that $\Gamma\alpha_i \cap \alpha_i'\Gamma \neq \varnothing$ for all i, since we can then pick $\beta_i \in \Gamma\alpha_i \cap \alpha_i'\Gamma$ for every i and obtain the desired equality because $\Gamma\beta_i = \Gamma\alpha_i$ and $\beta_i\Gamma = \alpha_i'\Gamma$. If $\Gamma\alpha_i \cap \alpha_i'\Gamma = \varnothing$, we would have $\Gamma\alpha_i \subset \bigsqcup_{j\neq i} \alpha_j'\Gamma$, so that $\Gamma\alpha\Gamma = \bigsqcup_{j\neq i} \alpha_j'\Gamma$, which is impossible.

We can now prove the proposition:

1. For $\alpha \in \Delta$, let β_i $(1 \leq i \leq n)$ be such that $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{n} \Gamma\beta_i$. Note that $\Gamma\alpha\Gamma = \Gamma\varphi(\alpha)\Gamma = \varphi(\Gamma\alpha\Gamma) = \bigsqcup_{i=1}^{n} \varphi(\beta_i)\Gamma$. Hence $|\Gamma\backslash\Gamma\alpha\Gamma| = |\Gamma\alpha\Gamma/\Gamma|$.

   Let $\alpha, \alpha' \in \Delta$. By the above, there exist $\beta_i \in \Gamma\alpha\Gamma$ $(1 \leq i \leq n)$ and $\beta_i' \in \Gamma\alpha'\Gamma$ $(1 \leq i \leq m)$ such that

   $$\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{n} \Gamma\beta_i = \bigsqcup_{i=1}^{n} \beta_i\Gamma \text{ and } \Gamma\alpha'\Gamma = \bigsqcup_{i=1}^{m} \Gamma\beta_i' = \bigsqcup_{i=1}^{m} \beta_i'\Gamma.$$

   Thus

   $$(\Gamma\alpha\Gamma)(\Gamma\alpha'\Gamma) = \sum c_\gamma \Gamma\gamma\Gamma \text{ and } (\Gamma\alpha'\Gamma)(\Gamma\alpha\Gamma) = \sum c_\gamma' \Gamma\gamma\Gamma,$$

   where $c_\gamma = |\{(i,j) : \Gamma\gamma = \Gamma\beta_i\beta_j'\}|$ and $c_\gamma' = |\{(i,j) : \Gamma\gamma = \Gamma\beta_j'\beta_i\}|$. Using Equation (3.2), we see that $c_\gamma = c_{\gamma'}$.

2. It suffices to prove that $(m\zeta_1)\zeta_2 = m(\zeta_1\zeta_2)$ for all $m \in M^\Gamma$ and $\zeta_1, \zeta_2 \in R(\Gamma, \Delta)$. This is clear by the definition of the product.

□

Henceforth, we will consider the following two cases:

Example 3.7. Let $\Gamma = \Gamma_1(N)$ and

$$\Delta = \Delta^1(N) = \{\alpha \in M_2(\mathbb{Z}) : \det\alpha > 0,\ \alpha \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \pmod N\}.$$

As we will shortly see in Lemma 3.10, we have an anti-involution $\left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & c \\ bN & d \end{smallmatrix}\right)$ verifying the two conditions of Proposition 3.6. Therefore, $R(\Gamma, \Delta)$ is commutative.

Example 3.8. Let $\Gamma = \Gamma_0(N)$ and

$$\Delta = \Delta^0(N) = \{\alpha \in M_2(\mathbb{Z}) : \det\alpha > 0,\ \alpha \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod N\}.$$

An anti-involution verifying the conditions of Proposition 3.6 can be defined as above, showing that $R(\Gamma, \Delta)$ is also commutative.

2.1. Hecke operators and diamond operators

We now define two important classes of elements of the ring $R(\Gamma_1(N), \Delta^1(N))$, called *Hecke and diamond operators.* We will shortly see how they act on modular forms, modular curves and their Jacobians, and moduli spaces.

In what follows, we let $\Gamma = \Gamma_1(N)$ and $\Delta = \Delta^1(N)$.

The Hecke operators

Definition 3.9. For any integer $n \geq 1$, we define an element $T_n \in R(\Gamma, \Delta)$ by

$$T_n = \sum_{\substack{\Gamma\alpha\Gamma \\ \alpha\in\Delta^n}} \Gamma\alpha\Gamma,$$

where $\Delta^n = \{\alpha \in \Delta : \det \alpha = n\}$.

The following Lemma shows that this definition makes sense (i.e. that the sum is finite[2]) and gives decomposition (3.1) for the double cosets involved:

Lemma 3.10. *For any $\alpha \in \Delta^n$, we have that*

$$\Gamma\alpha\Gamma = \Delta^n = \bigsqcup_{a} \bigsqcup_{b=0}^{n/a-1} \Gamma\sigma_a \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix}$$

where the union is over the integers $a > 0$ such that $a \mid n$ and $(a, N) = 1$, and $\sigma_a \in \mathrm{SL}_2(\mathbb{Z})$ is such that $\sigma_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \pmod N$.

Proof. This is a particular case of [Shi71, Proposition 3.36] with $t = 1$ and $\mathfrak{h} = \{1\}$ or [Miy06, Section 4.5]. For the particular case n prime, see [DS06, pp. 104-105]. The idea is to consider actions of Δ^n on lattices. □

Remark 3.11. If p is prime, note that we get $T_p = \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma \in R(\Gamma, \Delta)$. Moreover, let us define

$$\beta_j = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \text{ for } 1 \leq j < p \text{ and } \beta_\infty = \begin{pmatrix} mp & m' \\ Np & p \end{pmatrix}, \tag{3.3}$$

where β_∞ is defined when $p \nmid N$, with $m, m' \in \mathbb{Z}$ such that $mp - m'N = 1$. Then, by Lemma 3.10, the decomposition (3.1) is given by $\beta_1, \ldots, \beta_{p-1}$ if $p \mid N$ and $\beta_1, \ldots, \beta_{p-1}, \beta_\infty$ if $p \nmid N$.

Lemma 3.12. *If m, n are coprime integers, we have $T_{mn} = T_m T_n$.*

Proof. This also follows from considering actions of Δ^n on lattices and applying the Chinese theorem. See [Shi71, Proposition 3.34] or [Miy06, 4.5.8(2) and 4.5.18(1)]. □

[2] In fact reduced to one element. We could have defined T_n from Lemma 3.10, but Definition 3.9 generalizes to other pairs (Γ, Δ). For example, for $(\Gamma_0(N), \Delta_0(N))$, the sum is not reduced to one element.

The diamond operators

Definition 3.13. For $d \in (\mathbb{Z}/N)^{\times}$, we define the *diamond operator*

$$\langle d \rangle = \Gamma\alpha\Gamma \in R(\Gamma, \Delta),$$

where $\alpha \in \Gamma_0(N) \subset \Delta$ is such that its bottom-right coefficient is equal to d in $(\mathbb{Z}/N)^{\times}$. If $d \in \mathbb{Z}$ is such that $N \mid d$, we let $\langle d \rangle = 0 \in R(\Gamma, \Delta)$.

Lemma 3.14. *This element is well-defined.*

Proof. We need to check that the definition of $\langle d \rangle$ does not depend on the element α chosen. Recall that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$, so that $\Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N)\alpha$. Moreover, $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N)^{\times}$, where the isomorphism is induced by the map $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto [d]$. Hence, $\Gamma_1(N)\alpha$ depends only on the image of the bottom-right coefficient of α in $(\mathbb{Z}/N)^{\times}$. □

Lemma 3.15. *If p is prime and $e \geq 1$, we have $T_{p^e} = T_p T_{p^{e-1}} - p^{e-1}\langle p \rangle T_{p^{e-2}}$.*

Proof. See [Shi71, Proposition 3.34] or [Miy06, 4.5.7 and 4.5.18(1)]. □

Remark 3.16. In [DS06], the elements T_n are defined only for n prime, and extended with Lemmas 3.15 along with this property.

3. Actions on modular curves, their Jacobians, and moduli spaces

We begin by studying actions of double cosets on modular curves and related objects: their Jacobians and moduli spaces of enhanced elliptic curves.

In what follows, we let Γ_1, Γ_2 be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$

3.1. Modular correspondences on modular curves

First, let us consider the modular curves $X(\Gamma_2), X(\Gamma_1)$.

Proposition 3.17. *There is a well-defined morphism* $[\Gamma_1\alpha\Gamma_2] : \mathrm{Div}(X(\Gamma_2)) \to \mathrm{Div}(X(\Gamma_1))$ *given by*

$$[z] \mapsto \sum_{j=1}^{n} [\beta_j z]$$

where $\beta_j \in \Gamma_1\alpha\Gamma_2$ $(1 \leq j \leq n)$ are as in Equation (3.1).

Proof. As in the proof of Proposition 3.3, we see that the sum above does not depend on the decomposition $\Gamma_1\alpha\Gamma_2 = \sqcup_{j=1}^{n}\Gamma\beta_j$ chosen. On the other hand, if $\gamma_2 \in \Gamma_2$, the sum evaluated at z is equal to the sum evaluated at $\gamma_2 z$ since $\Gamma_1\alpha\Gamma_2 = \sqcup_{j=1}^{n}\Gamma\beta_j\gamma_2$. □

We will call such a map a *modular correspondence.*

Remark 3.18. If $\Gamma = \Gamma_1 = \Gamma_2$ and if Γ, Δ satisfy the hypotheses of Proposition 3.6, then $\mathrm{Div}(X(\Gamma))$ is a $R(\Gamma, \Delta)$-module.

Remark 3.19. We can define the map above in a more natural way as follows: as in Proposition 3.2, let $\Gamma^{(1)} = \Gamma_1 \cap \alpha\Gamma_2\alpha^{-1} \subset \Gamma_1$ and $\Gamma^{(2)} = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 = \alpha^{-1}\Gamma^{(1)}\alpha \subset \Gamma_2$. We then have the commutative diagram

$$\begin{tikzcd}
X(\Gamma^{(1)}) \arrow[r, "\cong"] \arrow[d, "\pi_1"'] & X(\Gamma^{(2)}) \arrow[d, "\pi_2"] \\
X(\Gamma_1) & X(\Gamma_2),
\end{tikzcd} \tag{3.4}$$

and the map $\mathrm{Div}(X(\Gamma_2)) \to \mathrm{Div}(X(\Gamma_2))$ is the composition

$$\begin{tikzcd}
\mathrm{Div}(X(\Gamma_2)) \arrow[r, "\pi_2^*"] & \mathrm{Div}(X(\Gamma^{(2)})) \arrow[r] & \mathrm{Div}(X(\Gamma^{(1)})) \arrow[r, "(\pi_1)_*"] & \mathrm{Div}(X(\Gamma_1)).
\end{tikzcd}$$

Indeed, the map π_2^* is given by

$$[z] \mapsto \sum_{[w]\in\pi_2^{-1}([z])} \mathrm{mult}_{\pi_2}([w])[w] \in \mathrm{Div}(X(\Gamma^{(2)})).$$

Writing $\Gamma_2 = \bigsqcup_j \Gamma^{(2)}\gamma_j$ for $\gamma_j \in \Gamma_2$, we have that $\pi_2^{-1}([z]) = \{[\gamma_j z]\}$ and the sum above becomes $\sum_j [\gamma_j z]$. The image of $[z]$ in $\mathrm{Div}(X(\Gamma_1))$ is thus

$$\sum_j [\alpha\gamma_j z]_{\Gamma_1} = [\Gamma_1\alpha\Gamma_2][z]_{\Gamma_2}$$

since $\Gamma_1\alpha\Gamma_2 = \sqcup_j \Gamma_1\alpha\gamma_j$ by Proposition 3.2.

Hecke operators For any integer d and any integer $n \geq 1$, we obtain operators T_n and $\langle d\rangle$ on $\mathrm{Div}(X(\Gamma_1(N)))$.

3.2. Action on Jacobians of modular curves

Let Γ_1, Γ_2 be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Proposition 3.20. *For any $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, the map $[\Gamma_1\alpha\Gamma_2] : \mathrm{Div}(X(\Gamma_2)) \to \mathrm{Div}(X(\Gamma_1))$ induces a map $\mathrm{Pic}^0(X(\Gamma_2)) \to \mathrm{Pic}^0(X(\Gamma_1))$.*

Proof. The result is clear from the point of view of Remark 3.19, since pushforwards and pullbacks of maps between curves to maps between divisor groups induce maps between the respective Picard groups. □

By the Abel-Jacobi theorem, $\mathrm{Pic}^0(X(\Gamma)) \cong \mathrm{Jac}(X(\Gamma))$ as groups, so for any $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, Proposition 3.20 gives a map $[\Gamma_1\alpha\Gamma_2] : \mathrm{Jac}(X(\Gamma_2)) \to \mathrm{Jac}(X(\Gamma_1))$ such that

$$\begin{tikzcd}
\mathrm{Jac}(X(\Gamma_2)) \arrow[r, "{[\Gamma_1\alpha\Gamma_2]}"] \arrow[d, dash] & \mathrm{Jac}(X(\Gamma_1)) \arrow[d, dash] \\
\mathrm{Pic}^0(X(\Gamma_2)) \arrow[r, "{[\Gamma_1\alpha\Gamma_2]}"] & \mathrm{Pic}^0(X(\Gamma_1))
\end{tikzcd}$$

commutes.

Remark 3.21. Under the same hypotheses as in Remark 3.18, $\mathrm{Pic}^0(X(\Gamma))$ is a $R(\Gamma, \Delta)$-module and $\mathrm{Pic}^0(X(\Gamma)) \cong \mathrm{Jac}(X(\Gamma))$ as $R(\Gamma, \Delta)$-modules, by definition.

Proposition 3.22. *The map* $[\Gamma_1\alpha\Gamma_2] : \mathrm{Jac}(X(\Gamma_2)) \to \mathrm{Jac}(X(\Gamma_1))$ *is given by the composition*

$$\begin{tikzcd}
\mathrm{Jac}(X(\Gamma_2)) \arrow[r, "\pi_1^*"] & \mathrm{Jac}(X(\Gamma^{(2)})) \arrow[r, "\cong"] & \mathrm{Jac}(X(\Gamma^{(1)})) \arrow[r, "(\pi_2)_*"] & \mathrm{Jac}(X(\Gamma_1)),
\end{tikzcd}$$

where $\Gamma^{(i)}, \pi_i$ *are as in Diagram* (3.4)*.*

Proof. Since pushforwards (or traces) and pullbacks on divisor groups commute with the Abel-Jacobi isomorphism, we obtain that the diagram

$$\begin{tikzcd}
\mathrm{Jac}(X(\Gamma_2)) \arrow[r, "\pi_1^*"] \arrow[d, dash] & \mathrm{Jac}(X(\Gamma^{(2)})) \arrow[r, "\cong"] \arrow[d, dash] & \mathrm{Jac}(X(\Gamma^{(1)})) \arrow[r, "(\pi_2)_*"] \arrow[d, dash] & \mathrm{Jac}(X(\Gamma_1)) \arrow[d, dash] \\
\mathrm{Pic}^0(X(\Gamma_2)) \arrow[r, "\pi_1^*"] \arrow[rrr, bend right=10, "{[\Gamma_1\alpha\Gamma_2]}"'] & \mathrm{Pic}^0(X(\Gamma^{(2)})) \arrow[r, "\cong"] & \mathrm{Pic}^0(X(\Gamma^{(1)})) \arrow[r, "(\pi_2)_*"] & \mathrm{Pic}^0(X(\Gamma_1))
\end{tikzcd}$$

commutes (where the vertical maps are the isomorphisms given by the Abel-Jacobi theorem), proving the statement. □

Corollary 3.23. *The map* $[\Gamma_1\alpha\Gamma_2] : \mathrm{Jac}(X(\Gamma_2)) \to \mathrm{Jac}(X(\Gamma_1))$ *is a morphism of complex abelian varieties.*

Proof. By Proposition 3.22, we obtain that the map is a smooth morphism of complex Lie groups, since π_1^* and $(\pi_2)_*$ are linear. By Corollary 1.20, it follows that the map is a morphism of complex abelian varieties. □

3.3. Action on moduli spaces

Recall that there is a bijection between the modular curve $Y_1(N) \subset X_1(N)$ and the moduli space $S_1(N)$ of enhanced elliptic curves for $\Gamma_1(N)$. Moreover, note that the action of double cosets on $\mathrm{Div}(X_1(N))$ restricts to an action on $\mathrm{Div}(Y_1(N))$:

$$\begin{tikzcd}
\mathrm{Div}(S_1(N)) \arrow[r, "T"] \arrow[d, dash, "\cong"'] & \mathrm{Div}(S_1(N)) \arrow[d, dash, "\cong"] \\
\mathrm{Div}(Y_1(N)) \arrow[r, "T"] \arrow[d] & \mathrm{Div}(Y_1(N)) \arrow[d] \\
\mathrm{Div}(X_1(N)) \arrow[r, "T"] & \mathrm{Div}(X_1(N)).
\end{tikzcd} \tag{3.5}$$

The same holds true for $X_0(N)$ and $S_0(N)$ (respectively $X(N)$ and $S(N)$).

Remark 3.24. By Remark 3.18, $\mathrm{Div}(Y_1(N))$ is a $R(\Gamma,\Delta)$-submodule of $\mathrm{Div}(X_1(N))$ and $\mathrm{Div}(S_1(N))$ is a $R(\Gamma,\Delta)$-module isomorphic to $\mathrm{Div}(Y_1(N))$.

In this paragraph, we compute explicit expressions for the operators T_n and $\langle d\rangle$ on the moduli space. We will see that these are particularly simple.

The diamond operators

Proposition 3.25. *The operator* $\langle d\rangle$ *on* $\mathrm{Div}(S_1(N))$ *is given by*

$$[E,Q]\mapsto[E,[d]Q].$$

Proof. Without loss of generality, by Proposition 2.25, let $[E,Q]=[\mathbb{C}/\Lambda_z,[1/N]]\in S_1(N)$. Let $\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma\equiv\left(\begin{smallmatrix}d^{-1}&0\\0&d\end{smallmatrix}\right)\pmod N$. Then, identifying $Y_1(N)$ and $S_1(N)$,

$$\langle d\rangle[E,Q]=\langle d\rangle[z]=[\gamma z]=[\mathbb{C}/\Lambda_{\gamma z},[1/N]].$$

If we let $\lambda=cz+d$, we get that $\lambda\Lambda_{\gamma z}=\Lambda_z$ and an isomorphism $\mathbb{C}/\Lambda_{\gamma z}\to\mathbb{C}/\Lambda_z$ is given by $[z]\mapsto[\lambda z]$, as in the proof of Proposition 2.25. Thus,

$$\langle d\rangle[E,Q]=[\mathbb{C}/\Lambda_z,[\lambda/N]]=[\mathbb{C}/\Lambda_z,[d/N]]=[E,[d]Q]$$

since $c\equiv0\pmod N$. □

Similarly, we find that:

Proposition 3.26. *The operator* $\langle d\rangle$ *on* $\mathrm{Div}(S_0(N))$ *is given by*

$$[E,\langle Q\rangle]\mapsto[E,\langle[d]Q\rangle].$$

The T_p operators

Proposition 3.27. *Let p be a prime such that $p\nmid N$. The operator T_p on* $\mathrm{Div}(S_1(N))$ *is given by*

$$[E,Q]\mapsto\sum_C[E/C,[Q]_C],$$

where C varies over all p-subgroups of E such that $C\cap\langle Q\rangle=0$.

Remark 3.28. The quotient of an elliptic curve by a finite subgroup is made sense of by Proposition 1.56 or [Sil09, III.4.12].

Proof. Let $\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)=\bigsqcup_j\Gamma_1(N)\beta_j$ as in Proposition 3.11 (where $j=0,\dots,p-1,\infty$). By linearity and Proposition 2.25, it is sufficient to check the identity for an element $[E,Q]=[\mathbb{C}/\Lambda_z,[1/N]]\in S_1(N)$, where $z\in\mathbb{H}$. By definition, $T_p[z]=\sum_j[\beta_jz]$, thus

$$T_p[\mathbb{C}/\Lambda_z,[1/N]]=\sum_j[\mathbb{C}/\Lambda_{\beta_jz},[1/N]].$$

- If $0\le j<p-1$, we have $\beta_jz=(z+j)/p$. Note that $\Lambda_z\subset\Lambda_{\beta_jz}$, so that $\mathbb{C}/\Lambda_{\beta_jz}\cong E/(\Lambda_{\beta_jz}/\Lambda_z)$. The quotient $C_j=\Lambda_{\beta_jz}/\Lambda_z$ is a subgroup of $\mathbb{C}/\Lambda$ of order p, such that $C_j\cap\langle[1/N]\rangle=0$.
- If $j=\infty$, we note that $L_\infty=(Nz+1)\Lambda_{\beta_\infty z}$ contains Λ_z, so $\mathbb{C}/\Lambda_{\beta_\infty z}\cong\mathbb{C}/L_\infty\cong E/C_\infty$ with $C_\infty=L_\infty/\Lambda_z$, a subgroup of $\mathbb{C}/\Lambda$ of order p such that $C_\infty\cap\langle[1/N]\rangle=0$

Now, $C_0,\dots,C_{p-1},C_\infty$ are $p+1$ subgroups of order p with trivial intersections, contained in $E[p]=(\mathbb{C}/\Lambda_z)[p]\cong(\mathbb{Z}/p)^2$. Hence their union is $E[p]$ and any subgroup of order p of E is equal to one of the C_j. Thus, we finally get that the sum above corresponds to the sum in the statement. □

4. Action on modular forms

Let Γ_1 and Γ_2 be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ and $k \in \mathbb{Z}$.

The space of meromorphic maps $\mathbb{C}(\mathbb{H})$ on $\mathbb{H}$ has a right-action $[\cdot]_k$ of $\mathrm{GL}_2^+(\mathbb{Q})$ (see Appendix B). By Proposition 3.3, there is a right-action of $A(\Gamma_1, \Gamma_2)$ on $\mathbb{C}(\mathbb{H})^{\Gamma_1} \supset M_k(\Gamma_1)$.

Proposition 3.29. *The right-action of $A(\Gamma_1, \Gamma_2)$ on $\mathbb{C}(\mathbb{H})^{\Gamma_1}$ induces maps $M_k(\Gamma_1) \to M_k(\Gamma_2)$ given by*

$$f \mapsto f\zeta$$

for each $\zeta \in A(\Gamma_1, \Gamma_2)$. Moreover, these maps restrict and corestrict to maps $S_k(\Gamma_1) \to S_k(\Gamma_2)$. Finally, if $\Gamma = \Gamma_1 = \Gamma_2$ and if Γ, Δ satisfy the hypotheses of Proposition 3.6, then the space $M_k(\Gamma)$ is a $R(\Gamma, \Delta)$-module with $S_k(\Gamma)$ as a submodule.

Proof. Explicitly, if $\zeta = \Gamma_1 \alpha \Gamma_2$ for some $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, then

$$f[\Gamma_1 \alpha \Gamma_2]_k = \sum_{j=1}^{n} f[\beta_j]_k,$$

where $\Gamma_1 \alpha \Gamma_2 = \bigsqcup_{j=1}^{n} \Gamma_1 \beta_j$. First of all, let us prove that $f[\Gamma_1 \alpha \Gamma_2]_k$ is weakly modular of weight k with respect to Γ_2. Indeed, if $\gamma_2 \in \Gamma_2$, we have $\Gamma_1 \alpha \Gamma_2 = \sqcup_j \Gamma_1 \beta_j \gamma_2$ and thus

$$f[\Gamma_1 \alpha \Gamma_2]_k [\gamma_2]_k = \sum_{j=1}^{n} f[\beta_j]_k [\gamma_2]_k = \sum_{j=1}^{n} f[\beta_j \gamma_2]_k = f[\Gamma_1 \alpha \Gamma_2]_k.$$

Next, let us show that $f[\Gamma_1 \alpha \Gamma_2]_k$ is holomorphic at the cusps. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then

$$f[\Gamma_1 \alpha \Gamma_2]_k [\gamma]_k = \sum_{j=1}^{n} f[\beta_j \gamma]_k,$$

but since f is holomorphic at the cusps, $f[\beta_j \gamma]_k$ is holomorphic at ∞, so the same holds true for the sum. By the same equation, it is clear that if $f \in M_k(\Gamma_1)$ vanishes at all the cusps, thus so does $f[\Gamma_1 \alpha \Gamma_2]_k \in M_k(\Gamma_2)$. □

Remark 3.30. Suppose that Γ_1, Γ_2 are congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ such that there exists $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ with $\alpha \Gamma_2 \alpha^{-1} \subset \Gamma_1$. Then we prove similarly that $[\alpha]_k : M_k(\Gamma_1) \to M_k(\Gamma_2)$ is well-defined and (co)restricts to give $[\alpha]_k : S_k(\Gamma_1) \to S_k(\Gamma_2)$.

Remark 3.31. Note that for any integer a and any modular form f of weight k, we have $f[\sigma_a] = \langle a \rangle f$.

Remark 3.32. Recall that modular forms for $\mathrm{SL}_2(\mathbb{Z})$ can also be seen as homogeneous functions from the set of lattices to $\mathbb{C}$ (Proposition 2.25). Under this point of view, the Hecke operator T_n on $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ has the very simple expression

$$T_n f(\Lambda) = \sum_{\Lambda'} f(\Lambda')$$

for any lattice $\Lambda \subset \mathbb{C}$, where the (finite) sum is over all sublattices $\Lambda' \subset \Lambda$ of index n. This generalizes to other congruence subgroups. See [Zag08, Section 4.1] or [Lan76, Ch. II] for more details.

4.1. Relationship with the action on Jacobians of modular curves

Let Γ_1, Γ_2 be a congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. In Section 3.3.2, we have defined operators

$$[\Gamma_1 \alpha \Gamma_2] : \mathrm{Jac}(X(\Gamma_2)) \to \mathrm{Jac}(X(\Gamma_1))$$

for all $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. On the other hand, recall that Jacobians of modular curves are related to cusp forms by

$$\mathrm{Jac}(X(\Gamma_i)) \cong S_2(\Gamma_i)^*/\Lambda_i \ (i = 1, 2),$$

where Λ_i corresponds to the subgroup of periods $H_1(X(\Gamma_i))$ (see Paragraph 2.7.6).

We see that the operators on Jacobians are compatible with the operators on modular forms, and they relate through composition.

Proposition 3.33. *For any $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, the map $[\Gamma_1 \alpha \Gamma_2] : S_2(\Gamma_2)^*/\Lambda_2 \to S_2(\Gamma_1)^*/\Lambda_1$ is given by*

$$[\psi] \mapsto [\psi \circ [\Gamma_1 \alpha \Gamma_2]_2].$$

Remark 3.34. Under the same hypotheses as in Remark 3.18, this means that $S_2(\Gamma)^*/\Lambda \cong \mathrm{Jac}(X(\Gamma))$ as $R(\Gamma, \Delta)$-modules.

Before proving this result, we interpret pushforwards and pullbacks of holomorphic forms in the point of view of $S_2(\Gamma)$:

Lemma 3.35. *Let Γ_1, Γ_2 be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ such that there exists $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ with $\alpha \Gamma_1 \alpha^{-1} \subset \Gamma_2$, and consider the morphism $h : X(\Gamma_1) \to X(\Gamma_2)$ given by $[z] \mapsto [\alpha z]$. Then the diagrams*

$$\begin{tikzcd} S_2(\Gamma_1) \arrow[r, "\sum_j [\beta_j]_2"] \arrow[d] & S_2(\Gamma_2) \arrow[d] \\ \Omega^1_{hol}(X(\Gamma_1)) \arrow[r, "h_*"] & \Omega^1_{hol}(X(\Gamma_2)) \end{tikzcd} \qquad \begin{tikzcd} S_2(\Gamma_2) \arrow[r, "{[\alpha]_2}"] \arrow[d] & S_2(\Gamma_1) \arrow[d] \\ \Omega^1_{hol}(X(\Gamma_2)) \arrow[r, "h^*"] & \Omega^1_{hol}(X(\Gamma_1)) \end{tikzcd}$$

commute, where h^* is the pullback, h_* the trace map, and $\beta_j \in \Gamma_2$ are such that $\Gamma_2 = \bigsqcup_j (\alpha \Gamma_1 \alpha^{-1}) \beta_j$.

Proof. For $i = 1, 2$, let $\pi_i : \mathbb{H} \to X(\Gamma_i)$ be the projection.

1. Let $\omega \in \Omega^1_{\mathrm{hol}}(X(\Gamma_1))$ corresponding to $f \in S_2(\Gamma_1)$ (i.e. $\pi_1^*(\omega) = f(z)dz$). Let $z \in \mathbb{H}$ such that $[\alpha z] \in X(\Gamma_2)$ is not a branch point of h. Away from the finite subset of elliptic points and cusps, the preimage $h^{-1}([\alpha z])$ is $[\alpha^{-1}\Gamma_2 \alpha z] = \bigsqcup_j [\beta_j z]$, so we can choose a chart U in $X(\Gamma_2)$ around $[\alpha z]$ such that $h^{-1}(U)$ is the disjoint union of charts V_j in $X(\Gamma_1)$ on which $h_j := h|_{V_j} = \beta_j^{-1}$. On U, $h_*(\omega)$ is then given by $h_*(\omega) = \sum_j (h_j^{-1})^*(\omega|_{V_j})$. Hence, locally,

$$\begin{aligned} \pi_2^*(h_*(\omega)) &= \sum_j (h_j^{-1} \circ \pi_2)^*(\omega|_{V_j}) \\ &= \sum_j (\pi_1 \circ \beta_j)^*(\omega|_{V_j}) = \sum_j (\beta_j)^*(\pi_1^*(\omega|_{V_j})) \\ &= \sum_j (\beta_j)^*(f(z)dz) = \sum_j f[\beta_j]_2(z)dz. \end{aligned}$$

   which shows that $\pi_2^*(h_*(\omega)) = f[\alpha]_2 dz$.

2. Let $f \in S_2(\Gamma_2)$ and $\omega \in \Omega^1_{\mathrm{hol}}(X(\Gamma_2))$ the differential form associated to f (i.e. $\pi_2^*(\omega) = f(z)dz$). Then $\pi_1^* \circ h^* = (h \circ \pi_1)^* = (\pi_2 \circ \alpha)^* = \alpha^* \circ \pi_2^*$. Thus, we get that

$$\pi_1^*(h^*(\omega)) = \alpha^*(\pi_2^*(\omega)) = \alpha^*(f(z)dz) = f[\alpha]_2(z)dz.$$

□

Proof of Proposition 3.33. By Proposition 3.22 and Lemma 3.35, the diagram

$$\begin{tikzcd}
S_2(\Gamma_2)^* \arrow[r, "(\sum_j [\beta_j]_2)^*"] \arrow[d] & S_2(\Gamma^{(2)})^* \arrow[r, "([\alpha]_2)^*"] \arrow[d] & S_2(\Gamma^{(1)})^* \arrow[r, "\iota"] \arrow[d] & S_2(\Gamma_1)^* \arrow[d] \\
\mathrm{Jac}(X(\Gamma_2)) \arrow[r, "\pi_1^*"] \arrow[d] & \mathrm{Jac}(X(\Gamma^{(2)})) \arrow[r, "\cong"] \arrow[d] & \mathrm{Jac}(X(\Gamma^{(1)})) \arrow[r, "(\pi_2)_*"] \arrow[d] & \mathrm{Jac}(X(\Gamma_1)) \arrow[d] \\
\mathrm{Pic}^0(X(\Gamma_2)) \arrow[r, "\pi_1^*"] & \mathrm{Pic}^0(X(\Gamma^{(2)})) \arrow[r, "\cong"] & \mathrm{Pic}^0(X(\Gamma^{(1)})) \arrow[r, "(\pi_2)_*"] & \mathrm{Pic}^0(X(\Gamma_1))
\end{tikzcd}$$

commutes, where the star on the maps on the top row denote dualization and $\Gamma^{(2)}\backslash\Gamma^2 = \sqcup_j \Gamma^{(2)}\beta_j$. But $[\alpha]_2 \circ (\sum_j [\beta_j]_2) = [\Gamma_1\alpha\Gamma_2]_2$ since $\Gamma_1\alpha\Gamma_2 = \sqcup_j \Gamma_1\alpha\beta_j$, whence the claimed equality. □

4.2. Hecke operators explicitly

We now compute explicit expressions for the Hecke operators in the case $\Gamma = \Gamma_1(N)$ and $\Delta = \Delta^1(N)$ as in Example 3.7. By Lemma 3.10, $T_n : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ is explicitly given by

$$T_n f = \sum_a \sum_{b=0}^{n/a-1} f\left[\sigma_a \begin{pmatrix} a & b \\ 0 & n/a \end{pmatrix}\right]_k, \tag{3.6}$$

where the first sum is over the integers $a > 0$ such that $a \mid n$ and $(a, N) = 1$.

Proposition 3.36. *Suppose that $(n, N) = 1$. For $f = \sum_m a_m(f)q^m \in M_k(\Gamma_1(N))$, the Fourier series of $T_n f$ is given by $\sum_m a_m(T_n f)q^m$, where*

$$a_m(T_n f) = \sum_{d \mid (m,n)} d^{k-1} a_{mn/d^2}(\langle d \rangle f).$$

Proof. For $a \geq 1$ an integer, let $g_a = \langle a \rangle f = \sum_{l \geq 0} a_l(g_a)q^l$. According to Equation (3.6), we have

$$\begin{aligned}
T_n f &= \sum_a \sum_{b=0}^{n/a-1} g_a\left(\frac{az+b}{n/a}\right)(n/a)^{-k} n^{k-1} \\
&= \sum_a \sum_{b=0}^{n/a-1} \sum_{l \geq 0} a_l(g_a)(n/a)^{-k} e\left(\frac{az+b}{n/a}\right)^l n^{k-1} \\
&= \sum_a \sum_{l \geq 0} a_l(g_a)(n/a)^{-k} e(a^2z/n)^l n^{k-1} \sum_{b=0}^{n/a-1} e\left(\frac{l}{n/a}\right)^b \\
&= \sum_{l \geq 0} \sum_a \chi_{n/a}(l) a_l(g_a) a^{k-1} q^{la^2/n},
\end{aligned}$$

where $\chi_{n/a} = 1 - \mathbb{1}_{n/a} : \mathbb{Z}/(n/a) \to \mathbb{Z}$ for $\mathbb{1}_{n/a}$ the trivial Dirichlet character modulo n/a. This gives the result by identifying the coefficient of q^m in this expression for $m \geq 0$. □

Remark 3.37. This gives easily that

$$a_l(T_m T_n f) = \sum_{d|(m,n)} d^{k-1} a_l(T_{mn/d^2} f)$$

for all $l, m, n \geq 0$, hence proving Lemmas 3.15 and 3.12 where we see the Hecke operators as operators on modular forms.

5. Modules over the Hecke ring

Let Γ, Δ satisfy the hypotheses of Proposition 3.6, so that we can consider the Hecke ring $R = R(\Gamma, \Delta)$. By the previous sections,

1. $\mathrm{Div}(X(\Gamma))$ is a R-module, with $\mathrm{Div}(Y(\Gamma))$ and $\mathrm{Div}^0(X(\Gamma))$ as submodules.
2. $\mathrm{Pic}^0(X(\Gamma))$ and $\mathrm{Jac}(X(\Gamma))$ are isomorphic R-modules.
3. For all integers k, $M_k(\Gamma)$ is a R-module with $S_k(\Gamma)$ as a submodule.

Moreover, in the particular case $\Gamma = \Gamma_1(N)$, $\Delta = \Delta^1(N)$, we have that

1. $\mathrm{Div}(S_1(N))$ is a R-module, isomorphic to $\mathrm{Div}(Y_1(N))$ (by transfer of structure).
2. $S_2(\Gamma_1(N))^*/\Lambda \cong \mathrm{Jac}(X_1(N))$ as R-modules.

In what follows, let $\Gamma = \Gamma_1(N)$ and $\Delta = \Delta^1(N)$.

5.1. The Hecke algebra

Definition 3.38. The *Hecke algebra* $T_{\mathbb{Z}}$ is the subring $T_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n\rangle : n \geq 0\}]$ of the Hecke ring $R(\Gamma, \Delta)$.

Definition 3.39. The *Hecke algebra* $T_{\mathbb{Z}}$ of level k with respect to Γ is the image of T in $\mathrm{End}(S_k(\Gamma))$. The complex Hecke algebra $T_{\mathbb{C}}$ of level k with respect to Γ is the complex algebra generated by $T_{\mathbb{Z}}$ in $\mathrm{End}(S_k(\Gamma))$.

5.2. Duality between $S_2(\Gamma_1(N))$ and the complex Hecke algebra

By analyzing how Hecke operators act on coefficients of cusp forms, we find the following:

Proposition 3.40. *There is a perfect pairing $T_{\mathbb{C}} \times S_2(\Gamma_1(N)) \to \mathbb{C}$, inducing an isomorphism of $T_{\mathbb{Z}}$-modules $T_{\mathbb{C}} \cong S_2(\Gamma_1(N))^*$.*

Proof. We define $\Phi : T_{\mathbb{C}} \times S_2(\Gamma_1(N)) \to \mathbb{C}$ by $\Phi(T, f) = a_1(Tf)$, which is clearly $\mathbb{C}$-linear in both components. To prove nondegeneracy, we use the fact that for $T \in T_{\mathbb{C}}$ and $f \in S_2(\Gamma_1(N))$, we have by Proposition 3.36 that

$$a_1(T_n f) = a_n(f)$$

for all $n \geq 0$. If $f \in S_2(\Gamma_1(N))$ is such that $\Phi(T, f) = 0$ for all $T \in T_{\mathbb{C}}$, then $a_n(f) = a_1(T_n f) = \Phi(T_n, f) = 0$ for all $n \geq 0$, so $f = 0$. On the other hand, if $T \in T_{\mathbb{C}}$ is such that $\Phi(T, f) = 0$ for all $f \in S_2(\Gamma_1(N))$, we get that $a_n(Tf) = a_1(T_nTf) = a_1(TT_nf) = \Phi(T, T_nf) = 0$ for all f and $n \geq 0$, which implies that T is the zero operator on $S_2(\Gamma_1(N))$. □

6. Hecke operators on cusp forms

In this section, we study Hecke operators on the spaces of cusp forms in more detail. In particular, we see that there exists a canonical basis for cusp forms at any given level and weight, which is made of simultaneous eigenvectors for almost all Hecke operators.

6.1. Normal Hecke operators

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Recall the *Petersson inner product* on the space of cusp forms of weight k with respect to Γ, defined by

$$\begin{aligned} \langle \cdot , \cdot \rangle : S_k(\Gamma) \times S_k(\Gamma) &\to \mathbb{C} \\ (f, g) &\mapsto \frac{1}{\mathrm{Vol}_{d\mu}(X(\Gamma))} \int_{X(\Gamma)} f(z)\overline{g(z)}\,\mathrm{Im}(z)^k d\mu(z), \end{aligned}$$

where $d\mu$ is the measure on $X(\Gamma)$ induced by the $\mathrm{GL}_2^+(\mathbb{R})$-invariant hyperbolic measure $(dx \wedge dy)/y^2$ on $\mathbb{H}$ (see [Miy06, 1.9,2.2] and [DS06, 5.4]). Note that, although f, g are not Γ-invariant, the integral makes sense since $z \mapsto f(z)\overline{g(z)}\,\mathrm{Im}(z)^k$ is.

Hence, $S_k(\Gamma)$ is an inner product space.

Proposition 3.41. *For n coprime to N, the Hecke operators T_n and $\langle n \rangle$ on $S_k(\Gamma_1(N))$ are normal. More precisely, we have $\langle p \rangle^* = \langle p \rangle$ and $T_p^* = \langle p \rangle^{-1} T_p$ for $p \nmid N$.*

Sketch of the proof. The first step is to prove that $[\Gamma\alpha\Gamma]_k^* = [\Gamma \det(\alpha)\alpha^{-1}\Gamma]_k$ for all $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. From there, we can deduce the expressions for $\langle p \rangle^*$ and T_p^*. Since the Hecke algebra is commutative, it follows that $\langle p \rangle$ and T_p are normal. The general result follows by Lemmas 3.12 and 3.15. See [DS06, 5.5] or [Miy06, 4.5] for the details. □

This implies the following very important result:

Theorem 3.42. *There exists a basis of $S_2(\Gamma_1(N))$ constituted of simultaneous eigenvectors of the operators $T_n, \langle n \rangle$ for n coprime to N.*

Proof. Immediately follows from the spectral theorem, since $\{T_n, \langle n \rangle : (n, N) = 1\}$ is a commuting family of normal operators of the finite-dimensional inner-product space $S_2(\Gamma_1(N))$. □

6.2. Oldforms and newforms

The elements of the basis of Theorem 3.42 are a priori only simultaneous eigenvectors for the Hecke operators away from the level N. By distinguishing forms "coming from" the lower level, this restriction can be removed.

Let us fix a level $N \geq 1$. For any $M \mid N$, we have an inclusion $\Gamma_1(N) \subset \Gamma_1(M)$, so an inclusion

$$S_k(\Gamma_1(M)) \subset S_k(\Gamma_1(N)).$$

For any $d \mid N/M$, we also have by Remark 3.30 an injective map $S_k(\Gamma_1(M)) \to S_k(\Gamma_1(Md))$, since $\alpha\Gamma_1(Md)\alpha^{-1} \subset \Gamma_1(M)$ for $\alpha = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$. Thus, we get an injective map

$$\iota_d : S_k(\Gamma_1(M)) \to S_1(\Gamma_1(Md)) \subset S_1(\Gamma_1(N)).$$

To distinguish the forms coming from lower levels, we make the following definition:

Definition 3.43. The *space of oldforms* of $S_k(\Gamma_1(N))$ is

$$S_k(\Gamma_1(N))^{\mathrm{old}} = \sum_{M \mid N} \left(S_k(\Gamma_1(M)) + \sum_{d \mid N/M} \iota_d(S_k(\Gamma_1(M))) \right) \subset S_k(\Gamma_1(N)).$$

Definition 3.44. The *space of newforms* $S_k(\Gamma_1(N))^{\mathrm{new}}$ is the orthogonal complement of $S_k(\Gamma_1(N))^{\mathrm{new}}$ in $S_k(\Gamma_1(N))$ with respect to the Petersson inner product.

6.3. Canonical orthogonal basis of eigenforms

We will now see that the space of newforms has a canonical orthogonal basis with eigenvectors for *all* Hecke operators (and not only those away from the level). From this basis, it will be possible to obtain a basis of $S_k(\Gamma_1(N))$.

Proposition 3.45. *The subspaces $S_k(\Gamma_1(N))^{new}$ and $S_k(\Gamma_1(N))^{old}$ are stable under the Hecke algebra.*

Proof. This is a computation that can be found [DS06, Proposition 5.6.2]. □

Corollary 3.46. *The spaces $S_k(\Gamma_1(N))^{new}$ and $S_k(\Gamma_1(N))^{old}$ both admit a basis of simultaneous eigenvectors for the operators $T_n, \langle n \rangle$ for $(n, N) = 1$.*

Definition 3.47. An eigenvector in $M_k(\Gamma_1(N))$ for *all* the Hecke operators $T_n, \langle n \rangle$ $(n \geq 1)$ on $M_k(\Gamma_1(N))$ will be called a *(Hecke) eigenform.*

Definition 3.48. A *newform* for $S_k(\Gamma_1(N))$ is a normalized (i.e. $a_1(f) = 1$) eigenform in $S_k(\Gamma_1(N))^{\mathrm{new}}$.

Remark 3.49. Note that under this nomenclature, newforms are *not* the elements of the space of newforms, only some particular elements.

The fundamental theorem is now the following:

Theorem 3.50. *The set of newforms for $S_k(\Gamma_1(N))$ is an orthogonal basis of $S_k(\Gamma_1(N))^{new}$, and if $f \in S_k(\Gamma_1(N))^{new}$ is a newform, then*

$$T_n f = a_n(f) f \text{ for all } n \geq 0.$$

More precisely, any eigenvector in $S_2(\Gamma_1(N))^{new}$ for the Hecke operators $T_n, \langle n \rangle$ with $(n, N) = 1$ is a Hecke eigenform.

Proof.

- The main step is the following result of Atkin and Lehner: *if $f \in S_k(\Gamma_1(N))$ is such that $a_n(f) = 0$ for all integers $n \geq 1$ coprime to N, then $f \in S_k(\Gamma_1(N))^{old}$.* For the details, see [DS06, 5.7] or [Miy06, 4.6].
- Let $f \in S_k(\Gamma_1(N))$ be an eigenform for the operators $T_n, \langle n \rangle$ when $(n, N) = 1$. For any such n, let $c_n \in \mathbb{C}$ be such that $T_n(f) = c_n f$. By Proposition 3.36, we have
$$c_n a_1(f) = a_1(c_n f) = a_1(T_n f) = a_n(f)$$
when $(n, N) = 1$. If $f \in S_k(\Gamma_1(N))^{\mathrm{new}}$ is nonzero, this implies that $a_1(f) \neq 0$ by the previous paragraph. By scaling f, we can suppose that $a_1(f) = 1$. For *any* $n \geq 0$, the form $g_n = T_n f - a_n(f) f$ is an element of $S_k(\Gamma_1(N))^{\mathrm{new}}$ and an eigenform for the operators $T_m, \langle m \rangle$ when $(m, N) = 1$. But
$$a_1(g_n) = a_1(T_n f) - a_1(a_n(f) f) = a_n(f) - a_n(f) = 0$$
by Proposition 3.36, so that $g_n \in S_k(\Gamma_1(N))^{\mathrm{old}}$, as above. It follows that $g_n = 0$, i.e. $T_n(f) = a_n(f) f$ for *all* $n \geq 0$.
- By Corollary 3.46, there exists a basis of $S_k(\Gamma_1(N))^{\mathrm{new}}$ composed of simultaneous eigenforms for the operators $T_n, \langle n \rangle$ when $(n, N) = 1$. By the previous paragraph, we can suppose that these elements are normalized, and we then get that they are newforms. Thus, $S_1(\Gamma_1(N))^{\mathrm{new}}$ has a basis of newforms by the previous paragraph.
- Finally, we prove that the set of newforms in $S_1(\Gamma_1(N))^{\mathrm{new}}$ is linearly independent. If there exist $\alpha_i \in \mathbb{C}$ $(1 \leq i \leq n)$ such that
$$\sum_{i=1}^{n} \alpha_i f_i = 0$$
for newforms $f_i \in S_1(\Gamma_1(N))^{\mathrm{new}}$, then
$$\sum_{i=1}^{n} \alpha_i (a_m(f_1) - a_m(f_i)) f_i = 0$$
for any integer $m \geq 0$ by applying the operator $a_m(f_1) - T_m$. If we suppose that $n \geq 2$ is the minimal number of basis elements needed to have a relationship of linear dependence, it gives $a_m(f_i) = a_m(f_1)$ for all integers $m \geq 0$ and $i = 1, \ldots, n$. Hence, $f_1 = \cdots = f_n$, a contradiction. This shows that the set of newforms in $S_1(\Gamma_1(N))^{\mathrm{new}}$ is a basis of that space.

□

6.4. Basis for the space of cusp forms

From this canonical basis, we can now obtain a basis of the full space of cusp forms $S_k(\Gamma_1(N))$. Recall that by definition,

$$\begin{aligned} S_k(\Gamma_1(N)) &= S_k(\Gamma_1(N))^{\mathrm{new}} \oplus S_k(\Gamma_1(N))^{\mathrm{old}} \\ &= S_k(\Gamma_1(N))^{\mathrm{new}} \oplus \sum_{M \mid N} \left(S_k(\Gamma_1(M)) + \sum_{n \mid N/M} \iota_n(S_k(\Gamma_1(M))) \right). \end{aligned}$$

Since $\iota_n(f)(z) = f(nz)$ for any $f \in S_k(\Gamma_1(M))$, $nM \mid N$ and $z \in \mathbb{H}$, we get by Theorem 3.50 that the set

$$B_k(N) = \{ f(nz) : f \in S_k(\Gamma_1(M)) \text{ newform}, nM \mid N \}$$

spans $S_k(\Gamma_1(N))$. Actually, we find that these elements are linearly independent as well:

Theorem 3.51. *The set $B_k(N)$ is a basis of $S_k(\Gamma_1(N))$.*

Proof. See [DS06, 5.8] for a sketch of the proof, using the *Strong multiplicity one Theorem.* □

Remark 3.52. Most of the above results also hold with $\Gamma_1(N)$ replaced by $\Gamma_0(N)$; this is proven in [AL70].

7. *L*-functions

Recall that if $f \in M_k(\Gamma_1(N))$, we defined a L-function associated to f by the series $L(f,s) = \sum_{n\geq 0} \frac{a_n(f)}{n^s}$ (see Appendix B).

Proposition 3.53. *If $f \in M_k(\Gamma_1(N))$ is a normalized eigenform, then we have an Euler product expansion*

$$L(f,s) = \prod_p (1 - a_p(f)p^{-s} + p^{k-1-2s})^{-1}.$$

Proof. By hypothesis, $a_1(f) = 1$. By Lemma 3.12 or Remark 3.37, the arithmetic function $n \mapsto a_n(f)$ is multiplicative, since f is a normalized eigenform. Thus, the theory of Dirichlet series implies that we have an expansion $L(f,s) = \prod_p L_p(f,s)$, where the local factor is

$$L_p(f,s) = \sum_{n\geq 0} a_{p^n}(f)p^{-ns} = (1 - a_p(f)p^{-s} + p^{k-1-2s})^{-1}.$$

The last equality comes from the fact that

$$a_{p^n}(f) = a_p(f)a_{p^{n-1}}(f) - p^{e-1}a_{p^{n-2}}(f)$$

for all $n \geq 1$ by Lemma 3.15 or Remark 3.37. □

Remark 3.54. It is easy to show that the converse also holds true: if the L-function of a modular form $f \in M_k(\Gamma_1(N))$ has an Euler product expansion, then f is a normalized eigenform. See [Miy06, Lemma 4.5.12] or [DS06, 5.9].

Note the similarity with the L-function of an elliptic curve E defined over $\mathbb{Q}$, whose local factor at a prime p of good reduction is $(1 - a_p(E)p^{-s} + p^{1-2s})^{-1}$. This gives an indication of the relationship between elliptic curves and modular forms.

Remark 3.55. Hecke proved that L-functions of cusp forms extend to entire functions satisfying a functional equation. See [Miy06, 4.3.5] or [Shi71, 3.6]. Hence, the Hasse-Weil conjecture for elliptic curves over $\mathbb{Q}$ follows from the modularity theorem.

Chapter 4

Associating abelian varieties to modular forms

For any newform $f \in S_2(\Gamma_1(N))^{\text{new}}$, we will now construct an associated abelian variety that satisfy the conditions enumerated in the introduction.

Note that since $S_2(\Gamma_0(N)) \subset S_2(\Gamma_1(N))$, the construction will actually be done more generally than the setting presented in the introduction.

The main references for this chapter are [DS06, Ch. 6], [Shi71, Ch. 7] and [Kna92, Ch. XI].

In what follows, $T_{\mathbb{Z}}$ denotes the Hecke algebra of weight k with respect to $\Gamma_1(N)$.

1. Number field associated to an eigenform

Let $f \in S_2(\Gamma_1(N))^{\text{new}}$ be a newform. Since f is a simultaneous eigenform for all Hecke operators, we have a homomorphism

$$\lambda_f : T_{\mathbb{Z}} \to \mathbb{C}$$

defined by $Tf = \lambda_f(T)f$ for every $T \in T_{\mathbb{Z}}$. By definition, $\operatorname{im}\lambda_f = \mathbb{Z}[\{a_n(f)\}]$.

Proposition 4.1. *The ring $\mathbb{Z}[\{a_n(f)\}]$ is finitely generated, and $\mathbb{Q}(\{a_n(f)\})$ is a number field of degree equal to the rank of $\mathbb{Z}[\{a_n(f)\}]$.*

Proof. By Section 3.3.2, Hecke operators act on Jacobians of modular curves. In particular, we have a map

$$T_{\mathbb{Z}} \to \operatorname{End}(H_1(X_1(N)).$$

This is actually injective. Indeed, by Section 2.7.6, recall that

$$\operatorname{Jac}(X_1(N)) \cong S_2(\Gamma_1(N))^*/\Lambda$$

for Λ the lattice of periods, and the action on the right-hand side is given by composition with Hecke operators on cusp forms. Since $\Lambda \otimes \mathbb{R} = S_2(\Gamma_1(N))^*$, the action on $S_2(\Gamma_1(N))^*$ is determined by the action on $\Lambda \subset S_2(\Gamma_1(N))^*$, whence the injectivity. Since Λ is a finitely generated $\mathbb{Z}$-module, the same holds then true for $\operatorname{End}(\Lambda)$ and $T_{\mathbb{Z}}$. Thus, $\operatorname{im}\lambda_f$ is finitely generated, as a quotient of a finitely generated $\mathbb{Z}$-module. Finally, $\dim_{\mathbb{Q}} \mathbb{Q}(\{a_n(f)\}) = \dim_{\mathbb{Q}}(\mathbb{Z}[\{a_n(f)\}] \otimes \mathbb{Q}) = \operatorname{rank}\mathbb{Z}[\{a_n(f)\}]$. □

Thus, we can make the following definition:

Definition 4.2. The *number field* of f is the field $K_f = \mathbb{Q}(\{a_n(f)\})$.

Corollary 4.3. *If $f \in S_2(\Gamma_1(N))^{new}$ is a newform, then all Fourier coefficients $a_n(f)$ are algebraic integers.*

Proof. Clear, since $a_n(f)$ lies in the ring of integers of the number field $\mathbb{Q}(\{a_n(f)\})$. □

Finally, we let $I_f = \ker \lambda_f$, so that

$$T_{\mathbb{Z}}/I_f \cong \mathbb{Z}[\{a_n(f)\}].$$

1.1. Action on cusp forms

We see that the set of complex embeddings of the number field of a normalized eigenform in $S_2(\Gamma_1(N))$ acts on the set of such forms.

Definition 4.4. For $f = \sum_n a_n(f)q^n \in S_2(\Gamma_1(N))$ and $\sigma : K_f \to \mathbb{C}$ an embedding, we denote by f_τ the function $\sum_n \sigma(a_n(f))q^n$.

Theorem 4.5. *Let $f \in S_2(\Gamma_1(N))$ be a normalized eigenform. If $\sigma : K_f \to \mathbb{C}$ is an embedding of K_f, then f_σ belongs to $S_2(\Gamma_1(N))$. Moreover, f_σ is a newform if f is a newform.*

Sketch of the proof. Recall that Hecke operators act on the Jacobian $\mathrm{Jac}(X_1(N)) \cong S_2(\Gamma_1(N))^*/\Lambda$ by composition (Proposition 3.33). Let $\varphi_1, \dots, \varphi_r$ be a $\mathbb{Z}$-basis of the lattice of periods $\Lambda \subset S_2(\Gamma_1(N))^*$, and let $V = \mathbb{C}\varphi_1 \oplus \cdots \oplus \mathbb{C}\varphi_r$ so that

$$S_2(\Gamma_1(N))^* = \mathbb{R}\varphi_1 \oplus \cdots \oplus \mathbb{R}\varphi_r \subset V.$$

The action of $T_{\mathbb{Z}}$ on Λ extends to an action of $T_{\mathbb{C}}$ on V, say $\varphi \mapsto \varphi A_T$ with $A_T \in M_r(\mathbb{Z})$, for all Hecke operators $T \in T_{\mathbb{Z}}$.

The technical step is to show that there exists a $T_{\mathbb{Z}}$-module V' such that

$$V = S_2(\Gamma_1(N))^* \oplus V'$$

as $T_{\mathbb{Z}}$-modules and such that the systems of eigenvalues for $T_{\mathbb{Z}}$ on the right-hand side correspond to the systems of eigenvalues for $T_{\mathbb{Z}}$ on $S_2(\Gamma_1(N))$ (see [DS06, Ch. 6.5]).

Note that if $\{a_T : T \in T_{\mathbb{Z}}\} \subset \mathbb{C}$ is a system of eigenvalues for $T_{\mathbb{C}}$ corresponding to an eigenvector $\varphi \in V$, then the same holds true for $\{\sigma(a_T) : T \in T_{\mathbb{Z}}\}$. Indeed,

$$\varphi_\sigma A_T = \sigma(\varphi A_T) = \sigma(a_T \varphi A_T) = \sigma(a_T)\varphi_\sigma A_T.$$

Hence, if $f \in S_1(\Gamma_1(N))$ is a normalized eigenform corresponding to the system of eigenvalues $\lambda_f : T_{\mathbb{Z}} \to \mathbb{C}$, and if $\sigma : K_f \to \mathbb{C}$ is an embedding, the technical step implies that $\sigma \circ \lambda_f$ is the system of eigenvalues of an element in $S_2(\Gamma_1(N))$, the function f_σ. The fact that images of newforms are newforms is proved using the basis of Theorem 3.51. □

Thus, we can define an equivalence relation $\sim$ on newforms in $S_1(\Gamma_1(N))$ by $f \sim g$ if $f = g_\sigma$ for some $\sigma \in \mathrm{Aut}(\mathbb{C})$.

By "averaging", we also find that:

Corollary 4.6. *$S_2(\Gamma_1(N))$ has a basis of forms with integral coefficients.*

Proof. Let $f \in S_2(\Gamma_1(M))$ be a newform for some $M \mid N$. Let $\sigma_1, \dots, \sigma_r : K_f \to \mathbb{C}$ be the complex embeddings of K_f and let $\alpha_1, \dots, \alpha_r$ be a basis of the $\mathbb{Z}$-module $\mathcal{O}_{K_f}$. For $i = 1, \dots, r$, define

$$f_i = \sum_{j=1}^{r} \sigma_j(\alpha_i) f_{\sigma_j}.$$

Then $(f_i)_{\sigma_j} = f_i$ for all i, j, whence f_i has rational Fourier coefficients for all i. Since the latter are algebraic integers by Corollary 4.3, we obtain that f_i has integral Fourier coefficients. Finally, since $(\sigma_j(\alpha_i)) \in M_r(\mathbb{C})$ is invertible, we get that $\operatorname{span}(f_{\sigma_j} : 1 \leq i \leq r) = \operatorname{span}(f_i : 1 \leq i \leq r)$, so that $f \in \operatorname{span}(f_i : 1 \leq i \leq r)$. By Theorem 3.50, it follows that $S_2(\Gamma_1(N))$ is spanned by forms with integral coefficients. □

2. The abelian variety associated to an eigenform

We can now define the abelian variety associated to an eigenform. Recall that the Jacobian $J_1(N) = \operatorname{Jac}(X_1(N))$ is an abelian variety of dimension equal to the genus g of $X_1(N)$. The Hecke algebra $T_\mathbb{Z}$ acts on $J_1(N)$ by morphisms. Thus

$$Q_f = \sum_{\alpha \in I_f} \alpha(J_1(N)) \subset J_1(N)$$

is an abelian subvariety of $J_1(N)$ by Section 1.1.2. Therefore, the quotient

$$A_f := J_1(N)/Q_f$$

is an abelian variety of dimension $g - \dim Q_f$ by Proposition 1.56.

Definition 4.7. We call A_f the *abelian variety associated to the newform* $f \in S_2(\Gamma_1(N))^{\text{new}}$.

Remark 4.8. In [Shi71], the abelian variety considered is in fact the variety B such that $J_1(N)$ is isogenous to $B \times Q_f$, given by Proposition 1.14. The final results are the same since A_f is isogenous to B. Actually, Shimura therefore avoids Poincaré reducibility by using by Wedderburn's theorem on semisimple algebras to decompose $T_\mathbb{Q}$: we have

$$T_\mathbb{Q} \cong R \oplus K_1 \oplus \cdots \oplus K_r,$$

where R is the nilradical and $K_1, \ldots, K_r$ are number fields (since $T_\mathbb{Q}$ is commutative). As above, consider the morphism $\lambda_f : T_\mathbb{Q} \to K_f$, which is surjective. For $i = 1, \ldots, r$, this gives a morphism $\lambda_f : K_i \to K_f$. Since $\lambda_f(T_\mathbb{Q}) = K_f$ and $\lambda_f(R) = 0$, this implies that there exists a unique i such that $\lambda_f(K_i) \neq 0$, and $\lambda_f(K_i) \cong K_f$. Supposing without loss of generality that $i = 1$, this yields $I_f = (R \oplus K_2 \oplus \ldots K_r) \cap T_\mathbb{Z}$.

2.1. The dimension of A_f

We now compute the dimension of A_f by finding a more explicit expression for the complex abelian variety $J_1(N)/Q_f$ as a complex torus.

Let $S_2 = S_2(\Gamma_1(N))$ and $\Lambda \subset S_2^*$ the lattice of periods. Recall that there is:

1. an isomorphism between $\Omega^1_{\text{hol}}(X_1(N))$ and S_2 (Proposition 2.30), which gives an isomorphism of $T_\mathbb{Z}$-modules between S_2^* and $\operatorname{Jac}(X_1(N))$ (Proposition 3.33).
2. a duality between S_2 and $T_\mathbb{C}$ (Proposition 3.40).

Using these two relationships, we transfer A_f from (a quotient of) $\Omega^1_{\text{hol}}(X_1(N))^*$ to (a quotient of) the complex Hecke algebra. Let $\overline{\Lambda}$ be the image of Λ in $S_2^*/I_f S_2^*$.

We have

$$A_f \cong \frac{S_2^*/\Lambda}{I_f(S_2^*/\Lambda)} \cong \frac{S_2^*/\Lambda}{(I_f S_2^* + \Lambda)/\Lambda} \cong \frac{S_2^*}{I_f S_2^* + \Lambda} \cong \frac{S_2^*/I_f S_2^*}{\overline{\Lambda}} \cong \frac{S_2[I_f]^*}{\Lambda_{|S_2[I_f]}}$$

as complex Lie group, where $S_2[I_f]$ denotes the elements of S_2 annihilated by I_f. Using the duality of S_2 and $T_{\mathbb{C}}$, we find that

$$S_2[I_f]^* \cong T_{\mathbb{C}}/I_f T_{\mathbb{C}}.$$

But there is a surjection $(T_{\mathbb{Z}}/I_f) \otimes \mathbb{C} \to T_{\mathbb{C}}/I_f T_{\mathbb{C}}$, so that

$$\dim(S_2[I_f]^*) \leq \dim((T_{\mathbb{Z}}/I_f) \otimes \mathbb{C}) = \operatorname{rank}(T_{\mathbb{Z}}/I_f) = [K_f : \mathbb{Q}].$$

If we let $V_f \subset S_2$ be the $\mathbb{C}$-linear span of $\{f_\sigma : \sigma : K_f \to \mathbb{C} \text{ embedding}\}$, we note that $\dim V_f = [K_f : \mathbb{Q}]$ and $V_f \subset S_2[I_f]$. Thus, $\dim V_f = \dim S_2[I_f]$ and therefore, we have $S_2[I_f]^* = V_f^*$ because the dimensions are equal. Hence,

$$A_f \cong V_f^*/\Lambda_f$$

as complex Lie groups, where $\Lambda_f = \Lambda_{|V_f}$. Note that Λ_f is discrete in V_f^* since Λ is discrete is S_2^*. From the compacity of A_f, we finally obtain that Λ_f is a lattice in V_f^*. Hence, we get:

Proposition 4.9. *The dimension of A_f is equal to $\deg K_f$. More precisely, we have*

$$A_f \cong V_f^*/\Lambda_f,$$

where V_f^* is a complex vector space of dimension $\deg K_f$ and Λ_f is a lattice.

2.2. The action of $\mathbb{Z}[\{a_n(f)\}]$

Note that by definition $T_{\mathbb{Z}}/I_f \cong \mathbb{Z}[\{a_n(f)\}]$ acts on A_f. Moreover, if $a_n(f)$ is an integer, it acts by multiplication. The following will be useful later:

Proposition 4.10. *If $x \in \mathbb{Z}[\{a_n(f)\}]$ is nonzero, the morphism $x : A_f \to A_f$ is surjective.*

Proof. By Corollary 4.3, $a_n(f)$ is an algebraic integer. Let $X^r + \cdots + b_1 X + b_0 \in \mathbb{Z}[X]$ be its minimal polynomial over $\mathbb{Q}$. As an operator, $a_n(f)$ therefore satisfies

$$a_n(f) \circ (a_n(f)^{r-1} + \cdots + b_1) = -b_0.$$

Since multiplication by a nonzero integer is surjective (it is even an isogeny, see Example 1.42), we have that $a_n(f) : A_f \to A_f$ is surjective and the general result follows. □

3. Decomposition of the Jacobian

We know that any complex abelian variety is completely reducible: it is isogenous to a sum of simple abelian subvarieties (Corollary 1.16). Here, we decompose $J_1(N)$ as a sum of varieties A_f associated to newforms in $S_2(\Gamma_1(N))$.

Theorem 4.11. *There is an isogeny*

$$J_1(N) \sim \bigoplus_f A_f^{m_f}$$

where the sum is over a set of representatives of $\cup_{M_f|N} S_2(\Gamma_1(M_f))$ *by the actions of the complex embeddings of* K_f*, and* m_f *is the number of divisors of* N/M_f*.*

Proof. For any integer $n \geq 1$, let $\alpha_n = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$. By Theorem 3.50, a basis of $S_k(\Gamma_1(N))$ is given by

$$\{f[\alpha_n]_2 : f \in S_2(\Gamma_1(M)) \text{ newform}, nM \mid N\}.$$

For all $nM \mid N$ and $f \in S_2(\Gamma_1(M))$, let

$$\Phi_{f,n} : S_2(\Gamma_1(N))^* \to V_f^*$$

be defined by $\Phi_{f,n}(\varphi)(h) = \varphi(h[\alpha_n]_2)$ for any $\varphi \in S_2(\Gamma_1(N))^*$ and $h \in V_f$. We note that $\Phi_{f,n}(\Lambda) \subset \Lambda_f$. Indeed, let $\int_\gamma \in \Omega^1_{\text{hol}}(X_1(N))^*$ be a period corresponding to $\varphi \in \Lambda \subset S_2(\Gamma_1(N))^*$, where γ is a curve in $X_1(N)$. In other words, for $g \in S_1(\Gamma_1(N))$,

$$\varphi(g) = \int_\gamma \omega,$$

where $\omega \in \Omega^1_{\text{hol}}(X_1(N))$ is such that $\pi_N^*(\omega) = g(z)dz$, with $\pi_N : \mathbb{H} \to X_1(N)$ the projection. Then, for $h \in S_2(\Gamma_1(M))$,

$$\Phi_{f,n}(\varphi)(h) = \varphi(h[\alpha_n]_2) = \int_\gamma \omega = \int_{\hat{\gamma}} \pi_N^*(\omega) = \int_{\hat{\gamma}} h[\alpha_n]_2(z)dz = \int_{\gamma_2} h(z)dz,$$

where

- $\omega \in \Omega^1_{\text{hol}}(X_1(N))$ is such that $(\pi_N)^*(\omega) = h[\alpha_n]_2(z)dz$.
- $\hat{\gamma}$ is a curve in $\mathbb{H}$ such that $(\pi_N)_*(\hat{\gamma}) = \gamma$, i.e. any lift of γ in $\mathbb{H}$.
- γ_2 is the curve in $\mathbb{H}$ given by $\gamma_2(t) = n\hat{\gamma}(t)$.

Let us take $\omega' \in \Omega^1_{\text{hol}}(X_1(M))$ such that $h(z)dz = \pi_M^*(\omega')$. Therefore,

$$\Phi_{f,n}(\varphi)(h) = \int_{\gamma_2} (\pi_M)^*(\omega') = \int_{(\pi_M)_*(\gamma_2)} \omega'.$$

The curve γ_2 is *not* closed in $\mathbb{H}$, but $(\pi_M)_*(\gamma_2)$ is. Indeed, let $\delta_N \in \Gamma_1(N))$ be such that $\hat{\gamma}(0) = \delta_N \hat{\gamma}(1)$. Then

$$n\hat{\gamma}(0) = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \hat{\gamma}(0) = \left[\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \delta_N \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}^{-1}\right] n\hat{\gamma}(1),$$

and the product in square brackets belongs to $\Gamma_1(M)$. Hence, we finally obtain that $\Phi_{f,n}(\varphi) \in \Lambda_f$ as claimed.

Moreover, since $\Phi_{f,n}$ is clearly surjective, we get a surjective morphism

$$\Phi : S_2(\Gamma_1(N))^* \xrightarrow{\bigoplus_{f,n} \Phi_{f,n}} \bigoplus_{f,n} V_f^*$$

such that $\Phi(\Lambda) \subset \bigoplus_{f,n} \Lambda_f$. This is actually an isomorphism. Indeed,

$$\dim \bigoplus_{f,n} V_f^* = \sum_f \frac{1}{[K_f : \mathbb{Q}]} \dim S_2(\Gamma_1(N)) \dim V_f^* = \dim S_2(\Gamma_1(N))^*.$$

Consequently, we get an isomorphism

$$\hat{\Phi} : J_1(N) \to \bigoplus_{f,n} V_f^* / \Phi(\Lambda).$$

The natural surjective map

$$\bigoplus_{f,n} V_f^* / \Phi(\Lambda) \to \bigoplus_{f,n} A_f = \bigoplus_{f,n} V_f^* / \Lambda_f$$

has kernel $\bigoplus_{f,n} \Lambda_f / \Phi(\Lambda)$, which is finite since $\bigoplus_{f,n} \Lambda_f$ and $\Phi(\Lambda)$ are two free abelian groups of equal rank. Hence, by composing the two previous maps, we get the desired isogeny $J_1(N) \to \bigoplus_{f,n} A_f$.

□

The action of $a_p(f)$ on A_f (see above) corresponds to the action of T_p on $J_1(N)$ in the following way:

Proposition 4.12. *If $p \nmid N$, there are commutative diagrams*

$$\begin{tikzcd} J_1(N) \arrow[r, "T_p"] \arrow[d] & J_1(N) \arrow[d] \\ \bigoplus_{f,n} A_f \arrow[r, "\prod_{f,n} a_p(f)"] & \bigoplus_{n,f} A_f \end{tikzcd} \qquad \begin{tikzcd} \bigoplus_{f,n} A_f \arrow[r, "\prod_{f,n} a_p(f)"] \arrow[d] & \bigoplus_{n,f} A_f \arrow[d] \\ J_1(N) \arrow[r, "T_p"] & J_1(N), \end{tikzcd} \tag{4.1}$$

where the vertical map in the first diagram is the isogeny of Theorem 4.11, while the vertical map in the second diagram is its dual isogeny.

Proof. 1. The map $J_1(N) \to \oplus_{f,n} A_f \to \oplus_{f,n} A_f$ is given by

$$[\varphi] \mapsto ([\Phi_{f,n}(\varphi) \circ T_p])_{f,n}$$

while the map $J_1(N) \to J_1(N) \to \oplus_{f,n} A_f$ is given by

$$[\varphi] \mapsto ([\Phi_{f,n}(\varphi \circ T_p)])_{f,n}.$$

Let $nM \mid N$ and $f \in S_2(\Gamma_1(M))$. Note that for any $g \in V_f$,

$$\begin{aligned} \Phi_{f,n}(\varphi)(T_p g) &= \varphi((T_p g)[\alpha_n]_2) \\ \Phi_{f,n}(\varphi \circ T_p)(g) &= \varphi(T_p(g[\alpha_n]_2)), \end{aligned}$$

so that it is sufficient to prove that the diagram

$$\begin{tikzcd} S_2(\Gamma_1(M)) \arrow[r, "T_p"] \arrow[d, "{[\alpha_n]_2}"'] & S_2(\Gamma_1(M)) \arrow[d, "{[\alpha_n]_2}"] \\ S_2(\Gamma_1(Mn)) \arrow[d] & S_2(\Gamma_1(Mn)) \arrow[d] \\ S_2(\Gamma_1(N)) \arrow[r, "T_p"] & S_2(\Gamma_1(N)) \end{tikzcd} \tag{4.2}$$

commutes, where the vertical arrows from the second row are the inclusions. First of all, note that the result is obvious for $\langle p\rangle$ instead of T_p. By the formula of Proposition 3.36, we have

$$a_m(T_p f) = a_{mp}(f) + p^{k-1}\chi_m(p)a_{m/p}(\langle p\rangle f)$$

independently from the level, where $\chi_m = 1 - \mathbb{1}_m : \mathbb{Z}/m \to \mathbb{Z}$ for $\mathbb{1}_m$ the trivial Dirichlet character modulo m. Note that $a_m([\alpha_n]_f) = \chi_m(n)a_{m/n}(f)$, thus

$$\begin{aligned}
a_m(T_p(f[\alpha_n]_2)) &= a_{mp}(f[\alpha_n]_2) + p^{k-1}\chi_m(p)a_{m/p}(\langle p\rangle(f[\alpha_n]_2)) \\
&= \chi_{mp}(n)na_{mp/n}(f) + p^{k-1}\chi_m(p)a_{m/p}(\langle p\rangle(f[\alpha_n]_2)) \\
&= \chi_{mp}(n)na_{mp/n}(f) + p^{k-1}\chi_m(p)a_{m/p}((\langle p\rangle f)[\alpha_n]_2) \\
&= \chi_{mp}(n)na_{mp/n}(f) + p^{k-1}\chi_{m/p}(n)\chi_m(p)na_{m/(np)}(\langle p\rangle f)
\end{aligned}$$

$$\begin{aligned}
a_m((T_p f)[\alpha_n]_2) &= \chi_m(n)na_{m/n}(T_p f) \\
&= \chi_m(n)n\left(a_{mp/n}(f) + p^{k-1}\chi_m(np)a_{m/(np)}(\langle p\rangle f)\right),
\end{aligned}$$

where the third equality used the commutativity of Diagram (4.2) for $\langle p\rangle$. Since $p \nmid N$, it follows that $(n,p) = 1$ and that the two expressions above are equal.

2. The diagram

$$\begin{tikzcd}
J_1(N) \arrow[r, "T_p"] \arrow[d] \arrow[dd, dashed, bend right=60] & J_1(N) \arrow[d] \arrow[dd, dashed, bend left=60] \\
\bigoplus_{n,f} A_f \arrow[r, "\prod_{f,n} a_p(f)"] \arrow[d] & \bigoplus_{n,f} A_f \arrow[d] \\
J_1(N) \arrow[r, "T_p"] & J_1(N)
\end{tikzcd}$$

is such that the top square commutes, the vertical arrows are surjective (being isogenies), and the dotted arrows are multiplication by an integer (the degree of the isogenies). Since multiplication by integers commutes with T_p on $J_1(N)$, the outer square commutes. Hence, we get that the bottom square commutes as well.

□

4. Construction for $\Gamma_0(N)$

By Remark 3.52, the theory of newforms and oldforms for $\Gamma_1(N)$ also holds for $\Gamma_0(N)$. Using the same constructions as above, we could also associate an abelian variety to a newform in $\Gamma_0(N)$, and the same results would hold, with a decomposition of $J_0(N)$ as in Theorem 4.11.

If $f \in S_2(\Gamma_0(N))$ is a newform, then f is also a newform in $S_2(\Gamma_1(N))$, and we have two abelian varieties

$$A_f = \mathrm{Jac}(X_1(N))/I_f\,\mathrm{Jac}(X_1(N)) \text{ and } A'_f = \mathrm{Jac}(X_0(N))/I_f\,\mathrm{Jac}(X_0(N))$$

associated to f.

Proposition 4.13. *The complex abelian varieties A_f and A'_f are isogenous.*

Proof. Let again V_f be the linear subspace of $S_2(\Gamma_0(N))$ generated by the set $[f] = \{\sigma_f : \sigma : K_f \to \mathbb{C} \text{ embedding}\}$. Then,

$$A_f \cong V_f^*/\Lambda_f \text{ and } A'_f \cong V_f^*/\Lambda'_f,$$

where $\Lambda'_f = \Lambda' \mid_{V_f}$ for Λ' the lattice of periods of $S_2(\Gamma_0(N))^*$. Consider the natural surjective morphism $\varphi : X_1(N) \to X_0(N)$ and the induced homomorphism $\varphi_* : H_1(X_1(N)) \to H_1(X_0(N))$. Then $\varphi_*(H_1(X_1(N)))$ is a subgroup of $H_1(X_0(N))$ of finite index. Indeed, the map $\varphi_* \circ \varphi^* : \Omega^1(X) \to \Omega^1(X)$ is given by multiplication by $\deg\varphi$, which implies that $(\deg\varphi)H_1(X_0(N)) \subset \varphi_*(H_1(X_1(N)))$. Hence,

$$H_1(X_0(N))/\varphi_*(H_1(X_1(N))) \cong \frac{H_1(X_0(N))/(\deg\varphi)H_1(X_0(N))}{\varphi_*(H_1(X_1(N)))/(\deg\varphi)H_1(X_1(N))},$$

which is a quotient of $(\mathbb{Z}/\deg\varphi)^{2g}$ for g the genus of $X_0(N)$. It follows that Λ_f is a subgroup of Λ'_f of finite index as well, so that the natural map $A_f \to A'_f$ is an isogeny. □

CHAPTER 5

Definition over $\mathbb{Q}$

A priori, the abelian varieties we associated to cusp forms in $S_2(\Gamma_1(N))$ in Chapter 4 are defined over $\mathbb{C}$. However, in this chapter we will see that the modular curves $X_1(N)$ and $X_0(N)$ (as algebraic curves), their Jacobians (as abelian varieties) and the Hecke operators (as morphisms of abelian varieties) can be defined over $\mathbb{Q}$, showing that abelian varieties associated to newforms can actually be defined over $\mathbb{Q}$ as well. In some sense, Corollary 4.6 gives an indication of that.

Since the abelian varieties obtained from $\mathrm{Jac}(X_1(N))$ are isomorphic to the abelian varieties obtained from $\mathrm{Jac}(X_0(N))$ (see Proposition 4.13), we will mainly focus on $X_1(N)$.

This chapter is based on [DS06, Ch. 7] and its exercises, which are a particular/explicit case of the work of Shimura on canonical models for modular curves in [Shi71] (see Remark 5.2 below). Additional and more advanced details can be found in [DI95, III.8].

Some parts of this chapter may seem a bit technical, but the underlying ideas are very interesting: we relate functions on modular curves to coordinates of points of an elliptic curve over $\mathbb{Q}(j)$ (as algebraic functions), to make use of the arithmetic of elliptic curves, in particular the Weil pairing.

1. The modular curve is defined over $\mathbb{Q}$

For Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, recall that $X(\Gamma)_{\mathrm{alg}}$ is the unique complex projective curve that is isomorphic to $X(\Gamma)$ as compact Riemann surfaces. The goal of this section is to prove the following:

Theorem 5.1. *The curve $X_1(N)_{alg}$ can be defined over $\mathbb{Q}$, that is, there exists an algebraic curve $X_1(N)_{\mathbb{Q}}$ defined over $\mathbb{Q}$ such that $X_1(N)_{\mathbb{Q}} \cong X_1(N)_{alg}$ as complex algebraic curves. The same result holds true for $X_0(N)$.*

Remark 5.2. In [Shi71, 6.6-6.7], Shimura gives compatible models over number fields for modular curves with respect to congruence subgroups. In Chapter 6, we will see other models, in relation to moduli spaces of elliptic curves.

Remark 5.3. We will only prove Theorem 5.1 for $X_1(N)$, but the method for $X_0(N)$ is exactly the same and would follow easily. Moreover, the proof will also show that $X(N)$ can be defined over $\mathbb{Q}(\mu_N)$, where $\mu_N \in \mathbb{C}$ is a primitive Nth root of unity.

To prove this result, we use the correspondence between function fields and curves (see [Har77, I.6] and [Ful08, Ch. 7] for a more explicit point of view) and Galois theory on the function fields.

1.1. Function fields of modular curves

The first step is to determine the function fields of the modular curves $X(N)_{\text{alg}}$ and $X_1(N)_{\text{alg}}$. Recall that these are equal to the function fields of the corresponding compact Riemann surfaces. By composition with the surjections $X(N) \to X_1(N)$ and $X_1(N) \to X(1)$, we have inclusions

$$\mathbb{C}(X(1)) \subset \mathbb{C}(X_1(N)) \subset \mathbb{C}(X(N)).$$

Proposition 5.4. *We have $\mathbb{C}(X(1)) = \mathbb{C}(j)$.*

Proof. Note that $\mathbb{C}(X(1))$ is the space of meromorphic modular form of weight 0 with respect to $\mathrm{SL}_2(\mathbb{Z})$. Hence, $\mathbb{C}(j) \subset \mathbb{C}(X(1))$. On the other hand, if $f \in \mathbb{C}(X(1))$ is meromorphic, let $z_1, \ldots, z_n$ be its zeros and poles in $Y(1)$. Then the meromorphic function $g \in \mathbb{C}(X(1))$ defined by $g(z) = \prod_{i=1}^{n}(j(z) - j(z_i))^{\mathrm{ord}_{z_i}(f)}$ is such that f/g has no zeros or poles except possibly at $[\infty]$. Since the degree of the divisor of a meromorphic function on a compact Riemann surface is zero, it follows that f/g is constant, whence $f \in \mathbb{C}(j)$. □

Lemma 5.5. *For any $v = (v_1, v_2) \in \mathbb{Z}^2 - 0$, the function $f^v : X(\Gamma(N)) \to \mathbb{C}$ of Paragraph 2.6.2, defined by*

$$f^v(z) = \frac{g_2(z)}{g_3(z)} \wp_z \left(\frac{v_1 z + v_2}{N} \right)$$

belongs to $\mathbb{C}(X(N))$. Moreover, $f^v = f^w$ if and only if $v \equiv \pm w \pmod N$ and $f^v(\gamma z) = f^{\gamma v}(z)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, $z \in \mathbb{H}$.

Proof. First of all, we note that if $v = (v_1, v_2) \in \mathbb{Z}^2 - 0, \gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$, then

$$f^v(\gamma z) \quad = \quad (cz+d)^2 \frac{g_2(z)}{g_3(z)} \wp_{\gamma z} \left(\frac{1}{cz+d} \frac{(av_1 + bv_2)z + (cv_1 + dv_2)}{N} \right) = f^{\gamma v}(z),$$

using that $\Lambda_{\gamma z} = (cz+d)^{-1} \Lambda_z$ and $\wp_{\lambda z}(\lambda z) = \lambda^{-2} \wp_z(z)$ for all $\lambda \in \mathbb{C}^*$. The assertion $f^v = f^w$ if and only if $v \equiv \pm w \mod N$ follows from the fact that $(\wp_z, \wp_z')$ gives an isomorphism from $\mathbb{C}/\Lambda_z$ to an elliptic curve. It remains to check that f^v is meromorphic on $\mathbb{H}$ and at the cusps. The first assertion is clear. For the second, it suffices to show that f^v is meromorphic at ∞ for all $v = (v_1, v_2) \in \mathbb{Z}^2 - 0$ by the above transformation law. By invoking uniform convergence to permute sums and limits, we see that $\lim_{\mathrm{Im}(z) \to \infty} \wp_z((v_1 z + v_2)/N)$ exists and is finite, leading to the assertion. □

Proposition 5.6. *The field extension $\mathbb{C}(X(N))/\mathbb{C}(1)$ is Galois with Galois group $\mathrm{SL}_2(\mathbb{Z}/N)/\pm$. Moreover, we have*

$$\mathbb{C}(X(N)) = \mathbb{C}(j, \{f^v : v \in \mathbb{Z}^2 - 0\}) \text{ and } \mathbb{C}(X_1(N)) = \mathbb{C}(j, f_1),$$

where $f_1 = f^{(0,1)^t}$.

Proof.

- By Proposition 5.4 and Lemma 5.5, we have the inclusions

  $$\mathbb{C}(j) \subset \mathbb{C}(j, \{f^v : v \in \mathbb{Z}^2 - 0\}) \subset \mathbb{C}(X(N)).$$

  Let us consider the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{C}(X(N))$ given by composition: $\gamma f = f \circ \gamma$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This is well-defined, since if $\gamma_N \in \Gamma(N)$, then $\gamma_N \gamma \equiv \gamma\gamma_N \pmod{\Gamma(N)}$, so that $f([\gamma\gamma_N z]) = f([\gamma_N \gamma z]) = f([\gamma z])$ for all $z \in \mathbb{H}$. For $v \in \mathbb{Z}^2 - 0$, Lemma 5.5 says that the action of $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ on f^v is given by

  $$\gamma f^v = f^{\gamma v}.$$

  If we let $\Phi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}(X(N)))$ be the associated homomorphism, we note that $\pm\Gamma(N) \subset \ker\Phi$ by Lemma 5.5. Conversely, if $\gamma \in \ker\Phi$, we get $f^{v\gamma} = f^v$ for all $v \in \mathbb{Z}^2 - 0$, so $v\gamma \equiv \pm v \pmod N$; this implies that $\gamma \in \pm\Gamma(N)$. Hence, $\ker\Phi = \pm\Gamma(N)$ and we have an isomorphism

  $$\mathrm{SL}_2(\mathbb{Z})/\pm\Gamma(N) \cong \Phi(\mathrm{SL}_2(\mathbb{Z})) \subset \mathrm{Aut}(\mathbb{C}(X(N))).$$

  By Galois theory, $\mathbb{C}(X(N))/\mathbb{C}(X(N))^{\Phi(\mathrm{SL}_2(\mathbb{Z}))}$ is a Galois extension with Galois group $\mathrm{SL}_2(\mathbb{Z})/\pm\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N)/\pm$. An element $f \in \mathbb{C}(X(N))$ belongs to $\mathbb{C}(X(N))^{\Phi(\mathrm{SL}_2(\mathbb{Z}))}$ if and only if it is $\mathrm{SL}_2(\mathbb{Z})$-invariant, i.e. $f \in \mathbb{C}(X(1))$.

- As we have just seen, $\mathrm{Gal}(X(N)/\mathbb{C}(j, \{f^v : v \in \mathbb{Z}^2 - 0\}))$ is the trivial subgroup in $\mathrm{SL}_2(\mathbb{Z}/N)/\pm$, so $\mathbb{C}(j, \{f^v : v \in \mathbb{Z}^2 - 0\}) = \mathbb{C}(X(N))$.

- Note that $f_1 \in \mathbb{C}(X_1(N))$, so that $\mathbb{C}(j, f_1) \subset \mathbb{C}(X_1(N))$. Indeed, if $\gamma \in \Gamma_1(N)$, we have $f_1(\gamma z) = f^{\gamma(0,1)^t}(z) = f_1(z)$ for all $z \in \mathbb{H}$.

  Then, we note that $\mathrm{Gal}(\mathbb{C}(X(N))/\mathbb{C}(j, f_1)) = \pm\Gamma_1(N)/\pm\Gamma(N)$. Indeed, if γ belongs to this Galois group, we have $f_1 = \gamma f_1 = f^{\gamma(0,1)^t}$, so $\gamma \in \pm\Gamma_1(N)/\pm\Gamma(N)$ and conversely. By definition, $\mathbb{C}(X(N))^{\pm\Gamma_1(N)/\pm\Gamma(N)} = \mathbb{C}(X_1(N))$, thus $\mathbb{C}(X_1(N)) = \mathbb{C}(j, f_1)$ as claimed.

□

Remark 5.7. We can very similarly determine the function field of $\mathbb{C}(X_0(N))$, see [DS06, 7.5.1].

Corollary 5.8. *For all $v \in \mathbb{Z}^2 - 0$, we have $f^v \in \overline{\mathbb{C}(j)}$.*

1.2. Outline of the proof of Theorem 5.1

By the previous paragraph, we have

$$\begin{array}{ccccc} \mathbb{C}(X(1)) & \subset & \mathbb{C}(X_1(N)) & \subset & \mathbb{C}(X(N)) \\ \| & & \| & & \| \\ \mathbb{C}(j)) & \subset & \mathbb{C}(j, f_1) & \subset & \mathbb{C}(j, \{f^v : v \in \mathbb{Z}^2 - 0\}). \end{array}$$

Let us write $\mathbb{Q}(j, f_1) = \mathbb{Q}(j)[X]/(p_1)$ for $p_1 \in \mathbb{Q}(j)[X]$ the minimal polynomial of f_1 over $\mathbb{Q}(j)$. Suppose that we can prove the two following points:

Lemma 5.9. *$\mathbb{Q}(j, f_1)$ is a function field over $\mathbb{Q}$.*

Lemma 5.10. *The minimal polynomial of f_1 over $\mathbb{C}(j)$ is still p_1.*

Then, by Lemma 5.9, there would exist a curve C defined over $\mathbb{Q}$ such that

$$\mathbb{Q}(C) \cong \mathbb{Q}(j, f_1) \cong \mathbb{Q}(j)[X]/(p_1).$$

Over the complex numbers, we get that

$$\mathbb{C}(C) \cong \mathbb{C}(j)[X]/(p_1) \cong \mathbb{C}(j, f_1)$$

by Lemma 5.10, which gives Theorem 5.1.

1.3. The function field of $X(N)$ and the universal elliptic curve

To prove the two Lemmas above, we begin with a more natural way to see f_1 that is related to elliptic curves. This occurs naturally, as modular curves correspond to moduli spaces of elliptic curves.

Recall that for any $z \in \mathbb{H}$, we have an isomorphism $(\wp_z, \wp_z') : \mathbb{C}/\Lambda_z \to E$, where E is a complex elliptic curve of j-invariant $j(z)$. If $j(z) \neq 0, 1728$, composing with the change of variable $(x, y) \mapsto (u^2 x, u^3 y)$ for $u = (g_2(z)/g_3(z))^{1/2}$ gives the elliptic curve

$$E_{j(z)} : y^2 = 4x^3 - \left(\frac{27j(z)}{j(z) - 1728}\right) x - \left(\frac{27j(z)}{j(z) - 1728}\right),$$

isomorphic to E. Thus, any elliptic curve over $\mathbb{C}$ with j-invariant $j(z) \neq 0, 1728$ is isomorphic to $E_{j(z)}$.

Lemma 5.11. *For any $z \in \mathbb{H}$ such that $j(z) \neq 0, 1728$, we have*

$$x(E_{j(z)}[N]) = \{f^v(z) : v \in \mathbb{Z}^2 - 0\},$$

where $x(E_{j(z)}[N]) \subset \mathbb{C}$ denotes the set of first coordinates of affine points of $E_{j(z)}[N]$.

Proof. For any $z \in \mathbb{H}$, we have seen above that $E_{j(z)} \cong \mathbb{C}/\Lambda_z$ as abelian varieties. In particular,

$$E_{j(z)}[N] \cong (\mathbb{C}/\Lambda_z)[N] = \langle [1/N]_{\Lambda_z}, [z/N]_{\Lambda_z} \rangle.$$

By computing the image of $v_1[1/N]_{\Lambda_z} + v_2[z/N]_{\Lambda_z} \in (\mathbb{C}/\Lambda_z)[N]$ by the above isomorphism for $v = (v_1, v_2) \in \mathbb{Z}^2 - 0$, we directly find that the first coordinate of the corresponding point in $E_{j(z)}[N]$ is

$$\frac{g_2(z)}{g_3(z)} \wp_z \left(\frac{v_1 z + v_2}{N}\right) = f^v(z).$$

□

Extension to algebraic functions By considering j as a variable, we can furthermore consider the *universal elliptic curve*

$$E_j : y^2 = 4x^3 - \left(\frac{27j}{j - 1728}\right) x - \left(\frac{27j}{j - 1728}\right)$$

defined over $\mathbb{Q}(j)$. Lemma 5.11 then extends as follows:

Proposition 5.12. *Considering f^v as an element of $\overline{\mathbb{C}(j)}$ for all $v \in \mathbb{Z}^2 - 0$, we have*

$$x(E_j[N]) = \{f^v : v \in \mathbb{Z}^2 - 0\},$$

where $x(E_j[N]) \subset \overline{\mathbb{C}(j)}$ denotes the set of first coordinates of affine points of $E_j[N]$.

Before giving the proof, we review a few facts from the theory of algebraic functions (see [vdW03, XIII.92]). For an algebraically closed field k, let us consider the function field $k(X)$ and its algebraic closure $\overline{k(X)}$. An *algebraic function* f, i.e. $f \in \overline{k(X)}$, can be seen as a partial multi-valued function on $\overline{k}$. Indeed, let $\varphi \in k(X)[Y]$ be the minimal polynomial of f over $k(X)$, and let $\varphi_1, \dots, \varphi_n$ be the denominators of its coefficients, where we suppose without loss of generality that all coefficients are reduced fractions. For each $x \in k - V(\varphi_1, \dots, \varphi_n)$, we can consider the polynomial $\varphi_x \in \overline{k}[Y]$ given by the evaluation of the coefficients of φ at $X = x$, and we call such an x an *admissible argument.* The *values* of f at x are then

$$f(x) := V(\varphi_x) = \{y \in k : \varphi_x(y) = 0\}.$$

The following result generalizes the fact that a polynomial in $k[X]$ vanishes if and only if it is zero as a function on k.

Lemma 5.13. *Let $f \in \overline{k(X)}$ and $F \in k[X, Y]$. Then $F(X, f) = 0 \in \overline{k(X)}$ if and only if $F(x, y) = 0 \in k$ for any admissible argument $x \in k$ and $y \in f(x)$.*

Proof. See the two theorems of [vdW03, XIII.92]. □

Proof of Proposition 5.12. Let $v \in \mathbb{Z}^2 - 0$ and let $\varphi \in \mathbb{C}(j)[X]$ be the minimal polynomial of $f^v \in \overline{\mathbb{C}(j)}$. Since $\varphi(f^v) = 0$, Lemma 5.13 gives that $\varphi_{j(z)}(f^v(z)) = 0$ for almost all $z \in \mathbb{H}$. Moreover, Proposition 5.6 shows that the values for f^v at z are $f^w(z)$ for $w \in \mathbb{Z}^2 - 0$. By [Sil09, Ex. III.3.7], there is a polynomial $\psi_N \in \mathbb{Z}[j, X]$ such that for $x \in \overline{\mathbb{C}(j)}$, we have

$$f \in x(E_j[N]) \subset \overline{\mathbb{C}(j)} \text{ if and only if } \psi_N(j, f) = 0.$$

If $z \in \mathbb{H}$ is such that $j(z) \neq 0, 1728$, then E_j specializes to the curve $E_{j(z)}$ and also

$$x \in x(E_{j(z)}[N]) \subset \mathbb{C} \text{ if and only if } \psi_N(j(z), x) = 0.$$

Thus, by Lemma 5.11, we have $\psi_N(j(z), f^v(z)) = 0$ for all $z \in \mathbb{H}$ such that $j(z) \neq 0, 1728$ and for all $v \in \mathbb{Z}^2 - 0$, which implies that $\psi_N(j, f^v) = 0$ by the Lemma. Hence, $f^v \in x(E_j[N])$ and

$$\{f^v : v \in \mathbb{Z}^2 - 0\} \subset x(E_j[N]) - \{0\}.$$

By Lemma 5.5, the left-hand side set has size

$$|((\mathbb{Z}/N)^2 - 0)/\pm| = |(\mathbb{Z}/N)^2/\pm| - 1 = \begin{cases} N^2/2 + 1 & \text{if } N \text{ is even} \\ (N^2 + 1)/2 - 1 & \text{if } N \text{ is odd.} \end{cases}$$

On the other hand $|E_j[N]| = N^2$, and an element in $x(E_j[N]) - 0$ corresponds to two points in $E_j[N]$ except in the case that it corresponds to one of the points

$(x_i, 0) \in E$ $(i = 1, 2, 3)$. Since $[N](x_i, 0) = 0$ if N is even and $[N](x_i, 0) = (x_i, 0)$ otherwise, we find that

$$|x(E_j[N])| = \begin{cases} N^2/2 + 2 & \text{if } N \text{ is even} \\ (N^2+1)/2 & \text{if } N \text{ is odd,} \end{cases}$$

whence the result. □

Corollary 5.14. *We have* $\mathbb{C}(X(N)) = \mathbb{C}(j, x(E_j[N]))$.

Proposition 5.15. *The field extension* $\mathbb{C}(j, \pi(E_j[N]))/\mathbb{C}(j)$ *is Galois and there is a commutative diagram*

$$\begin{tikzcd}
\operatorname{Gal}(\mathbb{C}(j, \pi(E_j[N]))/\mathbb{C}(j)) \arrow[r, "\Phi", "\cong"'] \arrow[d] & \mathrm{SL}_2(\mathbb{Z}/N) \arrow[d] \\
\operatorname{Gal}(\mathbb{C}(j, x(E_j[N]))/\mathbb{C}(j)) \arrow[r, "\cong"] & \mathrm{SL}_2(\mathbb{Z}/N)/\pm,
\end{tikzcd}$$

where the bottom isomorphism is the one defined in Proposition 5.6.

Proof. The field $\mathbb{C}(j, \pi(E_j[N]))$ is obtained from $\mathbb{C}(j, x(E_j[N]))$ by adjoining a square root for each element of $x(E_j[N])$. Since $E_j[N] \subset \overline{\mathbb{C}(j)}$ is finite, the extension $\mathbb{C}(j, \pi(E_j[N]))$ is finite over $\mathbb{C}(j)$ as well. Moreover, it is then also normal: if $\sigma : \mathbb{C}(j, \pi(E_j[N])) \to \overline{\mathbb{C}(j)}$ is a $\mathbb{C}(j)$-embedding, then the restriction of σ on $\mathbb{C}(j, x(E_j[N]))$ has its image in $\mathbb{C}(j, x(E_j[N]))$. Since σ permutes $x(E_j[N])$, it permutes the square roots adjoined so that σ is an automorphism of $\mathbb{C}(j, \pi(E_j[N]))$.

Let $G = \operatorname{Gal}(\mathbb{C}(j, \pi(E_j[N]))/\mathbb{C}(j))$. By taking a $\mathbb{Z}$-basis (P, Q) for $E_j[N] \cong (\mathbb{Z}/N)^2$, we obtain a faithful representation $\Phi : G \to \mathrm{GL}_2(\mathbb{Z}/N)$. We will now show that $\operatorname{im}\Phi = \mathrm{SL}_2(\mathbb{Z}/N)$.

- On one hand, for any $\sigma \in G$, the Weil pairing e_N satisfies (see [Sil09, III.8])

  $$e_N(P, Q) = \sigma(e_N(P, Q)) = e_N(\sigma(P), \sigma(Q)) = e_N(P, Q)^{\det \Phi(\sigma)}, \tag{5.1}$$

  where the first equality comes from the fact that σ fixes $\mathbb{C}$, which contains all roots of unity. Since $e_N(P, Q)$ is a primitive Nth root of unity, we can conclude that $\det \Phi(\sigma) \equiv 1 \pmod{N}$, so that $\operatorname{im}\Phi \subset \mathrm{SL}_2(\mathbb{Z}/N)$.

- On the other hand, if we let $J = \operatorname{Gal}(\mathbb{C}(j, \pi(E_j[N]))/\mathbb{C}(j, x(E_j[N])))$, we get that $G/J \cong \mathrm{SL}_2(\mathbb{Z}/N)/\pm$, thus

  $$|G| = |J| \frac{|\mathrm{SL}_2(\mathbb{Z}/N)|}{2}.$$

  The following diagram summarizes the setting:

  $$\begin{tikzcd}
  \mathbb{C}(j, \pi(E_j[N])) \arrow[d, dash, "J"'] \arrow[dd, dash, bend left=60, "G"] \\
  \mathbb{C}(j, x(E_j[N])) \arrow[d, dash, "\mathrm{SL}_2(\mathbb{Z}/N)/\pm"'] \\
  \mathbb{C}(j).
  \end{tikzcd}$$

  It is then sufficient to show that that $|J| = 2$. Remark that $\Phi(J) \subset \{\pm I\}$: if $\sigma \in J$, then σP (resp. σQ) has the same x-coordinate as P (resp. Q), so that $\sigma P = \pm P$ and $\sigma Q = \pm Q$; since $\Phi(\sigma) \in \mathrm{SL}_2(\mathbb{Z}/N)$, we must have $\sigma \in \{\pm I\}$. Conversely, note that $\Phi^{-1}(\{\pm I\}) \subset J$. Indeed, if $\sigma \in G$ is such that $\Phi(\sigma) = -I$, we have $\sigma(R) = -R$ for all $R \in E_j[N]$, whence $\sigma \in J$.

Suppose that $|J| = 1$, or equivalently $-I \notin \Phi(G)$ by the above. Then $|\pm \operatorname{im}\Phi| = 2|G| = |\mathrm{SL}_2(\mathbb{Z}/N)|$, which implies that $\pm \operatorname{im}\Phi = \mathrm{SL}_2(\mathbb{Z}/N)$. Hence, $-I = \left[\pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\right]^2 \in \operatorname{im}\Phi$, a contradiction.

Thus, $\operatorname{im}\Phi = \mathrm{SL}_2(\mathbb{Z}/N)$. Since a $\mathbb{Z}$-basis of $E_j[N]$ is given by $f^{(1,0)^t}, f^{(0,1)^t}$, the diagram of the statement is commutative. □

1.4. Function fields over $\mathbb{Q}$

By the above, we get the field extensions

$$\mathbb{C}(j) \subset \mathbb{C}(j, f_1) \subset \mathbb{C}(j, x(E_j[N])) \subset \mathbb{C}(j, \pi(E_j[N])) \subset \overline{\mathbb{C}(j)},$$

where $\pi(E_j[N]) \subset \overline{\mathbb{Q}(j)}$ denotes in this context the set of first and second coordinates of the affine points of $E_j[N]$. Moreover, we can also consider E_j as a curve defined over $\mathbb{Q}(j)$ and get the field extensions

$$\mathbb{Q}(j) \subset \mathbb{Q}(j, f_1) \subset \mathbb{Q}(j, x(E_j[N])) \subset \mathbb{Q}(j, \pi(E_j[N])) \subset \overline{\mathbb{Q}(j)}.$$

Note that to prove Lemma 5.9, it suffices to prove that

$$\mathbb{Q}(j, f_1) \cap \overline{\mathbb{Q}} = \mathbb{Q},$$

since $\mathbb{Q}(j, f_1)$ has transcendence degree 1 over $\mathbb{Q}$.

Proposition 5.16.

a) *The field extension $\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j)$ is Galois.*

b) *All Nth roots of unity are contained in $\mathbb{Q}(j, \pi(E_j[N]))$.*

c) *We have $\mathbb{Q}(j, \mu_N) = \mathbb{C}(j) \cap \mathbb{Q}(j, \pi(E_j[N]))$.*

d) *The diagram*

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{C}(j, \pi(E_j[N]))/\mathbb{C}(j)) \arrow[r, "\Phi", "\cong"'] \arrow[d, "\cong"] & \mathrm{SL}_2(\mathbb{Z}/N) \arrow[dd] \\
\mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j, \mu_N)) \arrow[ur] \arrow[d] & \\
\mathrm{Gal}(\mathbb{Q}(j, x(E_j[N]))/\mathbb{Q}(j)) \arrow[r, "\cong"] & \mathrm{GL}_2(\mathbb{Z}/N)
\end{tikzcd}$$

commutes.

Proof.

a) This is proved as in Proposition 5.15.

b) We prove that all Nth roots of unity are contained in $\mathbb{Q}(j, \pi(E_j[N]))$ so that, even if we restricted from $\mathbb{C}$ to $\mathbb{Q}$, we will still be able to use the ideas of Proposition 5.15. As before, let

$$G = \mathrm{Gal}(\mathbb{Q}(\mu_N, j, \pi(E_j[N]))/\mathbb{Q}(j))$$

where $\mu_N \in \overline{\mathbb{Q}}$ is a primitive Nth root of unity, and consider the representation

$$\rho : G \to \mathrm{GL}_2(\mathbb{Z}/N)$$

obtained as above by acting on a basis of $E_j[N] \cong (\mathbb{Z}/N)^2$. By Equation (5.1) (except the first equality), we have

$$\sigma(\mu_N) = \mu_N^{\det \rho(\sigma)}$$

for any $\sigma \in G$. Consider the intermediate field $\mathbb{Q}(j, \pi(E_j[N]))$. If $\sigma \in G$ fixes $\pi(E_j[N])$ pointwise, then $\rho(\sigma) = \pm I$, which implies that $\sigma(\mu_N) = \mu_N$. Thus, $\mu_N \in \mathbb{Q}(j, \pi(E_j[N]))$ and $G = \mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j))$.

c)-d) Consider now the following tower of extensions:

$$\begin{tikzcd}
& \mathbb{C}(j, \pi(E_j[N])) \arrow[dl, dash, "\mathrm{SL}_2(\mathbb{Z}/N)"'] \arrow[dr, dash] & \\
\mathbb{C}(j) \arrow[dr, dash] & & \mathbb{Q}(j, \pi(E_j[N])) \arrow[dl, dash] \arrow[ddl, dashed, dash, "H"'] \arrow[dddl, dashed, dash, "G"] \\
& \mathbb{C}(j) \cap \mathbb{Q}(j, \pi(E_j[N])) \arrow[d, dash] & \\
& \mathbb{Q}(j, \mu_N) \arrow[d, dash, "(\mathbb{Z}/N)^\times"'] & \\
& \mathbb{Q}(j) &
\end{tikzcd}$$

Let $H = \mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j, \mu_N)) \subset G$. Arguing as in the complex case, we get a faithful representation $\Phi : H \to \mathrm{SL}_2(\mathbb{Z}/N)$. But

$$\begin{aligned}
\mathrm{SL}_2(\mathbb{Z}/N) &\cong \mathrm{Gal}(\mathbb{C}(j, \pi(E_j[N]))/\mathbb{C}(j)) \qquad (5.2)\\
&\cong \mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{C}(j) \cap \mathbb{Q}(j, \pi(E_j[N]))) \subset H.
\end{aligned}$$

On the other hand, H injects into $\Phi(H) \subset \mathrm{SL}_2(\mathbb{Z}/N)$, so $H \cong \mathrm{SL}_2(\mathbb{Z}/N)$ since these are finite groups of the same size. Moreover, since $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) = (\mathbb{Z}/N)^\times$, we get $G/H \cong (\mathbb{Z}/N)^\times$. To conclude, note that $\rho : G \to \mathrm{GL}_2(\mathbb{Z}/N)$ is faithful. Since $\mathrm{GL}_2(\mathbb{Z}/N)/\mathrm{SL}_2(\mathbb{Z}/N) \cong (\mathbb{Z}/N)^\times$, the groups G and $\mathrm{GL}_2(\mathbb{Z}/N)$ have the same cardinality, so the representation is an isomorphism.

□

1.5. Proof of Lemma 5.9

Lemma 5.17. *We have* $\mathbb{Q}(j, \pi(E_j[N])) \cap \overline{\mathbb{Q}} = \mathbb{Q}(\mu_N)$.

Proof. This follows directly from Proposition 5.16(c), intersecting $\mathbb{Q}(j, \mu_N) = \mathbb{C}(j) \cap \mathbb{Q}(j, \pi(E_j[N]))$ with $\overline{\mathbb{Q}}$. □

Proposition 5.18. *Let*

$$\rho : \mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j)) \to \mathrm{GL}_2(\mathbb{Z}/N)$$

be the isomorphism of Proposition 5.16. Then an intermediate field K of $\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j)$ is a function field over $\mathbb{Q}$ if and only if

$$\det \rho : \mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/K) \to (\mathbb{Z}/N)^\times$$

surjects.

Proof. Since K has transcendence degree 1 over $\mathbb{Q}$, it is a function field if and only if $K \cap \overline{\mathbb{Q}} = \mathbb{Q}$. By Lemma 5.17, this rewrites as $K \cap \mathbb{Q}(\mu_N) = \mathbb{Q}$. Consider the following tower of extensions:

$$\begin{tikzcd}
 & \mathbb{Q}(j, \pi(E_j[N])) \arrow[dl, dash, "G"'] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{Q}(\mu_N) \arrow[dl, dash] \arrow[ddl, dash, bend left, "(\mathbb{Z}/N)^\times"] \\
 & K \cap \mathbb{Q}(\mu_N) \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Let $G = \mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/K)$. By Proposition 5.16, $\det \rho : G \to (\mathbb{Z}/N)^\times$ describes the action of G on $\mathbb{Q}(\mu_N)$ through the surjective morphism $G \to \mathrm{Gal}(\mathbb{Q}(\mu_N)/K \cap \mathbb{Q}(\mu_N)) \hookrightarrow (\mathbb{Z}/N)^\times$. Then $\det \rho : G \to (\mathbb{Z}/N)^\times$ surjects if and only if $\mathrm{Gal}(\mathbb{Q}(\mu_N)/K \cap \mathbb{Q}(\mu_N)) \cong (\mathbb{Z}/N)^\times$, which is equivalent to $K \cap \mathbb{Q}(\mu_N) = \mathbb{Q}$. □

Proof of Lemma 5.9. According to Proposition 5.18, it suffices to determine the image of $G = \mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j, f_1))$ by ρ. By Proposition 5.16, $\sigma \in G$ acts on f^v as $\sigma f^v = f^{\sigma v}$, so we find that

$$\rho(G) = \{\pm \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in (\mathbb{Z}/N)^\times, b \in \mathbb{Z}/N\}.$$

Thus, the surjectivity of $\det \rho : G \to (\mathbb{Z}/N)^\times$ is clear. □

1.6. Proof of Lemma 5.10

Proof of Lemma 5.10. Let $p_\mathbb{C}$ (resp. $p_\mathbb{Q}$) be the minimal polynomial of $f_1 \in \mathbb{Q}(j)[X]$ over $\mathbb{C}(i)$ (resp. $\mathbb{Q}(i)$). Certainly, $p_\mathbb{C}$ divides $p_\mathbb{Q}$ and the two polynomials are monic, so it suffices to prove that their degree are equal to obtain that they are equal. The degree of $p_\mathbb{C}$ is equal to

$$|\mathrm{Gal}(\mathbb{C}(j, f_1)/\mathbb{C}(j))| = \frac{|\mathrm{Gal}(\mathbb{C}(j, \pi(E_j[N]))/\mathbb{C}(j))|}{|\mathrm{Gal}(\mathbb{C}(j, \pi(E_j[N]))/\mathbb{C}(j, f_1))|} = \frac{|\mathrm{SL}_2(\mathbb{Z}/N)|}{|\pm \Gamma_1(N)/\Gamma(N)|}.$$

On the other hand,

$$\deg(p_\mathbb{Q}) = \frac{|\mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j))|}{|\mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j, f_1))|} = \frac{|\mathrm{GL}_2(\mathbb{Z}/N)|}{|\pm \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N)\}|}.$$

$$\begin{tikzcd}
 & \mathbb{C}(j,\pi(E_j[N])) \arrow[d, dash, "\pm\Gamma_1(N)/\Gamma(N)"] & \mathbb{Q}(j,\pi(E_j[N])) \arrow[d, dash, "\pm\left\{\left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right)\right\}"] & \\
\mathrm{SL}_2(\mathbb{Z}/N) & \mathbb{C}(j,f_1)\cong\mathbb{C}(j)[X]/(p_{\mathbb{C}}) \arrow[d, dash] & \mathbb{Q}(j,f_1)\cong\mathbb{Q}(j)[X]/(p_{\mathbb{Q}}) \arrow[d, dash] & \mathrm{GL}_2(\mathbb{Z}/N) \\
 & \mathbb{C}(j) & \mathbb{Q}(j) &
\end{tikzcd}$$

Now, note that:

- $|\pm\Gamma_1(N)/\Gamma(N)| = |\pm\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z}/N)\}| = 2N$ if $N>2$, and N if $N=1,2$.
- $|\pm\{\left(\begin{smallmatrix} a & b \\ 0 & 1\end{smallmatrix}\right)\in\mathrm{GL}_2(\mathbb{Z}/N)\}| = 2\varphi(N)N$ if $N>2$ and $\varphi(N)N$ if $N=1,2$.
- $|\mathrm{GL}_2(\mathbb{Z}/N)| = \varphi(N)|\mathrm{SL}_2(\mathbb{Z}/N)|$.

Thus, we can conclude that the degrees agree as needed. □

1.7. Planar models

Recall from Section 2.4 that we have a planar model for $X_1(N)_{\mathrm{alg}}$ given by

$$X_1(N)^{\mathrm{planar}} = \{(j,x)\in\overline{\mathbb{C}}^2 : \hat{p}_1(j,x)=0\}$$

for $\hat{p}_1$ the minimal polynomial of f_1 over $\mathbb{C}(j)$, with a birational map $(j,f_1) : X_1(N)_{\mathrm{alg}}\to X_1(N)^{\mathrm{planar}}$. By Theorem 5.1 and its proof, we have $\hat{p}_1\in\mathbb{Q}(j)[X]$ and we obtain a corresponding planar model

$$X_1(N)^{\mathrm{planar}}_{\mathbb{Q}} = \{(j,x)\in\overline{\mathbb{Q}}^2 : \hat{p}_1(j,x)=0\}$$

of $X_1(N)_{\mathbb{Q}}$ with the birational map $(j,f_1) : X_1(N)_{\mathbb{Q}}\to X_1(N)^{\mathrm{planar}}_{\mathbb{Q}}$.

1.8. Example

Let us illustrate the content of the previous section with the case $N=1$. We have $X_1(1)=X(1)=\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$. The j-invariant $j:\mathbb{H}\to\mathbb{C}$ gives an isomorphism $X(1)\cong\mathbb{P}^1(\mathbb{C})$. Then, by the results above:

- The algebraic modular curve $X(1)_{\mathrm{alg}}$ is $\mathbb{P}^1(\mathbb{C})$ as an algebraic curve.
- The function field of $X(1)$ is $\mathbb{C}(j)$.
- The rational algebraic modular curve is $X(1)_{\mathbb{Q}}=\mathbb{P}^1(\overline{\mathbb{Q}})$ with function field $\mathbb{Q}(j)$.

We will complete this example later.

2. The Jacobians are defined over $\mathbb{Q}$

Lemma 5.19. *For all $N\geq 1$, we have $X_1(N)_{\mathbb{Q}}(\mathbb{Q})\neq\varnothing$.*

Proof. First, note that the planar model shows that the cusp 0 belongs to $X_1(N)_{\mathbb{Q}}(\overline{\mathbb{Q}})$. We prove by induction on N that it belongs to $X_1(N)_{\mathbb{Q}}(\mathbb{Q})$. If $N=1$, the assertion is clear by Section 5.1.8. Let us suppose that the assertions holds for some N and let p be a prime. From Section 2.3, we can compute that the projection $\pi : X_1(Np) \to X_1(N)$ has degree p or $p+1$, which is equal to the degree of the algebraic map $\pi : X_1(Np)_{\mathbb{Q}} \to X_1(N)_{\mathbb{Q}}$, which is defined over $\mathbb{Q}$. If $P \in X_1(Np)_{\mathbb{Q}}$ is the point corresponding to the cusp 0, then Section 2.3 also shows that π has ramification degree p at P. Let us consider the pullback $\pi^* : \mathrm{Div}(X_1(N)) \to \mathrm{Div}(X_1(Np))$. We have $\pi^*(\pi(P)) = p(P)$ or $p(P) + (Q)$ for some $Q \in X_1(N)_{\mathrm{alg}}$, $Q \neq P$. By hypothesis

$$\sigma(\pi^*(\pi(P))) = \pi^*(\pi(\sigma(P))) = \pi^*(\pi(P))$$

which implies that $\sigma(P) = P$, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Hence, $P \in X_1(N)_{\mathbb{Q}}(\mathbb{Q})$. □

Theorem 5.20. *The Jacobian variety* $\mathrm{Jac}(X_1(N))$ *can be defined over* $\mathbb{Q}$*: there exists an abelian variety* $\mathrm{Jac}(X_1(N))_{\mathbb{Q}}$ *defined over* $\mathbb{Q}$ *such that* $\mathrm{Jac}(X_1(N))_{\mathbb{Q}} \cong \mathrm{Jac}(X_1(N))$ *as complex abelian varieties. The same result holds true for* $\mathrm{Jac}(X_0(N))$.

Proof. By Proposition 1.73 and Lemma 5.19, we have

$$\mathrm{Jac}(X_1(N)) \cong \mathrm{Jac}(X_1(N)_{\mathrm{alg}}) \cong \mathrm{Jac}(X_1(N)_{\mathbb{Q}})$$

as complex abelian varieties. By the work of Weil and Chow (Theorem 1.70), $\mathrm{Jac}(X_1(N)_{\mathbb{Q}})$ is an abelian variety defined over $\mathbb{Q}$. □

By construction, we have the following containments:

$$\begin{tikzcd}
\mathrm{Jac}(X_1(N)_{\mathbb{Q}}) \arrow[r, phantom, "\subset"] \arrow[d, dash, "\cong"] & \mathrm{Jac}(X_1(N)) \arrow[d, dash, "\cong"] \\
\mathrm{Pic}^0(X_1(N)_{\mathbb{Q}}) \arrow[r, phantom, "\subset"] & \mathrm{Pic}^0(X_1(N)) \\
\mathrm{Div}^0(X_1(N)_{\mathbb{Q}}) \arrow[r, phantom, "\subset"] \arrow[u] & \mathrm{Div}^0(X_1(N)). \arrow[u]
\end{tikzcd} \tag{5.3}$$

3. The Hecke operators are defined over $\mathbb{Q}$

Recall that the Hecke algebra $T_{\mathbb{Z}}$ acts on $\mathrm{Div}(X_1(N))$, so that it also acts on $\mathrm{Div}(X_1(N)_{\mathrm{alg}})$.

Proposition 5.21. *For* $\alpha \in T_{\mathbb{Z}}$*, the homomorphism*

$$\alpha : \mathrm{Div}(X_1(N)_{alg}) \to \mathrm{Div}(X_1(N)_{alg})$$

(co)restricts to a homomorphism on $\mathrm{Div}(X_1(N)_{\mathbb{Q}})$.

Proof.

- For $\langle d \rangle$, note that the map $\mathrm{Div}(X_1(N)_{\mathrm{alg}}) \to \mathrm{Div}(X_1(N)_{\mathrm{alg}})$ is induced by the morphism $\langle d \rangle : X_1(N)_{\mathrm{alg}} \to X_1(N)_{\mathrm{alg}}$. Since the j-invariant is $\mathrm{SL}_2(\mathbb{Z})$-invariant, the corresponding morphism of function fields is

$$\begin{array}{ccc} \mathbb{C}(j, f_1) & \to & \mathbb{C}(j, f_1) \\ j \mapsto j & & f_1 \mapsto f^{(0,d)^t}. \end{array}$$

  To obtain the result, it suffices to prove that $f^{(0,d)^t} \in \mathbb{Q}(j, f_1)$. We proved that $\mathrm{Gal}(\mathbb{Q}(j, \pi(E_j[N]))/\mathbb{Q}(j, f_1))$ corresponds to the subgroup

$$H = \{\pm \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in (\mathbb{Z}/N)^\times, b \in \mathbb{Z}/N\}$$

in $\mathrm{Gal}(\mathbb{Q}(j,\pi(E_j[N]))/\mathbb{Q}(j,f_1)) \cong \mathrm{GL}_2(\mathbb{Z}/N)$. Since $\gamma f^{(0,d)^t} = f^{\gamma(0,d)^t} = f^{(0,d)^t}$ for any $\gamma \in H$, it follows that $f^{(0,d)^t} \in \mathbb{Q}(j,f_1)$ as wanted.

- For T_p, the proof is a bit harder since the map on divisors groups is not directly induced by a morphism on $X_1(N)$, as above. However, we can show that there exists a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ such that T_p is given by a composition

$$\mathrm{Div}(X_1(N)) \xrightarrow{(\varphi_1)_*} \mathrm{Div}(X(\Gamma)) \xrightarrow{\varphi_2^*} \mathrm{Div}(X_1(N)),$$

where $\varphi_1 : X_1(N) \to X(\Gamma)$ and $\varphi_2 : X(\Gamma) \to X_1(N)$ are morphism (see [DI95, 8.3] or [DS06, Ex. 7.9.3] for the details). As above, it is relatively easy to show that $X(\Gamma)$ and φ_1, φ_2 can be defined over $\mathbb{Q}$, giving the result. The result for T_n ($n \geq 1$ an integer) is deduced as in the proof of Proposition 3.41.

□

Corollary 5.22. *For $\alpha \in T_{\mathbb{Z}}$, the morphism*

$$\alpha : \mathrm{Jac}(X_1(N)) \to \mathrm{Jac}(X_1(N))$$

(co)restricts to a morphism $\alpha : \mathrm{Jac}(X_1(N))_{\mathbb{Q}} \to \mathrm{Jac}(X_1(N))_{\mathbb{Q}}$ defined over $\mathbb{Q}$.

Proof. By Proposition 5.21 and Diagram (5.3), the diagram

$$\begin{tikzcd}
\mathrm{Jac}(X_1(N)) \arrow[r, "\alpha"] \arrow[d, dash, "\cong"] & \mathrm{Jac}(X_1(N)) \arrow[d, dash, "\cong"] \\
\mathrm{Pic}^0(X_1(N)) \arrow[r] & \mathrm{Pic}^0(X_1(N)) \\
\mathrm{Pic}^0(X_1(N)_{\mathbb{Q}}) \arrow[r] \arrow[u] \arrow[d, dash] & \mathrm{Pic}^0(X_1(N)_{\mathbb{Q}}) \arrow[u] \arrow[d, dash] \\
\mathrm{Jac}(X_1(N))_{\mathbb{Q}} \arrow[r, "\alpha"] & \mathrm{Jac}(X_1(N))_{\mathbb{Q}}
\end{tikzcd}$$

commutes, giving the result. □

4. The abelian variety associated to a newform is defined over $\mathbb{Q}$

We can finally prove the following:

Theorem 5.23. *Let $f \in S_2(\Gamma_1(N))^{new}$ be a newform. Then, the abelian variety A_f associated to f can be defined over $\mathbb{Q}$, i.e. there exists an abelian variety $(A_f)_{\mathbb{Q}}$ defined over $\mathbb{Q}$ such that $(A_f)_{\mathbb{Q}} \cong A_f$ as complex abelian varieties.*

Proof. Recall that

$$A_f = \mathrm{Jac}(X_1(N))/I_f\,\mathrm{Jac}(X_1(N)),$$

for I_f an ideal in $T_{\mathbb{Z}}$. But:

- $\mathrm{Jac}(X_1(N))$ can be defined over $\mathbb{Q}$ by Theorem 5.20.
- By Corollary 5.22, $(Q_f)_{\mathbb{Q}} = I_f\,\mathrm{Jac}(X_1(N))_{\mathbb{Q}}$ is a subvariety of $\mathrm{Jac}(X_1(N))_{\mathbb{Q}}$, defined over $\mathbb{Q}$. Moreover, $(Q_f)_{\mathbb{Q}} \cong I_f\,\mathrm{Jac}(X_1(N))$ as complex abelian varieties.

Hence, the quotient $(A_f)_{\mathbb{Q}} = \mathrm{Jac}(X_1(N))_{\mathbb{Q}}/(Q_f)_{\mathbb{Q}}$ is an abelian variety defined over $\mathbb{Q}$ (see Remark 1.58). From the universal property of the quotient (Proposition 1.56), we have $A_f \cong (A_f)_{\mathbb{Q}}$ as complex abelian varieties.

□

5. Moduli spaces algebraically

Let us now consider $S_1(N)_{\mathbb{Q}}$, the "rational" moduli space, i.e. the moduli space of enhanced elliptic curves *defined over* $\overline{\mathbb{Q}}$, defined as in Definition 2.24. Note that we can see $S_1(N)_{\mathbb{Q}}$ as a subset of $S_1(N)$: if E, E' are two elliptic curves defined over $\overline{\mathbb{Q}}$, then $E \cong E'$ over $\mathbb{C}$ if and only if $j(E) = j(E')$, which holds if and only if $E \cong E'$ over $\overline{\mathbb{Q}}$, since $j(E), j(E') \in \overline{\mathbb{Q}}$.

Example 5.24. In the example from Section 5.1.8, we considered the curve $X_1(1) = X(1)$. Note that $S_1(1) \cong \mathbb{C}$ and $S_1(1)_{\mathbb{Q}} \cong j^{-1}(\overline{\mathbb{Q}})$.

5.1. Hecke operators

Proposition 5.25. *The operator* T_p *on* $\mathrm{Div}(S_1(N))$ *induces an operator*

$$T_p : \mathrm{Div}(S_1(N)_{\mathbb{Q}}) \to \mathrm{Div}(S_1(N)_{\mathbb{Q}}).$$

Proof. By Proposition 3.27, T_p on $\mathrm{Div}(S_1(N))$ is given by

$$T_p[E, Q] = \sum_C [E/C, [Q]_C],$$

where the sum is over all subgroups $C \subset E$ of order p such that $C \cap \langle Q \rangle = 0$. Suppose that E is defined over $\mathbb{Q}$ and $Q \in E(\overline{\mathbb{Q}})$. Since $E[p] \cong (\mathbb{Z}/p)^2 \cong E(\mathbb{C})[p]$, it follows that the set of subgroups of order p of $E(\mathbb{C})$ is equal to the set of subgroups of order p of E. By [Sil09, III.4.12] (or Remark 1.58), we have that $[E/C, [Q]_C] \in S_1(N)_{\mathbb{Q}}$ for all subgroups C of order p in E. □

5.2. The map $S_1(N) \to X_1(N)$ algebraically and over $\mathbb{Q}$

Recall that $S_1(N)$ identifies with $Y_1(N) \subset X_1(N) \cong X_1(N)_{\mathrm{alg}}$. First, we give a more explicit form for the map $S_1(N) \to X_1(N)_{\mathrm{alg}}$ using the planar model of the modular curve:

Lemma 5.26. *The composition* $S_1(N) \to X_1(N)_{alg} \to X_1(N)^{planar}$ *is defined on* $S_1(N)' = \{[E, Q] \in S_1(N) : j(E) \neq 0, 1728\}$ *and is given by*

$$[E, Q] \mapsto (j(E), x(Q)),$$

where $x(Q) \in \mathbb{C}$ *is the first coordinate of* $Q \in E(\mathbb{C})$.

Proof. The rational map of the statement is given by

$$[\mathbb{C}/\Lambda_z, [1/N]] \mapsto [z] \mapsto (j(z), f_1(z)).$$

If $j(z) \neq 0, 1728$, we have that $\mathbb{C}/\Lambda_z \cong E_{j(z)}$ and $f_1(z)$ is the first coordinate of $[1/N] \in \mathbb{C}/\Lambda_z$. □

Example 5.27. Continuing Example 5.24, we get that the map $S_1(1) \to X_1(1)_{\mathrm{alg}}$ is given by $[E] \mapsto j(E)$.

The map $S_1(N) \to X_1(N)_{\mathrm{alg}}$ restricts to a map $S_1(N)_{\mathbb{Q}} \to X_1(N)_{\mathrm{alg}}$. We note that the image has rational points, allowing us to obtain a version of Diagram (3.5) over $\mathbb{Q}$:

Proposition 5.28. *The map $S_1(N)_{\mathbb{Q}} \to X_1(N)_{alg}$ corestricts to a map $S_1(N)_{\mathbb{Q}} \to X_1(N)_{\mathbb{Q}}$, and gives a commutative diagram for any prime p*

$$\begin{tikzcd}
\mathrm{Div}(S_1(N)_{\mathbb{Q}}) \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}(S_1(N)_{\mathbb{Q}}) \arrow[d] \\
\mathrm{Div}(X_1(N)_{\mathbb{Q}}) \arrow[r, "T_p"] & \mathrm{Div}(X_1(N)_{\mathbb{Q}}),
\end{tikzcd}$$

which induces a commutative diagram

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)_{\mathbb{Q}}) \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}^0(S_1(N)_{\mathbb{Q}}) \arrow[d] \\
\mathrm{Pic}^0(X_1(N)_{\mathbb{Q}}) \arrow[r, "T_p"] & \mathrm{Pic}^0(X_1(N)_{\mathbb{Q}}).
\end{tikzcd} \tag{5.4}$$

Lemma 5.29. *Let $f : X \to Y$ be a surjective morphism of curves defined over $\mathbb{Q}$ inducing a morphism $f_{\mathbb{C}} : X_{\mathbb{C}} \to Y_{\mathbb{C}}$ of complex curves. Then $f_{\mathbb{C}}^{-1}(Y_{\mathbb{C}}(\overline{\mathbb{Q}})) \subset X_{\mathbb{C}}(\overline{\mathbb{Q}})$.*

Proof. Let $y \in Y_{\mathbb{C}}(\overline{\mathbb{Q}})$ and $x \in f_{\mathbb{C}}^{-1}(y)$. If $\sigma \in \mathrm{Aut}_{\overline{\mathbb{Q}}}(\mathbb{C})$, we see that

$$y = \sigma(y) = \sigma(f_{\mathbb{C}}(x)) = f_{\mathbb{C}}(\sigma(x)),$$

and thus $\sigma(x) \in f_{\mathbb{C}}^{-1}(y)$, which implies that x has finitely many conjugates with respect to $\mathrm{Aut}_{\overline{\mathbb{Q}}}(\mathbb{C})$. Thus, there exists a polynomial $\varphi \in \mathbb{C}^{\mathrm{Aut}_{\overline{\mathbb{Q}}}(\mathbb{C})}[X]$ such that $\varphi(x) = 0$. The extension $\mathbb{C}/\overline{\mathbb{Q}}$ is transcendental, but transcendental Galois theory still gives $\mathbb{C}^{\mathrm{Aut}_{\overline{\mathbb{Q}}}(\mathbb{C})} = \overline{\mathbb{Q}}$ (see [Mil14, Theorem 9.29]). Hence, x is algebraic over $\overline{\mathbb{Q}}$, so that $x \in X_{\mathbb{C}}(\overline{\mathbb{Q}})$ as stated. □

Proof of Proposition 5.28. The surjective morphism

$$X_1(N) \to X_1(1)$$

induces morphisms $X_1(N)_{\mathrm{alg}} \to X_1(1)_{\mathrm{alg}}$ and $X_1(N)_{\mathbb{Q}}(\mathbb{C}) \to X_1(1)_{\mathbb{Q}}$ which are compatible with the isomorphisms $X_1(\cdot)_{\mathbb{Q}} \cong X_1(\cdot)_{\mathrm{alg}}$ of complex curves. Consider the commutative diagram

$$\begin{tikzcd}
S_1(N)_{\mathrm{alg}} \arrow[r] \arrow[d] & S_1(1)_{\mathrm{alg}} \arrow[d] \\
X_1(N)_{\mathrm{alg}} \arrow[r] & X_1(1)_{\mathrm{alg}}.
\end{tikzcd}$$

According to Example 5.27, the composition $S_1(N)_{\mathrm{alg}} \to S_1(1)_{\mathrm{alg}} \to X_1(1)_{\mathrm{alg}}$ is given by $[E, Q] \mapsto j(E)$. If E is an elliptic curve over $\overline{\mathbb{Q}}$, we have that $j(E) \in \overline{\mathbb{Q}}$, whence the image of $[E, Q]_{\mathbb{Q}}$ lies in $X_1(1)_{\mathbb{Q}} = \mathbb{P}^1(\overline{\mathbb{Q}})$. By Lemma 5.29 applied to the morphism $X_1(N)_{\mathrm{alg}} \to X_1(1)_{\mathrm{alg}}$, it follows that the image of $S_1(N)_{\mathbb{Q}}$ through the map $S_1(N)_{\mathrm{alg}} \to X_1(N)_{\mathrm{alg}}$ lies in $X_1(N)_{\mathbb{Q}}$ as wanted. □

Chapter 6

Reductions and the Eichler-Shimura relation

Let us fix an integer $N \geq 1$. In what follows, we will denote by $X_i(N)$ the modular curve associated to $\Gamma_i(N)$, seen as an algebraic curve defined over $\mathbb{Q}$ (i.e. $X_i(N)_{\mathbb{Q}}$), for $i = 0, 1$. The goal of this section will be to study the following result, relating the reduction of the Hecke operator T_p on $\mathrm{Pic}^0(X_0(N))$ to the Frobenius morphism:

Theorem (Igusa, Eichler-Shimura)**.** *For every prime $p \nmid N$, the modular curve $X_0(N)$ has good reduction modulo p and we have the* Eichler-Shimura relation*, the commutative diagram*

$$\begin{tikzcd}
\mathrm{Div}^0(X_0(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}^0(X_0(N)) \arrow[d] \\
\mathrm{Pic}^0(X_0(N)_p) \arrow[r, "(\sigma_p)_*+(\sigma_p)^*"] & \mathrm{Pic}^0(X_0(N)_p).
\end{tikzcd}$$

This will be the key to proving the relationship between a newform and its associated abelian variety through their L-functions.

The heart of the proof is a result of Igusa (in the classical setting), Katz-Mazur and Deligne-Rapoport, which asserts the existence of a solution to a moduli problem generalizing the moduli space $S_i(N)$. As a consequence of this, the modular curve $Y_i(N)$ admits a model such that reduction modulo a prime p is compatible with "reducing the moduli space" modulo p. The Eichler-Shimura relation is then proved in the moduli space, and finally transferred back in the setting of the modular curve.

The main references for this chapter are [DS06, Ch. 8], [Shi71, Ch. 6-7] and [DI95, II.8-10]. For the theory of reduction of curves and varieties, we refer to [Liu06, Chapter 10]. Note that in [Shi71], Shimura proves the Eichler-Shimura relation by means of the theory of complex multiplication. The simpler proof described above was given in [Shi58].

1. Generalized moduli spaces and Igusa's theorem

1.1. Generalized moduli spaces

Let us define a *moduli problem* generalizing the moduli space $S_1(N)$ defined in Chapter 2.

Definition 6.1. A *family of elliptic curves over a scheme S* is a smooth proper group scheme $\mathcal{E}$ over S whose geometric fibers[1] are elliptic curves.

Example 6.2. A complex elliptic curve can be given the structure of a smooth proper group scheme over $\mathbb{C}$ (as a closed subscheme of $\mathbb{P}^2_{\mathbb{C}}$), and be viewed as a

[1] If $s \in S$, recall that the *geometric fiber* of $\mathcal{E}$ at s is $\mathcal{E} \times_S \overline{k(s)}$, for $k(s)$ the residue field of S at s.

family of elliptic curves over $\mathbb{C}$. A more interesting example is that an elliptic curve defined over $\mathbb{Q}$ with good reduction at all primes except $p_1, \ldots, p_r$ can be given the structure of a family of elliptic curves over $\mathbb{Z}[1/(p_1 \cdots p_r)]$. More generally, the Néron model (see Section 1.8) of an elliptic curve E defined over $\mathbb{Q}$ can be seen as the best smooth group scheme over $\mathbb{Z}$ extending E (but whose fibers may not all be elliptic curves). See [Sil94, Chapter 4], [Liu06, Chapter 10.2] or more globally [KM85, Chapter 2].

Example 6.3. The universal elliptic curve consider in Section 5.1.3 can be seen as a closed subscheme $\mathcal{E}$ of $\mathbb{P}^2_S$, for $S = \operatorname{Spec}(\mathbb{Z}[j, j^{-1}(j-1728)^{-1})$. If K is a field and $j_0 \in K$ is not equal to 0 or 1728, then $\mathcal{E}_K$ (obtained from the geometric point $\operatorname{Spec} K \to S$ given by $j \mapsto j_0$) is an elliptic curve over K with j-invariant j_0.

Definition 6.4. Let $\mathcal{E}$ be a family of elliptic curves over a $\mathbb{Z}[1/N]$-scheme S. A section $\mathcal{P} \in \mathcal{E}(S)$ has *order* N if $\mathcal{P} \circ s$ has order N in $\mathcal{E}(k)$ for all geometric points $s : \operatorname{Spec}(k) \to S$.

We define a contravariant functor $\mathcal{F}_1(N)$ from the category of schemes over $\mathbb{Z}[1/N]$ to the category of sets by

- If S is a scheme over $\mathbb{Z}[1/N]$, then $\mathcal{F}_1(N)(S)$ is the set of isomorphism classes of pairs $(\mathcal{E}, \mathcal{P})$, where $\mathcal{E}$ is a family of elliptic curve over S and $\mathcal{P} \in \mathcal{E}(S)$ has order N.
- If $\varphi : S \to S'$ is a morphism of $\mathbb{Z}[1/N]$-schemes, then $\mathcal{F}_1(N)(\varphi) : \mathcal{F}_1(N)(S') \to \mathcal{F}_1(N)(S)$ is defined by base change.

Example 6.5. We have $\mathcal{F}_1(N)(\mathbb{C}) = S_1(N)$ and $\mathcal{F}_1(N)(\overline{\mathbb{Q}}) = S_1(N)_{\mathbb{Q}}$, as defined in the previous chapters.

Example 6.6. If p is a prime not dividing N, then $\mathbb{F}_p$ is a scheme over $\mathbb{Z}[1/N]$ (induced by the ring homomorphisms $\mathbb{Z}[1/N] \to \mathbb{F}_p$), and we define

$$S_1(N)_p = \mathcal{F}_1(N)(\overline{\mathbb{F}}_p),$$

the “reduction” of the moduli space $S_1(N)$.

Example 6.7. Let $\mathfrak{p}$ be an ideal of $\overline{\mathbb{Z}}$, the ring of algebraic integers in $\overline{\mathbb{Q}}$, above the rational prime p. If $p \nmid N$, consider the localization $\overline{\mathbb{Z}}_{\mathfrak{p}}$ of $\overline{\mathbb{Z}}$ at $\mathfrak{p}$. We have a ring homomorphism $\mathbb{Z}[1/N] \to \overline{\mathbb{Z}}_{\mathfrak{p}}$, which shows that $S = \operatorname{Spec} \overline{\mathbb{Z}}_{\mathfrak{p}}$ is a scheme over $\mathbb{Z}[1/N]$. The spectrum of $\overline{\mathbb{Z}}_{\mathfrak{p}}$ has two elements: $\mathfrak{p}$ and the zero ideal. A family of elliptic curves over S corresponds to an enhanced elliptic curve over $\overline{\mathbb{Q}}$ with good reduction at $\mathfrak{p}$. We define

$$S_1(N)_{\mathfrak{p}-\mathrm{good}} = \mathcal{F}_1(N)(\overline{\mathbb{Z}}_{\mathfrak{p}}).$$

The reduction map

$$\pi_{\mathfrak{p}} : \overline{\mathbb{Z}}_{\mathfrak{p}} \to \overline{\mathbb{Z}}_{\mathfrak{p}}/\mathfrak{p} \cong \overline{\mathbb{Z}}/\mathfrak{p} \cong \overline{\mathbb{F}}_p$$

gives a morphism of schemes $\operatorname{Spec} \overline{\mathbb{F}}_p \to S$, which induces by functoriality a map

$$S_1(N)_{\mathfrak{p}-\mathrm{good}} \to S_1(N)_p.$$

Elementarily, this map sends $[E, Q]$ to $[\pi_{\mathfrak{p}}(E), \pi_{\mathfrak{p}}(Q)]$ if E is an elliptic curve defined over $\overline{\mathbb{Q}}$ with good reduction at $\mathfrak{p}$ and $Q \in E(\overline{\mathbb{Q}})$ a point of order N.

1.2. Igusa's theorem

The important result we announced in the introduction is the following, which asserts the existence of a solution to the moduli problem set above, and thus giving a model for $Y_1(N)$, which is compatible with the moduli spaces.

Theorem 6.8 (Igusa ([Igu59]), Katz-Mazur ([KM85]), Deligne-Rapoport)**.** *There exists a smooth scheme $\mathcal{Y}_1(N)$ of relative dimension one over $\mathbb{Z}[1/N]$ which* represents the functor $\mathcal{F}_1(N)$*: for any scheme S over $\mathbb{Z}[1/N]$, there is a bijection functorial in S*

$$\mathcal{Y}_1(N)(S) \equiv \mathcal{F}_1(N)(S).$$

Moreover, $\mathcal{Y}_1(N)$ has irreducible geometric fibers.

Corollary 6.9. *A model for $Y_1(N)$ over $\mathbb{Z}[1/N]$ is given by $\mathcal{Y}_1(N)$. The modular curve $Y_1(N)$ has good reduction modulo p for all primes $p \nmid N$.*

Proof. By considering the scheme $S = \overline{\mathbb{Q}}$, we find that $\mathcal{Y}_1(N)(\overline{\mathbb{Q}}) \equiv S_1(N)_{\mathbb{Q}}$ by Example 6.5. This induces an isomorphism $\mathcal{Y}_1(N)(\overline{\mathbb{Q}}) \cong Y_1(N)$, so that $\mathcal{Y}_1(N)$ is a model for the modular curve $Y_1(N)$. Since the prime ideals of $\mathbb{Z}[1/N]$ correspond to the primes not dividing N, it follows that $Y_1(N)$ has good reduction modulo any prime not dividing N. □

Remark 6.10. By taking $S = \mathcal{Y}_1(N)$ itself in Theorem 6.8, we get that $\mathcal{F}_1(N)(\mathcal{Y}_1(N))$ is reduced to an element, say $(\mathcal{E}_{\text{univ}}, \mathcal{P}_{\text{univ}})$. Hence, if $(\mathcal{E}, \mathcal{P}) \in \mathcal{F}_1(N)(T)$ for T a scheme over $\mathbb{Z}[1/N]$, Theorem 6.8 implies that $(\mathcal{E}, \mathcal{P})$ is obtained from $(\mathcal{E}_{\text{univ}}, \mathcal{P}_{\text{univ}})$ by a unique base-change $T \to \mathcal{Y}_1(N)$, by functoriality.

The particular case we will be interested in is the following:

Corollary 6.11. *The morphism of schemes* $\operatorname{Spec}\overline{\mathbb{F}}_p \to \operatorname{Spec}\overline{\mathbb{Z}}_{\mathfrak{p}}$ *induces a commutative diagram*

$$\begin{tikzcd} S_1(N)_{\mathfrak{p}-good} \arrow[r] \arrow[d] & Y_1(N)(\overline{\mathbb{Q}}) \arrow[d] \\ S_1(N)_p \arrow[r] & Y_1(N)_p(\overline{\mathbb{F}}_p). \end{tikzcd} \tag{6.1}$$

Proof. Follows immediately from the functoriality in Theorem 6.8 and Corollary 6.9, with $S = \operatorname{Spec}\overline{\mathbb{Z}}_{\mathfrak{p}}$, respectively $S = \operatorname{Spec}\overline{\mathbb{F}}_p$. □

In other words, *reducing the modular curve is compatible with reducing the moduli space.*

Results for $X_1(N)$ By the work of Deligne and Rapoport, similar results can be obtained for $X_1(N)$, considering moduli spaces of enhanced *generalized elliptic curves* to interpret the cusps. The reader can refer to [DI95, II.9.2] for the details.

Results for $\Gamma_0(N)$ Similar constructions can be made with $\Gamma_0(N)$, but this is more delicate, and it yields a slightly weaker result; see [DI95, II.8]. In what follows, we will only consider $\Gamma_1(N)$ for simplicity, obtaining an Eichler-Shimura relation for $X_1(N)$, while keeping in mind that all the results generalize to $\Gamma_0(N)$. Moreover, we will note that the relation we obtain for $X_1(N)$ is more general in some sense.

2. The Eichler-Shimura relation in the moduli space

As sketched in the introduction of this chapter, we now prove an analogue of the Eichler-Shimura relation in the context of the moduli space $S_1(N)$. Using Diagram (6.1), which shows the compatibility of the reduction of the modular curve and the moduli space, we will be able to transfer this in the context of the modular curve.

2.1. Reduction of the moduli space

In what follows, we fix a prime number $p \nmid N$ and a prime ideal $\mathfrak{p}$ of $\overline{\mathbb{Z}}$ above p.

In the previous section, we defined the reduced moduli space $S_1(N)_p$, the subset $S_1(N)_{\mathfrak{p}-\mathrm{good}} \subset S_1(N)$, and the reduction map

$$S_1(N)_{\mathfrak{p}-\mathrm{good}} \to S_1(N)_p.$$

Note that the latter is surjective since the reduction map $E[N] \to E_{\mathfrak{p}}[N]$ is surjective[2] for all elliptic curves E over $\overline{\mathbb{Q}}$ with good reduction at $\mathfrak{p}$.

The moduli-space analogue of the Eichler-Shimura relation will be to obtain a commutative diagram

$$\begin{tikzcd}
\mathrm{Div}(S_1(N)_{\mathfrak{p}-\mathrm{good}}) \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}(S_1(N)_{\mathfrak{p}-\mathrm{good}}) \arrow[d] \\
\mathrm{Div}(S_1(N)_p) \arrow[r, dashed] & \mathrm{Div}(S_1(N)_p)
\end{tikzcd}$$

where the dotted map is to be determined.

2.2. Hecke operators on the reduced space

Recall that by Propositions 3.27 and 3.25, the action of Hecke operators on the moduli space can be described quite easily:

- $T_p : \mathrm{Div}(S_1(N)) \to \mathrm{Div}(S_1(N))$ is given by

  $$[E, Q] \mapsto \sum_C [E/C, [Q]_C],$$

  where C sums on all subgroups of order p of E with $C \cap \langle Q \rangle = 0$.
- $\langle d \rangle : \mathrm{Div}(S_1(N)) \to \mathrm{Div}(S_1(N))$ is given by

  $$[E, Q] \mapsto [E, [d]Q].$$

In this paragraph, we compute reductions of these operators in the reduced moduli space $S_1(N)_p$.

[2] By [Sil09, VII.3.1(b)], the map $E[N] \to E_{\mathfrak{p}}[N]$ is injective. Since $p \nmid N$, we have that $E[N] \cong \mathbb{Z}/N \cong E_{\mathfrak{p}}[N]$, so that the map is bijective.

The Diamond operators on $S_1(N)_p$

Proposition 6.12. *There is a commutative diagram*

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)_{\mathfrak{p}-good}) \arrow[r, "\langle d\rangle"] \arrow[d] & \mathrm{Div}^0(S_1(N)_{\mathfrak{p}-good}) \arrow[d] \\
\mathrm{Div}^0(S_1(N)_p) \arrow[r, "\langle d\rangle_p"] & \mathrm{Div}^0(S_1(N)_p),
\end{tikzcd}$$

where the map $\langle d\rangle_p : S_1(N)_p \to S_1(N)_p$ is given by $\langle d\rangle_p[E, Q] = [E, [d]Q]$.

Proof. Follows directly from Proposition 3.25. □

The T_p operators on $S_1(N)_p$ Then, we obtain an closed expression for T_p on the reduced moduli space $S_1(N)_p$. This is the main part of the proof.

Proposition 6.13. *If Q is a point of order N of an elliptic curve E defined over $\overline{\mathbb{Q}}$ with good reduction at $\mathfrak{p}$, then*

$$\sum_C [(E/C)_\mathfrak{p}, [Q]_\mathfrak{p}] = (\sigma_p + p\langle p\rangle_p \sigma_p^{-1})[E_\mathfrak{p}, Q_\mathfrak{p}],$$

where σ_p is the Frobenius morphism, and the sum is over all subgroups C of order p in E such that $C \cap \langle Q\rangle = 0$.

Proof. For C a subgroup of E of order p, let us consider the isogeny $f : E \to E/C$ and the dual isogeny $\hat{f} : E/C \to C$, such that $f \circ \hat{f} = [p] \in \mathrm{End}(E/C)$ and $\hat{f} \circ f = [p] \in \mathrm{End}(E)$. By [Sil09, VII.7.2], it follows that E/C has good reduction at $\mathfrak{p}$. By [Sil09, II.2.12], recall that $f_p : E_\mathfrak{p} \to (E/C)_\mathfrak{p}$ factors as

$$f_p = f_p^{\mathrm{sep}} \circ \sigma_p^e : \qquad E_\mathfrak{p} \xrightarrow{\sigma_p^e} \sigma_p^e(E_\mathfrak{p}) \xrightarrow{f_p^{\mathrm{sep}}} (E/C)_\mathfrak{p}$$

with f_p^{sep} a separable morphism of degree $\deg_{\mathrm{sep}}(f_p)$ and $\deg_{\mathrm{ins}}(f_p) = p^e$. Similarly, we have $\hat{f}_p = \hat{f}_p^{\mathrm{sep}} \circ \sigma_p^f$, where $\hat{f}_p^{\mathrm{sep}}$ is a separable morphism of degree $\deg_{\mathrm{sep}}(\hat{f}_p)$ and $\deg_{\mathrm{ins}}(\hat{f}_p) = p^f$. The degree of an isogeny is preserved under reduction[3], so that

$$\deg f_p = \deg \hat{f}_p = \deg f = p \text{ and } \deg([p]_\mathfrak{p}) = \deg[p] = p^2.$$

We distinguish two cases:

– Suppose that E has ordinary reduction at $\mathfrak{p}$, so that $E_\mathfrak{p}[p] \cong \mathbb{Z}/p$, the kernel of the map $[p] : E_\mathfrak{p} \to E_\mathfrak{p}$. Hence,

$$\deg_{\mathrm{sep}}([p]_\mathfrak{p} \in \mathrm{End}(E_\mathfrak{p})) = |\ker[p]_\mathfrak{p}| = |E_\mathfrak{p}[p]| = p,$$

so $\deg_{\mathrm{ins}}([p]_\mathfrak{p} \in \mathrm{End}(E_\mathfrak{p})) = p$ as well, since the total degree is equal to the product of the separable and the inseparable degree. Since ordinary/-supersingular reduction is preserved under isogeny, it similarly follows that $(E/C)_\mathfrak{p}[p] \cong \mathbb{Z}/p$, so that

$$\deg_{\mathrm{sep}}([p]_\mathfrak{p} \in \mathrm{End}((E/C)_\mathfrak{p})) = \deg_{\mathrm{ins}}([p] \in \mathrm{End}((E/C)_\mathfrak{p})) = p.$$

[3] Indeed, the reduction $\mathrm{End}(E) \to \mathrm{End}(E_\mathfrak{p})$ preserves dual isogenies (this is clear from the construction of the dual isogeny by pushforwards on Picard groups, cf. [Sil09, III.6]), so that multiplication by $\deg f$ is equal to multiplication by $\deg f_\mathfrak{p}$ on $E_\mathfrak{p}$, for all $f \in \mathrm{End}(E)$. We conclude using that $\mathbb{Z} \to \mathrm{End}(E_\mathfrak{p})$ is an injective homomorphism ([Sil09, III.4.2]).

Since separable and inseparable degrees are multiplicative, two cases can arise:

	$\deg_{\text{sep}}(f_p)$	$\deg_{\text{sep}}(\hat{f}_p)$	$\deg_{\text{ins}}(f_p)$	$\deg_{\text{ins}}(\hat{f}_p)$
Case 1	1	p	p	1
Case 2	p	1	1	p

In the first case, we get $f_p = i \circ \sigma_p$, where $i : \sigma_p(E_\mathfrak{p}) \to (E/C)_\mathfrak{p}$ is an isomorphism such that $i(\sigma_p(Q_\mathfrak{p})) = [Q]_\mathfrak{p}$. Thus,

$$[(E/C)_\mathfrak{p}, [Q]_\mathfrak{p}] = [\sigma_p(E_\mathfrak{p}), \sigma_p(Q_\mathfrak{p})] = \sigma_p[E_\mathfrak{p}, Q_\mathfrak{p}].$$

In the second case, we similarly get $\hat{f}_p = i \circ \sigma_p$, where $i : \sigma_p((E/C)_\mathfrak{p}) \to E_\mathfrak{p}$ is an isomorphism such that $i(\sigma_p([Q]_\mathfrak{p})) = (\hat{f}_p \circ f_p)(Q) = [p]Q$. The Frobenius morphism is an isomorphism, so that

$$[(E/C)_\mathfrak{p}, [Q]_\mathfrak{p}] = [\sigma_p^{-1}(E_\mathfrak{p}), \sigma_p^{-1}([p]Q_\mathfrak{p})] = \langle p \rangle_p \sigma_p^{-1}[E_\mathfrak{p}, Q_\mathfrak{p}].$$

- Suppose now that E has supersingular reduction at $\mathfrak{p}$, i.e. $E_\mathfrak{p}[p] = 0$. Thus, $\deg_{\text{sep}}([p]_\mathfrak{p} \in \operatorname{End}(E_\mathfrak{p})) = 1$, $\deg_{\text{ins}}([p]_\mathfrak{p} \in \operatorname{End}(E_\mathfrak{p})) = p^2$, $\deg_{\text{sep}}([p]_\mathfrak{p} \in \operatorname{End}((E/C)_\mathfrak{p})) = 1$ and $\deg_{\text{ins}}([p]_\mathfrak{p} \in \operatorname{End}((E/C)_\mathfrak{p})) = p$. It follows that $\deg_{\text{sep}}(f_p) = \deg_{\text{sep}}(\hat{f}_p) = 1$ and $\deg_{\text{ins}}(f_p) = \deg_{\text{ins}}(\hat{f}_p) = p$. Hence,

$$f_p = i_1 \circ \sigma_p \text{ and } \hat{f}_p = i_2 \circ \sigma_p$$

where $i_1 : \sigma_p(E_\mathfrak{p}) \to (E/C)_\mathfrak{p}$ and $i_2 : \sigma_p((E/C)_\mathfrak{p}) \to E_\mathfrak{p}$ are isomorphisms, which implies as before that

$$[(E/C)_\mathfrak{p}, [Q]_\mathfrak{p}] = \langle p \rangle_p \sigma_p^{-1}[E_\mathfrak{p}, Q_\mathfrak{p}] = \sigma_p[E_\mathfrak{p}, Q_\mathfrak{p}].$$

Now, note that the sum in the statement is in fact on *all* subgroups of order p of E, since Q has order N and $p \nmid N$. Since any subgroup of order p is contained in $E[p] \cong \mathbb{Z}/p \times \mathbb{Z}/p$, there exist $(p^2-1)/(p-1) = p+1$ such subgroups. Thus, it suffices to prove that the Case 1 above occurs for exactly one such subgroup to get that

$$\sum_C [(E/C)_\mathfrak{p}, [Q]_\mathfrak{p}] = (\sigma_p + p\langle p \rangle_p \sigma_p^{-1})[E_\mathfrak{p}, Q_\mathfrak{p}].$$

Suppose again that E has ordinary reduction at $\mathfrak{p}$ and let C_0 be the kernel of the map $E[p] \to E_\mathfrak{p}[p]$. This map is surjective[4], so that C_0 has order $p^2/p = p$. Let C be a subgroup of E of order p. Similarly, the kernel C_0' of the reduction $(E/C)[p] \to (E/C)_\mathfrak{p}[p]$ has order p.

- If $C = C_0$, then $\ker \hat{f}_p = (E/C)_\mathfrak{p}[p]$, so that $\deg_{\text{sep}}(\hat{f}_p) = |\ker \hat{f}_p| = p$, and Case 1 holds. These assertions are proved as follows: since $f \circ \hat{f} = [p]$, we have that $\ker \hat{f} \subset (E/C)[p]$ and similarly that $\ker \hat{f}_p \subset (E/C)_\mathfrak{p}[p]$. On the other hand, $\hat{f}((E/C)[p]) \subset \ker f = C$ for the same reason, implying that $\hat{f}((E/C)[p])$ has order 1 or p. We have

$$\hat{f}((E/C)[p]) \cong (E/C)[p]/(\ker \hat{f} \cap (E/C)[p]) = (E/C)[p]/\ker \hat{f},$$

[4] When have seen in note 2 on page 79 that this result holds true for $E[N] \to E_\mathfrak{p}[N]$ when $p \nmid N$. For $E[p] \to E_\mathfrak{p}[p]$, this result quoted in [DS06, Proposition 8.4.4], but without proof nor further reference. This is probably true for abelian varieties as well, but we have not found a reference about that so far.

which implies that $\hat{f}((E/C)[p])$ has order p^2 or p. Hence, $\hat{f}((E/C)[p]) = C$ since we then have an inclusion of groups of the same order. In other words, the right-outer composition of the commutative diagram

$$\begin{tikzcd}
(E/C)[p] \arrow[r, "\hat{f}"] \arrow[d] & E[p] \arrow[d] \\
(E/C)_{\mathfrak{p}}[p] \arrow[r, "\hat{f}_p"] & E_{\mathfrak{p}}[p]
\end{tikzcd}$$

is zero by the definition of $C = C_0$. Since the right vertical map is surjective, it follows that $(E/C)_{\mathfrak{p}}[p] \subset \ker \hat{f}_p$ as wanted.

- If $C \neq C_0$, then Case 2 holds. Indeed, let us consider the image $f(C_0)$. Since $C \neq C_0$, we have $C \cap C_0 = 0$, thus $f(C_0) \cong C_0$. On one hand, we see as before that $f(C_0) \subset \ker \hat{f}$, so $f(C_0) = \ker \hat{f}$ since both groups have order p. On the other hand, since the diagram

$$\begin{tikzcd}
E[p] \arrow[r, "\hat{f}"] \arrow[d] & (E/C)[p] \arrow[d] \\
E_{\mathfrak{p}}[p] \arrow[r, "\hat{f}_p"] & (E/C)_{\mathfrak{p}}[p]
\end{tikzcd}$$

commutes, it follows that $f(C_0) \subset C_0'$, so $f(C_0) = C_0'$ again because both groups have order p. Hence, $C_0' = \ker \hat{f}$. The previous argument with E (resp. C, f) replaced by E/C (resp. C_0', $\hat{f}$) shows that $p = \deg_{\mathrm{sep}}(\hat{\hat{f}}_p) = \deg_{\mathrm{sep}}(f_p)$, so that the second case holds.

This analysis concludes the argument. □

In other words, Proposition 6.13 shows that we have a commutative diagram

$$\begin{tikzcd}
S_1(N)_{\mathfrak{p}-\mathrm{good}} \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}(S_1(N)_{\mathfrak{p}-\mathrm{good}}) \arrow[d] \\
S_1(N)_p \arrow[r, "\sigma_p + p\langle p\rangle_p \sigma_p^{-1}"] & \mathrm{Div}(S_1(N)_p)
\end{tikzcd}$$

which restricts and corestricts to a commutative diagram

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)_{\mathfrak{p}-\mathrm{good}}) \arrow[r, "T_p"] \arrow[d] & \mathrm{Div}^0(S_1(N)_{\mathfrak{p}-\mathrm{good}}) \arrow[d] \\
\mathrm{Div}^0(S_1(N)_p) \arrow[r, "\sigma_p + p\langle p\rangle_p \sigma_p^{-1}"] & \mathrm{Div}^0(S_1(N)_p)
\end{tikzcd} \tag{6.2}$$

This computation of T_p on the reduced moduli space is the equivalent in the moduli space of the Eichler-Shimura relation.

3. The reduced modular curve and the reduced moduli space

As explained, the goal is now to transfer Diagram (6.2) back to modular curves.

3.1. Planar models and Igusa's theorem

Since continuing to study the modern approach sketched in Section 6.1 would be too long for us (see [DI95, II.7-10] for a survey), we return to the classical setting developed by Igusa in [Igu59] and exposed in [DS06]. In particular, we give the classical formulation of Theorem 6.8.

Reduction of the planar model In what follows, let us continue to denote $X_1(N)_{\mathbb{Q}}$ by $X_1(N)$. Recall the planar model of $X_1(N)$ given by

$$X_1(N)^{\text{planar}} = \{(j,x) \in \overline{\mathbb{Q}}^2 : p_1(j,x) = 0\},$$

where $p_1 \in \mathbb{Q}[j,X]$ is obtained from the minimal polynomial of $f_1 \in \overline{\mathbb{Q}(j)}$. We saw in the previous chapter that f_1 is equal to the first coordinate of the point $Q_0 = [z/N]_{\Lambda_z} \in E_j[N]$, where E_j is the "universal" elliptic curve, defined over $\mathbb{Q}(j)$.

Consider the reduction $X_1(N)_p^{\text{planar}}$ defined by the polynomial $\pi_p(p_1)$, where $\pi_p : \mathbb{Q}_{(p)} \to \mathbb{F}_p$ is the projection. Note that the universal elliptic curve E_j can also be seen as a curve over $\overline{\mathbb{F}_p(j)}$. As in characteristic zero, we can consider the first coordinate $(f_1)_p \in \overline{\mathbb{F}_p(j)}$ of the point $Q_0 \in E_j[N](\overline{\mathbb{F}_p(j)})$. Then, $\pi_p(p_1)$ is also equal to the polynomial in $\mathbb{F}_p[j,X]$ obtained from the minimal polynomial of $(f_1)_p$.

Igusa's theorem The version of Theorem 6.8 shown by Igusa is the following (see [Igu59, Theorem 1][5]):

Theorem 6.14. *The field $\mathbb{F}_p(j,(f_1)_p)$ is a function field and there exists a model of $X_1(N)$ whose reduction $X_1(N)_p$ at p has function field $\mathbb{F}_p(j,(f_1)_p)$. In other words, there are birational maps $X_1(N)^{planar} \to X_1(N)$ and $X_1(N)_p^{planar} \to X_1(N)_p$ such that the diagram*

$$\begin{tikzcd} X_1(N)^{planar} \arrow[r] \arrow[d] & X_1(N) \arrow[d] \\ X_1(N)_p^{planar} \arrow[r] & X_1(N)_p \end{tikzcd}$$

commutes where it is defined.

Compatibility with the moduli space Let us see how Theorem 6.14 also gives a compatibility of reductions between the curve and the moduli space. By Lemma 5.26, the map $S_1(N)'_{\mathfrak{p}-\text{good}} \to X_1(N)^{\text{planar}}$ is given by $[E,Q] \mapsto (j(E),x(Q))$. If we let $S_1(N)'_p$ be the image of $S_1(N)'_{\mathfrak{p}-\text{good}}$ by the map $S_1(N)_{\mathfrak{p}-\text{good}} \to S_1(N)_p$, there is similarly a map $S_1(N)'_p \to X_1(N)_p^{\text{planar}}$ given by $[E,Q] \mapsto (j(E),x(Q))$

[5] The introduction of [Igu59] summarizes particularly well the contents of the article: *"We shall construct a non-singular projective model of the field of modular functions of level N in characteristic zero over the field of rational numbers such that its reduction with respect to every prime number $p \nmid N$ is a non-singular projective model of the field of modular functions of level N in characteristic p over the prime field."*.

such that

$$\begin{tikzcd}
S_1(N)'_{\mathfrak{p}-\text{good}} \arrow[r] \arrow[d] & X_1(N)^{\text{planar}} \arrow[d] \\
S_1(N)'_p \arrow[r] & X_1(N)_p^{\text{planar}}
\end{tikzcd}$$

commutes, and the vertical maps are surjective. If we again denote by $S_1(N)'_{\mathfrak{p}-\text{good}}$ (resp. $S_1(N)'_p$) the subset of $S_1(N)'_{\mathfrak{p}-\text{good}}$ (resp. $S_1(N)'_p$) of finite complement needed to have a well-defined composition $S_1(N)'_{\mathfrak{p}-\text{good}} \to X_1(N)^{\text{planar}} \to X_1(N)$ (resp. $S_1(N)'_p \to X_1(N)_p^{\text{planar}} \to X_1(N)_p$), we obtain a commutative diagram

$$\begin{tikzcd}
S_1(N)'_{\mathfrak{p}-\text{good}} \arrow[r] \arrow[d] & X_1(N)^{\text{planar}} \arrow[r] \arrow[d] & X_1(N) \arrow[d] \\
S_1(N)'_p \arrow[r] & X_1(N)_p^{\text{planar}} \arrow[r] & X_1(N)_p,
\end{tikzcd} \tag{6.3}$$

analogous to (6.1). The maps in the Diagram (6.3) restrict and corestrict to induce a commutative diagram

$$\begin{tikzcd}
\operatorname{Div}^0(S_1(N)'_{\mathfrak{p}-\text{good}}) \arrow[r] \arrow[d] & \operatorname{Pic}^0(X_1(N)) \arrow[d] \\
\operatorname{Div}^0(S_1(N)'_p) \arrow[r] & \operatorname{Pic}^0(X_1(N)_p).
\end{tikzcd} \tag{6.4}$$

Proposition 6.15. *The two compositions from the top-left to the bottom-right in Diagram* (6.4) *are surjective.*

Lemma 6.16. *Let C be a nonsingular projective curve and $S \subset C$ a finite subset. Then the map*

$$\{D \in \operatorname{Div}^0(C) : D(P) = 0 \textit{ if } P \in S\} \to \operatorname{Pic}^0(C)$$

is surjective.

Proof. See [DS06, Proposition 7.3.1]. □

Proof of Proposition 6.15.

– The reduction map $S_1(N)'_{\mathfrak{p}-\text{good}} \to S_1(N)'_p$ is surjective, so the same holds for the induced map $\operatorname{Div}^0(S_1(N)'_{\mathfrak{p}-\text{good}}) \to \operatorname{Div}^0(S_1(N)'_p)$.

– The map $S_1(N) \to X_1(N)$ is surjective up to finitely many points in the image (the cusps). Since $X_1(N)$ is birationally equivalent to $X_1(N)^{\text{planar}}$, the same holds true for the map $S'_1(N) \to X_1(N)^{\text{planar}}$. By (6.3) and the surjectivity of the vertical maps, the map $S_1(N)'_p \to X_1(N)_p$ is also surjective up to finitely many points. By the Lemma, the map $\operatorname{Div}^0(S_1(N)'_p) \to \operatorname{Pic}^0(X_1(N)_p)$ is surjective, so that the composition

$$\operatorname{Div}^0(S_1(N)'_{\mathfrak{p}-\text{good}}) \to \operatorname{Div}^0(S_1(N)'_p) \to \operatorname{Pic}^0(X_1(N)_p)$$

is surjective as well.

□

3.2. Operators on the reduced modular curve and on the reduced moduli space

Igusa's theorem shows that there is a model for the modular curve such that reducing the latter is compatible with reducing the moduli space. Furthermore, we show how operators on the reduced moduli space correspond to operators on the reduced modular curve.

Proposition 6.17. *The diagrams*

$$\begin{tikzcd}
\mathrm{Div}(S_1(N)'_p) \arrow[r, "\sigma_p"] \arrow[d] & \mathrm{Div}(S_1(N)'_p) \arrow[d] & \mathrm{Div}(S_1(N)'_p) \arrow[r, "p\sigma_p^{-1}"] \arrow[d] & \mathrm{Div}(S_1(N)'_p) \arrow[d] \\
\mathrm{Div}(X_1(N)_p) \arrow[r, "(\sigma_p)_*"] & \mathrm{Div}(X_1(N)_p) & \mathrm{Div}(X_1(N)_p) \arrow[r, "(\sigma_p)^*"] & \mathrm{Div}(X_1(N)_p)
\end{tikzcd}$$

commute, where $\sigma_p : \mathrm{Div}(S_1(N)_p) \to \mathrm{Div}(S_1(N)_p)$ *is given by* $[E, Q] \mapsto [\sigma_p(E), \sigma_p(Q)]$.

Proof. First, note that the same diagrams with $X_1(N)_p^{\text{planar}}$ instead of $X_1(N)_p$ commute. Indeed, recall that the map $S_1(N)'_p \to X_1(N)_p^{\text{planar}}$ is given by $[E, Q] \mapsto (j(E), x(Q))$; if $[E, Q] \in S_1(N)'_p$, we have

$$\begin{aligned}\sigma_p([E,Q]) &= [\sigma_p(E), \sigma_p(Q)] \mapsto (j(\sigma_p(E)), x(\sigma_p(Q))) \\ &= (\sigma_p(j(E)), \sigma_p(x(Q))) = (\sigma_p)_*(j(E), x(Q))\end{aligned}$$

and[6]

$$\begin{aligned}p\sigma_p^{-1}([E,Q]) &= p[\sigma_p^{-1}(E), \sigma_p^{-1}(Q)] \mapsto p(j(\sigma_p^{-1}(E)), \sigma_p^{-1}(Q)) \\ &= p(\sigma_p^{-1}(j(E)), \sigma_p^{-1}(x(Q))) = (\sigma_p)^*(j(E), x(Q)).\end{aligned}$$

We can then conclude by using the fact that the diagram

$$\begin{tikzcd}
\mathrm{Div}(X_1(N)_p^{\text{planar}}) \arrow[r, "(\sigma_p)_*"] \arrow[d] & \mathrm{Div}(X_1(N)_p^{\text{planar}}) \arrow[d] \\
\mathrm{Div}(X_1(N)_p) \arrow[r, "(\sigma_p)_*"] & \mathrm{Div}(X_1(N)_p)
\end{tikzcd}$$

commutes where defined by the properties of the Frobenius morphism, where the vertical maps are induced by the birational equivalence between $X_1(N)_p^{\text{planar}}$ and $X_1(N)_p$, and similarly for σ_p^*. □

4. The Eichler-Shimura relation

We can finally prove the Eichler-Shimura relation for the modular curve.

4.1. Reduction of the Hecke operators

By Igusa's theorem, the modular curve $X_1(N)$ reduces modulo p for any prime $p \nmid N$.

[6] Recall that the Frobenius is purely inseparable of degree p, see [Sil09, II.2.11].

Consider the Jacobian variety $\mathrm{Pic}^0(X_1(N))$ (see Section 1.7) and its Néron model $\mathcal{P}$ for it (see Section 1.8). By the universal property of Néron models, the morphism T_p on $\mathrm{Pic}^0(X_1(N))$ extends to a morphism on $\mathcal{P}$. For all but finitely many primes q, the Jacobian variety has good reduction mod q (i.e. the fiber $\mathcal{P}_q$ is an abelian variety) and T_p reduces to a morphism on $\mathrm{Pic}^0(X_0(N))_q := \mathcal{A}_q$.

By [BLR90, Theorem 9.5.1] (see also [DI95, II.10.1-2]), we have $\mathrm{Pic}^0(X_1(N))_p \cong \mathrm{Pic}^0(X_1(N)_p)$, so that there is good reduction at p when $p \nmid N$ by Theorem 6.8, and we obtain a commutative diagram

$$\begin{tikzcd}
\mathrm{Pic}^0(X_1(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_1(N)) \arrow[d] \\
\mathrm{Pic}^0(X_1(N)_p) \arrow[r, "(T_p)_p"] & \mathrm{Pic}^0(X_1(N)_p).
\end{tikzcd} \tag{6.5}$$

The same holds true for the diamond operators $\langle d \rangle$.

4.2. Pushforward of the map $\sigma_p + p\langle p\rangle_p \sigma_p^{-1}$

The last step before being able to transfer Diagram (6.2) from the moduli space to the modular curve is to transfer the map $\sigma_p + p\langle p\rangle_p\sigma_p^{-1}$ from the reduced moduli space to the reduced modular curve, via the map $S_1(N)'_p \to X_1(N)_p$.

Lemma 6.18. *We have a commutative diagram*

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)'_p) \arrow[r, "\langle d\rangle_p"] \arrow[d] & \mathrm{Div}^0(S_1(N)'_p) \arrow[d] \\
\mathrm{Div}^0(X_1(N)_p) \arrow[r, "\langle d\rangle_p"] & \mathrm{Div}^0(X_1(N)_p).
\end{tikzcd}$$

Proof. Consider the diagram

$$\begin{tikzcd}
& \mathrm{Pic}^0(X_1(N)) \arrow[rr, "\langle d\rangle"] \arrow[dd] & & \mathrm{Pic}^0(X_1(N)) \arrow[dd] \\
\mathrm{Div}^0(S_1(N)'_{\mathfrak{p}-\mathrm{good}}) \arrow[ur] \arrow[rr, "\langle d\rangle"] \arrow[dd] & & \mathrm{Div}^0(S_1(N)'_{\mathfrak{p}-\mathrm{good}}) \arrow[ur] \arrow[dd] & \\
& \mathrm{Pic}^0(X_1(N)_p) \arrow[rr, "\langle d\rangle_p"] & & \mathrm{Pic}^0(X_1(N)_p). \\
\mathrm{Div}^0(S_1(N)'_p) \arrow[ur] \arrow[rr, "\langle d\rangle_p"] & & \mathrm{Div}^0(S_1(N)'_p) \arrow[ur] &
\end{tikzcd}$$

where

- The top face commutes by definition of the Hecke operators on the moduli space.
- The sides are the commutative diagram (6.4).
- The front face is the commutative diagram of Proposition 6.12.
- The back face commutes by the analogue of (6.5) for $\langle d\rangle$.

Since the map $\mathrm{Div}^0(S_1(N)'_{\mathfrak{p}-\mathrm{good}}) \to \mathrm{Div}^0(S_1(N)'_p)$ is surjective, we get that the bottom side commutes as well. □

Proposition 6.19. *The diagram*

$$\begin{tikzcd}
\mathrm{Div}^0(S_1(N)'_p) \arrow[r, "\sigma_p+p\langle p\rangle_p\sigma_p^{-1}"] \arrow[d] & \mathrm{Div}^0(S_1(N)'_p) \arrow[d] \\
\mathrm{Pic}^0(X_1(N)_p) \arrow[r, "(\sigma_p)_*+(\langle p\rangle_p)_*(\sigma_p)^*"] & \mathrm{Pic}^0(X_1(N)_p)
\end{tikzcd} \tag{6.6}$$

commutes, the vertical maps being those of Theorem 6.8.

Proof. Follows directly from Propositions 6.17 and Lemma 6.18. □

4.3. Transfer to the modular curve

Putting the previous sections together, we finally get the following vertically-symmetric cube-shaped diagram:

$$\begin{tikzcd}
 & \mathrm{Pic}^0(X_1(N)) \arrow[rr, "T_p"] \arrow[dd] & & \mathrm{Pic}^0(X_1(N)) \arrow[dd] \\
\mathrm{Div}^0(S_1(N)'_{\mathfrak{p}-\mathrm{good}}) \arrow[ur] \arrow[rr, "T_p"] \arrow[dd] & & \mathrm{Div}^0(S_1(N)'_{\mathfrak{p}-\mathrm{good}}) \arrow[ur] \arrow[dd] & \\
 & \mathrm{Pic}^0(X_1(N)_p) \arrow[rr, dashed, "(\sigma_p)_*+(\langle p\rangle_p)_*(\sigma_p)^*"] \arrow[rr, bend right, "(T_p)_p"'] & & \mathrm{Pic}^0(X_1(N)_p) \\
\mathrm{Div}^0(S_1(N)'_p) \arrow[ur] \arrow[rr, "\sigma_p+p\langle p\rangle_p\sigma_p^{-1}"] & & \mathrm{Div}^0(S_1(N)'_p) \arrow[ur] &
\end{tikzcd}$$

- The two sides are the commutative diagram (6.4): the compatibility of the reduction of moduli spaces and modular curves.
- The top face is the commutative diagram (5.4): the compatibility of T_p on modular curves and moduli spaces.
- The front face is the commutative diagram (6.2): the reduction of T_p on the moduli space.
- The bottom face with $(\sigma_p)_*+(\langle p\rangle_p)_*(\sigma_p)^*$ is the commutative diagram (6.6): the transfer of the map $\sigma_p + p\langle p\rangle_p\sigma_p^{-1}$ on $\mathrm{Div}^0(S_1(N)'_p)$ to $\mathrm{Pic}^0(X_1(N)_p)$.
- The back face with $(T_p)_p$ is the commutative diagram (6.5): the reduction of T_p.

Moreover, note that the composition

$$\mathrm{Div}^0(S_1(N)'_{\mathfrak{p}-\mathrm{good}}) \to \mathrm{Pic}^0(X_1(N)) \to \mathrm{Pic}^0(X_1(N)_p)$$

is surjective by Proposition 6.15.

Thus, we get that the back diagram with $(\sigma_p)_* + \langle p\rangle_p(\sigma_p)^*$ is commutative by the following general result:

Lemma 6.20. *Let*

$$\begin{tikzcd}
 & C \arrow[rr] \arrow[dd] & & C \arrow[dd] \\
A \arrow[ur] \arrow[rr] \arrow[dd] & & A \arrow[ur] \arrow[dd] & \\
 & D \arrow[rr, dashed, "\psi"] \arrow[rr, bend right, "\varphi"'] & & D \\
B \arrow[ur] \arrow[rr] & & B \arrow[ur] &
\end{tikzcd}$$

be a diagram in an additive category $\mathcal{C}$, such that

1. *The top, left and right faces are commutative.*
2. *The back face with φ is commutative.*
3. *The bottom face with ψ is commutative.*
4. *The composition $A \to C \to D$ in the left-side face is surjective.*

Then the back side with ψ is commutative.

Proof. Let us consider the map $A \to B \to D \xrightarrow{\psi} D$ from the top-left to the right-back-bottom of the diagram. Then:

- On one hand, since the left face commutes, it is equal to the composition $A \to C \to D \xrightarrow{\psi} D$.
- On the other hand:
  - it is equal to $A \to B \to B \to D$, since the bottom face with ψ commutes;
  - the previous map is equal to the composition $A \to A \to B \to D$, since the front face commutes;
  - since the right face commutes, it is equal to the composition $A \to A \to C \to D$;
  - this is equal to the composition $A \to C \to C \to D$, since the top face commutes;
  - finally, since the back face with φ is commutative, this is equal to $A \to C \to D \xrightarrow{\varphi} D$.

Hence, $\varphi = \psi$ since the composition $A \to C \to D$ is surjective. □

Therefore, we finally obtain:

Proposition 6.21 (Eichler-Shimura relation)**.** *We have commutative diagrams*

$$\begin{tikzcd}
\mathrm{Pic}^0(X_1(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_1(N)) \arrow[d] \\
\mathrm{Pic}^0(X_1(N)_p) \arrow[r, "(\sigma_p)_* + (\langle p \rangle_p)_* (\sigma_p)^*"] & \mathrm{Pic}^0(X_1(N)_p)
\end{tikzcd}$$

and

$$\begin{tikzcd}
\mathrm{Pic}^0(X_0(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_0(N)) \arrow[d] \\
\mathrm{Pic}^0(X_0(N)_p) \arrow[r, "(\sigma_p)_* + (\sigma_p)^*"] & \mathrm{Pic}^0(X_0(N)_p).
\end{tikzcd}$$

Remark 6.22. The second diagram is obtained similarly, using the generalizations to $\Gamma_0(N)$ evoked in the text. More precisely, we obtain that T_p on $\mathrm{Pic}^0(X_0(N)_p)$ is given by $(\sigma_p)_* + (\langle p\rangle_p)_*(\sigma_p)^*$ as for $\Gamma_1(N)$. But we have a commutative diagram

$$\begin{tikzcd}
S_0(N)'_p \arrow[r, "\langle p\rangle_p"] \arrow[d] & S_0(N)'_p \arrow[d] \\
X_0(N)_p \arrow[r, "\langle p\rangle_p"] & X_0(N)_p.
\end{tikzcd}$$

as in Lemma 6.18. By Proposition 3.26, if $[E, \langle Q\rangle] \in S_1(N)_p$, we have $\langle p\rangle_p[E, \langle Q\rangle] = [E, \langle [p]Q\rangle]$. Since $p \nmid N$, this implies that $\langle [p]Q\rangle = \langle Q\rangle$ and that $\langle p\rangle_p$ acts trivially on $S_0(N)_p$. The vertical maps $S_0(N)'_p \to X_0(N)_p$ are surjective up to finitely many points, so that $\langle p\rangle_p$ is trivial on all but finitely many points of $X_1(N)_p$. Since a rational map between curves uniquely extends to a morphism, we get that $\langle p\rangle_p$ acts trivially on $X_0(N)_p$. Hence, T_p on $\mathrm{Pic}^0(X_0(N)_p)$ is given by $(\sigma_p)_* + (\sigma_p)^*$.

Chapter 7

Equality of L-functions

In this last chapter, we finally conclude the proof of the theorem we have been interested in (up to finitely many primes for the last point):

Theorem 7.1 (Eichler-Shimura, Carayol, Langlands, Deligne). *Let $f \in S_2(\Gamma_0(N))$ be a newform. There exists an abelian variety A_f such that*

1. *A_f is defined over $\mathbb{Q}$;*
2. *A_f has dimension $[K_f : \mathbb{Q}]$;*
3. *A_f and f are related by their L-functions: we have*

$$L(A_f, s) = \prod_{\tau} L(f_\tau, s),$$

where the product is over the complex embeddings $\tau : K_f \to \mathbb{C}$. Alternatively, $a_p(A_f) = \sum_\tau a_p(f_\tau)$ for all primes p.

In what follows, we let $f \in S_2(\Gamma_0(N))$ be a fixed newform. In the previous chapters, we have constructed an abelian variety A_f associated to f satisfying the first two properties of Theorem 7.1. It remains to prove the relationship with f through the L-functions.

Our approach combines ideas from [DS06, Chapter 8] and [Shi71, Chapter 7]. In [DS06, Chapter 8], the proof is not explicitly given, and the method would work only for elliptic curves.

1. Idea of the proof

The reason why the relationship between f and A_f holds true is the following: recall the Eichler-Shimura relation, given by the commutative diagram

$$\begin{tikzcd}
\operatorname{Pic}^0(X_0(N)) \arrow[r, "T_p"] \arrow[d] & \operatorname{Pic}^0(X_0(N)) \arrow[d] \\
\operatorname{Pic}^0(X_0(N)_p) \arrow[r, "(\sigma_p)_* + (\sigma_p)^*"] & \operatorname{Pic}^0(X_0(N)_p),
\end{tikzcd}$$

when $p \nmid N$ (Proposition 6.21). Using the surjective morphism $\operatorname{Jac}(X_0(N)) \to (A_f)_{\mathbb{C}}$, we will transfer the Eichler-Shimura relation to A_f, obtaining a commutative diagram

$$\begin{tikzcd}
A_f \arrow[r, "T_p = a_p(f)"] \arrow[d] & A_f \arrow[d] \\
(A_f)_p \arrow[r, "\sigma_p + \hat{\sigma}_p"] & (A_f)_p
\end{tikzcd} \tag{7.1}$$

for every prime $p \nmid N$ of good reduction for A_f. In other words,

$$(T_p)_p = \sigma_p + \hat{\sigma}_p \in \operatorname{End}((A_f)_p). \tag{7.2}$$

Let $\rho_p : \mathrm{End}_{\mathbb{Q}}((A_f)_p) \to M_{2d}(\mathbb{Q}_\ell)$ be the ℓ-adic representation, for $\ell \neq p$ a prime, after choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(A_f)_p$. From relation (7.2), we can compute the characteristic polynomial of $\rho_p(\sigma_p)$ in terms of the characteristic polynomial of $\rho_{\mathbb{C}}(T_p)$, where $\rho_{\mathbb{C}}$ is the representation $\rho_{\mathbb{C}} : \mathrm{End}(A_f) \to \mathrm{End}(V_f^*)$. But $\rho_{\mathbb{C}}(T_p)$ with respect to a basis of K_f-conjugates of f is diagonal, with entries given by the eigenvalues $a_p(f_\sigma)$, which gives the relationship between the L-function of A_f and the L-functions of the conjugates of f.

When A_f is an elliptic curve (i.e. $K_f = \mathbb{Q}$), this last step can be done more simply. For elliptic curves, we have $L(A_f, s) = L(f, s)$ if and only if $a_p(A_f) = a_p(f)$ for all primes p. From Diagram (7.1), we obtain a commutative diagram

$$\begin{tikzcd}
A_f \arrow[r, "a_p(f)"] \arrow[d] & A_f \arrow[d] \\
\mathrm{Pic}^0((A_f)_p) \arrow[r, "(\sigma_p)_*+(\sigma_p)^*"] & \mathrm{Pic}^0((A_f)_p).
\end{tikzcd}$$

But $(\sigma_p)_* + (\sigma_p)^*$ on $(A_f)_p$ is equal to the multiplication by $a_p(A_f)$. Hence, we have a commutative diagram

$$\begin{tikzcd}
A_f \arrow[r, "a_p(f)-a_p(A_f)"] \arrow[d] & A_f \arrow[d] \\
\mathrm{Pic}^0((A_f)_p) \arrow[r, "0"] & \mathrm{Pic}^0((A_f)_p),
\end{tikzcd}$$

implying that $\psi = a_p(f) - a_p(E)$ does not surject on A_f. This morphism induces a morphism $\hat{\psi} : (A_f)_{\mathbb{C}} \to (A_f)_{\mathbb{C}}$. Since a morphism of curves (resp. of compact Riemann surfaces) is either constant or surjective (see [Har77, II.6.8] and [Mir95, Proposition 3.11]), we have that $\hat{\psi}$ does not surject either. By Proposition 4.10, this implies that $a_p(f) = a_p(A_f)$.

The equality at all primes results from the work of Carayol, who also proves that when A_f is an elliptic curve, its conductor is equal to N.

2. Transferring the Eichler-Shimura relation to the abelian variety

In what follows, let $p \nmid N$ be a prime number of good reduction for the abelian variety A_f. In other words, if $\mathcal{A}_f$ is the Néron model for A_f, then we suppose that the fiber $(A_f)_p = (\mathcal{A}_f)_p$ is an abelian variety (see Section 1.8).

2.1. Transfer of analytic maps to the algebraic setting

Recall that $(A_f)_{\mathbb{C}}$ is defined as a quotient of $\mathrm{Jac}(X_0(N))$ by an abelian subvariety. Let us consider the projection

$$\alpha : \mathrm{Jac}(X_0(N)) \to (A_f)_{\mathbb{C}}$$

as a morphism of compact Riemann surfaces. It is induced by the morphism $\hat{\alpha} : \mathrm{Pic}^0(X_0(N)) \to A_f$ of algebraic curves defined over $\mathbb{Q}$.

Proposition 7.2. *The morphism $\hat{\alpha}$ is surjective.*

Proof. The morphism α is clearly surjective. By Lemma 5.29, $\alpha^{-1}((A_f)_{\mathbb{C}}(\overline{\mathbb{Q}})) \subset \mathrm{Pic}^0(X_0(N))_{\mathbb{C}}(\overline{\mathbb{Q}})$, which implies that the morphism $\hat{\alpha}$ is still surjective. □

2.2. Reduction modulo p

As a morphism between abelian varieties, it follows from the properties of Néron models (see Section 1.8) that $\hat{\alpha}$ reduces mod p to induce a morphism $\hat{\alpha}_p : \mathrm{Pic}^0(X_0(N)_p) \cong \mathrm{Pic}^0(X_0(N))_p \to (A_f)_p$ and a commutative diagram

$$\begin{tikzcd}
\mathrm{Pic}^0(X_0(N)) \arrow[r, "\hat{\alpha}"] \arrow[d] & A_f \arrow[d] \\
\mathrm{Pic}^0(X_0(N)_p) \arrow[r, "\hat{\alpha}_p"] & (A_f)_p.
\end{tikzcd} \tag{7.3}$$

Similarly, the morphism $a_p(f) : A_f \to A_f$ reduces mod p to $a_p(f)_p$, giving a commutative diagram

$$\begin{tikzcd}
A_f \arrow[r, "a_p(f)"] \arrow[d] & A_f \arrow[d] \\
(A_f)_p \arrow[r, "a_p(f)_p"] & (A_f)_p.
\end{tikzcd} \tag{7.4}$$

2.3. Transferring the Eichler-Shimura relation to the abelian variety

Proposition 7.3. *The diagram*

$$\begin{tikzcd}
A_f \arrow[r, "a_p(f)"] \arrow[d] & A_f \arrow[d] \\
(A_f)_p \arrow[r, "\sigma_p+\widehat{\sigma_p}"] & (A_f)_p
\end{tikzcd}$$

commutes, where $a_p(f)_p$ is the reduction of $a_p(f)$ on $(A_f)_p$.

Proof. As in the proof of the Eichler-Shimura relation, we have a cube-shaped diagram

$$\begin{tikzcd}
 & A_f \arrow[rr, "a_p(f)"] \arrow[dd] & & A_f \arrow[dd] \\
\mathrm{Pic}^0(X_0(N)) \arrow[ur, two heads, "\hat{\alpha}"] \arrow[rr, "T_p"] \arrow[dd] & & \mathrm{Pic}^0(X_0(N)) \arrow[ur] \arrow[dd] & \\
 & (A_f)_p \arrow[rr, dashed, "\sigma_p+\widehat{\sigma_p}"] \arrow[rr, bend right, "a_p(f)_p"'] & & (A_f)_p \\
\mathrm{Pic}^0(X_0(N)_p) \arrow[ur] \arrow[rr, "(\sigma_p)_*+(\sigma_p)^*"] & & \mathrm{Pic}^0(X_0(N)_p) \arrow[ur] &
\end{tikzcd}$$

Let us note that:

- The front face commutes by the Eichler-Shimura relation (Proposition 6.21).
- The side faces are commutative Diagram (7.3).
- The bottom face with $\sigma_p + \hat{\sigma}_p$ commutes by the properties of the Frobenius.
- The top face commutes by Proposition 4.12.

- The back face with $a_p(f)_p$ is commutative Diagram (7.4).
- The map $\hat{\alpha}$ is surjective by Proposition 7.2.
- The reduction map $A_f \to (A_f)_p$ is surjective.

By Lemma 6.20, it follows that the back face with $\sigma_p + \hat{\sigma}_p$ commutes. □

3. Equality of L functions (up to finitely many factors)

We can finally prove that the L functions agree up to finitely many Euler factors:

Proposition 7.4. *We have*

$$L(A_f, s) = \prod_{\tau} L(f_\tau, s)$$

up to a finite number of Euler factors, where the product is over complex embeddings $\tau : K_f \to \mathbb{C}$. More precisely, we have $L_p(A_f, s) = \prod_\tau L_p(f_\tau, s)$ for all primes $p \nmid N$ such that A_f has good reduction at p.

Proof. Let $d = \dim A_f$ and let $p \nmid N$ be a prime of good reduction for A_f. Recall that we have compatible representations

$$\begin{aligned} \rho : \operatorname{End}(A_f) &\to M_{2d}(\mathbb{Q}_\ell) \\ \rho_p : \operatorname{End}((A_f)_p) &\to M_{2d}(\mathbb{Q}_\ell), \end{aligned}$$

where $\ell \neq p$ is any prime (see Section 1.9). Moreover, we also have compatible representations

$$\begin{aligned} \rho_{\mathbb{C}} : \operatorname{End}(A_f) \to \operatorname{End}(A_f(\mathbb{C})) &\to \operatorname{Hom}_{\mathbb{C}}(V_f^*) \cong M_d(\mathbb{C}) \\ \rho_{\mathbb{Z}} : \operatorname{End}(A_f) \to \operatorname{End}(A_f(\mathbb{C})) &\to \operatorname{Hom}_{\mathbb{Z}}(\Lambda_f) \cong M_{2d}(\mathbb{Z}) \subset M_{2d}(\mathbb{C}) \end{aligned}$$

(see Section 1.4.1). We begin to note that:

1. *$\rho_{\mathbb{Z}}$ is equivalent to $\rho_{\mathbb{C}} + \overline{\rho_{\mathbb{C}}}$.* Indeed, for $\alpha \in \operatorname{End}(A_f)$ let us denote again $\rho_{\mathbb{C}}(\alpha) \in M_d(\mathbb{C})$ the matrix of $\rho_{\mathbb{C}}(\alpha)$ with respect to any complex basis of V_f^*. Let us choose a $\mathbb{Z}$-basis $b_1, \ldots, b_{2d}$ of Λ_f which is a $\mathbb{R}$-basis of V_f^* and denote again by $\rho_{\mathbb{Z}}(\alpha) \in M_{2d}(\mathbb{R})$ the matrix of $\rho_{\mathbb{Z}}(\alpha)$ with respect to this basis. If we denote by $B \in M_{d \times 2d}(\mathbb{C})$ the transition matrix, we get that

   $$\rho_{\mathbb{C}}(\alpha) B = B \rho_{\mathbb{Z}}(\alpha).$$

   Hence, $\overline{\rho_{\mathbb{C}}}(\alpha)\overline{B} = \overline{B}\rho_{\mathbb{Z}}(\alpha)$, which implies that

   $$\begin{pmatrix} B \\ \overline{B} \end{pmatrix} \rho_{\mathbb{Z}}(\alpha) = \begin{pmatrix} \rho_{\mathbb{C}}(\alpha) & 0 \\ 0 & \overline{\rho_{\mathbb{C}}}(\alpha) \end{pmatrix} \begin{pmatrix} B \\ \overline{B} \end{pmatrix}.$$

   To conclude, it suffices then to show that $C = (B\ \overline{B})^t \in M_{2d}(\mathbb{C})$ is invertible. Suppose that there exist $\lambda_1, \ldots, \lambda_{2d} \in \mathbb{C}$ such that $\sum \lambda_i b_i = \sum \lambda_i \overline{b_i} = 0$. This implies $\sum(\lambda_i + \overline{\lambda_i}) b_i = 0$ and $\sum(i\lambda_i + \overline{i\lambda_i}) b_i = 0$, which gives $\lambda_i = 0$ for all i since b_i is a $\mathbb{R}$-basis for V_f^*.

2. *ρ is equivalent to $\rho_{\mathbb{Z}}$.* Indeed, let $\alpha \in \operatorname{End}(A_f)$ and let $n \geq 1$. By Example 1.42, $A_f(\mathbb{C})[\ell^n] \cong \Lambda_f / \ell^n \Lambda_f$ so that if we fix a $\mathbb{Z}$-basis of Λ_f as above, we get that the matrix of $\alpha_\ell : A[\ell^n] \to A[\ell^n]$ in $M_{2d}(\mathbb{Z}/\ell^n)$ is the projection of $\rho_{\mathbb{Z}}(\alpha) \in M_{2d}(\mathbb{Z})$. Passing to the limit gives the result.

3. *$\rho_p(\sigma_p)$ and $\rho_p(\hat{\sigma}_p)$ have the same characteristic polynomial.* This follows by point 4. of Theorem 1.76, since the degree is invariant by isogeny.

By Proposition 7.3, we have $(T_p)_p = \sigma_p + \hat{\sigma}_p$ on $(A_f)_p$, so that

$$\begin{aligned}(1-\rho_p(\sigma_p)X)(1-\rho_p(\hat{\sigma}_p)X) &= 1-\rho_p((T_p)_p)X + pX^2 \\ &= 1-\rho(T_p)X + pX^2.\end{aligned}$$

By the three assertions above, this implies that

$$\begin{aligned}\det(1-\rho_p(\sigma_p)X)^2 &= \det(1-\rho_{\mathbb{Z}}(T_p)X + pX^2) \\ &= \det(1-\rho_{\mathbb{C}}(T_p)X + pX^2)^2,\end{aligned}$$

whence $\det(1-\rho_p(\sigma_p)X) = \det(1-\rho_{\mathbb{C}}(T_p)X + pX^2)$. Let $\sigma_1, \ldots, \sigma_d : K_f \to \mathbb{C}$ be the complex embeddings of K_f, so that $f_{\sigma_1}, \ldots, f_{\sigma_d}$ is a basis for V_f. Since $T_p(f_{\sigma_i}) = a_p(f_{\sigma_i})f_{\sigma_i}$ by Theorem 4.5, it follows that $\rho_{\mathbb{C}}(T_p)$ with respect to this matrix is diagonal and

$$\det(1-\rho_p(\sigma_p)X) = \prod_{\tau}(1-a_p(f_\tau)X + pX^2), \tag{7.5}$$

where the product is over complex embeddings $\tau : K_f \to \mathbb{C}$. By definition of the local factors, this is implies that $L_p(A_f, s) = \prod_\tau L_p(f_\tau, s)$. □

Remark 7.5. If A_f is an elliptic curve, then the condition on p rephrases as "$p \nmid NN_{A_f}$, where N_{A_f} is the conductor of A_f.

Corollary 7.6. *We have $a_p(A_f) = \sum_\tau a_p(f_\tau)$ for all primes $p \nmid N$ such that A_f has good reduction modulo p, where the sum is over complex embeddings $\tau : K_f \to \mathbb{C}$.*

Proof. Let d be the dimension of A_f. By Theorem 1.76, $a_p(A_f)$ is equal to the coefficient of X^{2d-1} in $\det(1-\rho_p(\sigma_p)X)$. On the other hand, it is equal to $\sum_\tau a_p(f_\tau)$ by Equation (7.5). □

4. Equality at all primes

In Proposition 7.4, we had to exclude finitely many primes, corresponding the the places of bad reduction for the modular curve and the abelian variety associated to the modular form.

The equality $L_p(f, s) = L_p(A_f, s)$ at *all* primes follows from the work of Carayol [Car86][1]. If A_f is an elliptic curve (i.e. $[K_f : \mathbb{Q}] = 1$), then the conductor of A_f is equal to the level of the form.

These are hard theorems, which use more advanced tools and results, and we shall therefore stop there for now.

[1] See the *Corollaire* of *Théorème(A)* in Paragraph (0.8).

Perspectives

The following topics would naturally extend the discussions of this document:

- *Correspondences* We could have viewed Hecke operators as correspondences on modular curves. The Eichler-Shimura relation translates to an equality between correspondences. See [DI95, II.8.5] and [RS11, Chapter 12].
- *Another proof of the Eichler-Shimura relation and various generalizations:* In [Shi71], the Eichler-Shimura relation is proven using the theory of complex multiplication, along with many generalizations.
- *Unicity of A_f* We could wonder whether there exists a *unique* abelian variety whose L-function agrees with that of a given newform. Faltings' isogeny theorem asserts that two such varieties are indeed isogenous. Thus, the modularity theorem means that the Eichler-Shimura construction gives all isogeny classes of rational elliptic curves.
- *Galois representations, and generalization of the construction* By considering the Tate module of A_f as we did in the last chapter, we can associate 2-dimensional ℓ-adic Galois representations to weight-2 modular forms. Then, the Eichler-Shimura construction can be generalized to higher-weight modular forms by associating higher-dimensional representations. This was done by Deligne in 1971 and a generalization for the weight 1 was done by Deligne and Serre in 1974. An appendix by Brian Conrad in Ribet-Stein's notes on *Serre's conjecture* (2010) gives the weight-2 version of Deligne's proof.
- *Hasse-Weil conjecture for Jacobians of modular curves* In [Shi71, 7.5], the Hasse-Weil conjecture is proved for Jacobians of some modular curves by computing the L-functions explicitly as we did in the last chapter, through (generalizations of) the Eichler-Shimura relation, relating them with Dirichlet series.
- *Endomorphisms of A_f* We have seen that the Hecke algebra acts on A_f by morphisms, so that there is an injection $K_f \to \mathrm{End}_{\mathbb{Q}}(A_f)$. We could actually have shown that this is an isomorphism. Recall that $\dim A_f = \dim K_f$. By the first chapter, there is a faithful representation $\rho_{\mathbb{C}} : \mathrm{End}_{\mathbb{Q}}(A) \to M_{\dim A_f}(\mathbb{C})$. To conclude, it would have sufficed to show that there is similarly a faithful representation $\rho_{\mathbb{Q}} : \mathrm{End}_{\mathbb{Q}}(A_f) \to M_{\dim A_f}(\mathbb{Q})$, since this would show that $\dim \mathrm{End}_{\mathbb{Q}}(A_f) = \dim M_{\dim A_f}(\mathbb{Q})$.
- *Abelian varieties of the form A_f* Ribet and Serre conjectured that an abelian variety A over $\mathbb{Q}$ comes from the Eichler-Shimura construction if and only if $\mathrm{End}_{\mathbb{Q}}(A)$ is a number field of degree $\dim A$ (see also the previous point). This now follows from Serre's modularity theorem (established in 2008).
- *Numerical examples* We could consider examples of the association for modular curves of higher genera. This is done for $\Gamma_0(389)$ (whose modular curve has genus 32) in [RS11, Chapter 26].
- *Relationships between the different forms of the modularity theorem* We could have proven some of the relationships between the different formulations of the modularity theorem. See [DI95, III.13] and [DS06].

- *Relationship with distribution problems* In [Per13], we studied the Sato-Tate and Lang-Trotter conjectures. By the Eichler-Shimura construction and the modularity theorem, these questions rephrase in the setting of modular forms. We wonder whether this gives interesting ideas about these problems.
- Finally, a very interesting account of the “big picture” of the Eichler-Shimura relation is given by Kevin Buzzard’s message in [YEB].

Appendix A

Numerical examples

In this appendix, we give some examples of the association of abelian varieties to newforms in $S_2(\Gamma_0(N))$ in a simple case. Let $N \geq 1$ and let $f \in S_2(\Gamma_0(N))$ be a newform. By Proposition 4.9, the abelian variety A_f associated to f is isomorphic to the complex torus

$$V_f^*/\Lambda_f,$$

where V_f is the $\mathbb{C}$-linear span of $\{f_\sigma : \sigma : K_f \to \mathbb{C} \text{ embedding}\}$ and Λ_f is the restriction of the elements in Λ to V_f. This point of view is useful to compute explicit examples.

The simplest case is when f has rational Fourier coefficients: by Theorem 7.1, this means that A_f is an elliptic curve defined over $\mathbb{Q}$, and hence has an easy description with a Weierstrass equation. Let us suppose furthermore that $X_0(N)$ has genus 1. Since a curve of genus 1 is isomorphic to its Jacobian, we get:

Proposition A.1. *If $X_0(N)$ has genus 1, then A_f is an elliptic curve and $A_f \cong \operatorname{Pic}^0(X_0(N)) \cong X_0(N)$.*

To compute an equation for A_f in this case, we can therefore:

1. Compute the period lattice Λ of $X_0(N)$;
2. Compute invariants of the elliptic curve $\mathbb{C}/\Lambda$;
3. Determine an equation over $\mathbb{Q}$ with these invariants.

Using the theory of *modular symbols*, the homology of $X_0(N)$ can be computed very explicitly, and therefore the period lattice too. The invariants c_4, c_6 are in fact integers by a result of Edixhoven, and from there it is easy to determine an equation for the curve. Moreover, the newform in $S_2(\Gamma_0(N))$ can also be computed. Algorithms for this are developed in [Cre97].

For higher genera, we would need to compute a basis for $\Gamma_0(N)$, and then a basis for Λ_f. This is also developed in [Cre97].

The genus one cases when $N < 1000$

The integers $N \leq 1000$ with $X_0(N)$ having genus 1 are 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49. The following table gives for each of these integers the first Fourier coefficients of the newform in $S_2(\Gamma_0(N))$, an equation over $\mathbb{Z}$ for A_f, and the coefficients $a_p(A_f)$ and $a_p(f)$.

Level N	newform $f \in S_2(\Gamma_0(N))^{\text{new}}$	A_f	$a_p(A_f)$ for $p \le 7$	$a_p(f)$ for $p \le 7$
11	$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + O(q^{10})$	$y^2 + y = x^3 - x^2 - 10x - 20$	(-2, -1, 1, -2, -, 4)	(-2, -1, 1, -2, -, 4)
14	$q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 + O(q^{10})$	$y^2 + xy + y = x^3 + 4x - 6$	(-, -2, 0, -, 0, -4)	(-, -2, 0, -, 0, -4)
15	$q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 + q^9 + O(q^{10})$	$y^2 + xy + y = x^3 + x^2 - 10x - 10$	(-1, -, -, 0, -4, -2)	(-1, -, -, 0, -4, -2)
17	$q - q^2 - q^4 - 2q^5 + 4q^7 + 3q^8 - 3q^9 + O(q^{10})$	$y^2 + xy + y = x^3 - x^2 - x - 14$	(-1, 0, -2, 4, 0, -2)	(-1, 0, -2, 4, 0, -2)
19	$q - 2q^3 - 2q^4 + 3q^5 - q^7 + q^9 + O(q^{10})$	$y^2 + y = x^3 + x^2 - 9x - 15$	(0, -2, 3, -1, 3, -4)	(0, -2, 3, -1, 3, -4)
20	$q - 2q^3 - q^5 + 2q^7 + q^9 + O(q^{10})$	$y^2 = x^3 + x^2 + 4x + 4$	(-, -2, -, 2, 0, 2)	(-, -2, -, 2, 0, 2)
21	$q - q^2 + q^3 - q^4 - 2q^5 - q^6 - q^7 + 3q^8 + q^9 + O(q^{10})$	$y^2 + xy = x^3 - 4x - 1$	(-1, -, -2, -, 4, -2)	(-1, -, -2, -, 4, -2)
24	$q - q^3 - 2q^5 + q^9 + O(q^{10})$	$y^2 = x^3 - x^2 - 4x + 4$	(-, -, -2, 0, 4, -2)	(-, -, -2, 0, 4, -2)
27	$q - 2q^4 - q^7 + O(q^{10})$	$y^2 + y = x^3 - 7$	(0, -, 0, -1, 0, 5)	(0, -, 0, -1, 0, 5)
32	$q - 2q^5 - 3q^9 + O(q^{10})$	$y^2 = x^3 + 4x$	(-, 0, -2, 0, 0, 6)	(-, 0, -2, 0, 0, 6)
36	$q - 4q^7 + O(q^{10})$	$y^2 = x^3 + 1$	(-, -, 0, -4, 0, 2)	(-, -, 0, -4, 0, 2)
49	$q + q^2 - q^4 - 3q^8 - 3q^9 + O(q^{10})$	$y^2 + xy = x^3 - x^2 - 2x - 1$	(1, 0, 0, -, 4, 0)	(1, 0, 0, -, 4, 0)

This table was computed using SAGE (`sagemath.org`), which implements some of John Cremona's algorithms.

Appendix B

Modular forms

In this appendix, we briefly recall the definition and fundamental properties of modular forms, as well as the notations used, to serve as a reference in the text. Details can be found in [DS06], [Miy06] or [Lan76].

1. Weakly-modular functions

1.1. Factor of automorphy

Definition B.1. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$, the *factor of automorphy* is the function $j(\gamma, \cdot) : \mathbb{C} \to \mathbb{C}$ defined by

$$j(\gamma, z) = cz + d.$$

Lemma B.2. *The factor of automorphy has the following elementary properties for $z \in \mathbb{C}, \gamma, \gamma' \in \mathrm{GL}_2(\mathbb{C})$:*

1. $j(\gamma\gamma', z) = j(\gamma, \gamma' z) j(\gamma', z)$.
2. $j(\gamma)^{-1} = j(\gamma^{-1}, \gamma z)$.
3. $\frac{d\gamma(z)}{dz} = \det(\gamma) j(\gamma, z)^{-2}$.

1.2. Action of $\mathrm{GL}_2(\mathbb{C})^+$ on $\mathbb{C}(\mathbb{H})$

Definition B.3. For $k \in \mathbb{Z}$ an integer and $\gamma \in \mathrm{GL}_2^+(\mathbb{C})$, the *weight-$k$ operator* $[\gamma]_k$ on meromorphic functions on $\mathbb{H}$ is defined by

$$f[\gamma]_k(z) = \det(\gamma)^{k-1} j(\gamma, z)^{-k} f(\gamma z)$$

for $f \in \mathbb{C}(\mathbb{H})$ and $z \in \mathbb{H}$.

Proposition B.4. *For every integer $k \in \mathbb{Z}$, the weight-k operators give a right-action of $\mathrm{GL}_2^+(\mathbb{C})$ on $\mathbb{C}(\mathbb{H})$.*

1.3. Meromorphic modular forms

In what follows, let us fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ and $k \in \mathbb{Z}$ an integer.

Definition B.5. A fixed point of $\mathbb{C}(\mathbb{H})$ with respect to the weight-k-action of Γ is called a *weakly-modular function of weight k with respect to* Γ.

In other words, a weakly-modular function of weight k with respect to Γ is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \text{ for all } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma, \ z \in \mathbb{H}.$$

2. Meromorphic modular forms

In what follows, we fix a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ and an integer $k \in \mathbb{Z}$.

Let us consider the Riemann surface $\hat{\mathbb{H}} = \mathbb{H} \cup \{\infty\}$ with the topology given in Section 2.3.3 (which is *not* the subspace topology from the compactification $\mathbb{P}^1(\mathbb{C})$).

Definition B.6. A *meromorphic modular form of weight k with respect to* Γ is a weakly-modular function f of weight k with respect to Γ such that $f[\gamma]_k$ is meromorphic at ∞ (i.e. $f[\gamma]_k \in \mathbb{C}(\hat{\mathbb{H}})$) for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. The complex vector space of meromorphic modular forms of weight k with respect to Γ is denoted by $A_k(\Gamma)$.

Remark B.7. By Γ-invariance of f for the weight k, the second condition needs only to be checked for representatives γ_i of $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$. Since $\{[\gamma_i\infty]\}$ is the set of cusps of $X(\Gamma)$, it is often phrased as "*f is meromorphic at the cusps of $X(\Gamma)$*".

2.1. Fourier expansion

Let $f \in A_k(\Gamma)$ be a meromorphic modular form. By hypothesis, there exists an integer $M \geq 1$ such that $U = \{z \in \hat{\mathbb{H}} : \mathrm{Im}(z) > M\}$ is an open neighborhood of ∞ where f has no poles.

Since Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, there exists an integer $h \geq 1$ such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$. Hence, we have

$$f(z+h) = f(z)$$

where this is defined. Thus, the function $g : B(0, e^{-2\pi M/h}) \to \mathbb{C}$ given by $g(q) = f(\log(q)h/2\pi i)$ is well-defined and meromorphic, so that we have a power series development

$$f(z) = \sum_{n \geq -m} a_n q^n \ (q = e(z/h)) \tag{B.1}$$

valid for all $z \in U \cap \mathbb{H}$, where $a_n \in \mathbb{C}$ and $m \in \mathbb{Z}$ is an integer. We note that this is the Laurent series of f at ∞ obtained by taking the chart $e(z/h) : U \to B(0, e^{-2\pi M/h})$ near ∞.

3. Modular forms

Definition B.8. A *modular form of weight k with respect to* Γ is a meromorphic modular form of weight k with respect to Γ that is holomorphic on $\mathbb{H}$ and at the cusps. The complex vector space of modular forms of weight k with respect to Γ is denoted by $M_k(\Gamma)$.

By Section B.2.1, if $f \in M_k(\Gamma)$, there is a Fourier expansion

$$f(z) = \sum_{n \geq 0} a_n q^n \quad (q = e(z/h)) \tag{B.2}$$

valid for all $z \in \mathbb{H}$, where h is as above and $a_n \in \mathbb{C}$.

The most important property of the space of modular forms $M_k(\Gamma)$, its finite-dimensionality as a complex vector space, is explained in Chapter 2.

3.1. Cusp forms

Definition B.9. We say that a modular form $f \in M_k(\Gamma)$ *vanishes at* ∞ if $a_0 = 0$ in the Fourier series (B.2) of f. For $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, we say that f *vanishes at the cusp* $[\alpha\infty] \in X(\Gamma)$ if $f[\alpha]_k$ vanishes at ∞.

Remark B.10. Note that $f[\alpha]_k$ is weakly-modular of weight k with respect to $\alpha^{-1}\Gamma\alpha$, which is again a congruence subgroup by Proposition 2.4. The Fourier series (B.2) is not uniquely determined, but the vanishing of the first coefficient is. Moreover, if $\alpha, \beta \in \mathrm{SL}_2(\mathbb{Z})$ are such that $[\alpha\infty] = [\beta\infty] \in X(\Gamma)$, then $f[\alpha]_k$ vanishes at ∞ if and only if $f[\beta]_k$ vanishes at ∞. Hence, the definition makes sense.

Definition B.11. A *cusp form* of weight k with respect to Γ is an element of $M_k(\Gamma)$ that vanishes at all cusps. The set of cusp forms is denoted by $S_k(\Gamma)$.

3.2. L-functions

Definition B.12. The L-function associated to a modular form $f = \sum_{n\geq 0} a_n(f)q^n \in M_k(\Gamma)$ is the series

$$L(f,s) = \sum_{n\geq 0} \frac{a_n}{n^s}.$$

Proposition B.13. *If $f \in M_k(\Gamma_1(N))$, the series $L(f,s)$ converges absolutely for* $\mathrm{Re}(s) > k$. *If f is a cusp form, then $L(f,s)$ converges absolutely for* $\mathrm{Re}(s) > k/2+1$.

Proof. See [DS06, 5.9]. If f is a cusp form, the result follows by using Cauchy's integral formula and the fact that $|f(z)|\,\mathrm{Im}(z)^{k/2}$ is bounded on $\mathbb{H}$. If f is an Eisenstein series, the result follows from the explicit expressions for the Fourier coefficients. The general result follows from these two cases since a modular form is the sum of a cusp form and an Eisenstein series. □

Bibliography

[AL70] Arthur O.L. Atkin and Joseph Lehner. Hecke operators on $\gamma_0(m)$. *Mathematische Annalen*, 185(2):134–160, 1970.

[BL04] Christina Birkenhake and Herbert Lange. *Complex Abelian varieties.* Springer, Berlin New York, 2004.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models.* Springer, Berlin New York, 1990.

[Car86] Henri Carayol. Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert. *Annales scientifiques de l'École Normale Supérieure*, 19(3):409–468, 1986.

[CCP] B. Cais, Brian Conrad, and Francesco Polizzi. Quotient of abelian variety by an abelian subvariety. MathOverflow. `http://mathoverflow.net/q/37536` (version: 2010-09-02).

[Cre97] John E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge New York, 1997.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In Vijaya Kumar Murty, editor, *Seminar on Fermat's Last Theorem: 1993-1994, the Fields Institute for Research in the Mathematical Sciences, Toronto, Ontario, Canada*, volume 17 of *CMS Conference Proceedings.* American Mathematical Society, 1995.

[DS06] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms.* Graduate Texts in Mathematics. Springer, 2006.

[Fri02] Klaus Fritzsche. *From holomorphic functions to complex manifolds.* Springer, Berlin New York, 2002.

[Ful08] William Fulton. *Algebraic curves : an introduction to algebraic geometry.* Addison Wesley, Reading, MA, third edition, 2008.

[Har77] Robin Hartshorne. *Algebraic geometry.* Springer, Berlin New York, 1977.

[Igu59] Jun-Ichi Igusa. Kroneckerian model of fields of elliptic modular functions. *American Journal of Mathematics*, 81(3):pp. 561–577, 1959.

[KM85] Nicholas Katz and Barry Mazur. *Arithmetic moduli of elliptic curves.* Princeton University Press, Princeton, N.J, 1985.

[KM93] Vijaya Kumar Murty. *Introduction to Abelian varieties.* American Mathematical Society, Providence, R.I., 1993.

[Kna92] Anthony Knapp. *Elliptic curves.* Princeton University Press, Princeton, N.J, 1992.

[Lan76] Serge Lang. *Introduction to modular forms.* Springer, Berlin New York, 1976.

[Lee12] John Lee. *Introduction to Smooth Manifolds.* Springer, New York London, 2012.

[Liu06] Qing Liu. *Algebraic geometry and arithmetic curves.* Oxford University Press, Oxford, 2006.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at `www.jmilne.org/math/`.

[Mil14] James S. Milne. Fields and galois theory (v4.50), 2014. Available at `www.jmilne.org/math/`.

[Mir95] Rick Miranda. *Algebraic curves and Riemann surfaces.* American Mathematical Society, Providence, R.I, 1995.

[Miy06] Toshitsune Miyake. *Modular forms.* Springer, Berlin New York, 2006.

[Mum08] David Mumford. *Abelian varieties.* Published for the Tata Institute of Fundamental Research, distribution by the American Mathematical Society, Mumbai New Delhi, 2008.

[Mun00] James Munkres. *Topology.* Prentice Hall, Upper Saddle River, NJ, 2000.

[Per13] Corentin Perret. Répartition de frobenius et application aux courbes elliptiques. `http://sma.epfl.ch/~cperret/`, 2013.

[RS11] Kenneth Ribet and William Stein. *Lectures on Modular Forms and Hecke Operators.* 2011. `http://wstein.org/books/ribet-stein/main.pdf`.

[Sha94] Igor R. Shafarevich, editor. *Algebraic geometry I : algebraic curves, algebraic manifolds and schemes.* Springer, Berlin New York, 1994.

[Shi58] Goro Shimura. Correspondances modulaires et les fonctions ζ de courbes algébriques. *Journal of the Mathematical Society of Japan*, 10(1):1–28, 01 1958.

[Shi71] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Kanô memorial lectures. Princeton University Press, 1971.

[Sil94] Joseph Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer, Berlin New York, 1994.

[Sil09] Joseph Silverman. *The arithmetic of elliptic curves.* Springer, Berlin New York, 2009.

[tD87] Tammo tom Dieck. *Transformation groups.* W. de Gruyter, Berlin New York, 1987.

[Var84] Veeravalli S. Varadarajan. *Lie groups, Lie algebras, and their representations.* Springer, Berlin New York, 1984.

[vdGM14] Gerard van der Geer and Ben Moonen. Abelian varieties, 2014. `http://staff.science.uva.nl/~bmoonen/boek/BookAV.html`.

[vdW03] Bartel L. van der Waerden. *Algebra.* Springer, Berlin New York, 2003.

[Wer11] Kay Werndli. Elementary GAGA. Master's thesis, Universität Basel, 2011.

[YEB] Qiaochu Yuan, Matthew Emerton, and Kevin Buzzard. Intuition behind the eichler-shimura relation. MathOverflow. `http://mathoverflow.net/q/19390` (version: 2010-03-26).

[Zag08] Don Zagier. Elliptic modular forms and their applications. In Kristian Ranestad, editor, *The 1-2-3 of Modular Forms*, Universitext, pages 1–103. Springer, 2008.