MATHEMATISCHES INSTITUT DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

The Modularity Theorem and Fermat's Last Theorem

Ertl Veronika

Diplomarbeit
Betreuer: Prof. Dr. Fabien Morel
Abgabedatum: 31.07.2009

MATHEMATISCHES INSTITUT DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

The Modularity Theorem and Fermat's Last Theorem

Ertl Veronika

Diplomarbeit
Betreuer: Prof. Dr. Fabien Morel
Abgabedatum: 31.07.2009

Introduction

Motivation

The most popular DIOPHANTINE equation is perhaps the equation

$$x^n + y^n = z^n, \tag{0.1}$$

where n is a natural number. A non-trivial solution of (0.1) is a triple $(a, b, c) \in \mathbb{Z}^3$ with $abc \neq 0$, $\gcd(a, b, c) = 1$ and satisfying (0.1). It is well known that for $n = 1, 2$ there are infinitely many solutions whereas there are no non-trivial integral solutions for higher n.

Although or because it took a lot of time to prove "FERMAT's Last Theorem" the various attempts produced results which are ultimately of much greater significance for modern mathematics.

In an Oberwolfach lecture in 1985 GERHARD FREY wrote down a semistable elliptic curve coming from the equation (0.1) ([12] and [13]) with remarkable arithmetic properties so as to suspect that such a curve cannot exist appearing not to satisfy TANIYAMA's conjecture.

YUKATA TANIYAMA's conjecture to the effect that every elliptic curve over $\mathbb{Q}$ is modular was first proposed in the mid 1950s. Its statement was refined through the efforts of GORO SHIMURA and ANDRÉ WEIL; it has been known variously as WEIL's conjecture, the TANIYAMA-SHIMURA conjecture, the modularity conjecture and so on. In its usual formulation this conjecture associates objects of representation theory to objects of algebraic geometry.

FREY outlined an incomplete proof that the curve he constructed from the FERMAT equation was not modular. The missing piece – the so-called ε-conjecture – was identified by JEAN-PIERRE SERRE in [39]. In fact there was a pair of conjectures of SERRE in which KENNETH A. RIBET recognized a generalization of a problem that had occured to him while reading BARRY MAZUR's article [23]. He succeeded to prove the conjectures in 1986 (see [33] and [34]).

After the announcement that RIBET had proven "TANIYAMA $\Rightarrow$ FERMAT", the mathematical community was convinced that FERMAT's Last Theorem must be true. It turned out that they were not mistaken as ANDREW WILES with the help of RICHARD TAYLOR proved the TANIYAMA conjecture for the large class of semi-stable elliptic curves.

Abstract

This diploma thesis is arranged in two parts. The first part gives a fairly detailed introduction of the basic theory of elliptic curves, GALOIS representations and modular curves as far as it is needed to state the modularity conjecture and the theorem of RIBET and to outline the connection to FERMAT based on the idea of FREY. The aim of the second part is to prove the theorem of RIBET which is applied in the first part. It is based on his article [33] and therefore adapts most of the notation. It requires a deeper background, inter alia results of algebraic geometry, in particular about abelian varieties, of the theory of quaternion algebras and of representation theory.

The introductory part of Chapter 1 is devoted to the explicit definition of elliptic curves over arbitrary fields (later we restrict ourselves to number fields) and their normal form given by their WEIERSTRASS equation. Several results which can be found in any introductory book to elliptic curves like [45] are just stated without proof. We also introduce the group law on elliptic curves which turns them into abelian varieties. In this chapter this scheme theoretic point of view of elliptic curves is not of great importance, however, this will be the point of view which we adopt later on. Basic comments on isogenies help us to study m-division points of elliptic curves, i.e. the kernel of the map induced by multiplication by a natural number m. This is the first point when we get down to ℓ-adic representations. Next, we consider the question of what happens when reducing an elliptic curve modulo a prime. It turns out that an important class of curves, which are called semistable, are elliptic curves, whose reduction at a prime are again smooth or have only an ordinary double point.
We follow the method of FREY to construct elliptic curves arising from equations of the form $A + B + C = 0$ and show that they are of semistable reduction.
The following part turns towards ℓ-adic GALOIS representations attached to these FREY curves. We show that they are irreducible and compute their determinant as the cyclotomic character at ℓ. Studying the ramification of these representations reveals that they are finite at almost all primes.
It follows an introduction into the theory of modular curves $X_0(N)$ of level N. We study their RIEMANNIAN structure over $\mathbb{C}$ and identify their points over $\mathbb{Q}$ as pairs (E, C) of elliptic curves and cyclic subgroups. Closely related are modular forms – for the subspace of cusp forms of the space of modular forms of level N we obtain the identification $\mathcal{S}_2(N) \cong \mathrm{H}^0(X_0(N), \Omega^1)$. The space of cusp forms comes equipped with a class of endomorphisms, the HECKE operators, which help to divide $\mathcal{S}_2(N)$ into two orthogonal subspaces – old and new forms.
In Section 1.5 we state the Modularity Theorem in different variants. Variant 1.5.8, on which we focus, refers to modular representations which are shortly introduced.
To conclude the first chapter, we show that from this variant together with the theorem of RIBET stated as Theorem 1.6.1 on page 41 FERMAT's Last Theorem follows.

In Chapter 2 we recall material due to RAYNAUD concerning NÉRON models of JACOBIANS. This work is well known and has already been summarized by GROTHENDIECK [14] and MAZUR-RAPOPORT [23, Appendix].
We start with a short introduction of the concept of NÉRON models.
It follows the definition of JACOBIAN varieties via PICARD and ALBANESE functoriality which are dual to each other with the result that the JACOBIAN is autodual. We study the regular minimal model of a curve over a p-adic field of characteristic 0. The dual graph of this curve reveals results concerning the toric part of the connected component of zero of the special fiber of the NÉRON model of the JACOBIAN of the original curve. The main results establish a natural pairing of the character group of this torus and are outlined on page 48 in Theorem 2.2.9 and its corollary.
The next section transfers these results to a larger class of curves – so-called admissible curves.

In Chapter 3 we recall the work of DELIGNE-RAPOPORT [4] on the bad reduction of classical modular curves.
Starting from the description of points of modular curves as paires (E, C) of enhanced elliptic curves introduced in Chapter 1, we link them with certain (EICHLER) orders of quaternion algebras. We discover that the set of supersingular points of a modular curve at a prime q is a coset space of the adelization of a quaternion algebra (3.1.14). We relate the endomorphism ring of enhanced and non-enhanced elliptic curves to maximal orders and EICHLER orders of quaternion algebras.
We combine these results with the results of Chapter 2 to obtain information about the NÉRON models of the JACOBIANS $J_0(N)$ of these curves. Thereto, we give a purely algebraic definition of HECKE correspondences on modular curves and see that this definition is compatible with the complex analytic approach given in Chapter 1. We study the HECKE action on the torus and its

character group attached to the mentioned Néron models. The examination of the reduction at a prime p dividing the modular level is explained rather detailed.
A crucial point is that the associated component groups are Eisenstein in the sense of [23] (cf. Theorem 3.2.14 on page 68) If we take two different primes p and q and consider the reduction at each of them, the situation becomes more complicated but provides results that enables us to switch later between two primes in appropriate situations. One of the main points of this comparison is to connect the q-old and the p-new action of the Hecke algebra in Theorem 3.3.10 (p. 75).

In Chapter 4 we derive similar results on the bad reduction of Shimura curves and combine them again with the results of Chapter 2. Starting with the definition of Shimura curves, we mention [17, Theorem 4.3] of Cerednik-Drinfeld which enabels us to carry over the results derived with help of the dual graph of an admissible curve and to establish an analogy between modular curves and Shimura curves.
Especially, we derive a geometric result which mirrors a special case of the well-known correspondence between modular forms on $\mathbf{GL}_2$ and modular forms on the multiplicative group of a quaternion algebra. To establish this correspondence, we use again Eichler orders of quaternion algebras (see Lemma 4.2.10 and Proposition 4.2.11).
Shimura curves supports also Hecke correspondences. These induce an action on the character group Z of the connected component of zero in the fiber over $\mathbb{F}_p$ of the Néron model of the Jacobian. The main result of this section, Theorem 4.3.1 on page 91, connects the Hecke module Z with an analogous module derived from the Jacobian $J_0(pqM)_{\mathbb{F}_q}$ of the modular curve. The switch between p and q enriches the analogy and turns out to be quite useful – it allows us to permute p and q in situations where the connections of the two Jacobians is strong enough.

The first part of Chapter 5 is purely technical and discusses relations between maximal ideals of Hecke algebras and representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. At the beginning, we mention well known theorems concerning Galois representations such as the Čebotarev Density Theorem. We also state results on restricted ramification [32, 3.3]. In the next step, we define modular representations and show their existence and uniqueness (cf. Theorem 5.1.12). They are determined by their trace and determinant. Their level is that of the attached Hecke algebra. The idea developed in Theorem 5.1.16 is to show that the attached Galois module which is a vector space over a residue field of a maximal ideal of a Hecke algebra is contained in the kernel of this ideal in the Jacobian $J_0(N)$.
The last sections contain arguments leading to the main theorem. We begin with a theorem of Mazur. It is similar to the theorem of Ribet in a more restricted context and concerns irreducible modular representations, which are finite at a prime p. The mentioned restrictions are that the residue characteristic ℓ of the attached maximal Hecke ideal is odd and satisfies $p \not\equiv 1(\mathrm{mod}\,\ell)$. It states that, if the representation is modular of level Mp, it is modular of level M. The proof makes only use of results of Chapter 3 and is independent of Chapter 4.
We study now how to change the level in a more general case. Since $p \equiv 1(\mathrm{mod}\,\ell)$ certainly does not hold if $p = \ell$, we are now able to assume that p and ℓ are distinct. We show in Proposition 5.3.2, p.109, that there is no problem in raising the modular level. We introduce an auxiliary prime q assuming that the representation ρ arises from a newform of level dividing $N = Mp$. Further, we prove that there are infinitely many primes $q \equiv -1(\mathrm{mod}\,\ell)$ such that ρ comes from a newform whose level devides pqM and is divisible by pq. In fact this is the case when q is prime to ℓN and the image under ρ of the according Frobenius element has eigenvalues ±1. The existence of infinitely many such primes is induced by the Čebotarev Density Theorem as explained in Lemma 5.3.3 and the proof of this assertion strongly uses the correspondence between Shimura curves and modular curves established in Chapter 4 (see Theorem 5.3.6). In the last section we finally prove the main theorem. With the auxiliary prime q, we show that, if ρ is modular of level pqM, under the assumptions of the main theorem it is modular of level qM. Now we can show that the level-pM representation ρ is modular of level M under the assumptions by first raising the level and then interchanging p and q via the theory of Chapter 4.

Acknowledgements

I am grateful to Prof. Dr. Fabien Morel, who acted as my supervisor for this diploma thesis, for useful discussions and helpful suggestions. I would like to thank Thomas Weber and Alexander Niske for agreeing to read my work and Lukas-Fabian Moser, Katharina Halbhuber and Holger Schrödl for useful hints and inspiring professional and non-professional discussions. Also, I would like to express my gratitude to the various authors whose names appear in the reference section of my work and whose works and ideas I have used, in particular to Kenneth A. Ribet, who kindly agreed to answer questions by email. Lastly I would like to thank all those, who had patience with me during the last months, in particular my parents.

Contents

Chapter 1

FERMAT's Last Theorem and Elliptic Curves

1.1 Preliminaries on Elliptic Curves

1.1.1 Introduction and Definition

In a certain way, it is natural to study elliptic curves, since they are as curves of genus 1 the first examples of abelian varieties. Furthermore their points of finite order give non-trivial examples of étale cohomology groups.

Definition 1.1.1. An *elliptic curve* is a pair $(E, \mathcal{O})$, where E is an irreducible smooth (or non-singular) projective curve of genus 1 and $\mathcal{O}$ is a distinguished point on E called the origin.The curve is defined over a field K if E is defined over K and $\mathcal{O}$ is in $E(K)$, that means it is a K-rational point of E.

By misuse of notation we often write E instead of $(E, \mathcal{O})$.
In the following we list some notions and properties concerning elliptic curves over arbitrary fields, over $\mathbb{Q}$ and over number fields respectively.

1.1.2 WEIERSTRASS Models

Let E be an elliptic curve over K as defined above. By the theorem of RIEMANN-ROCH there exist plane projective cubics which are models for E, such that $\mathcal{O}$ is the only point at infinity of E. The corresponding equations can be chosen in normal form as follows:

Definition 1.1.2. The *generalized* WEIERSTRASS *Normal Form* is given projectively by

$$y^2z + a_1xyz + a_3yz^2 \quad = \quad x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{1.1}$$

with coefficients in K.

It is known that the only $\overline{K}$-rational point at the line at infinity $[0:1:0]$ is easily seen to be non-singular. Since the behaviour at this point is so well understood it is often sufficient to use the affine form of the curve

$$y^2 + a_1xy + a_3y \quad = \quad x^3 + a_2x^2 + a_4x + a_6, \tag{1.2}$$

which has the advantage that the notation is easier to handle.

Theorem 1.1.3. *A pair $(E, \mathcal{O})$ is an elliptic curve defined over a field K if and only if E can be given by a non-singular* WEIERSTRASS *equation over K where $\mathcal{O}$ is taken as the usual point at infinity.*

PROOF: You find a scetch of the proof in [20, p.362]. □

Consider the following standard notations:

Notation 1.1.4.

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2, \\ b_4 &:= 2a_4 + a_1a_3, \\ b_6 &:= a_3^2 + 4a_6, \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

and

$$\begin{aligned} c_4 &:= b_2^2 - 24b_4, \\ c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Under assumption that $\mathrm{char}(K) \neq 2$ or 3 there exist two biregular transformations simplifying the original WEIERSTRASS equation. Replacing $y + \frac{1}{2}(a_1x + a_3)$ by $\frac{1}{2}y$ gives back

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{1.3}$$

Again changing in this equation x to $\frac{x-3b_2}{36}$ and y to $\frac{y}{108}$ results in

$$y^2 = x^3 - 27c_4x - 54c_6, \tag{1.4}$$

whith b_2, b_4, b_6, c_4 and c_6 as in (1.1.4). An elliptic curve given in this form is said to be given in WEIERSTRASS *Normal Form*.

It is evident by definition that for elliptic curves over $K = \mathbb{Q}$ these changes of variables are defined over $\mathbb{Z}[\frac{1}{2}]$ and $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}]$ respectively. Although our main interest will be in elliptic curves over $\mathbb{Q}$ it is not enough to consider these simplified WEIERSTRASS equations. The reason lies in the beaviour of such a curve under reduction modulo a prime p which we will study later.

The WEIERTRASS Normal Form is very convenient to define certain quantities and invariants of an elliptic curve.

Definition 1.1.5. Let $\mathrm{char}(K) \neq 2, 3$. The *discriminant* of the WEIERSTRASS equation is defined by

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

The quantity

$$j := c_4^3/\Delta$$

is called the *j-invariant* of the elliptic curve E, and

$$\omega := dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y)$$

is the *invariant differential* associated to the WEIERSTRASS equation.

Remark 1.1.6. For arbitrary characteristic see [45, Appendix A].

The most general transformations which preserve a Weierstrass Normal Form, so-called *Admissible Changes of Variables* are of the form

$$x = u^2\tilde{x} + r \qquad \text{and} \qquad y = u^3\tilde{y} + su^2\tilde{x} + t \tag{1.5}$$

with u, r, s, t in K and $u \neq 0$, fixing $[0:1:0]$ and carrying the tangent line $z = 0$ to itself.

The j-invariant is also called *absolute invariant* as it is stable under admissible changes and therefore independent of the chosen equation. Furthermore, E is determined by the j-invariant in the following sense:

Theorem 1.1.7. *Two elliptic curves are isomorphic (over $\overline{K}$) if and only if they have the same j-invariant.*

Proof: Two elliptic curves are isomorphic if and only if one can deduce one equation from the other by an admissible change of variables. Thus one can show the claim by relatively simple calculations. See [45, III,Proposition 1.4.(b)]. □

1.1.3 The Group Law

It is essential to view E as a commutative algebraic group. Consider E as projective curve in $\mathbb{P}^2$ and let L be a line in $\mathbb{P}^2$. Then by Bezout's theorem [15, I.7.8] L intersects E at exactly three points (which may not be distinct). Define a composition law on E by the following rule.

Definition 1.1.8. Let P, $Q \in E$, L the line connecting these points (respectively the tangent line if $P = Q$), and R the third point of the intersection of E and L. Further let L' be the line connecting R and $\mathcal{O}$. Then $P + Q$ is the third point of intersection of L' with E.

Straight computations as in [45, III Proposition 2.2] give the following result.

Proposition 1.1.9. *The composition law defined above has the following properties:*

1. *$P + \mathcal{O} = P$ for all $P \in E$.*
2. *$P + Q = Q + P$ for all P, $Q \in E$.*
3. *Let $P \in E$. There is a unique point of E denoted by $-P$ such that $P + (-P) = \mathcal{O}$.*
4. *Let P, Q, $R \in E$. Then $(P + Q) + R = P + (Q + R)$.*

In other words, E form an abelian group with identity $\mathcal{O}$. Furthermore:

5. *Three distinct points sum to $\mathcal{O}$ if and only if they are collinear.*
6. *Suppose E is defined over K. Then $E(K)$ is a subgroup of E.*

Notation 1.1.10. For $m \in \mathbb{Z}$ and $P \in E$ let

$$\begin{aligned} [m]P &:= \underbrace{P + \cdots + P}_{m \text{ times}} \qquad \text{for} \quad m > 0, \\ [0]P &:= \mathcal{O}, \\ [m]P &:= [-m](-P) \qquad \text{for} \quad m < 0. \end{aligned}$$

The computation of explicit formulas is left to the interested reader.

1.1.4 Isogenies

In order to make statements about the TATE module and GALOIS representations, it is adjuvant to repeat general facts about maps between elliptic curves.

Definition 1.1.11. Let E_1 and E_2 be elliptic curves. An *isogeny* between E_1 and E_2 is a morphism

$$\varphi : E_1 \to E_2$$

in the sense of HARTSHORNE'S Algebraic Geometry [15] satisfying in addition $\varphi(\mathcal{O}) = \mathcal{O}$. Two elliptic curves are *isogenous* if there exists a non-trivial isogeny between them.

From [15, II.6.10] it is evident that an isogeny is either surjective and finite or constant. In this case it is the zero isogeny defined by $[0]P = \mathcal{O}$ for all $P \in E_1$. Hence we obtain the usual injection of function fields (ibid.)

$$\varphi^* : \overline{K}(E_2) \to \overline{K}(E_1),$$

and the degree (resp. seperable and inseperable degree) of φ is the according degree of the finite field extension $\overline{K}(E_1)/\varphi^*\overline{K}(E_2)$. By convention we set $\deg[0] = 0$. Using properties of the corresponding PICARD groups and the induced morphism between their degree zero parts, one can show that isogenies are even group homomorphisms [45, III.Prop.4.8].

The set of isogenies between two elliptic curves, denoted by $\mathrm{Hom}(E_1, E_2)$, is a group under pointwise addition. Moreover, if $E_1 = E_2 = E$ we get the so-called *endomorphism ring of* E, where multiplication is given by composition. The invertible elements form the *automorphism group of* E. If the considered elliptic curves are defined over a field K, we can denote this by an index as usual. The group of isogenies is a torsion-free $\mathbb{Z}$-module ([45, III.Prop.4.2]). There are some distinguished isogenies.

Examples 1.1.12. For each integer we can define an isogeny $[m] : E \to E$ in the natural way, the *multiplication-by-m-map* which is non-constant for $m \neq 0$.

In characteristic $p > 0$, for any polynomial $f \in K[X]$ let $f^{(q)}$ be the polynomial obtained by raising each coefficient to the q^{th} power where $q = p^r$. Then for an elliptic curve E given by a homogenious polynomial f in $K[X, Y, Z]$ we can define a new curve $E^{(q)}$ by $f^{(q)}$. Further, there is a natural map

$$\Phi : E \to E^{(q)} \quad , \quad \Phi([x : y : z]) = [x^q : y^q : z^q].$$

Φ indeed maps E to $E^{(q)}$, for, if $P = [x : y : z] \in E$, we have

$$\begin{aligned} f^{(q)}(\Phi(P)) &= f^{(q)}(x^q : y^q : z^q) \\ &= (f(x : y : z))^q \qquad \text{since} \quad \mathrm{char}(K) = p \\ &= 0 \qquad \text{since} \quad f(P) = 0. \end{aligned}$$

Over a field of characteristic $p > 0$ every isogeny between two elliptic curves factors into the q^{th}-power *Frobenius map* and a separable part.

Theorem and Definition 1.1.13. *Let $\varphi : E_1 \to E_2$ be a non-constant isogeny of degree m. There exists a unique isogeny, called the dual isogeny*

$$\widehat{\varphi} : E_2 \to E_1$$

satisfying

$$\widehat{\varphi} \circ \varphi = [m].$$

It has the following properties:

1. $\widehat{\varphi} \circ \varphi = [m]$ *on* E_1 *and* $\varphi \circ \widehat{\varphi} = [m]$ *on* E_2.
2. *For a second isogeny* $\lambda : E_2 \to E_3$ *one has* $\widehat{\lambda \circ \varphi} = \widehat{\varphi} \circ \hat{\lambda}$.
3. *Let* $\psi : E_1 \to E_2$ *another isogeny. Then* $\widehat{\varphi + \psi} = \hat{\varphi} + \widehat{\psi}$.
4. $\deg \widehat{\varphi} = \deg \varphi$.
5. $\widehat{\widehat{\varphi}} = \varphi$.
6. *For all integers* m, $\widehat{[m]} = [m]$ *and* $\deg[m] = m^2$.

Proof: For existence and uniqness of the dual isogenie see [45, III.Theorem 6.1]. The properties follow quite easy by direct computations [45, III.Theorem 6.2]. □

1.1.5 m-division Points

For an arbitrary elliptic curve the only isogenies which are immediate are the multiplication-by-m-maps, which provide a powerful tool to study elliptic curves.

Definition 1.1.14. Let E be an elliptic curve and $m \neq 0$ an integer. The *m-torsion subgroup of* E is the set of points of order dividing m in E,

$$E[m] = \{P \in E \mid [m]P = \mathcal{O}\}.$$

The *torsion subgroup of* E is the set of points of finite order, that is the following union of subgroups:

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m].$$

$E_{\text{tors}}(K)$ denotes the points of finite order in $E(K)$.

The following proposition is a consequence of basic facts shown in [45, III.6.4].

Proposition 1.1.15. *Let* E *be an elliptic curve and* $m \neq 0$ *an integer.*

1. $\deg[m] = m^2$.
2. *If* $\operatorname{char}(K) = 0$ *or if* m *is prime to* $\operatorname{char}(K)$, *then* $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.
3. *If* $\operatorname{char}(K) = p$, *then* $E[p^e] \cong 0$ *for all* $e \in \mathbb{N}$ *or* $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ *for all* $e \in \mathbb{N}$.

This shows that in the first case (the isomorphism being one between abstract groups) $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2 and in particular has order m^2. The points of $E[m]$ over K are those whose coordinates satisfy certain algebraic equations with rational (over K) coefficients, depending on the defining (Weierstrass) equation of E. However, the group $E[m]$ comes equiped with considerably more structure.

Remark 1.1.16. According to Weierstrass Theory (see e.g. [16, Chapter 9] or [20, VI.]) it is often convenient to describe E over $\mathbb{C}$ as a torus $\mathbb{C}/\Lambda$ where

$$\Lambda = \left\{ \int_\gamma \omega \;\middle|\; \gamma \in H_1(E(\mathbb{C}), \mathbb{Z}) \right\}$$

is a lattice attached to an appropriate nonzero holomorphic differential ω on E and the homology group is the abelian group of smooth closed paths on the complex points of E and isomorphic to $\mathbb{Z} \times \mathbb{Z}$. This is another way to see the equivalencies of the previous proposition over $\mathbb{C}$. Indeed, there is an isomorphism $E[m] \cong \frac{1}{m}L/L$ and L is free of rank 2 over $\mathbb{Z}$.

We are about to establish an additional structure on $E[m]$ over a field K (which will later be $\mathbb{Q}$ or a number field). Let σ be an element of the Galois group $\mathrm{Gal}(K_s/K)$. If $[m]P = \mathcal{O}$ then $[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}$ because conjugation is compatible with the addition law on E (that is given by formulas with coefficients in K). Hence this Galois group acts on the m-division points and we therefore obtain a representation

$$\rho_m : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]), \tag{1.6}$$

and the choice of a basis furnishes an isomorphism $\mathrm{Aut}(E[m]) \cong \mathbf{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Remark 1.1.17. In the case $K = \mathbb{Q}$ the kernel H_m of ρ_m is an open normal subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let K_m be its fixed field which is a finite Galois extension of $\mathbb{Q}$ as $E[m]$ is finite and H_m normal. Concretely, K_m is the extension of $\mathbb{Q}$ by adjoining the coordinates of all points of $E[m]$. This means that

$$\mathrm{Gal}(K_m/\mathbb{Q}) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\operatorname{Ker}\rho_m \cong \operatorname{Im}\rho_m \subseteq \mathbf{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

and so we obtain subgroups of $\mathbf{GL}_2(\mathbb{Z}/m\mathbb{Z})$ as Galois groups.

Individually, i.e. for each m, these representations are not completely satisfactory because it is in general easier to deal with matrices with coefficients in a ring of characteristic zero. So we want, as it is ususal, to adapt an idea of TATE and fit them together for varying m.

Definition 1.1.18. Let ℓ be a prime $\neq \mathrm{char}(K)$. The *ℓ-adic* TATE *module of E* is the group

$$T_\ell(E) := \lim_{\infty \leftarrow n} E[\ell^n],$$

where we take the inverse limit with respect to the multiplication-by-ℓ-map.
Conversely, the TATE *co-module* is the ℓ-divisible group

$$\Phi_\ell(E) := \lim_{n\to\infty} E[\ell^n] = \bigcup_{n=1}^{\infty} E[\ell^n] =: E[\ell^\infty],$$

the direct limit taken with respect to the natural inclusion.

The earlier considerations show immediately that $T_\ell(E)$ has a natural structure as $\mathbb{Z}_\ell$-module, the inverse limit topology induced by $\mathbb{Z}_\ell$. Furthermore, Proposition 1.1.15 establishes the following structure:

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell \qquad \text{if } \ell \neq \mathrm{char}(K), \tag{1.7}$$

$$T_p(E) \cong \{0\} \text{ or } \mathbb{Z}_p \qquad \text{if } p = \mathrm{char}(K). \tag{1.8}$$

The action of the pro-finite Galois group $\mathrm{Gal}(K_s/K)$ on each $E[\ell]$ commuting with the multiplication-by-ℓ-maps gives a continuous action on $T_\ell(E)$.

Definition 1.1.19. The *ℓ-adic representation of* $\mathrm{Gal}(K_s/K)$ *on* E, also denoted by ρ_ℓ is the induced map

$$\rho_\ell : \mathrm{Gal}(K_s/K) \to \mathrm{Aut}(T_\ell(E)). \tag{1.9}$$

Remark 1.1.20. In general, the number ℓ refers to a prime different from the characteristic of the field, whereas p refers to the characteristic of the field if applicable.

1.1.6 The Concept of Semistability

An important concept in this context is stability – rather semistability. As a matter of fact, it was sufficient to prove the TANIYAMA-SHIMURA-WEIL conjecture for semistable elliptic curves to prove FERMAT's Last Theorem. The restriction on semistable elliptic curves turned out to be an effective one.

In the following, let K be a number field, $\mathcal{O}_K$ its ring of integers, which is a DEDEKIND domain, and $k_{\mathfrak{P}}$ the residue field with respect to a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$.
It is easy to see that for an elliptic curve defined over K one always finds a cubic equation in normal form with all coefficients a_i in $\mathcal{O}_K$. Indeed, choose any normal form over K. Let u be a common denominator for all a_i, i.e. $ua_i \in \mathcal{O}_K$ and make the change of variables $x \to u^2x$, $y \to u^3y$, which means for the coefficients $a_i \to u^ia_i \in \mathcal{O}_K$ for all i. Moreover, there exists a best possible equation for E, its *minimal* WEIERSTRASS *model.*

Definition 1.1.21. A WEIERSTRASS equation is called *minimal for a prime number p* if the corresponding valuation ν_p of its discriminant cannot be decreased by an admissible change of variables (see (1.5)) at which the coefficients must stay p-integral.
The equation is called *global minimal* WEIERSTRASS *equation* if it is minimal for all primes p and if the coefficients are integers.

A theorem of NÉRON considers existence and uniqueness questions for these notions [20, X.Theorem 10.3]:

Theorem 1.1.22. *For an elliptic curve E/K there exists an admissible change of variables such that the resulting equation is a global minimal* WEIERSTRASS *equation. It is unique up to an admissible change of variables with $u = \pm 1$ and r, s, t in $\mathcal{O}_K$.*

Now we can come to reduction theory.

Definition 1.1.23. Let E be given in minimal normal form (1.1.2). The reduction of E modulo a prime ideal $\mathfrak{P}$ is

$$E_{\mathfrak{P}}: \quad y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6. \tag{1.10}$$

It is a plane cubic curve over $k_{\mathfrak{P}}$.

One studies the behaviour of E under reduction. There are three possibilities for its projective closure:

1. **Good reduction case**: This best possible case appears if $E_{\mathfrak{P}}$ is again an elliptic curve, that is, it has no singular points. In case that $2, 3 \notin \mathfrak{P}$, E has good reduction if and only if $\nu_{\mathfrak{P}}(\Delta) = 0$.

2. **Multiplicative case**: One says that E is of *multiplicative type* modulo $\mathfrak{P}$ if $E_{\mathfrak{P}}$ has a singularity with two different tangent lines, a so-called *node.* Provided $2, 3 \notin \mathfrak{P}$, E has multiplicative reduction with respect to $\mathfrak{P}$ if and only if $\nu_{\mathfrak{P}}(\Delta) > 0$ and $\nu_{\mathfrak{P}}(c_4) = 0$ (c.f. Notation 1.1.4).

3. **Additive case**: Finally E is of *additive type* modulo $\mathfrak{P}$ if $E_{\mathfrak{P}}$ has a singularity with only one tangent line through this point. This is called a *cusp.* Again in the case when $2, 3 \notin \mathfrak{P}$, this is the case if and only if $\nu_{\mathfrak{P}}(\Delta) > 0$ and $\nu_{\mathfrak{P}}(c_4) > 0$

Indeed, a cubic curve is singular if and only if its discriminant is zero [20, III.Theorem 3.2]. So if E is not singular, $\Delta \neq 0$ and $E_{\mathfrak{P}}$ is not singular if and only if Δ is not zero modulo $\mathfrak{P}$ and this is the case if and only if $\nu_{\mathfrak{P}}(\Delta) = 0$. In [45, III.Proposition 1.4] SILVERMAN specifies that a WEIERSTRASS cubic can only have one singularity and that the two types of singularities can be distinguished by the fact whether c_4 is zero or not.

Remark 1.1.24. The notion *multiplicative type* respectively *additive type* derives from the fact that the non-singular points of $E_{\mathfrak{P}}$ over the algebraic closure of $k_{\mathfrak{P}}$ are (as algebraic groups) isomorphic to the multiplicative group $\overline{k}_{\mathfrak{P}}^{*}$ and the additive group $\overline{k}_{\mathfrak{P}}^{+}$ respectively.

Definition 1.1.25. An elliptic curve E over a number field K is said to be *semistable* if for every prime $\mathfrak{P}$ it has either good or multiplicative reduction. It is *stable* if for every prime $\mathfrak{P}$ it has good reduction.

A non-zero integer associated to a curve E over K is its *minimal discriminant* Δ_E which is, roughly speaking, the discriminant of the minimal WEIERSTRASS equation for E. An analogues definition gives the minimal discriminant in terms of an integral ideal of K by

$$\mathcal{D}_{E/K} = \prod_{\nu \in M_K^0} \mathfrak{P}^{\nu(\Delta_E)},$$

where the product runs over all non-archimedian valuations of K.

Definition 1.1.26. The *(geometric) conductor of* E is defined by

$$N := \prod_{p|\Delta_E} p^{f_p},$$

where f_p is an integer which measures the badness of the reduction of E at p and is invariant under isogeny. f_p is zero for good reduction and 1 for multiplicative reduction. For additive reduction we have $f_p = 2 + \delta_p$ where $\delta_p \geq 0$ is a measure of wild ramification (cf. [31]).

To say that E is semistable is equivalent to say that its conductor is squarefree. It has then the form $N = \prod_{\nu_p(\Delta_E)>0} p$.

Now let $\mathfrak{P}$ be a prime of good reduction and q the cardinality of $k_{\mathfrak{P}}$. Recall that $q+1$ is the number of points on the projective line $\mathbb{P}^1$ over $k_{\mathfrak{P}}$. It is of interest to consider the difference

$$a_{\mathfrak{P}}(E) \quad = \quad q + 1 - \# E_{\mathfrak{P}}(k_{\mathfrak{P}}), \tag{1.11}$$

of the number of points on the projective line and of the number of rational points of the reduced curve over the appropriate field. In the case of $K = \mathbb{Q}$ this is denoted as

$$a_p(E) = p + 1 - \#E_p(\mathbb{F}_p).$$

This number will play an important role for the formulation of the TANIYAMA-SHIMURA-WEIL conjecture.

Among other things it helps us to define the L-function of an elliptic curve.

Definition 1.1.27. The *local L factor* of E for the prime p is the formal power series over $\mathbb{Q}$ given by

$$L_p(u) = \begin{cases} \frac{1}{1-a_p u + p u^2} & \text{if } p \nmid \Delta_E, \\ \frac{1}{1-a_p u} & \text{if } p|\Delta_E \end{cases}.$$

The *L function* of E is the product of the local L factors with $u = p^{-s}$ in the p^{th} factor:

$$L(s, E) \quad = \quad \prod_{p|\Delta_E} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}. \tag{1.12}$$

It is well known that the EULER product defining $L(s, E)$ converges for complex numbers s such that $\Re(s) > 2$ and is then given by an absolutely convergent DIRICHLET series.

1.2 Elliptic Curves Arising from Equations $A+B+C=0$

Now we follow an idea of FREY to construct semistable elliptic curves over $\mathbb{Q}$. To start let A and B be relatively prime integers with the additional conditions that

$$A \equiv 3 \mod 2^2 \qquad \text{and} \qquad B \equiv 0 \mod 2^5 \tag{1.13}$$

and set $C := -A-B$. We will see later why in our case these assumptions don't restrict generality. Now consider the curve

$$E_{A,B,C} : y^2 = x(x-A)(x+B) = x^3 - (A-B)x^2 - ABx \tag{1.14}$$

respectively its homogenuous equivalent $y^2z = x^3 - (A-B)x^2z - ABxz^2$.

As we have seen $E_{A,B,C}[2] \cong (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/2\,\mathbb{Z})$ and therefore there are three points of order 2 (besides $\mathcal{O}$):

$$P_0 = (0,0)\,,\; P_1 = (A,0)\,,\; P_2 = (-B,0)$$

(indeed $2P = 0$ if and only if $P = -P$; that means for a general WEIERSTRASS equation according to [45, III.Group Law Algorithm 2.3] $(x,y) = (x, -y - a_1x - a_3)$; in case of (1.14) $a_1 = a_3 = 0$, so $(x,y) = (x,-y)$ and we have to solve the equation $0 = x(x-A)(x+B)$).

We have the following constants for (1.14):

$$\begin{aligned}
a_1 &= a_3 = a_6 = 0\\
a_2 &= -(A_B)\\
a_4 &= -AB\\
b_2 &= -4(A-B)\\
b_4 &= -2AB\\
b_6 &= 0\\
b_8 &= -A^2B^2\\
c_4 &= 16(A^2+B^2+AB)\\
\Delta &= 2^4A^2B^2C^2\\
j &= \frac{2^8(C^2-AB)^3}{A^2B^2C^2}
\end{aligned} \tag{1.15}$$

Now we want to study the stability properties of the curve. There are three cases to be considered: $\ell \neq 2$ or 3, $\ell = 2$ and $\ell = 3$.

Let us start with $\ell \neq 2, 3$. Assume $\ell \nmid \Delta$ that is $\ell \nmid ABC$. Then by Section 1.1.6 $E_{A,B,C}$ has good reduction with respect to ℓ. Conversely if $\ell | \Delta$, i.e. $\ell | ABC$, ℓ doesn't divide $A^2+B^2+AB = c^2 - AB$ since A, B and C are relatively prime, so ℓ doesn't divide c_4 and again by (1.1.6) $E_{A,B,C}$ has reduction of multiplicative type at ℓ.

Next let $\ell = 3$. If $3 \nmid ABC$ we have in particular

$$A,\, B,\, C \not\equiv 0 \mod 3 \quad \text{and} \quad A \not\equiv -B \mod 3.$$

The reduction of $E_{A,B,C}$ at 3 has a singular point $P = (x_P, y_P)$ if and only if

$$\frac{\partial f}{\partial y}(P) = 2y_P \equiv 0 \quad \text{and} \quad \frac{\partial f}{\partial x}(P) = -3x_P^2 + 2(A-B)x_P + AB \equiv 0.$$

This is equivalent to say $y_P = 0$ and x_P is a multiple root of $x(x-\overline{A})(x+\overline{B})$ modulo 3 in contradiction to $A \not\equiv -B \mod 3$. Hence $E_{A,B,C}$ has good reduction at 3 .
If $3|ABC$ direct computations show that $E_{A,B,C}$ has multiplicative reduction at 3:
Firstly, let 3 be a divisor of A and $B \equiv 1 \mod 3$, so the resulting equation is

$$y^2 = x^2(x+\overline{1}) = x^3 + x^2,$$

which has a singular point at $P = (\overline{0}, \overline{0})$ and this is an ordinary double point, that means it has two distinct tangent lines rational over $\mathbb{F}_3$, since

$$y^2 - x^2 - x^3 = y^2 + 2x^2 - x^3 = (y + x)(y + 2x) - x^3 = (y + \alpha x)(y + \beta x) - x^3,$$

with $\alpha \neq \beta$.
Secondly, let 3 be a divisor of A and $B \equiv 2 \mod 3$. The resulting equation is

$$y^2 = x^2(x + \overline{2}) = x^3 + 2x^2,$$

which again has the singular point $P = (\overline{0}, \overline{0})$. Because

$$y^2 - 2x^2 - x^3 = y^2 + x^2 - x^3 = (y + \alpha x)(x + \beta x) - x^3,$$

over a finite extension of $\mathbb{F}_3$, where $\alpha \neq \beta$, given that $\alpha + \beta = 0$ and $\alpha\beta = 1$, P has distint tangent lines albeit they are not rational over $\mathbb{F}_3$.
The case $3|B$ can be treated similarly up to change of signs and the case $3|C$ up to a linear change of variables.

Last we enlighten the reduction modulo 2. The curve is given by the equation $y^2 = x^3 + x^2$ over $\mathbb{F}_2$. Its rational points are $(\overline{0}, \overline{0})$ and $(\overline{1}, \overline{0})$. Since $\frac{\partial f}{\partial x} = x^2$ and $\frac{\partial f}{\partial y} = \overline{0}$ there is one singularity at $(\overline{0}, \overline{0})$ and this is a node. Thereto one considers the admissible change of variables

$$x = 4X \quad \text{and} \quad y = 8Y + 4X$$

of the original equation over $\mathbb{Q}$ which results in

$$Y^2 + XY \quad = \quad X^3 + \frac{B - 1 - A}{4} X^2 - \frac{AB}{16}, \tag{1.16}$$

whose reduction modulo 2 is

$$Y^2 + XY = X^3 \quad \text{if} \quad A \equiv 7 \mod 8$$

(as then $8|B - 1 - A$, i.e. $2|\frac{B-1-A}{4}$) and

$$Y^2 + XY = X^3 + X^2 \quad \text{if} \quad A \equiv 3 \mod 8$$

(as then $2 \nmid \frac{B-1-A}{4}$). In both cases one obtains a cubic over $\mathbb{F}_2$ with double point $P = (\overline{0}, \overline{0})$ with distinct tangent lines. In the first case these tangent lines are rational over $\mathbb{F}_2$ given that

$$Y^2 + XY + X^3 = (Y + \overline{0}X)(Y + \overline{1}X) + X^3 = (Y + \alpha X)(Y + \beta X) + X^3.$$

In the second case the tangent lines are only rational over a finite extension of $\mathbb{F}_2$ since

$$Y^2 + XY + X^2 + X^3 = (Y + \alpha X)(Y + \beta X) + X^3 \quad \text{with} \quad \alpha + \beta = \alpha\beta = 1.$$

Hence $E_{A,B,C}$ has reduction of multiplicative type at 2.

Our observations yield that $E_{A,B,C}$ has good reduction at every prime $\ell \nmid ABC$ and multiplicative reduction at every prime $\ell|ABC$ and therefore is semistable. Equation (1.16) is a minimal equation for 2 and thus it is a minimal model over $\mathrm{Spec}(\mathbb{Z})$ (indeed the original equation was already minimal for $\ell \neq 2$). The minimal discriminant of the curve is

$$\Delta_{E_{A,B,C}} \quad = \quad \frac{A^2 B^2 C^2}{2^8}, \tag{1.17}$$

and its conductor

$$N_{E_{A,B,C}} \quad = \quad \prod_{\ell|ABC} \ell =: \mathsf{rad}\, ABC. \tag{1.18}$$

In the next paragraph we will discuss Galois representations provided by curves of this type.

1.3 ℓ-division Points and Galois Representations

We conserve the notations and assumptions (1.13) of the previous section, write $E = E_{A,B,C}$ and fix a prime $\ell \geq 5$. Hereto we consider the representation (1.6)

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \cong \mathbf{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Let K_ℓ be the Galois extension derived by adjoining to $\mathbb{Q}$ the points of $E[\ell]$. We begin by a discussion of two relatively simple global properties of the representation (1.6).

1.3.1 Irreducibility and Determinant of the Representation ρ_ℓ

We follow a proof of Serre using a well-known theorem of Mazur to show the following statement:

Proposition 1.3.1. *The representation ρ_ℓ is an irreducible two-dimensional representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Proof: We prove this by contradiction. Assume ρ_ℓ is reducible, which means (recall that $E[\ell]$ has order ℓ^2) that $E[\ell]$ and therefore E contains a subgroup X of order ℓ which is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (or in other words, which is a group scheme defined over $\mathbb{Q}$). Having shown in Section 1.2 that E is semistable we know that there are two possibilities for the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on X: by the character of unity or by the cyclotomic character (please find a precise explanation in [41, 5.2, Proof of Proposition 21]).
In the first case every generator of X is a $\mathbb{Q}$-rational point of order ℓ given that $\mathbb{Q}$ is the fixed field of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Further, all points of order two (and there are four of them) are also rational over $\mathbb{Q}$. Indeed, let $[2]P = \mathcal{O}$ or equivalently $P = -P$. A well-known formula (cf. for example [45, III.Group Law Algorithm 2.3]) induces $(x_P, y_P) = (x_{-P}, y_{-P}) = (x_P, -y_P)$ that is $y_P = -y_P$ or $y_P = \mathcal{O}$. So x_P satisfies the equation $0 = x(x-A)(x-B)$ having three rational (even integral) zeros. Consequently, the torsion subgroup of $E(\mathbb{Q})$ has order $\geq 4\ell \geq 20$. And this contradicts the Theorem 8 of Mazur in [23] saying that the order of the torsion subgroup has at most order 16.
In the second case the quotient E/X, which is again a curve, has a $\mathbb{Q}$-rational point of order ℓ as $E[\ell]$ was of order ℓ^2 and we have divided by the cyclotomic action. Now we can argue similarly as in the first case and again apply the theorem of Mazur. □

The representation ρ_ℓ is characterized by a further more elementary property.

Proposition 1.3.2. *The determinant of the representation ρ_ℓ is the cyclotomic character χ_ℓ :* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^*$

Definition 1.3.3. We first define the so-called *Weil pairing* on $E[\ell]$. Let T be in $E[\ell]$, then there exists a function f of the algebraic closure of the function field of E such that its divisor is

$$\mathrm{div}(f) = \ell(T) - \ell(\mathcal{O}).$$

Now for $T' \in E$ with $[\ell]T' = T$, there is equivalently a function g with

$$\mathrm{div}(g) = [\ell]^*(T) - [\ell]^*(\mathcal{O}) = \sum_{R \in E[\ell]} (T' + R) - (R),$$

where for a morphism $\phi : C_1 \to C_2$ of curves $\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ is the induced map on the divisor groups (see [45, II.p.33]). Verifying that $f \circ [\ell]$ and g^ℓ have the same divisor, one sees that they coincide up to a constant factor, so without loss of generality

$$f \circ [\ell] = g^\ell.$$

Suppose that S is another ℓ-torsion point and $X \in E$ arbitrary. Then

$$g(X+S)^{\ell} = f([\ell]X + [\ell]S) = f([\ell]X) = g(X)^{\ell}.$$

For this reason we can define a pairing

$$e_{\ell} : E[\ell] \times E[\ell] \to \mu_{\ell}\,, \quad (S,T) \mapsto \frac{g(X+S)}{g(X)} \tag{1.19}$$

By the above calculations the latter is actually in μ_{ℓ}. Although g is only defined up to a constant factor, the pairing is not only independent of this choice but also of the choice of the point X. Direct computations (cf. [45, III.Proposition 8.2]) show that the Weil pairing is bilinear, alternating, non-degenerate and Galois invariant.

Proof of the proposition: The first three of the above properties induce, in correspondence with the universal property of the outer product a homomorphism

$$\bigwedge^{2} E[\ell] \to \mu_{\ell}$$

which is by non-degeneracy yet an isomorphism. In the next step the Galois invariance plays a role – it allows us to simplify the expression for the determinant of the representation in the following way:

$$\det \circ \rho_{\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \to \mathrm{Aut}\left(\bigwedge^{2} E[\ell]\right) \cong \mathrm{Aut}(\mu_{\ell}) = \mathbb{Q}_{\ell}^{*},$$

which is the one dimensional Galois representation

$$\chi_{\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q}) \to \mathrm{Aut}(\mu_{\ell}) \quad , \quad \sigma(z) = z^{\chi_{\ell}},$$

what we wanted to show. □

Beside these global properties it is significant to mention the following local properties.

1.3.2 Ramification of the Representation ρ_{ℓ}

The following basic notions taken from [38] and [40] on number fields are meaningful in ramification theory. Let K be a number field and denote by Σ_K the set of all finite places of K, that is the set of all normalized discrete valuations on K (alternatively the set of all prime ideals in the ring of integers $\mathcal{O}_K$ of K – for $K = \mathbb{Q}$ the set of all prime numbers). The residue field

$$k_{\nu_K} = \mathcal{O}_K\,/(\nu_K)$$

corresponding to a valuation $\nu_K \in \Sigma_K$ is finite of cardinality

$$\mathrm{Norm}_{K/\,\mathbb{Q}}(\nu_K) = p_{\nu_K}^{\deg(\nu_K)},$$

where $p_{\nu_K} = \mathrm{char}(k_{\nu_K})$ is at the same time the prime *underlying* ν_K, $\mathrm{Norm}_{K/\,\mathbb{Q}}$ is the norm homomorphism and $\deg(\nu_K) = f_{\nu_K}$ is the residue degree of k_{ν_K} over $\mathbb{F}_{p_{\nu_K}}$. The ramification index e_{ν_K} is $\nu_K(p_{\nu_K})$. The extension $K/\,\mathbb{Q}$ is called unramified in ν_K if $e_{\nu_K} = 1$ and totally ramified if $f_{\nu_K} = 1$.

Let L/K be a finite Galois extension and ν_L be a place of L over ν_K – we say that ν_K is the restriction of ν_L to K or as well ν_L divides ν_K. The isotropy group

$$D_{\nu_L} := \{g \in \mathrm{Gal}(L/K) | g\nu_L = \nu_L\}$$

is called the *decomposition group of* ν_L. If L_{ν_L} respectively K_{ν_K} denotes the completion of L respectively K with respect to the chosen valuation we have

$$D_{\nu_L} \cong \mathrm{Gal}(L_{\nu_L}/K_{\nu_K}).$$

An element $\sigma \in D_{\nu_L}$ defines a k_{ν_K}-automorphism σ_{ν_K} of l_{ν_L} by taking quotients and so we obtain a homomorphism of groups

$$\mathsf{red}_\nu : D_{\nu_L} \to \mathrm{Gal}(l_{\nu_L}/k_{\nu_K})$$

whose kernel is called the *inertia group* I_{ν_L} *of* ν_L. The quotient D_{ν_L}/I_{ν_L} is a finite cylic group generated by the FROBENIUS substitution Frob_{ν_L} attached to ν_L. The extension L/K is unramified in ν_L if and only if the inertia group is trivial (see hereto [38, I.Corollaire à Proposition 21]). Any other place ν'_L over ν_K can be derived from ν'_L by conjugation ($\mathrm{Gal}(L/K)$ acting transitively on the fibers). Replacing ν_L by ν'_L means conjugating the triple $(D_{\nu_L}, I_{\nu_L}, \mathsf{Frob}_{\nu_L})$ by an element of $\mathrm{Gal}(L/K)$.

In our case it is essential to study the introduced concepts on arbitrary algebraic extensions: For an arbitrary algebraic extension L of $\mathbb{Q}$ let Σ_L be the projective limit

$$\Sigma_L = \varprojlim \Sigma_{L_\alpha}$$

L_α ranging over all finite subextensions of $L/\mathbb{Q}$. Under these notations, we can define for an arbitrary GALOIS extension L/K of a number field K the decomposition group D_{ν_L}, inertia group I_{ν_L} and FROBENIUS element Frob_{ν_L} as before. The quotient D_{ν_L}/I_{ν_L} is a procyclic group.

The following definition for ℓ-adic representations of a number field K can be adopted for our representation ρ_ℓ.

Definition 1.3.4. An ℓ-adic representation $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V)$ of K is said to be unramified at a place $\nu \in \Sigma_K$ if the image of the corresponding inertia group $\rho(I_{\nu_{\overline{K}}})$ is trivial for any valuation $\nu_{\overline{K}}$ of $\overline{K}$ extending ν.

This condition is visibly independent of the choice of $\nu_{\overline{K}}$ as the representation is GALOIS equivariant and the places lying over ν are all conjugate. It is clear that in the unramified case the representation factors through $D_{\nu_{\overline{K}}}/I_{\nu_{\overline{K}}}$ for any $\nu_{\overline{K}}$ over ν. Thus the image of the FROBENIUS element $\rho(\mathsf{Frob}_{\nu_{\overline{K}}})$ is well defined, i.e. independent of the choice of $\mathsf{Frob}_{\nu_{\overline{K}}}$ as a lifting of the FROBENIUS substitution. Moreover, the conjugacy class of $\rho(\mathsf{Frob}_{\nu_{\overline{K}}})$ in $\mathrm{Aut}(V)$ depends only on ν. The condition comes up to the equivalent statement that ν is unramified in the extension $\overline{K}^{\mathrm{Ker}(\rho)}/K$ where $\overline{K}^{\mathrm{Ker}(\rho)}$ is the fixed field of the kernel of ρ. Indeed, let ρ be unramified at ν. Then $\rho(I_{\nu_{\overline{K}}}) = 1$ – equivalently $I_{\nu_{\overline{K}}} \subseteq \mathrm{Ker}(\rho)$. Therefore with basic field theory

$$\overline{K} \supseteq \overline{K}^{I_{\nu_{\overline{K}}}} \supseteq \overline{K}^{\mathrm{Ker}(\rho)} \supseteq K.$$

We know that $\overline{K}^{I_{\nu_{\overline{K}}}}/K$ is unramified at ν and so is $\overline{K}^{\mathrm{Ker}(\rho)}/K$.

Let us now return to the case when $K = \mathbb{Q}$ and $L = \overline{\mathbb{Q}}$. Let p be a prime number and choose a place $\nu \in \Sigma_{\overline{\mathbb{Q}}}$ lying over p. The decomposition group D_ν is isomorphic to the GALOIS group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ where $\overline{\mathbb{Q}}_p$ is the algebraic closure of $\mathbb{Q}_p$ in the completion of $\overline{\mathbb{Q}}$ at ν. For the quotient with the inertia group we have $D_\nu/I_\nu \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ with an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$; thus it is isomorphic to the procyclic group $\mathbb{Z}_p$ generated by the FROBENIUS substitution $\mathsf{Frob}_\nu : x \mapsto x^p$.

The representation ρ_ℓ is unramified at p if $\rho_\ell(I_\nu) = 1$, i.e. if p is unramified in the extension K_ℓ/K (or according to [38, p.68], that p doesn't divide the discriminant of the extension). A first easy result is the following

Lemma 1.3.5. *The representation* ρ_ℓ *is ramified at the prime* $p = \ell$.

PROOF: Having shown in Proposition 1.3.2 that the determinant of ρ_ℓ is the cyclotomic character χ_ℓ, we know that the kernel of the latter contains the kernel of the representation and this means that K_ℓ as fixed field of $\mathrm{Ker}(\rho_\ell)$ contains the fixed field of $\mathrm{Ker}(\chi_\ell)$ in $\overline{\mathbb{Q}}$. By definition of the cyclotomic character this field incorporates the ℓ^{th} roots of unity. In particular, K_ℓ contains the cyclotomic field $\mathbb{Q}(\mu_\ell)$ which is already ramified at ℓ. □

Let us now study the ramification of ρ_ℓ at the remaining primes.

Proposition 1.3.6. *Under assumption that p is coprime to ℓN, where N is the conductor of the elliptic curve E, ρ_ℓ is unramified at p. More than that, for each place ν over p there is a congruence*

$$\mathrm{tr}\,(\rho_\ell(\mathsf{Frob}_\nu)) \equiv a_p \mod \ell,$$

where a_p is the number defined in (1.11).

PROOF: By assumption E has good reduction at p, in particular the reduction E_p is an elliptic curve over an algebraic closure $\overline{\mathbb{F}}_p$. Given that $\gcd(\ell, p) = 1$ the restriction of the reduction map to $E[\ell]$

$$\mathsf{red}_p : E[\ell] \to E_p$$

is injective and we obtain an isomorphism of the $\mathbb{Z}/\ell\mathbb{Z}$-modules $E[\ell]$ and $E_p[\ell]$. Thus the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell]$ factors through the reduction map whose kernel is by definition the inertia group I_ν. Thus it is clear that $\rho_\ell(I_\nu) = 1$ and ρ_ℓ is unramified at p.

This fact induces that the FROBENIUS automorphism $\rho_\ell(\mathsf{Frob}_p)$ of $E[\ell]$ corresponds to the FROBENIUS endomorphism Frob_p on the reduced curve E_p. Hence their determinants agree

$$\det(\rho_\ell(\mathsf{Frob}_p)) = \det(\mathsf{Frob}_p),$$

(which is incidentally the norm $\mathrm{Norm}_{\overline{\mathbb{Q}}/\mathbb{Q}}(p) = p$). By a well known formula (see for example [45, V.Proposition 2.3])

$$\mathrm{tr}(\mathsf{Frob}_p) = 1 + \det(\mathsf{Frob}_p) - \det(1 - \mathsf{Frob}_p).$$

By [45, III.Proposition 4.10c and Proposition 5.5]

$$\#E(\mathbb{F}_p) = \det(1 - \mathsf{Frob}_p)$$

and with $\det(\mathsf{Frob}_p) = p$ the right hand side of the equation equals (1.11)

$$a_p = 1 + p - \#E(\mathbb{F}_p).$$

Finally $\mathrm{tr}(\rho_\ell(\mathsf{Frob}_p))$ is equivalent to $\mathrm{tr}(\mathsf{Frob}_p)$ modulo ℓ and this shows the second part of the claim. □

The last case to be considered is when $p \neq \ell$ but $p|N$. Thereto, we will give a criterion depending on the minimal discriminant $\Delta_E = \frac{A^2B^2C^2}{2^8}$ of the elliptic curve. For that purpose we will apply the theory of TATE curves as stated in [40, Appendix A.1. to IV.]. For a more precise evaluation see [27]. Let K be a field complete with respect to a discrete valuation ν and its residue field perfect of characteristic $p \neq 0$. Further, let E be an elliptic curve and ℓ be a prime $\neq \mathrm{char}(K)$. There are two cases to be considered, namely $\nu(j) < 0$ and $\nu(j) \geq 0$, but the case we care about is the first one.

Let $q \in K$ such that $\nu(q) > 0$ and Γ_q the discrete subgroup of K^* generated by q as $\mathbb{Z}$-module. Then there exists an elliptic curve E_q over K such that for any finite extension L of K there is an isomorphism of analytic groups

$$L^*/\Gamma_q \quad \cong \quad E_q(L). \tag{1.20}$$

The equation of E_q can be written in a general WEIERSTRASS equation

$$y^2 + xy = x^3 - a_4 x - a_6,$$

with coefficients given as formal power series in $\mathbb{Z}[[q]]$

$$a_4 = 5\sum_{n\in\mathbb{N}} \frac{n^3 q^n}{1-q^n} \qquad \text{and} \qquad a_6 = \sum_{n\in\mathbb{N}} \frac{(7n^5+5n^3)q^n}{12(1-q^n)}$$

converging in K. The modular invariant of E_q is given by the usual formula as series with integral coefficients

$$j(q) = \frac{(1+48a_4)^3}{q\prod_{n\in\mathbb{N}}(1-q^n)^{24}} = \frac{1}{q} + 744 + 196884q + \cdots ,$$

and the discriminant by

$$\Delta \;=\; q\prod_{n\in\mathbb{N}}(1-q^n)^{24}. \tag{1.21}$$

Moreover, the elliptic curve E_q has in the power series ring $\mathbb{Z}[[q,u]]$ for any $u \in K^*$ the point

$$\begin{aligned} x &= x(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2\sum_{n\in\mathbb{N}} \frac{nq^n}{1-q^n} \\ y &= y(u,q) = \sum_{n\in\mathbb{N}} \frac{q^{2n}u^2}{(1-q^n u)^3} + \sum_{n\in\mathbb{N}} \frac{nq^n}{1-q^n}. \end{aligned}$$

The isomorphism (1.20) is then given through

$$u \mapsto (x(u,q), y(u,q)).$$

The function field of E_q consists of fractions $\frac{F}{G}$ of LAURENT series with coefficients in K converging outside of 0 and ∞ and such that

$$\frac{F(qz)}{G(qz)} = \frac{F(z)}{G(z)}.$$

Because the j-invariant of our given elliptic curve E has negative valuation the fact that the series for $j(q)$ has integral coefficients enables us to choose q so that $j = j(q)$. The elliptic curves then become isomorphic over a unique quadratic extension of K – after possibly replacing K we may assume without loss of generality $E = E_q$ and q is called the TATE *parameter attached to E*.

Now we hold all tools together to prove the following proposition for our elliptic curve $E = E_{A,B,C}$:

Proposition 1.3.7. *Suppose that p is prime to ℓ but divides the conductor N. Then ρ_ℓ is unramified at p if and only if* $\operatorname{ord}_p(\Delta_E) \equiv 0 \mod \ell$.

PROOF: One has to show that the extension $K_\ell/\mathbb{Q}$ is unramified at p if and only if $\operatorname{ord}_p(\Delta_E) \equiv 0 \mod \ell$. Note that $\operatorname{ord}_p(j) < 0$ because of the bad reduction of E at p. To bring to bear the theory of TATE curves we show the equivalent statement that $\mathbb{Q}_p(E[\ell])$ is unramified at p over the completion of $\mathbb{Q}$ at p which is possible to do in view of the fact that p and ℓ are relatively prime. We check under which conditions all points of $E[\ell]$ are defined over the maximal unramified extension $\mathbb{Q}_p^{\mathrm{nr}}$ of $\mathbb{Q}_p$. By the above presented arguments there is a TATE parameter $q \in \mathbb{Q}_p$ such that $E = E_q$ over a quadratic extension of $\mathbb{Q}_p$ and by the isomorphism (1.20) we can construct the extension $\mathbb{Q}_p^{\mathrm{nr}}(E[\ell])$ of $\mathbb{Q}_p^{\mathrm{nr}}$ by adjoining the ℓ^{th} roots of q. Since $\ell \neq p$ by assumption, q is an ℓ^{th} power in $\mathbb{Q}_p^{\mathrm{nr}}$ if and only if the p-valuation of q is a multiple of ℓ. Though quoting (1.21), (1.15) and (1.17) one sees that $\operatorname{ord}_p(q) = \operatorname{ord}_p(\Delta_E)$. This shows the claim. □

Remark 1.3.8. If p is prime to ℓN as in Proposition 1.3.6, $\operatorname{ord}_p(\Delta_E) = 0$. Hence a fortiori $\operatorname{ord}_p(\Delta_E) \equiv 0 \mod \ell$ and at the same time ρ_ℓ is unramified at p. So in Proposition 1.3.7 the hypothesis $p|N$ can be suppressed.

Remark 1.3.9. To outline all results of this paragraph in one statement, we introduce the notion of finiteness. Let p be a prime and ν a place over p. Constraining the action of the Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to the decomposition group D_ν which is as we have just seen the Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, ρ_ℓ makes $E[\ell]$ into an (étale) group scheme of type (ℓ,ℓ) (see [32]) over $\mathbb{Q}_p$, i.e. we may regard $E[\ell]$ as $\operatorname{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module. The representation ρ_ℓ is said to be finite at p if this group scheme can be prolonged to a finite flat group scheme over $\mathbb{Z}_p$. For $p \neq \ell$ this is equivalent to say that ρ_ℓ is unramified at p for in this case D_ν is isomorphic to the procyclic group $\mathbb{Z}_p$. Furthermore, Serre has shown in [39, (4.1.11), 2.8 Proposition 4 and 2.9 Proposition 5] that ρ_ℓ is finite at ℓ if and only if $\operatorname{ord}_\ell(\Delta_E)$ is divisible by ℓ.

Finally we can conclude:

Proposition 1.3.10. *The representation ρ_ℓ is finite at a prime number p if and only if* $\operatorname{ord}_p(\Delta_E) \equiv 0 \mod \ell$.

1.4 Modular Curves

There are several equivalent ways to establish the concept of modularity which plays an important role in the formulation of the TANIYAMA-SHIMURA-WEIL-Conjecture. We begin with a geometric approach.

1.4.1 Complex Structure of Modular Curves

Let

$$\mathfrak{H} = \{\tau \in \mathbb{C} \,|\, \Im(\tau) > 0\}$$

be the POINCARÉ upper half plane. The special linear group $\mathbf{SL}_2(\mathbb{R})$ acts by linear fractional transformation

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}$$

on $\mathbb{C} \cup \{\infty\}$. The following lemma shows that it also acts on $\mathfrak{H}$.

Lemma 1.4.1. *For $\alpha \in \mathbf{SL}_2(\mathbb{R})$ and $\tau \in \mathfrak{H}$*

$$\Im(\alpha\tau) = \frac{\Im(\tau)}{|c\tau + d|^2}.$$

PROOF: By definition we compute for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\begin{aligned} \Im(\alpha\tau) &= \frac{1}{2i}(\alpha\tau - \overline{\alpha\tau}) \\ &= \frac{1}{2i}\left(\frac{a\tau + b}{c\tau + d} - \frac{a\overline{\tau} + b}{c\overline{\tau} + d}\right) \\ &= \frac{(a\tau + b)(c\overline{\tau} + d) - (a\overline{\tau} + b)(c\tau + d)}{2i(c\tau + d)(c\overline{\tau} + d)} \\ &= \frac{(ad - bc)(\tau - \overline{\tau})}{2i|c\tau + d|^2} \\ &= \frac{\Im(\tau)}{|c\tau + d|^2} > 0 \end{aligned}$$

as $\Im(\tau) > 0$. □

The only element of $\mathbf{SL}_2(\mathbb{R})$ besides 1 that acts trivial on $\mathfrak{H}$ is -1, so

$$\mathbf{PSL}_2(\mathbb{R}) = \mathbf{SL}_2(\mathbb{R})/\{\pm 1\}$$

acts faithfully on $\mathfrak{H}$. The relevant subgroup in our context is the *full modular group* $\mathbf{SL}_2(\mathbb{Z})$ which is generated by

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Indeed, let $\tilde{\Gamma}$ be the subgroup of $\mathbf{SL}_2(\mathbb{Z})$ generated by T and S. Choose $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \backslash \tilde{\Gamma}$ such that $\max\{|a|, |c|\}$ is minimal – then this is also true for $\min\{|a|, |c|\}$. Without loss of generality (multiplying with S if necessary) we may assume that $|a| < |c|$. With $STS^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ in $\tilde{\Gamma}$ we see that

$$\begin{pmatrix} a & b \\ c \pm a & d \pm b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

are not in $\tilde{\Gamma}$. Unless $a = 0$, $|c + a|$ or $|c - a| < |c|$ contradicts the minimality assumption of α. Thus assume that $a = 0$. This induces that $c = -b = \pm 1$. Multiplying by S or S^{-1} from left, we obtain an element

$$\begin{pmatrix} 1 & d \pm 1 \\ 0 & 1 \end{pmatrix}$$

which is a power of T – contradiction.

Definition 1.4.2. For a natural number N we define the *principal congruence subgroup* $\Gamma(N)$ of $\mathbf{SL}_2(\mathbb{Z})$ by

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \operatorname{mod} N \right\}$$

which is the kernel of the reduction modulo N homomorphism $\mathbf{SL}_2(\mathbb{Z}) \to \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$, and therefore has finite index in $\mathbf{SL}_2(\mathbb{Z})$. Farther, we define the HECKE *subgroup* $\Gamma_0(N)$ of $\mathbf{SL}_2(\mathbb{Z})$ by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \operatorname{mod} N \right\}$$

which satisfies $\Gamma(N) \subset \Gamma_0(N)$, thus has finite index in $\mathbf{SL}_2(\mathbb{Z})$, too. Last, let

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \operatorname{mod} N,\ a \equiv b \equiv 1 \operatorname{mod} N \right\}.$$

More generally, a *congruence subgroup of* $\mathbf{SL}_2(\mathbb{Z})$ is a subgroup Γ which contains $\Gamma(N)$ for some natural number N.

According to what we have seen, $\Gamma_0(N)$ (and of course $\Gamma(N)$) acts on the POINCARÉ upper half plain, hence we can define the quotient

$$Y_0(N) = \Gamma_0(N) \backslash \mathfrak{H},$$

which is an open RIEMANN surface as will follow. Take the union $\mathfrak{H}^*$ of $\mathfrak{H}$ with the *cusps* with respect to $\Gamma_0(N)$, that is the equivalence classes of $\mathbb{Q} \cup \{\infty\}$ under the action of $\Gamma_0(N)$. A basic open set around a point in $\mathfrak{H}$ is an open disc in $\mathfrak{H}$, a basic open disc around ∞ is of the form $\{\Im(\tau) > r\}$ with $r > 0$ and a basic open disc around a rational number x is the union of an open disc in $\mathfrak{H}$ with radius $y > 0$ and center $x + iy$ and $\{x\}$. The resulting topology on $\mathfrak{H}^*$ is HAUSDORFF, $\mathfrak{H}$ is open and $\mathbf{SL}_2(\mathbb{Z})$ acts continuously [20].

Definition 1.4.3. The *modular curve* $X_0(N)$ *over* $\mathbb{C}$ is the standard compactification $\Gamma_0(N) \backslash \mathfrak{H}^*$ of $Y_0(N)$. It has a canonical model over $\mathbb{Q}$. In the same way, one defines $X_1(N)$ and $X(N)$.

We can introduce a system of complex charts which makes $X_0(N)$ into a compact RIEMANN surface (see for instance [20, XI.2.Lemma 11.2]).

Explaining the canonical model of $X_0(N)$ over $\mathbb{Q}$ or even over $\mathbb{Z}$ is beyond the skope of this work. But we should sketch at least its interpretation as modular variety.

1.4.2 Modular Curves over $\mathbb{Q}$ and over $\mathbb{Z}$

A basic idea is that points on modular curves parametrize elliptic curves with extra structure. The classical theory of the WEIERSTRASS $\wp$-function establishes a correspondence between isomorphism classes of elliptic curves over $\mathbb{C}$ and complex tori $\mathbb{C}/\Lambda$ (cf. [20, VI.] or [45, VI.]). Every elliptic curve over $\mathbb{C}$ can be realized in the form $E_\tau = \mathbb{C}/\Lambda_\tau$ where Λ_τ is the lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ for some $\tau \in \mathfrak{H}$ and vice versa. The following proposition initiates a natural bijection between isomorphism classes of elliptic curves and the orbit space $\mathbf{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}$.

Proposition 1.4.4. *Let τ, $\tau' \in \mathfrak{H}$. Then the induced elliptic curves are isomorphic if and only if there is an element $\gamma \in \mathbf{SL}_2(\mathbb{Z})$ such that $\tau = \gamma\tau'$.*

PROOF: If $E_\tau \cong E_{\tau'}$ there is a complex number α such that $\alpha\Lambda_\tau = \Lambda_{\tau'}$, so for the generators of the lattice $\alpha\tau = a\tau' + b$ and $\alpha 1 = c\tau' + d$ for appropriate natural numbers a, b, c, d. As image of the basis $a\tau' + b$ and $c\tau' + d$ form a basis of $\Lambda_{\tau'}$ so the matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant ± 1 and must be positive because it maps τ' on τ which are both in the upper half plane.

Conversely, suppose τ, $\tau' \in \mathfrak{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that

$$\tau = \gamma\tau'.$$

With $\alpha = c\tau' + d$, we have $\alpha\tau = a\tau' + b$. For $\det(\gamma) = 1$ this defines an isomorphism of lattices $\Lambda_\tau \cong \lambda_{\tau'}$, so the induced elliptic curves are isomorphic as claimed. □

The task is now to extend this idea on HECKE subgroups. To $\tau \in \mathfrak{H}$ we associate the subgroup

$$C_\tau = \langle \frac{1}{N} \rangle \subset E_\tau,$$

further, let $P_\tau \in E_\tau$ be the point of order N defined by $\frac{1}{N} \in \mathbb{C}$ and $Q_\tau \in E_\tau$ the point of order N defined by $\frac{\tau}{N} \in \mathbb{C}$. For an elliptic curve $E/\mathbb{C}$ we know already that $E[N] \cong \frac{1}{N}\Lambda/\Lambda \cong (\mathbb{Z}/N\mathbb{Z})^2$. Thus it is clear that$\{P_\tau, Q_\tau\}$ is a basis for $E_\tau[N]$.

Proposition 1.4.5. *Let E be an elliptic curve over $\mathbb{C}$. For a cyclic subgroup C of order N, there is $\tau \in \mathfrak{H}$ such that the pair (E, C) is isomorphic to (E_τ, C_τ). If P is a point of order N there is $\tau \in \mathfrak{H}$ such that (E, P) is isomorphic to (E_τ, P_τ). Finally, if P, Q is a basis for $E[N]$ such that for the* WEIL *pairing $e_N(P, Q) = \zeta_N^{N-1}$, then there exists $\tau \in \mathfrak{H}$ such that the triple (E, P, Q) is isomorphic to the triple (E_τ, P_τ, Q_τ).*

PROOF: Without loss of generality we can write $E(\mathbb{C}) = \mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and $\frac{\omega_1}{\omega_2} \in \mathfrak{H}$.

Consider a generator $P = \frac{a\omega_1}{N} + \frac{b\omega_2}{N}$ of the cyclic subgroup C, particularly a point of order N, which means that $\gcd(a, b, N) = 1$ (otherwise P would have order a proper divisor of N). By surjectivity of the restriction map $\mathbf{SL}_2(\mathbb{Z}) \to \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ it is legal to modify a and b by multiples of N until $\gcd(a, b) = 1$. BÉZOUT'S Identity provides $c, d \in \mathbb{Z}$ such that $ad - bc = 1$. Consequently, we get a new basis for Λ, namely $\omega_1' = a\omega_1 + b\omega_2$ and $\omega_2' = c\omega_1 + d\omega_2$ and C is generated by $P = \frac{\omega_1'}{N}$. Replacing eventually ω_2' by $-\omega_2'$ we can assume that $\tau = \frac{\omega_2'}{\omega_1'} \in \mathfrak{H}$ and see that $(E, P) \cong (E_\tau, P_\tau)$ and also $(E, C) \cong (E_\tau, C_\tau)$, the first two claims.

The proof of the third one is similar, but now we begin with a basis $P = \frac{a\omega_1}{N} + \frac{b\omega_2}{N}$, $Q = \frac{c\omega_1}{N} + \frac{d\omega_2}{N}$ of $E[N]$ with $e_N(P, Q) = \zeta_N^{N-1}$. The WEIL pairing can also be realized in more concrete terms with image in $\mathbb{Z}/N\mathbb{Z}$ in the following way: If $E = \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ with $\frac{\omega_1}{\omega_2} \in \mathfrak{H}$ and $P = \frac{a\omega_1}{N} + \frac{b\omega_2}{N}$, $Q = \frac{c\omega_1}{N} + \frac{d\omega_2}{N}$ then

$$e_N(P, Q) = ad - bc \in \mathbb{Z}/N\mathbb{Z}.$$

Note that $e_N(P_\tau, Q_\tau) = -1$ and if $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ via multiplication with α, for two N-division points $e_N(\alpha P, \alpha Q) = e_N(P, Q)$. In our concrete case, this interpretation of e_N means that $e_N(P, Q) = -1 \in \mathbb{Z}/N\mathbb{Z}$. Thus, $ad - bc \cong -1 \mod N$ and the matrix $\begin{pmatrix} a & b \\ -c & -d \end{pmatrix}$ has determinant 1 modulo N. So as before we can replace a, b, c, d by equivalent integers modulo N with $ad - bc = -1$ and we obtain a new basis $\omega_1' = a\omega_1 + b\omega_2$ and $\omega_2' = c\omega_1 + d\omega_2$. The fraction

$$\tau = \frac{\omega_2'}{\omega_1'} = \frac{c\omega_1 + d\omega_2}{a\omega_1 + b\omega_2} = \frac{c\frac{\omega_1}{\omega_2} + d}{a\frac{\omega_1}{\omega_2} + b}$$

is in $\mathfrak{H}$ since $\frac{\omega_1}{\omega_2} \in \mathfrak{H}$ by assumption and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z})$. Now it is clear that multiplication by $\frac{1}{\omega_1'}$ defines an isomorphism $E \to E_\tau$ sending P to $\frac{1}{N}$ and Q to $\frac{\tau}{N}$ and we obtain the desired result. □

The following proposition completes our discussion. Preserve the introduced notations.

Proposition 1.4.6. *Let τ, $\tau' \in \mathfrak{H}$. The pairs (E_τ, C_τ) and $(E_{\tau'}, C_{\tau'})$ are isomorphic if and only if there exists $\gamma \in \Gamma_0(N)$ such that $\gamma\tau = \tau'$. Likewise, (E_τ, P_τ) is isomorphic to $(E_{\tau'}, P_{\tau'})$ if and only if there is $\gamma \in \Gamma_1(N)$ such that $\gamma\tau = \tau'$. And (E_τ, P_τ, Q_τ) is isomorphic to $(E_{\tau'}, P_{\tau'}, Q_{\tau'})$ if and only if there exists $\gamma \in \Gamma(N)$ such that $\gamma\tau = \tau'$.*

Proof: Suppose $(E_\tau, C_\tau) \cong (E_{\tau'}, C_{\tau'})$. Following the argumentation in Proposition 1.4.4 there is $\lambda \in \mathbb{C}$ such that $\lambda\Lambda_\tau = \Lambda_{\tau'}$. Thus $\lambda\tau = a\tau' + b$ and $\lambda 1 = c\tau' + d$ with $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z})$. For λ sends C_τ to $C_{\tau'}$ it must send the generator of C_τ namely $\frac{1}{N}$ to $\mathbb{Z}\tau' + \frac{1}{N}\mathbb{Z}$. Dividing the second equation by N gives the image $\lambda\frac{1}{N} = \frac{c}{N}\tau' + \frac{d}{n}$. Thus c must be divisible by N and so $\gamma \in \Gamma_0(N)$. Conversely, if $\gamma\tau = \tau'$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ the scalar $\lambda = c\tau' + d$ defines by multiplication an isomorphism between E_τ and $E_{\tau'}$. Since $N|c$ the image of $\frac{1}{N}$ under λ, $\frac{c}{N}\tau' + \frac{d}{N}$ is in $\mathbb{Z}\tau' + \frac{1}{N}\mathbb{Z}$ so it maps C_τ to $C_{\tau'}$.

The argumentation for the second assertion is similar, apart from the additional condition that λ maps $\frac{1}{N}$ to $\frac{1}{N} \mod \Lambda_{\tau'}$, i.e. $c \equiv 0 \mod N$ and $d \equiv 1 \mod N$. Moreover, $\det(\gamma) = 1$ induces that $a \equiv 1 \mod N$.

For the last assertion one adds the equivalent condition for the second base point Q_τ and therefore obtains $\gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N$. □

After these argumentations our final result is the following

Theorem and Definition 1.4.7. *Let N be a natural number.*

1. *The non-cuspidal points (the points which are not in the classes of $\mathbb{Q}\cup\{\infty\}$) on $X_0(N)$ correspond to the isomorphism classes of pairs (E, C), where E is an elliptic curve over $\mathbb{C}$ and C a cyclic subgroup of order N. These pairs are sometimes called* enhanced elliptic curves.

2. *The non-cuspidal points of $X_1(N)$ correspond to pairs (E, P), where P is a point on E of order N.*

3. *The non-cuspidal points of $X(N)$ correspond to triples (E, P, Q), where $\{P, Q\}$ is a basis for $E[N]$ such that $e_N(P, Q) = \zeta_N^{N-1} \in \mu_N$.*

Via this interpretation one defines $Y_0(N)$ and $X_0(N)$ over $\mathbb{Q}$. We just want to sketch the proceeding following [20, XI.6,7,8]. To every isomorphism class of elliptic curves E over $\mathbb{C}$ one can associate an unique modular invariant $j(E)$. By the above said in interaction with the theory of the $\wp$-function we obtain a bijective analytic function

$$\begin{aligned} j : \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H} &\to \mathbb{C} \\ \tau &\mapsto j(E_\tau). \end{aligned} \tag{1.22}$$

If we respect the additional structure of subgroups of order N of elliptic curves as explained, we obtain as second analytic function

$$j_N = j \circ \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} : \Gamma_0(N)\backslash\mathfrak{H} \to \mathbb{C}\,. \tag{1.23}$$

Both functions are roots of the so-called *modular polynomial* Φ_N which has coefficients in $\mathbb{Z}[j]$ and remains irreducible over $\mathbb{C}(j)$ (cf. [20, Theorem 11.32]). What is more, j is by definition transcendental over $\mathbb{C}$ with transcendental degree 1 and j_N algebraic over $\mathbb{C}(j)$. In fact, one can show that $\mathbb{C}(j, j_N)$ is the function field of $X_0(N)$ over $\mathbb{C}$ ([20, Theorem 11.33]). The $\mathbb{Q}$ structure will result from a field theoretic relationship between $\mathbb{C}(j, j_N)$ and $\mathbb{Q}(j, j_N)$ by the equivalent conditions in the following theorem.

Theorem 1.4.8. *Let $k(x, y)$ be an extension of the algebraically closed field k with x transcendental over k and y algebraic over $k(x)$. Then the following conditions on a subfield k_0 are equivalent:*

1. *y is algebraic over $k_0(x)$ and the minimal polynomial of y over $k_0(x)$ remains irreducible over $k(x)$,*
2. *$[k_0(x, y) : k_0(x)] = [k(x, y) : k(x)]$,*
3. *$k \cap k_0(x, y) = k_0$,*
4. *$\overline{k}_0 \cap k_0(x, y) = k_0$.*

PROOF: The equivalence (1)⇔(2) and the direction (3)⇒(4) are clear. The direction (2)⇒(3) follows with basic field theory. The only non-trivial direction is (4)⇒(2). For this we refer to [20, Theorem 11.36]. □

As a corollary we can construct the canonical model of $X_0(N)$ over $\mathbb{Q}$:

Corollary 1.4.9. *There exists a non-singular projective curve C over $\mathbb{Q}$ unique up to $\mathbb{Q}$-isomorphism and a unique biholomorphic mapping $\varphi : X_0(N) \to C(\mathbb{C})$ such that for the function fields*

$$\varphi^*(\mathbb{C}(C)) = \mathbb{C}(j, j_N) \qquad \text{and} \qquad \varphi^*(\mathbb{Q}(C)) = \mathbb{Q}(j, j_N).$$

PROOF: We know already that the function field of $X_0(N)$, $\mathbb{C}(j, j_N)$, and $\mathbb{Q}(j, j_N)$ satisfies the first and therefore all conditions of Theorem 1.4.8. In particular, $\mathbb{C}(j, j_N)$ is a function field of dimension 1 over $\mathbb{C}$ and $\mathbb{C} \cap \mathbb{Q}(j, j_N) = \mathbb{Q}$. Thus there exists a nonsingular projective curve C over $\mathbb{Q}$ such that $\mathbb{Q}(C) \cong \mathbb{Q}(j, j_N)$ and $\mathbb{C}(C) \cong \mathbb{C}(j, j_N)$ (cf. [20, Theorem 11.46]), which can be interpreted as nonzero $\mathbb{C}$-algebra isomorphism. The equivalence of categories of function fields of dimension 1 over $\mathbb{C}$ with $\mathbb{C}$-homomorphisms and nonsingular projective curves over $\mathbb{C}$ with dominant morphisms (cf. [15, I.Corollary 6.12]), induces a dominant morphism $\varphi : X_0(N) \to C$ defined over $\mathbb{C}$ which is even holomorphic given that $X_0(N)$ and $C(\mathbb{C})$ are compact RIEMANN surfaces. By the mentioned equivalence of categories the model (φ, C) is unique up to $\mathbb{Q}$-isomorphism. □

Remark 1.4.10. The practice is to identify $C(\mathbb{C})$ with $X_0(N)$ and to refer to $X_0(N)/\mathbb{Q}$ as a $\mathbb{Q}$-structure on $X_0(N)$.

We content ourselves with this description of $X_0(N)$ as curve over $\mathbb{Q}$ as in this setting it goes much too far to establish a good definition over $\mathbb{Z}$. See for this [19].

1.4.3 Modular Forms

For the formulation of the Modularity Conjecture it is inevitable to define modular forms. Two pieces of notation are essential to continue.

Notation 1.4.11. For $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z})$, $\tau \in \mathfrak{H}$ and an integer k define the *factor of automorphy*

$$j(\alpha, \tau) = c\tau + d \in \mathbb{C},$$

and the *weight-k operator* on functions $f : \mathfrak{H} \to \mathbb{C}$

$$f|_k\alpha(\tau) = j(\alpha, \tau)^{-k} f(\alpha(\tau)).$$

This construction is a group operation for

$$\begin{aligned}
f|_k(\alpha_1\alpha_2)(\tau) &= j(\alpha_1\alpha_2, \tau)^{-k} f(\alpha_1\alpha_2\tau) \\
&= \frac{1}{((c_1a_2 + c_2d_1)\tau + (c_1b_2 + d_2d_1))^k} f(\alpha_1\alpha_2\tau) \\
&= \frac{1}{(c_1(a_2\tau + b_2) + d_1(c_2\tau + d_2))^k} f(\alpha_1\alpha_2\tau) \\
&= \frac{1}{(c_2\tau + d_2)^k} \frac{1}{\left(c_1\frac{a_2\tau+b_2}{c_2\tau+d_2} + d_1\right)^k} f(\alpha_1\alpha_2\tau) \\
&= j(\alpha_2, \tau)^{-k} j(\alpha_1, \alpha_2\tau)^{-k} f\left(\alpha_1(\alpha_2\tau)\right) \\
&= j(\alpha_2, \tau)^{-k} \left(f|_k\alpha_1\right)(\alpha_2\tau) = \left(f|_k\alpha_1\right)|_k\alpha_2(\tau)
\end{aligned}$$

thus

$$f|_k(\alpha_1\alpha_2) = (f|_k\alpha_1)|_k\alpha_2.$$

Definition 1.4.12. A function $f : \mathfrak{H} \to \mathbb{C}$ is a *modular form of weight $k \in \mathbb{Z}$ with respect to a congruence subgroup* $\Gamma \subset \mathbf{SL}_2(\mathbb{Z})$ if the following conditions are satisfied:

1. f is holomorphic on $\mathfrak{H}$,
2. f is weight-k invariant under Γ,
3. f is holomorphic at the cusps.

We talk of a *cusp form of weight k with respect to* Γ if in addition

4. f vanishes at the cusps.

The set of modular forms of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$ and the set of cusp forms by $\mathcal{S}_k(\Gamma)$.

If a function $f : \mathfrak{H} \to \mathbb{C}$ satisfies the first two conditions it is sometimes called an *unrestricted* or *weak* modular form. In particular, as holomorphic function on the Poincaré upper half plane, it has a Fourier expansion, respectively a Laurent expansion in $q = e^{2\pi i\tau}$

$$f(\tau) = \sum_{n\in\mathbb{Z}} c_n q^n$$

with $c_n = \int_{-1/2}^{1/2} f(\rho) e^{-2\pi i n\rho} d\rho$. Recall that the cusps with respect to a congruence subgroup Γ are the equivalent classes of $\mathbb{Q} \cup \{\infty\}$ under the action of Γ. If we consider the finite decomposition $\mathbf{SL}_2(\mathbb{Z}) = \bigcup_j \alpha_j\Gamma$ then each $\alpha_j^{-1}(\infty)$ represents a cusp. We say f is holomorphic at the cusp $\alpha_j^{-1}(\infty)$ if in the q-expansion of $f|_k\alpha_j^{-1}$ all coefficients for $n < 0$ are zero, and f vanishes at the cusp $\alpha_j^{-1}(\infty)$ if in addition the coefficient for $n = 0$ vanishes.

The congruence subgroups, which we are primarly interested in, are the Hecke subgroups. For $N \in \mathbb{N}$ we call the associated space of modular forms (respectively of cusp forms) the *modular (resp. cusp) forms of weight k and level* N and denote them by $\mathcal{M}_k(N)$ (resp. $\mathcal{S}_k(N)$).

Note that for any $\alpha \in \mathbf{SL}_2(N)$ and $f \in \mathcal{M}_k(N)$ the function $f|_k\alpha^{-1}$ is periodic with period N since

$$\begin{aligned} f|_k\alpha^{-1}(\tau+N) &= (f|_k\alpha^{-1})|_k\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}(\tau) \\ &= \left(f|_k(\alpha^{-1}\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}\alpha)\right)|_k\alpha^{-1}(\tau) \\ &= f|_k\alpha^{-1}(\tau) \end{aligned}$$

where the last equation holds if f is invariant under the action of $\Gamma_0(N)$ in view of $\alpha^{-1}\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}\alpha \in \alpha^{-1}\Gamma(N)\alpha \subseteq \Gamma_0(N)$. This is why the q-expansion of $f|_k\alpha^{-1}$ is in fact a $q^{1/N}$-expansion.

Let f be a cusp form of weight k and level N with q-expansion $f(\tau) = \sum_{n>0} c_n q^n =: f_\infty(q)$ at the cusp ∞.

Definition 1.4.13. The *L function of f* is the DIRICHLET series

$$L(s,f) = \sum_{n>0} \frac{c_n}{n^s}.$$

The MELLIN transform of $f(i\sigma)$ can with basic integration be computed as

$$\int_0^\infty f(i\sigma)\sigma^s \frac{d\sigma}{\sigma} = (2\pi)^{-s}\Gamma(s)L(s,f),$$

where $\Gamma(s)$ is the EULER gamma function (which converges for $\Re(s) > 0$ and the DIRICHLET series converges absolutely for $\Re(s) > \frac{k}{2} + 1$ as will show the following lemma.

Lemma 1.4.14. *For a cusp form $f \in \mathcal{S}_k(N)$ with q-expansion $f(\tau) = \sum_{n=1}^{n=\infty} c_n q^n$ at ∞, hold the following two statements:*

1. *The function $|f(\tau)||\tau|^{k/2}$ is bounded on $\mathfrak{H}$ and invariant under $\Gamma_0(N)$.*
2. *The coefficients satisfy $|c_n| \leq Cn^{k/2}$ for an appropriate constant C.*

PROOF: See [20, Lemma 9.6]. □

We construct a map that takes $\mathcal{S}_k(N)$ and $\mathcal{M}_k(N)$ respectively to themselves. Consider hereto the matrix $\alpha_N := \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. It is clear that conjugation with this matrix is a monomorphism of $\Gamma_0(N)$. For a modular form of weight k and level N define the ATKIN-LEHNER involution

$$w_k(N)f \quad = \quad f|_k\alpha_N. \tag{1.24}$$

In view of

$$(f|_k\alpha_N)|_k\gamma = \left(f|_k(\alpha_N\gamma\alpha_N^{-1})\right)|_k\alpha_N = f|_k\alpha_N,$$

where the first equality follows from the fact that we deal with a group operation and the second equality follows since f as modular form is stable under $\Gamma_0(N)$, we see that $w_k(N)f$ is a priory a weak modular form of the same weight and level as f. One has even the following statement:

Proposition 1.4.15. *The map $w_k(N)$ takes $\mathcal{M}_k(N)$ and $\mathcal{S}_k(N)$ to themselves respectively.*

PROOF: It is not difficult to see that for any $\beta \in \mathbf{SL}_2(\mathbb{Z})$ and $f \in \mathcal{M}_k(N)$ $f|_k\beta^{-1}$ has a FOURIER expansion in $q_N = e^{2\pi i\tau/N}$ at ∞ and for an invertible matrix α of determinant m, $(f|_k\alpha)|_k\beta^{-1}$

has a holomorphic expansion in q_{mN} (cf. [20, Proposition 9.5]). In our case this leads to an expansion

$$(w_k(N)f)|_k\beta^{-1}(\tau) = \sum_{n=0}^{n=\infty} c_n e^{2\pi i n\tau/N^2},$$

with the coefficients c_n coming from the expansion of f. But we already know that $w_k(N)f$ is a weak modular form for $\Gamma_0(N)$, in particular, $(w_k(N)f)|_k\beta^{-1}$ is N-periodic as can easily be computed. Hence, the coefficients c_n in the expansion vanish unless n is divisible by N and $w_k(N)f$ is holomorphic at the cusps. If $f \in \mathcal{S}_k(N)$ we have in addition that $c_0 = 0$ thus $w_k(N)f$ is again in $\mathcal{S}_k(N)$. □

Since the square of α_N is a multiple of -1, we know that $w_k(N)$ is an involution on the two spaces, which split under this action in two eigenspaces respectively for the eigenvalues ± 1. We denote them by $\mathcal{M}_k^{\pm}(N)$ and $\mathcal{S}_k^{\pm}(N)$.

An important result concerning the L-function of a cusp form is the following theorem due to Hecke.

Theorem 1.4.16. *Let $f \in \mathcal{S}_k^{\varepsilon}(N)$ be a cusp form in one of the eigenspaces of $w_k(N)$ where ε denotes the appropriate eigenvalue. Then $L(s,f)$ is defined for $\Re(s) > \frac{k}{2}+1$ and extends to be entire in s. Further, the function*

$$\Lambda(s,f) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s,f)$$

satisfies the functional equation

$$\Lambda(s,f) = \varepsilon(-1)^{k/2}\Lambda(k-s,f).$$

Proof: The claim about the region of convergence follows from the second part of the above lemma. The functional equation can be derived by calculating some integrals as done in [20, Theorem 9.8]. □

One could ask for the dimensions of the spaces of cusp forms. It is known, that $\mathcal{M}_k(N)$ and therefore $\mathcal{S}_k(N)$ is finite dimensional. Moreover, it can be shown (eg. [20, Theorem 9.10]) that the complex vector space of weight-2 cusp forms for $\Gamma_0(N)$ has dimension equal to the genus $g(N)$ of the modular curve $X_0(N)$. By the way, this is also the dimension of the complete group variety $J_0(N)$, the Jacobian of $X_0(N)$. One can informally come to this conclusion by identifying a weight-2 cusp form $f(\tau)$ with its differential $f(\tau)d\tau$, which is invariant under action of $\Gamma_0(N)$. So this differential may be seen as regular differential on the open curve $Y_0(N)$ which can be extended holomorphically to $X_0(N)$. Thus we have an identification

$$\mathcal{S}_2(N) \cong \mathrm{H}^0\left(X_0(N), \Omega^1\right), \tag{1.25}$$

a space of dimension $g(N)$. In particular, $\mathcal{S}_2(2)$ is trivial because the curve $X_0(2)$ has genus $g(2) = 0$ (see for example [20, Table 12.2]).

1.4.4 Hecke Operators

The spaces $\mathcal{S}_k(N)$ come equipped with a family of endomorphisms, the Hecke *operators.* Hecke operators are built on lattices, but additional structures have to be taken into consideration. Let (Λ, C) be a *modular pair* consisting of a complex lattice and a cyclic subgroup of $\mathbb{C}/\Gamma$ of exact order N. Denote $\mathcal{L}$ the free abelian group generated by the modular pairs (Λ, C).

Definition 1.4.17. The Hecke operator $\mathrm{T}(n)$ for a natural number n on modular pairs is defined by the map on $\mathcal{L}$

$$\mathrm{T}(n)(\Lambda, C) = \sum_{\substack{[\Lambda:\Lambda']=n,\\ nC\twoheadrightarrow C'}} (\Lambda', C'),$$

where $nC \twoheadrightarrow C'$ means that for an inclusion $n\Lambda \subseteq \Lambda'$ the induced map on tori $\mathbb{C}/(n\Lambda) \to \mathbb{C}/\Lambda'$ maps the cyclic group nC surjectively on C'.

It is not difficult to see that the modular pairs in the sum can be parametrized by the quotient $\Gamma_0(N)\backslash M(n,N)$, with $M(n,N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z}) \,\middle|\, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = n,\, c \equiv 0 \right.$ mod N and $\left.\gcd(a,N) = 1\right\}$, (see for instance [20, p.276]).

Let $\tilde{f}$ be a complex valued function on modular pairs homogeneous of degree $-k$, i.e.

$$\tilde{f}(\alpha\Lambda, \alpha C) = \alpha^{-k}\tilde{f}(\Lambda, C) \qquad \text{for} \quad \alpha \in \mathbb{C}^* .$$

Remark 1.4.18. There is a one to one correspondence of functions on modular pairs homogeneous of degree $-k$ and functions on $\mathfrak{H}$ satisfying the modular condition $f(\gamma\tau) = j(\gamma,\tau)^{-k}f(\tau)$.

Definition 1.4.19. We extend our definition of Hecke operators on functions on modular pairs homogeneous of degree $-k$ by

$$(\tilde{f}|\,\mathrm{T}_k(n))(\Lambda, C) = n^{k-1} \sum_{\substack{[\Lambda:\Lambda']=n,\\ nC \twoheadrightarrow C'}} \tilde{f}(\Lambda', C'),$$

and $\tilde{f}|\,\mathrm{T}_k(n)$ is again homogeneous of degree-k.

By the correspondence brought up in the remark, these operators act on weak modular forms of weight k for any level N. What is more, we shall see that they carry $\mathcal{M}_k(N)$ and $\mathcal{S}_k(N)$ to themselves.

Proposition 1.4.20. *Let $\{\alpha_i\}$ be a complete (and finite) set for the right cosets of $\Gamma_0(N)$ in $M(n,N)$, then $f|\,\mathrm{T}_k(n)$ is given by*

$$f|\,\mathrm{T}_k(n) = n^{\frac{k}{2}-1} \sum_i f|_k\alpha_i.$$

Proof: This follows with a slight modification of the proof to [20, Proposition 8.14]. □

Thus $f|\,\mathrm{T}_k(n)$ is a weak modular form of weight k and level N: let $\gamma \in \Gamma_0(N)$, then $\alpha\gamma\alpha^{-1} \in \Gamma_0(N)$ for $\alpha \in M(n,N)$. So

$$\begin{aligned}
(f|\,\mathrm{T}_k(n))|_k\gamma &= n^{\frac{k}{2}-1} \sum_i (f|_k\alpha_i)|_k\gamma \\
&= n^{\frac{k}{2}-1} \sum_i \left(f|_k(\alpha_i\gamma\alpha_i^{-1})\right)|_k\alpha_i \\
&= n^{\frac{k}{2}-1} \sum_i f|_k\alpha_i = f|\,\mathrm{T}_k(n).
\end{aligned}$$

Equipped with this result we can proof the stability of the mentioned spaces under action of $\mathrm{T}_k(n)$:

Corollary 1.4.21. *The* Hecke *operator $\mathrm{T}_k(n)$ takes $\mathcal{M}_k(N)$ and $\mathcal{S}_k(N)$ respectively to themselves.*

Proof: Similarly to the proof of Proposition 1.4.15, we see that for a representant α_i and $\beta \in \mathbf{SL}_2(\mathbb{Z})$ the function $f|_k\alpha_i|_k\beta^{-1}$ has a holomorphic $q^{\frac{1}{nM}}$ expansion at ∞. The last proposition shows that the same holds for $(f|\,\mathrm{T}_k(n))|_k\beta^{-1}$ – all coefficients with negative index are zero. Since $f|\,\mathrm{T}_k(n)$ is an unrestricted modular form it is periodic of period N and a similar argumentation as in Proposition 1.4.15 demonstrates that the coefficients, whose indices are not a multiple of n, vanish and consequently $f|\,\mathrm{T}_k(n)$ is holomorphic at the cusp $\beta^{-1}(\infty)$. As for a cusp form $f \in \mathcal{S}_k(N)$, it is clear that the coefficient with index zero remains zero, too. □

For a modular form $f \in \mathcal{M}_k(N)$ given as q-expansion $f(\tau) = \sum_{n=0}^{\infty} c_n q^n$ the modular form $f|\,\mathrm{T}_k(m)$ can be given in concrete terms by a q-expansion in terms of that of f by

$$f|\,\mathrm{T}_k(m) \quad = \quad \sum_{n=0}^{\infty} b_n q^n, \tag{1.26}$$

where

$$b_n \quad = \quad \begin{cases} c_O \sum_{\substack{a|m,\, a>0,\\ \gcd(a,N)=1}} a^{k-1} & \text{if } n=0; \\ c_m & \text{if } n=1; \\ \sum_{\substack{a|\gcd(n,m),\\ \gcd(a,N)=1}} a^{k-1} c_{nm/a^2} & \text{if } n>1. \end{cases} \tag{1.27}$$

For $k=2$ the formula expressing the q-expansion of $f|\,\mathrm{T}_k(p)$ becomes much more simple if $m=p$ is a prime:

$$f|\,\mathrm{T}_k(p) = \begin{cases} \sum_{n=0}^{\infty} a_{pn} q^n + p \sum_{n=0}^{\infty} a_n q^{pn} & \text{if } p \text{ is prime to } N; \\ \sum_{n=0}^{\infty} a_{pn} q^n & \text{if } p \text{ divides } N. \end{cases}$$

In general it is sufficient to know the Hecke operators for primes as shows the following theorem of Hecke.

Theorem 1.4.22. *On the modular space of weight k and level N the* Hecke *operators satisfy the following equations:*

1. *For a prime power $p^{r\geq 1}$ with $p \nmid N$*

$$\mathrm{T}_k(p^r)\,\mathrm{T}_k(p) = \mathrm{T}_k(p^{r+1}) + p^{k-1}\,\mathrm{T}_k(p^{r-1}).$$

2. *For a prime power $p^{r\geq 1}$ with $p \mid N$*

$$\mathrm{T}_k(p^r) = \mathrm{T}_k(p)^r.$$

3. *For two relatively prime naturals m, n*

$$\mathrm{T}_k(m)\,\mathrm{T}_k(n) = \mathrm{T}_k(mn).$$

In particular, the subring $\mathbf{T}_k(N) \subset \mathrm{End}_{\mathbb{C}}(\mathcal{S}_k(N))$ generated by the $\mathrm{T}_k(n)$ for $n \in \mathbb{N}$ is a $\mathbb{Z}$-algebra – the so-called Hecke *algebra – generated by the $\mathrm{T}_k(p)$ with p prime.*

Definition 1.4.23. Since for $f \in \mathcal{S}_k(N)$ $|f(\tau)||\tau|^{k/2}$ is bounded on $\mathfrak{H}$ and invariant under $\Gamma_0(N)$ (Lemma 1.4.14) we can define the Petersson *inner product* on $\mathcal{S}_k(N)$ on a fundamental domain R_N for $\Gamma_0(N)$ by

$$\langle f, g\rangle = \int_{R_N} f(\tau)\overline{g(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2},$$

where $\tau = \rho e^{i\sigma}$.

It is known by a theorem due to Petersson that the Hecke operators $\mathrm{T}_k(n)$ with $\gcd(n,N)$ on the space $\mathcal{S}_k(N)$ are self adjoint with respect to the Petersson inner product (cf. [20, Theorem 9.18]). Furthermore, those Hecke operators commute with the involution $w_k(N)$ from (1.24). Consequently the decomposition of $\mathcal{S}_k(N)$ into spaces of equivalent eigenforms is compatible with the decomposition in the two eigenspaces $\mathcal{S}_k^{\pm}(N)$ with respect to $w_k(N)$. Unfortunately we cannot say anything about the relationship between $w_k(N)$ and the $\mathrm{T}_k(n)$ with $\gcd(n,N) \neq 1$.

It is only natural to consider eigenforms in $\mathcal{S}_k(N)$ for the induced operators.

Proposition 1.4.24. *Let $f \in \mathcal{S}_k(N)$ with q-expansion $\sum_{n=1}^{n=\infty} c_n q^n$ at ∞ be an eigenform that is an eigenvector for all* HECKE *operators with eigenvalues $f|\,\mathrm{T}_k(n) = \lambda_n$. Then*

$$c_n = \lambda_n c_1.$$

PROOF: In the q-expansion of $f|\,\mathrm{T}_k(n)$ the coefficient of q has to be $\lambda_n c_1$. But (1.26) and (1.27) gives it as c_n. So we get the assertion. □

It is an easy consequence that the eigenvalues determine f up to a scalar and that $c_1 \neq 0$ if $f \not\equiv 0 \mod \Gamma_0(N)$. By HECKE-PETERSSON the space $\mathcal{S}_k(N)$ is the orthogonal sum of the spaces of equivalent eigenforms. Each such eigenspace has a member that is an eigenvector for all $\mathrm{T}_k(n)$. Any eigenform that is an eigenvector for all HECKE operators can be normalized such that in the q-expansion at one has ∞ $c_1 = 1$. With such a normalization the associated L function has an EULER product expansion

$$L(s,f) = \prod_{p|N} \left(\frac{1}{1 - c_p p^{-s}} \right) \prod_{p\nmid N} \left(\frac{1}{1 - c_p p^{-s} + p^{k-1-2s}} \right)$$

convergent for $\Re(s) > \frac{k}{2} + 1$.

1.4.5 Oldforms and Newforms

As a consequence of the missing relationship between $w_k(N)$ and the $\mathrm{T}_k(n)$ with $\gcd(n,N) \neq 1$ we ended up without correlation between L functions having EULER products and L functions having functional equations. The problem are cusp forms coming trivially from lower levels.

Examples 1.4.25. Consider a cusp form $f \in \mathcal{S}_k(N)$ which was given in $\mathcal{S}_k(N/r)$ for $r|N$. Given that $\gcd(n,N) = 1$, the formula for $f|\,\mathrm{T}_k(n)$ is the same relative to $\Gamma_0(N)$ as to $\Gamma_0(N/r)$. Thus an eigenform for $\Gamma_0(N/r)$ becomes automatically an eigenform for $\Gamma_0(N)$ with the same eigenvalues.

Conversely, consider for $r|N$ an eigenform $f(\tau) \in \mathcal{S}_k(N/r)$ such that $f(r\tau)$ is given in $\mathcal{S}_k(N)$. Let hereto $A_k(r)$ be the ATKIN-LEHNER operator

$$A_k(r)f = f|_k \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix},$$

which gives by definition for matrices with positive determinant $A_k(r)f(\tau) = r^{k/2} f(r\tau)$. This shows that $A_k(r)$ maps $\mathcal{S}_k(N/r)$ to $\mathcal{S}_k(N)$. In the following lemma we will see that $\mathrm{T}_k(n)$ commutes with $A_k(r)$ if $\gcd(n,N) = 1$ and as a consequence an eigenform $f(\tau)$ for $\Gamma_0(N/r)$ induces an eigenform $f(r\tau)$ for $\Gamma_0(N)$ with the same eigenvalues.

Lemma 1.4.26. *For natural numbers $r|N$ and $\gcd(n,N) = 1$ there is a commutation relation on $\mathcal{S}_k(N)$*

$$A_k(r)\,\mathrm{T}_k(n) = \mathrm{T}_k(n) A_k(r).$$

PROOF: Let $\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ range over the matrices in $M(n,N)$ (so $ad = n$ and $\gcd(a,N) = 1$) with the additional conditions that $d > 0$ and be in a complete residue system modulo d. This is a complete set of representatives for the right cosets of $\Gamma_0(N)$ in $M(n,N)$ [20, Lemma 9.14]. With Proposition 1.4.20 we obtain

$$\begin{aligned}
(A_k(r)f)|\,\mathrm{T}_k(n) &= n^{\frac{k}{2}-1} \sum_\alpha f|_k \left(\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \alpha \right) \\
&= n^{\frac{k}{2}-1} \sum f|_k \left(\begin{pmatrix} a & br \\ 0 & d \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \right) \\
&= A_k(r)(f|\,\mathrm{T}_k(n))
\end{aligned}$$

The last equality follows since br ranges also over a complete residue system modulo d, for r is relatively prime to d. This shows the lemma. □

The examples lead us to the following definition:

Definition 1.4.27. If $r_1 r_2 | N$ and $f(\tau)$ is an eigenform for $\Gamma_0(N/r_1 r_2)$, then by the example $f(r_2 \tau)$ is an eigenform for $\Gamma_0(N)$ with the same eigenvalues. Such an eigenform is called *oldform* and the linear span of all oldforms is denoted by $\mathcal{S}_k^{\mathrm{old}}(N)$. Its orthogonal complement, the space of newforms denoted by $\mathcal{S}_k^{\mathrm{new}}(N)$, is spanned by newforms as the HECKE operators are selfadjoint if $\gcd(n, N) = 1$.

The main result in this theory is the following *Multiplicity One Theorem* due to ATKIN and LEHNER.

Theorem 1.4.28. *If $f \in \mathcal{S}_k(N)$ is a newform, then its equivalence class is one dimensional.*

The involution $w_k(N)$ and the HECKE operator $\mathrm{T}_k(p)$ with $p|N$ commute with the prime HECKE operators $\mathrm{T}_k(q)$ with $q \nmid N$. Hence they map equivalence classes to themselves. The theorem states that for a newform f this is $\mathbb{C} f$. So f is an eigenvector for $w_k(N)$ and those $\mathrm{T}_k(p)$ such that $p|N$. Consequently, by the Theorem of HECKE 1.4.16 $L(s, f)$ has a functional equation. On the other hand, by the Theorem of HECKE-PETERSON $L(s, f)$ has an EULER expansion.

Remark 1.4.29. The for us relevant space of cusp forms is that of weight 2. So in the following we will suppress the index k and write T_n for the HECKE operator $\mathrm{T}_2(n)$ and denote the HECKE algebra $\mathbf{T}_N$ instead of $\mathbf{T}_2(N)$. Likewise we will denote the ATKIN-LEHNER involution $w_2(n)$ by w_n. The ATKIN-LEHNER operator $A_k(r)$ and the ATKIN-LEHNER involution w_n are not to be confused.

1.5 The Conjecture of Taniyama, Shimura and Weil

We want now to formulate different versions of the so called Taniyama-Shimura-Weil conjecture which is no longer a conjecture but known as the *Modularity Theorem.* Roughly spoken, it is about the statement that every elliptic curve over $\mathbb{Q}$ is *modular.* But what means modular in this context? The most simple form of the conjecture is the following:

Conjecture 1.5.1. *Every elliptic curve over $\mathbb{Q}$ is $\mathbb{Q}$-isogeneous to a quotient of the* Jacobian *$J_0(N)$ of the modular curve $X_0(N)$ for an appropriate natural number N.*

Or equivalently by the theory of abelian varieties:

Conjecture 1.5.2. *For every elliptic curve E over $\mathbb{Q}$ there exists a natural number N and a non-constant $\mathbb{Q}$-isomorphism $X_0(N) \to E$.*

In fact it turns out that the number N in the conjectures can be precised to be the conductor of the elliptic curve. The theory of Eichler-Shimura, on which we cannot dwell because it exceeds the scale of this work but on which the interested reader finds a good summary in [20, XI.,XII.], relates the above formulations with the following ones.

Conjecture 1.5.3. *For an elliptic curve over $\mathbb{Q}$ with conductor N there is an eigenform $f \in \mathcal{S}_2(N)$ such that for each prime $p \nmid N$ the integer a_p of (1.11) is the associated eigenvalue of f for the operator T_p.*

More precisely, this is, by a result of Weil, equivalent to

Conjecture 1.5.4. *Let E be an elliptic curve over $\mathbb{Q}$. Then there exists a newform $f = \sum_{n\geq 1} c_n q^n$ of weight 2 and level N such that the* Dirichlet *series $L(s,f) = \sum_{n\geq 1} \frac{a_n}{n^{-s}}$ equals the L function $L(s,E)$ associated to the elliptic curve. In particular $c_p = a_p$.*

For the last version we mention again some properties of representations. Recall that $\mathbf{T}_N$ is a free $\mathbb{Z}$-module of rank $g(N)$ with maximal ideal $\mathfrak{m}$ such that $k_\mathfrak{m} = \mathbf{T}_N / \mathfrak{m}$ is a finite field of characteristic ℓ. One can show that there is a representation

$$\rho_\mathfrak{m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(k_\mathfrak{m})$$

unique by the Cebotarev Density Theorem [40] with the properties

1. $\det \rho_\mathfrak{m} = \chi_\ell$,

2. $\rho_\mathfrak{m}$ is unramified at all primes $p \nmid \ell N$,

3. $\mathrm{tr}\, \rho_\mathfrak{m}(\mathsf{Frob}_{\nu_p}) = \mathrm{T}_p \mod \mathfrak{m}$ for all primes $p \nmid \ell N$.

Example 1.5.5. For a weight-2 cusp form of level N whose eigenvalues for the T_p are a_p, the action of $\mathbf{T}_N$ is given by the homomorphism $\phi : \mathbf{T}_N \to \mathbb{C}$ which takes an Hecke operator to the corresponding eigenvalue. For a prime ℓ and the maximal ideal $\phi^{-1}((\ell)) = \mathfrak{m}$ the representation $\rho_\mathfrak{m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\mathbb{F}_\ell)$ is the semisimplification of the representation ρ_ℓ of the elliptic curve. If the representation is already semisimple, the two representations coincide.

Now consider for a finite field $\mathbb{F}$ a semisimple continuous representation $\sigma : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\mathbb{F})$.

Definition 1.5.6. The representation σ is said to be *modular of level N* if there is a maximal ideal $\mathfrak{m}$ of $\mathbf{T}_N$ and an embedding $\iota : \mathbf{T}_N /\mathfrak{m} \to \overline{\mathbb{F}}$ such that the representations

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\sigma} \mathbf{GL}_2(\mathbb{F}) \hookrightarrow \mathbf{GL}_2(\overline{\mathbb{F}})$$

and

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{\mathfrak{m}}} \mathbf{GL}_2(k_{\mathfrak{m}}) \xrightarrow{\iota} \mathbf{GL}_2(\overline{\mathbb{F}})$$

are isomorphic.

Equivalently, one can require a homomorphism

$$\omega : \mathbf{T}_N \to \overline{\mathbb{F}}$$

such that

$$\mathrm{tr}\,(\sigma(\mathsf{Frob}_p)) = \omega(\mathrm{T}_p) \quad \text{and} \;\; \det\,(\sigma(\mathsf{Frob}_p)) = \overline{p}$$

for almost all primes. The term *modular of level N* indicates that the representation σ arises from the space $\mathcal{S}_2(N)$ of weight-2 cusp forms of level N.

Definition 1.5.7. If ρ is modular of level N, N is *minimal* for ρ if there is no proper divisor M of N such that ρ is modular of level M.

If ρ is modular of level N, ρ is always modular of some minimal level $N_0|N$. Conversely, if ρ is modular of level N it is modular of all levels N' which are multiples of N. As a converse of the example one can formulate the Taniyama-Shimura-Weil conjecture in terms of modular representations:

Conjecture 1.5.8. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. Then for a fixed prime $\ell \geq 5$ the representation $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[\ell])$ is modular of level N.*

1.6 Relation to FERMAT's Last Theorem

In this section we will mention some notions and concepts without comments since it has the function to build a bridge from the Conjecture of TANIYAMA-SHIMURA-WEIL to the famous theorem of FERMAT. It shows the motivation for our later studies and all necessary data will be introduced later.

The main theorem we will finally deduce is the following theorem of RIBET in [33] (see Theorem 5.3.9).

Main Theorem (Ribet) 1.6.1. *Let $\mathbb{F}$ be a finite field of characteristic $\ell \geq 3$ and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to$ $\mathbf{GL}_2(\mathbb{F})$ a Galois representation that is modular of level N and finite at p which exactly devides N. Then ρ is modular of level $\frac{N}{p}$ whenever one (or both) of the following conditions hold:*

1. *$p \not\equiv 1 \mod \ell$.*

2. *N is prime to ℓ.*

The basic idea of the following application of this theorem, namely the prove FERMAT's Last Theorem, is due to FREY ([12] or [13]) and was picked up by SERRE [39].

Corollary 1.6.2. *Under the assumption that all (semistable) elliptic curves over $\mathbb{Q}$ are modular, i.e. the Conjecture of* TANIYAMA-SHIMURA-WEIL *is true,* FERMAT*'s Last Theorem holds.*

PROOF: Beginning with a non-trivial relatively prime FERMAT triple (a, b, c) satisfying the equation

$$a^\ell + b^\ell + c^\ell = 0$$

for a prime $\ell \geq 5$ we may without loss of generality suppose that b is even and $a \equiv 3 \mod 4$ (being coprime one to each other, exactly one of the three integers must be divisible by 2; regard the FERMAT equation modulo 4; by assumption $b \equiv 2$ or $0 \mod 4$ hence $b^\ell \equiv 0 \mod 4$ and $a^\ell \equiv -c^\ell \mod 4$; since ℓ is an odd prime we even have $a \equiv -c \mod 4$ and a and b must be equivalent to 3 respectively 1 modulo 4). Note that on that account the triple (a^ℓ, b^ℓ, c^ℓ) fulfills the conditions (1.13) of the triple (A, B, C) of the previous section and we can analogously define an elliptic curve over $\mathbb{Q}$ by the WEIERSTRASS equation

$$y^2 = x(x - a^\ell)(x + b^\ell)$$

which is semistable and has bad reduction exactly at those primes dividing abc. Let $N_{E_{a^\ell,b^\ell,c^\ell}} = N$ be its conductor, which is especially divisible by 2. By our assumption on elliptic curves over $\mathbb{Q}$ E_{a^ℓ,b^ℓ,c^ℓ} is modular, i.e. there exists a modular form f of weight 2 and level N whose q-expansion has integral coefficients and whose MELLIN transform is the L-function of the elliptic curve over $\mathbb{Q}$. In particular, the group of ℓ-division points $E_{a^\ell,b^\ell,c^\ell}[\ell]$ provides an irreducible representation ρ_ℓ of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which is finite at every odd prime p dividing the conductor N, but not finite at 2 as we have seen during our discussion.

We are now in a position to apply the Main Theorem on ρ_ℓ and claim that it is modular of level 2. We first reduce our assumptions to the case that N is prime to ℓ such that the second condition of the theorem applies. Indeed, suppose that N be divisible by ℓ. Then ρ_ℓ is finite at $p = \ell \neq 2$ and $p = \ell \not\equiv 1 \mod \ell$. Hence ρ_ℓ is also modular of level $N_0 = \frac{N}{\ell}$. Replacing $N \to N_0 = \frac{N}{\ell}$ in this case and $N \to N_0 = N$ otherwise we find in all cases that ρ_ℓ is modular of some level $N_0|N$ prime to ℓ. By means of the main theorem all odd primes can be eliminated inductively from the level of ρ_ℓ. Lastly, we come to the conclusion that ρ_ℓ is modular of level 2. But this is impossible since the subring of HECKE operators $\mathbf{T}_2 \subseteq \mathrm{End}(S_2(N))$ is trivial in view of the fact that there are no non-zero cusp forms of weight 2 and level 2, and we have a contradiction.

Thus the existence of a non-trivial FERMAT triple is falsified. □

Chapter 2

The PICARD-LEFSCHETZ Formula

In this chapter we will recall results due to RAYNAUD concerning NÉRON Models of JACOBIANS. The arising notions might be familiar to the reader, but we will nevertheless give a sketchy introduction.

2.1 NÉRON Models

In the first chapter we have already mentioned the minimal WEIERSTRASS model of an elliptic curve (see Definition 1.1.21). Now we want to go a more complex way viewing an elliptic curve as abelian group scheme.

Let K be as usual a number field, R its ring of integers and $S = \mathrm{Spec}(R)$. For an abelian variety A_K over K, standard arguments show that it extends to an abelian scheme over a non-empty open part of $S' \subseteq S$. Hence A_K has good reduction at all points $s \in S'$, i.e. A_K extends to an abelian (smooth and proper) scheme over the local ring at s. However, one cannot expect A_K to have good reduction at the finitely many points in $S \backslash S'$. The idea of NÉRON models is to construct models providing a notion of good reduction even at those points. During the 1960^{ies}, ANDRÉ NÉRON suceeded in constructing such models in a canonical way by relaxing the condition of properness and by concentrating on the group structure and smoothness. We will not outline this construction, but instead state the universal property which characterises NÉRON models uniquely and give some examples.

Let S be a DEDEKIND scheme, that is a noetherian normal scheme of dimension ≤ 1 with field of rational functions K and consider an S-scheme X. We define its *scheme of generic fibers* by $X_K := X \otimes_S K$ as a scheme over K. Conversely, if we start with a K-scheme X_K, any S-scheme Y with generic fiber $Y_K = X_K$ is said to be an *S-model of X_K*.

Definition 2.1.1. Let X_K be a smooth and seperated K-scheme of finite type. A NÉRON *model* $\mathcal{N}(X_K)$ *of* X_K is an S-model X of X_K that is smooth, seperated of finite type and satisfies the following universal property, called NÉRON *mapping property*:

Let Y be a smooth S-scheme and $\phi_K : Y_K \to X_K$ a K-morphism. Then ϕ_K extends uniquely to an S-morphism $\phi_S : Y \to X$.

As reference for the following existence theorem due to NÉRON I suggest [2].

Theorem 2.1.2. *The* NÉRON *model* $\mathcal{N}(X_K)$ *exists and is of finite type.*

In the following example we will work over a base scheme S consisting of a strictly henselian discrete valuation ring R with field of fractions K and algebraically closed residue field $k = \overline{k}$. We want to clarify the interdependence between NÉRON models and regular proper minimal models respectively minimal WEIERSTRASS models of elliptic curves. By a *regular* or *non-singular* scheme we mean one whose local rings are regular.

Example 2.1.3. Consider an elliptic curve E_K over K, that is an abelian variety of dimension 1 over K. As we have stated in Theorem 2.1.2, E_K admits a NÉRON model. It is also known that E_K admits a proper regular model, that is a proper flat R-model E, which is a regular scheme. If E is chosen to be minimal among all models E' of this type in the sense that each R-morphism $E \to E'$ which is an isomorphism of generic fibers is an isomorphism itself, then E is unique. Consequently, every automorphism of E_K extends to an automorphism of E.

Proposition 2.1.4. *Let E be the minimal proper regular model over R of an elliptic curve E_K. Then the smooth locus of E is the* NÉRON *model $\mathcal{N}(E_K)$ of E_K.*

PROOF: See [2, 1.5, Proposition 1] or [1, Proposition 1.15] □

If one is just interested in a NÉRON model E of E_K and not so much in its regular minimal model, one can construct E in residue characteristic $\neq 2, 3$ directly without too much effort starting from a minimal WEIERSTRASS equation over R. See for instance [2, 1.5, Lemma 5].

2.2 Néron Models of Jacobian Varieties

2.2.1 Jacobian Varieties

According to [20, Proposition 11.13], we know that in the case of a compact Riemann surface X of genus $g \geq 1$ the Jacobian $J(X)$ of X is in concrete terms given as the quotient

$$\mathbb{C}^g /\Lambda(X),$$

where $\Lambda(X)$ is the lattice generated by the $2g$ $\mathbb{R}$-independent vectors

$$\begin{pmatrix} \int_{c_k} \omega_1 \\ \vdots \\ \int_{c_k} \omega_g \end{pmatrix},$$

with a $\mathbb{Z}$-basis $\{c_1, \ldots, c_{2g}\}$ of $\mathrm{H}_1(X, \mathbb{Z})$ and a $\mathbb{C}$-basis $\{\omega_1, \ldots, \omega_g\}$ of $\Omega_{\mathrm{hol}}(X)$. But I want to give a purely algebraic and more general approach following the article of Milne [26].

Recall the Picard functor $S \mapsto \mathrm{Pic}(S)$ from the category of schemes over a field k to that of abelian groups which maps S to the group $\mathrm{H}^1(S, \mathcal{O}_S^\times)$ of isomorphism classes of invertible sheaves on S. Let C be a non-singular curve over a field k. The degree of a divisor $D = \sum n_i P_i$ on C is $\sum n_i [k(P_i) : k]$. Note that divisor means Cartier divisor, except that in the case of non-singular varieties we can think of them as Weil divisors.

Definition 2.2.1. Let the divisor D be represented by $\{U_i, f_i\}_i$ where $\{U_i\}_i$ is an open covering of C and f_i is a local invertible section defined on U_i of the sheaf of total quotient rings of $\mathcal{O}_C$. Then the invertible sheaf associated to D is defined by taking $\mathcal{L}(D)$ to be the sub-$\mathcal{O}_C$-module generated by f_i^{-1} on U_i. Since $\frac{f_i}{f_j}$ is invertible on the section $U_i \cap U_j$ by definition, f_i^{-1} and f_j^{-1} generate the same $\mathcal{O}_C$-module and therefore $\mathcal{L}(D)$ is well-defined.

Knowing that every invertible sheaf $\mathcal{L}$ on C is of the form $\mathcal{L}(D)$ for a suitable divisor D, we can speak of the degree of $\mathcal{L}$ simply as the degree of D and the well-known Riemann-Roch theorem gives for the Euler characteristic

$$\chi(C, \mathcal{L}^n) = n \deg(\mathcal{L}) + 1 - g(C).$$

By convention, we write $\mathrm{Pic}^0(C)$ for the group of isomorphism classes of invertible sheaves of degree 0 on C. We will now define the functor, which the Jacobian attempts to represent – admittedly without the proof. Let T be a connected scheme over k and $\mathcal{L}$ an invertible sheaf on $C \times_{\mathrm{Spec}(k)} T$. Milne has shown that $\chi(C_t, \mathcal{L}_t^n)$ and therefore $\deg(\mathcal{L}_t)$ is independent of $t \in T$, where $\mathcal{L}_t$ is the inverse image of $\mathcal{L}$ on the fiber C_t of C over t. What is more, the constant degree of $\mathcal{L}_t$ is invariant under base change. Define the following functor from schemes over k to abelian groups:

$$P_C^0(T) := \left\{ \mathcal{L} \in \mathrm{Pic}(C \times T) \,\middle|\, \deg(\mathcal{L}_t) = 0 \text{ for all } t \right\} / \, \mathsf{proj}_2^* \, \mathrm{Pic}(T).$$

It may be helpful to think of $P_C^0(T)$ as being the group of families of invertible sheaves on C of degree 0 parametrized by T modulo the trivial families.

Theorem and Definition 2.2.2. *There exists an abelian variety J_C over k, the so called* Jacobian variety of C, *and a morphism of functors $\iota : P_C^0 \to J_C$, such that the induced morphism $\iota : P_C^0(T) \to J_C(T)$ is an isomorphism whenever $C(T)$ is not trivial.*

Proof: See [26, Theorem 1.1] □

Remark 2.2.3. For any extension field $k \subset k'$ in which C has at least one rational point, ι defines an isomorphism $\mathrm{Pic}^0(C) \cong J_C(k')$. We often refer to this by Picard *functoriality* or Pic functoriality.

We will not go into the construction of the JACOBIAN variety but note some important properties. Throughout this section, C will be a complete nonsingular curve of genus $g(C) > 0$ over a field k and J_C will be its JACOBIAN variety.

Proposition 2.2.4. *The tangent space to J_C at 0 is canonically isomorphic to* $\mathrm{H}^1(C, \mathcal{O}_C)$.

PROOF: The proof is a constructive one, which makes use of the relation between the JACOBIAN and the PICARD functor. It is outlined in [26, Proposition 2.1]. □

As a consequence, the dimension of J_C is equal to the genus of C.

Another useful property of the JACOBIAN variety is its autoduality. By the duality theory of abelian varieties, the dual variety $J_C^\vee$ of J_C is the ALBANESE *variety* of C. By [26, Theorem 6.6] J and $J^\vee$ are canonically isomorphic. So they may be interchanged in many applications. To distinguish the two concepts clearly, we will refer to either of them by PICARD functoriality and ALBANESE functoriality respectively.

2.2.2 Relations for the Regular Minimal Model of a Curve

Let p be a prime and C a curve over a p-adic field K of characteristic 0 with residue field k and residue characteristic p. Based on the work of RAYNAUD we recall some relations between the special fiber of the NÉRON model of J_C and the special fibers of suitable models of C which are mentioned in [33, Section 2]. For a detailed explanation see GROTHENDIECK'S [14, §12].

Denote $\mathcal{C}$ the regular minimal model of C over the ring of integers of K. The multiplicities of the irreducible components of the special fiber $\mathcal{C}_k$, which is connected, be relatively prime. Let P^0 be the connected component of zero of the special fiber of the NÉRON model $\mathcal{N}(J_C)_k$ of the JACOBIAN J_C. According to RAYNAUD, there is a canonical isomorphism

$$(\mathcal{N}(J_C)_k)^0 = P^0 \cong \mathrm{Pic}^0(\mathcal{C}_k) = J_{\mathcal{C}_k}.$$

We may in addition assume, that all singular points of the special fiber $\mathcal{C}_k$ as curve are knots (in local coordinates given by an equation of the form $xy = 0$). Though P^0 might not be an abelian variety, it is an extension of an abelian variety by a torus, a *semiabelian scheme*. That means, there is a short exact sequence

$$0 \to (\text{torus})_k \to P^0 \to (\text{abelian})_k \to 0.$$

More precisely, since the irreducible components of $\mathcal{C}_k$ are reduced – $\mathcal{C}_k$ being a projective curve – we can write the normalization of $\mathcal{C}_k$ as a disjoint union of non-singular curves, $\widetilde{\mathcal{C}_k} = \bigcup_j D_j$, which are unique up to isomorphism (see [21, 4.Proposition 1.22]). Note $\pi : \widetilde{\mathcal{C}_k} \to \mathcal{C}_k$ the projection map and for every point $P \in \mathcal{C}_k$ let $\widetilde{\mathcal{O}}_P$ be the integral closure of $\mathcal{O}_P$. There exists a short exact sequence

$$0 \to \bigoplus_{P \in \mathcal{C}_k} \widetilde{\mathcal{O}}_P^*/\,\mathcal{O}_P^* \to \mathrm{Pic}\,\mathcal{C}_k \xrightarrow{\pi^*} \mathrm{Pic}\,\widetilde{\mathcal{C}_k} \to 0,$$

so π induces a surjection

$$\pi^* : \mathrm{Pic}^0(\mathcal{C}_k) \to \prod_j \mathrm{Pic}^0(D_j)$$

whose kernel is a torus T.

2.2.3 The Dual Graph attached to $\mathcal{C}_k$

To finally derive the PICARD-LEFSCHETZ formula we introduce the so-called *dual graph* of $\mathcal{C}_k$.

Definition 2.2.5. Let $C > 0$ be a vertical divisor (in the sense of [21, 8.Def.3.5]) contained in a closed fiber X_s of a regular fibered surface $X \to S$. Let $\Gamma_1, \ldots, \Gamma_n$ be its irreducible components. We associate the *dual graph* $\mathcal{G}$ to C in the following manner. The vertices of $\mathcal{G}$ are the irreducible components $\Gamma_1, \ldots, \Gamma_n$ and there are $\Gamma_i \cdot \Gamma_j$ (which counts the intersection points of Γ_i and Γ_j) edges between Γ_i and Γ_j.

In our concrete case this means:

1. The vertices of $\mathcal{G}$ are the set $\mathcal{J}$ of irreducible components of $\mathcal{C}_k$.

2. The edges of $\mathcal{G}$ are the set $\mathcal{I}$ of singular points of $\mathcal{C}_k$.

The edge corresponding to a singular point $i \in \mathcal{I}$, which is an ordinary double point, connects the two components of $\mathcal{C}_k$ which meet at i. For each edge, one can choose an orientation, i.e. an ordering $j_1(i), j_2(i)$ of the two components passing through i.

For the proof of the following homological and cohomological identities see [14, (12.3.7)].

Proposition 2.2.6. *Let T be the torus introduced above. There is a canonical isomorphism*

$$T \cong \mathrm{H}^1(\mathcal{G}, \mathbb{Z}) \otimes \mathbb{G}_m \,.$$

By Hom-functoriality this is equivalent to an isomorphism

$$X \cong \mathrm{H}_1(\mathcal{G}, \mathbb{Z}), \tag{2.1}$$

where $X = X(T)$ is the character group of T. So it suffices to calculate $\mathrm{H}_1(\mathcal{G}, \mathbb{Z})$. To do this, we collaps all vertices of $\mathcal{G}$ to a single point such that we obtain a bouquet of circles $\overline{\mathcal{G}}$. The projection $\mathcal{G} \to \overline{\mathcal{G}}$ induces an inclusion

$$X = \mathrm{H}_1(\mathcal{G}, \mathbb{Z}) \hookrightarrow \mathrm{H}_1(\overline{\mathcal{G}}, \mathbb{Z}).$$

If we preserve the above introduced orientation of the edges of $\mathcal{G}$ for $\overline{\mathcal{G}}$, this determines an isomorphism

$$\mathrm{H}_1(\overline{\mathcal{G}}, \mathbb{Z}) \cong \mathbb{Z}^{\mathcal{I}}, \tag{2.2}$$

and consequently a (non-canonical) inclusion

$$X \hookrightarrow \mathbb{Z}^{\mathcal{I}}, \tag{2.3}$$

where $\mathbb{Z}^{\mathcal{I}}$ is the free abelian group generated by the singular points of $\mathcal{C}_k$. In order to identify X with a specific subgroup of $\mathbb{Z}^{\mathcal{I}}$, we consider the set D of elements of degree zero of the free abelian group $\mathbb{Z}^{\mathcal{J}}$ generated by the irreducible components of $\mathcal{C}_k$. The degree map is the evident map $\mathbb{Z}^{\mathcal{J}} \to \mathbb{Z}\,, \sum n_j j \mapsto \sum n_j$.

Proposition 2.2.7. *The character group X is isomorphic to the kernel of the group homomorphism*

$$\alpha : \mathbb{Z}^{\mathcal{I}} \to D\,,\ \alpha(i) = j_1(i) - j_2(i),$$

where the $\#\mathcal{I}$-tuple with 1 at the i^{th} place and 0s everywhere else is identified with the singular point $i \in \mathcal{I}$ via the identification (2.2) of vectors in $\mathbb{Z}^{\mathcal{I}}$ and loops in $\mathrm{H}_1(\overline{\mathcal{G}}, \mathbb{Z})$.

Proof: By linearity it is clear, that α is a well-defined homomorphism of groups. Indeed,

$$\alpha\left(\sum_{i\in\mathcal{I}} a_i i\right) = \sum_{i\in\mathcal{I}} a_i \left(j_1(i) - j_2(i)\right),$$

implies $\alpha(0) = 0$ and $\alpha(v_1 + v_2) = \alpha(v_1) + \alpha(v_2)$ for all vectors v_1 and v_2 in $\mathbb{Z}^{\mathcal{J}}$. Further, the image of α is in D, too, because for the degree of an element of $\mathbb{Z}^{\mathcal{J}}$ in the image we have

$$\begin{aligned} \deg\left(\alpha(\sum a_i i)\right) &= \sum a_i \deg(\alpha(i)) \\ &= \sum a_i \left(\deg(j_1(i)) - \deg(j_2(i))\right) \\ &= \sum a_i (1-1) = 0. \end{aligned}$$

We now prove in two steps the main part of the proposition.

First, let $\gamma \in X = \mathrm{H}_1(\mathcal{G}, \mathbb{Z})$ be a loop in $\mathcal{G}$ formed by taking edges $i_1, \ldots, i_m$ in order. In other words, $j_2(i_l) = j_1(i_{l+1})$ for $l \in \{1, \ldots, m-1\}$ and $j_2(i_m) = j_1(i_1)$. Then

$$\begin{aligned} \alpha(\gamma) &= \sum_{l=1}^{m} (j_1(i_l) - j_2(i_l)) \\ &= j_1(i_1) + (-j_2(i_1) + j_1(i_2)) + \ldots + (-j_2(i_{m-1}) + j_1(i_m)) - j_2(i_m) \\ &= j_1(i_1) + 0 + \ldots + 0 - j_2(i_m) = 0. \end{aligned}$$

Hence, $X \subset \mathrm{Ker}(\alpha)$

On the other hand, let $\gamma \in \mathbb{Z}^{\mathcal{J}} \setminus \mathrm{H}_1(\mathcal{G}, \mathbb{Z})$, that means γ is not a loop in $\mathcal{G}$. We can decompose γ as a union of a set L of loops and a set N of non-loops in such a manner that in N, all elements are connected disjoint non-loops and no non-loop is a subset of a loop. By the linearity of α and the first part of the proof, it follows that $\alpha(L) = 0$. Thus, $\alpha(L \cup N) = \alpha(L) + \alpha(N) = \alpha(N)$. As γ is a non-loop, N is not empty and has in particular a "free end", a vertex which is an end-point of just one edge, say i, occuring with multiplicity $n_i \neq 0$ in N. Then in the divisor $\alpha(N)$ the coefficient of the image of i is $\pm n_i \neq 0$, implying that $\alpha(N) \neq 0$. In particular, $\gamma \in \mathbb{Z} \setminus \mathrm{Ker}(\alpha)$. This proves $\mathrm{Ker}(\alpha) \subset X$, and therefore we get an equality. □

We will now analyse the group Φ of connected components of $\mathcal{N}(J_C)_k$. Hereto, we consider the ALBANESE variety $A_C = \mathrm{Alb}(C)$ of C. What X was for the JACOBIAN, should Y for the ALBANESE variety, namely the character group arising from the reduction of A_C. There is a standard bilinear pairing

$$u : X \times Y \to \mathbb{Z}$$

examined in [14, 11.5.2b] as *monodromy pairing*, which induces an injective homomorphism of groups

$$u : Y \to X^{\vee},$$

where $X^{\vee} = \mathrm{Hom}(X, \mathbb{Z})$. There is a canonical isomorphism of groups

$$\Phi \cong \mathrm{Coker}(u).$$

Remark 2.2.8. This isomorphism holds in a more general case, where X is not necessarily arising from a JACOBIAN variety.

But in the case which was considered, there is the supplemental PICARD-LEFSCHETZ formula. We use the autoduality of the JACOBIAN to obtain an isomorphism $X \cong Y$, such that u becomes a bilinear pairing on X. With the above mentioned inclusion of X in $\mathbb{Z}^{\mathcal{J}}$, we can state the following theorem.

Theorem 2.2.9. *The pairing $u : X \times X \to \mathbb{Z}$ is the restriction of the standard* EUCLIDEAN *pairing, $\mathbb{Z}^{\mathcal{J}} \times \mathbb{Z}^{\mathcal{J}} \to \mathbb{Z}$, on $\mathbb{Z}^{\mathcal{J}}$ to X.*

PROOF: This is Théorème 12.5 of [14]. □

Corollary 2.2.10. *Let $X \to X^{\vee}$ be the map obtained from the inclusion $X \subset \mathbb{Z}^{\mathcal{J}}$ and the* EUCLIDEAN *pairing on $\mathbb{Z}^{\mathcal{J}}$. Then the group Φ is isomorphic to its cokernel.*

PROOF: Since we already know that $\Phi \cong \mathrm{Coker}(u)$, this statement follows immediately with the theorem. □

2.3 Admissible Curves

2.3.1 The "Blow-up" of an Admissible Curve

Preserving the notations of the previous section, we relax now the condition, that the model $\mathcal{C}$ of C is regular, assuming instead that it is admissible in the sense of JORDAN-LIVNÉ [17].

Definition 2.3.1. Let R be a discrete valuation ring with perfect residue field k and uniformizer π. Let S be its spectrum, R^{nr} a strict henselization and $\overline{k} = R^{\mathrm{nr}}/\pi R^{\mathrm{nr}}$. For a positive integer note

$$Z^{(m)} := \operatorname{Spec}\left(R^{\mathrm{nr}}[x,y]/(xy - \pi^m)\right),$$

and let $z = z^{(m)}$ be the double point on the special fiber of $Z^{(m)} \times_R k$. A curve C over S is called *admissible* if it satisfies the following three properties:

1. C is proper and flat over S and its generic fiber is a nonsingular curve.

2. The special fiber of C has reduced normal crossings and all its components are rational.

3. If P is a double point on the special fiber of C, there exists an integer $m \geq 0$, for which the completions of the local rings $\mathcal{O}_{C,P} \otimes_R R^{\mathrm{nr}}$ and $\mathcal{O}_{Z^{(m)},z}$ are isomorphic as R^{nr}-modules:

$$\widehat{\mathcal{O}_{C,P} \otimes_R} R^{\mathrm{nr}} \cong_{R^{\mathrm{nr}}} \widehat{\mathcal{O}}_{Z^{(m)},z}.$$

We will use, that the special fiber of an admissible curve is describable using graphs analogously to the previous section. Returning to our case, the assumption of $\mathcal{C}$ being admissible implies that the singular points of the special fiber $\mathcal{C}_k$ are only ordinary double points by the second property in the definition. Defining the sets $\mathcal{I}$ and $\mathcal{J}$ as above, there is by the third property for every singular point $i \in \mathcal{I}$ a positive integer, which we denote $e(i)$. The special fiber of a regular minimal model for C can be obtained from $\mathcal{C}_k$ by replacing each singular point i with $e(i) > 1$ by a chain of $(e(i) - 1)$ copies of the projective line producing a *blow-up* of $\mathcal{C}_k$, where the sets $\mathcal{I}$ and $\mathcal{J}$ are replaced by analogues $\widetilde{\mathcal{I}}$ and $\widetilde{\mathcal{J}}$.

There is kind of a "projection" map

$$\widetilde{\mathsf{proj}} : \widetilde{\mathcal{I}} \to \mathcal{I},$$

gotten by contracting the projective lines to the corresponding point which is evidently surjective. Hereto, we can associate a map of free abelian groups

$$\tau : \mathbb{Z}^{\mathcal{I}} \to \mathbb{Z}^{\widetilde{\mathcal{I}}}\ ,\ i \mapsto \sum_{\tilde{\imath} \in \widetilde{\mathsf{proj}}^{-1}(i)} \tilde{\imath} \tag{2.4}$$

defined via linear extension by taking each $i \in \mathcal{I}$ to the sum of its preimages. The map is clearly injective because from

$$\sum_{\tilde{\imath} \in \widetilde{\mathsf{proj}}^{-1}(i)} \tilde{\imath} = \sum_{\tilde{\jmath} \in \widetilde{\mathsf{proj}}^{-1}(j)} \tilde{\jmath}$$

follows

$$\widetilde{\mathsf{proj}}^{-1}(i) = \widetilde{\mathsf{proj}}^{-1}(j)$$

and hence

$$i = \widetilde{\mathsf{proj}}\left(\widetilde{\mathsf{proj}}^{-1}(i)\right) = \widetilde{\mathsf{proj}}\left(\widetilde{\mathsf{proj}}^{-1}(j)\right) = j,$$

and has torsion free cokernel. Indeed, let $0 \neq m \in \mathbb{N}$. The formal sum

$$m \cdot \sum_{\tilde{\imath} \in \widetilde{\mathcal{I}}} n_{\tilde{\imath}} \tilde{\imath} = \sum_{\tilde{\imath} \in \widetilde{\mathcal{I}}} m n_{\tilde{\imath}} \tilde{\imath}$$

is zero in $\mathbb{Z}^{\widetilde{\mathfrak{I}}}\,/\,\mathbb{Z}^{\mathfrak{I}}$ if it is in the image of $\mathbb{Z}^{\mathfrak{I}}$. Thus there exists $\sum_{i\in\mathfrak{I}} l_i i \in \mathbb{Z}^{\mathfrak{I}}$ such that

$$\tau\left(\sum_{i\in\mathfrak{I}} l_i i\right) = \sum_{i\in\mathfrak{I}} l_i \sum_{\tilde\imath\in\widetilde{\mathsf{proj}}^{-1}(i)} \tilde\imath = \sum_{\tilde\imath\in\widetilde{\mathfrak{I}}} m n_{\tilde\imath}\tilde\imath.$$

Thus, for every $\tilde\imath \in \widetilde{\mathsf{proj}}^{-1}(i)$

$$m n_{\tilde\imath} = l_i$$

and since m is not zero all the $n_{\tilde\imath}$ for the same i coincide. This shows that $\sum_{\tilde\imath\in\widetilde{\mathfrak{I}}} n_{\tilde\imath}\tilde\imath$ is already in the image of $\mathbb{Z}^{\mathfrak{I}}$ and so zero in $\mathbb{Z}^{\widetilde{\mathfrak{I}}}\,/\,\mathbb{Z}^{\mathfrak{I}}$.

By contrast, the set $\mathcal{J}$ is a subset of $\widetilde{\mathcal{J}}$ and this injection can be extended linearly to the induced free abelian groups

$$\iota : \mathbb{Z}^{\mathcal{J}} \hookrightarrow \mathbb{Z}^{\widetilde{\mathcal{J}}}\,. \tag{2.5}$$

Its restriction to the subgroup of formal integral linear combinations of degree 0 gives an injection in the analogue subgroup for the blow-up

$$\iota : D \hookrightarrow \widetilde{D}.$$

2.3.2 The Dual Graph of a "Blow-up"

Recall the definition of X as character group of the torus T of $(\mathcal{N}(J_C)_k)^0$ (the connected component of 0 of the special fiber of the NÉRON model of the JACOBIAN of C) and Φ as the group of connected components of $\mathcal{N}(J_C)_k$. To relate X and Φ to the sets $\widetilde{\mathfrak{I}}$ and $\widetilde{\mathcal{J}}$ we will keep to the previous section as an orientation. We first orient the two components passing through each singular point $\tilde\imath$ in order to find a unique analogous ordering for the blow-up. The map

$$\widetilde{\alpha} : \mathbb{Z}^{\widetilde{\mathfrak{I}}} \to \widetilde{D}$$

is defined similarly as α above, such that we obtain a commutative square with τ and ι

$$\begin{tikzcd}
\mathbb{Z}^{\mathfrak{I}} \arrow[r, "\alpha"] \arrow[d, "\tau"'] & D \arrow[d, "\iota"] \\
\mathbb{Z}^{\widetilde{\mathfrak{I}}} \arrow[r, "\widetilde{\alpha}"] & \widetilde{D}.
\end{tikzcd}$$

Since the curve $\mathcal{C}_k$ is connected, the derived graph is connected and hence by the theory of graphs the map $\widetilde{\alpha}$ is surjective as well as the map α. We know already that X is the kernel of $\widetilde{\alpha}$ in analogy to the previous section. Letting Y be the kernel of α – this is not a priori X since we are not dealing with a regular minimal model as above – we see that τ and ι induce a map $\kappa : Y \to X$ together with a commutative diagramm of two short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & Y \arrow[r] \arrow[d, "\kappa"'] & \mathbb{Z}^{\mathfrak{I}} \arrow[r, "\alpha"] \arrow[d, "\tau"'] & D \arrow[r] \arrow[d, "\iota"'] & 0 \\
0 \arrow[r] & X \arrow[r] & \mathbb{Z}^{\widetilde{\mathfrak{I}}} \arrow[r, "\widetilde{\alpha}"] & \widetilde{D} \arrow[r] & 0.
\end{tikzcd} \tag{2.6}$$

We know already that τ and ι are injective, and so is κ as restriction of τ. The cokernel of κ, X/Y, is an abelian torsion group (which can be seen by counting ranks). But we have already shown that the cokernel of τ is torsion free. The Snake Lemma gives rise to a short exact sequence

$$0 \to \operatorname{Coker}(\kappa) \to \operatorname{Coker}(\tau) \to \operatorname{Coker}(\iota) \to 0,$$

and therewith a canonical injection $\operatorname{Coker}(\kappa) \hookrightarrow \operatorname{Coker}(\tau)$. So the group X/Y must in fact be zero. Therefore, κ is an isomorphism identifying Y with X.

Remark 2.3.2. This corresponds to the fact, that the dual graph of $\mathcal{C}_k$ is replaced by a homotopic graph when $\mathcal{C}_k$ is replaced by its blow-up. And we can continue to use the strategy above.

So we find (applying again Albanese respectively Picard functoriality) that

$$\Phi \cong \mathrm{Coker}(u),$$

where $u : X \to X^\vee = \mathrm{Hom}(X, \mathbb{Z})$ is the restriction of the Euclidean pairing on $\mathbb{Z}^{\widetilde{\mathcal{J}}}$ to X. By construction of the blow-up, one sees, that equivalently this pairing can be derived by restricting to $Y \cong X$ the non-degenerate diagonal pairing on $\mathbb{Z}^{\mathcal{J}}$ with strictly positive entries $e(i)$. Hence the cokernel of this pairing is isomorphic to the sum of quotients

$$\mathrm{Hom}(\mathbb{Z}^{\mathcal{J}}, \mathbb{Z}) / \mathbb{Z}^{\mathcal{J}} \cong \bigoplus_{i \in \mathcal{J}} (\mathbb{Z} / e(i)\, \mathbb{Z})\,.$$

By consequence, the calculation of X and Φ in the case that $\mathcal{C}$ is an admissible model of C runs as in the case of a minimal regular model, except for the complication, that for the pairing the positive integers $e(i)$ on the diagonal must be taken into account. Notably, there is the following continuative theorem.

Theorem 2.3.3. *There is a natural homomorphism of groups*

$$\vartheta : D \to \Phi,$$

whose cokernel is a quotient of the group $\mathrm{Hom}\left(\mathbb{Z}^{\mathcal{J}}, \mathbb{Z}\right) / \mathbb{Z}^{\mathcal{J}}$.

Proof: Recall that Φ is the cokernel of u, thus $\Phi \cong \mathrm{Hom}(X, \mathbb{Z})/X$ identifying X with its image. By (2.6) and the above said, we can write

$$\mathrm{Hom}(X, \mathbb{Z}) \cong \mathrm{Hom}\left(\mathbb{Z}^{\mathcal{J}}, \mathbb{Z}\right) / X^\perp,$$

where $X^\perp$ is sort of an "orthogonal complement" of X, i.e. the group of linear forms on $\mathbb{Z}^{\mathcal{J}}$ which vanish on X. It is an easy task to check injectivity, well-definition and surjectivity with linear algebra. This provides an isomorphism

$$\Phi \cong \mathrm{Hom}\left(\mathbb{Z}^{\mathcal{J}}, \mathbb{Z}\right) / \left(X^\perp \oplus X\right).$$

Consider the subgroup of the right-hand-side

$$\mathbb{Z}^{\mathcal{J}} \,/\, \left((X^\perp \cap \mathbb{Z}^{\mathcal{J}}) \oplus X\right),$$

which we will denote Φ_0 as subgroup of the left-hand-side. Finally we get an isomorphism

$$\Phi/\Phi_0 \cong \left(\mathrm{Hom}\left(\mathbb{Z}^{\mathcal{J}}, \mathbb{Z}\right) / \left(X^\perp \oplus X\right)\right) \Big/ \left(\mathbb{Z}^{\mathcal{J}} / (X^\perp \cap \mathbb{Z}^{\mathcal{J}})\right) \cong \left(\mathrm{Hom}(\mathbb{Z}^{\mathcal{J}}, \mathbb{Z}) / \mathbb{Z}^{\mathcal{J}}\right) / \sim,$$

which is a quotient of $\mathrm{Hom}(\mathbb{Z}^{\mathcal{J}}, \mathbb{Z})/\mathbb{Z}^{\mathcal{J}}$. We have already seen that this latter group is the sum of the quotient groups $\mathbb{Z}/e(i)\,\mathbb{Z}$. Note that Φ_0 is isomorphic to a quotient of $\mathbb{Z}^{\mathcal{J}}/X$ by

$$\mathbb{Z}^{\mathcal{J}} \,/\, \left((X^\perp \cap \mathbb{Z}^{\mathcal{J}}) \oplus X\right) \cong (X^{\mathcal{J}}/X) \,/\, \left(\left((X^\perp \cap \mathbb{Z}^{\mathcal{J}}) \oplus X\right)/X\right).$$

But $\mathbb{Z}^{\mathcal{J}}/X$ is the cokernel of α in (2.6), thence isomorphic to D. So we can define $\vartheta : D \to \Phi$ to be the projection map of D onto Φ_0

$$D \xrightarrow{\mathsf{proj}} D/\sim \quad \cong \quad \Phi_0 \hookrightarrow \Phi.$$

The cokernel Φ/Φ_0 of this map is clearly as desired. □

Chapter 3

Modular Curves and Quaternion Algebras

In this chapter p and q are distinct primes and M is a natural number not divisible by pq. We want to compare the reductions at q of the modular curves of level pqM and qM respectively.

3.1 Suitable Models of Modular Curves

In this first section, we are going to understand modular curves from the quaternion point of view. In order to do this, we need a few basic concepts, which we will introduce below.

3.1.1 Construction of Suitable Models of Modular Curves

Recall from the first chapter the construction of modular curves over $\mathbb{Q}$. By Theorem 1.4.7 the non-cuspidal points on $X_0(N)$ correspond to the isomorphism classes of pairs (E, B), where E is an elliptic curve and B a cyclic subgroup of order N. This interpretation turns out to be quite useful.

We want to apply the results and strategies of the previous chapter to the curve $C = X_0(qM)$ over $\mathbb{Q}_q$ (and later $C = X_0(pqM)$ over $\mathbb{Q}_q$). We just give an heuristic approach to the construction of the admissible model $\mathcal{C}$ of the curve C over $\mathbb{Z}_q$. For detailed information see [4]. Hereto, let us recall some facts about elliptic curves.

Let E be an elliptic curve over a field k of characteristic q.

Definition 3.1.1. The elliptic curve E is called *ordinary* if

$$E[q](\overline{k}) \cong \mathbb{Z}/q\mathbb{Z}.$$

It is called *supersingular* if

$$E[q](\overline{k}) \cong \{0\}.$$

Proposition 1.1.15 tells us that these are the only cases, which can occure.

While there is an infinite number of isomorphism classes of ordinary elliptic curves over k, there is only a finite number of isomorphism classes of supersingular elliptic curves over k. The latter ones are of interest for us. In general there are only two q-isogenies, i.e. isogenies of degree q, on E over k:

1. The FROBENIUS morphism $\mathsf{Frob}_q : E \to E^{(q)}$ introduced in Section 1.1.4.
2. Its dual, the so-called *Verschiebung*, $\mathsf{Ver}_q : E \to E^{(-q)}$.

The FROBENIUS isogeny is purely inseparable. If E is ordinary, the Verschiebung is *étale* and its kernel is easily seen to be

$$\mathrm{Ker}(\mathsf{Ver}_q)(\overline{k}) = E[q](\overline{k}) \cong \mathbb{Z}/q\,\mathbb{Z},$$

whereas in the supersingular case

$$\mathsf{Ver}_q = \mathsf{Frob}_q\,.$$

Remark 3.1.2. Let q and M be the integers introduced at the beginning of this chapter. To give an enhanced elliptic curve $(E, C_{qM}) \in X_0(qM)$, note that $C_{qM} \cong C_q \oplus C_M$, where C_q and C_M are cyclic subgroups of order q and M respectively, because $q \nmid M$ (and E abelian). So $(E, C_{qM}) \cong (E, C_M, C_q)$ and the subgroup of order q can be chosen to be $\mathrm{Ker}(\mathsf{Frob}_q)$ or $\mathrm{Ker}(\mathsf{Ver}_q)$. In the supersingular case both subgroups coincide.

In his article [6] DEURING stated the following equivalences for supersingular elliptic curves.

Theorem 3.1.3. *Let k be a (perfect) field of characteristic q and E/k an elliptic curve. Then the following are equivalent:*

1. *$E[q^r] = 0$ for one (all) $r \geq 1$.*
2. *Ver_{q^r} is purely inseparable for one (all) $r \geq 1$.*
3. *The multiplication-by-q map is purely inseparable and $j(E) \in \mathbb{F}_{q^2}$.*
4. *$\mathrm{End}_{\overline{k}}(E)$ is an order in a quaternion algebra.*
5. *The formal group associated to E has height 2.*

If these equivalent conditions do not hold, then $E[q^r] \cong \mathbb{Z}/q^r\,\mathbb{Z}$ for all $r \geq 1$ and the formal group associated to E has height 1. Further, if $j(E) \in \overline{\mathbb{F}}_q$, then $\mathrm{End}(E)$ is an order in a quadratic imaginary field.

PROOF: See [45, V.Theorem 3.1]. □

Let us return to our initial setting, that means $C = X_0(qM)$ and $\mathcal{C}$ its admissible model over $\mathbb{Z}_q$. It is known [4], that the curve $\mathcal{C}_{\mathbb{F}_q}$ is just the set of elliptic curves (E, C_{qM}) over $\overline{\mathbb{F}}_q$ enhanced by a subgroup of order qM. By Remark 3.1.2 during our review of elliptic curves, we know that $\mathcal{C}_{\mathbb{F}_q}$ is composed of two copies of the curve $X_0(M)_{\mathbb{F}_q}$ attached at their supersingular points, i.e. those arising from supersingular elliptic curves over $\overline{\mathbb{F}}_q$; a supersingular point on the first copy being identified with its FROBENIUS transform on the second copy. In the terminology of Chapter 2, the set $\mathcal{J}$ of irreducible components, that gives the vertices of the dual graph associated with $\mathcal{C}_{\mathbb{F}_q}$ has two elements. The set $\mathcal{I}$ of singular points – the edges of the graph – is the set

$$\Sigma(M) = \big\{(E, C_M) \,\big|\, C_M < E\,,\, \mathrm{ord}(C_M) = M\big\}$$

of $\overline{\mathbb{F}}_q$-isomorphism classes of supersingular elliptic curves enhanced of order M. Each edge in the dual graph connects the two distinct vertices, no edge starts and leaves from the same vertex. So we may for our convenience orient the $i \in \mathcal{I}$ in the "same direction", such that the ordering of the vertices $\{j_1(i), j_2(i)\}$ are in fact independent of i. With these conventions we get:

Proposition 3.1.4. *The character group X in the case $C = X_0(qM)$ is the group of divisors of degree 0 on the set $\Sigma(M)$ of supersingular points of $X_0(M)_{\overline{\mathbb{F}}_q}$.*

PROOF: In Proposition 2.2.7 we have seen that X is the kernel of the group homomorphism

$$\alpha : \mathbb{Z}^{\Sigma(M)} \to D\,,\; \alpha(i) = j_1(i) - j_2(i),$$

where D is the set of degree-0 divisors on $\mathcal{J}$. Let $\sum_{i\in\Sigma(M)} n_i i \in \operatorname{Ker}(\alpha)$. Then

$$\begin{aligned} 0 &= \alpha\left(\sum n_i i\right) \\ &= \sum n_i \left(j_1(i) - j_2(i)\right) \\ &= \left(\sum n_i\right)\left(j_1(i) - j_2(i)\right), \end{aligned}$$

where the last equality holds since $j_1(i)$ and $j_2(i)$ are independent of i. Hence, this is zero in the set of divisors if and only if

$$\sum n_i = 0 \in \mathbb{Z},$$

for the two concerned copies of $X_0(M)_{\mathbb{F}_q}$ are distinct. Moreover, $\sum n_i i$ is a zero divisor in $\mathbb{Z}^{\Sigma(M)}$. Since all the arguments work in both directions, this shows that the kernel of α, X, is the set of degree-0 divisors on $\Sigma(M)$ as claimed. □

3.1.2 Linking Eichler Orders with Enhanced Elliptic Curves

We will continue by using the same notations as in the previous sections. We will study the dual graph $\mathcal{G}$ of $\mathcal{C}_{\mathbb{F}_q}$ in terms of quaternions.

Definition 3.1.5. A *quaternion algebra* H of center K is a central algebra of dimension 4 as vector space over K, such that there is a separable algebra L of dimension 2 over K and an invertible element ϑ of K with

$$H = L + Lu,$$

where $u \in H$ verifies

$$u^2 = \vartheta \text{ and } um = \overline{m}u \tag{3.1}$$

for all $m \in L$, where $m \mapsto \overline{m}$ is the non-trivial K-automorphism of L.

This definition holds in every characteristic. It is easy to verify, that H over K is a central simple algebra, that is an algebra of center K without bilateral non-trivial ideal, or in other words a simple algebra which has finite dimension over its center. Conversely one can show, that every central simple algebra of dimension 4 over K is a quaternion algebra. The multiplication law is deduced from (3.1).

Definition 3.1.6. The *conjugation* is the K-endomorphism $h \mapsto \overline{h}$ of H extending the non-trivial K-automorphism of L defined by $u \mapsto -u$. It is an *involutive anti-automorphism.* The reduced trace of $h \in H$ is

$$\operatorname{tr}(h) = h + \overline{h}$$

and the reduced norm is

$$\operatorname{Norm}(h) = h\overline{h}.$$

In our approach, we have to deal with ramification of a quaternion algebra.

Definition 3.1.7. Let K be a global field and H/K a quaternion algebra. A place $\nu \in K$ ramifies in H if the tensor product $H_\nu = H \otimes_K K_\nu$ is a field, where K_ν is the local field associated to ν.

We will also take advantage of the Skolem-Noether *Theorem*:

Theorem 3.1.8. *Let A and B be simple rings, and $K = Z(B)$ the center of B. Suppose that the dimension of B over the field K is finite, that is, B is a central simple algebra. Then if $f, g : A \to B$ are K-algebra homomorphisms, there exists a unit b in B, such that $g(a) = bf(a)b^{-1}$ for all $a \in A$.*

If $D = p_1 \cdots p_{2m}$ is a product of an even number of distinct primes including ∞ (the archimedian prime) in $\mathbb{Z}$, there is a unique (up to isomorphism) quaternion algebra H_D over $\mathbb{Q}$ satisfying

$$H_D \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \begin{cases} \mathbf{M}_2(\mathbb{Q}_\ell) & \text{if } \ell \nmid D, \\ H_\ell & \text{if } \ell \mid D, \end{cases} \tag{3.2}$$

where H_ℓ is the unique quaternion algebra over $\mathbb{Q}_\ell$. The p_i are the *ramification primes* and D is the *discriminant* of H_D.

Now let $\mathbf{E} = (E, C_M)$ be a supersingular enhanced elliptic curve as above. In an evident way, one can define a morphism of enhanced elliptic curves of order M as morphism between elliptic curves taking one subgroup to the other. It is well known, that for each enhanced elliptic curve $\mathbf{E}$ the $\mathbb{Q}$-algebra

$$H = \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is the unique quaternion algebra over $\mathbb{Q}$, which is ramified at q and ∞. (We say H has discriminant q, although it is in fact "$q\infty$".) The fact that E is supersingular implies that the ring $\operatorname{End}(E)$ is a maximal order in H, while its subring $\operatorname{End}(\mathbf{E}) = \{\sigma \in \operatorname{End}(E) \big| \sigma(C_M) = C_M\}$ is an EICHLER order of level M.

Definition 3.1.9. By a *maximal order* of a quaternion algebra H over a number field K, we mean an $\mathcal{O}_K$-subalgebra $\mathcal{O}_H$ with $\mathcal{O}_H \otimes_{\mathcal{O}_K} K = H$. There exists at least one and any two are conjugate. An EICHLER *order* is the intersection of two maximal orders. The EICHLER order is oriented, if the two maximal orders are specified as ordered pair. For H_D, an EICHLER order is of level M, if for every prime $\ell \nmid D$ it is after tensoring with $\mathbb{Z}_\ell$ isomorphic to $\left\{\mathcal{M} \in \mathbf{M}_2(\mathbb{Z}_\ell) \,\middle|\, \mathcal{M} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod \ell^n\right\}$, where ℓ^n is the largest power of ℓ dividing M.

In our case, consider the canonical quotient map $\lambda : E \to E/C_M$. There is a natural inclusion of $\operatorname{End}(E/C_M)$ into $H = \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ given by

$$\sigma \mapsto \lambda^{-1}\sigma\lambda,$$

which makes $\operatorname{End}(E/C_M)$ into a maximal order of H. Taking into acount the definition of $\operatorname{End}(\mathbf{E})$, it is easy to see that

$$\operatorname{End}(\mathbf{E}) = \{\sigma \in \operatorname{End}(E) \big| \sigma(C_M) = C_M\} \subset \operatorname{End}(E/C_M),$$

and is therefore the intersection of the two maximal orders $\operatorname{End}(E)$ and $\operatorname{End}(E/C_M)$.

Let Φ be again the group of connected components of the special fiber $\mathcal{N}(J(X_0(qM)))_{\mathbb{F}_q}$ at q of the NÉRON model of the JACOBIAN of our modular curve, D the degree-0 divisors on $\mathcal{J}$ and ϑ the natural homomorphism of Theorem 2.3.3.

Proposition 3.1.10. *The finite group Φ is an extension by the cyclic group $\vartheta(D)$ of a group of exponent dividing* 12.

PROOF: The automorphism group of $\mathbf{E}$ is a subgroup of $\operatorname{Aut}(E)$. The latter one is well-known to be of order dividing 24. This is shown with the help of elementary calculations in [45, III.Theorem 10.1]. Further, since $\operatorname{Aut}(\mathbf{E})$ contains the subgroup $\{\pm 1\}$, it is of even order. According to DELIGNE-RAPOPORT in [4, VI.Theorem 6.9]

$$e(i) = \frac{\#\left(\operatorname{Aut}(\mathbf{E})\right)}{2}, \tag{3.3}$$

the $e(i)$ as defined in Section 2.3.1. So $e(i)$ is a divisor of 12.

By Theorem 2.3.3, we dispose of a short exact sequence

$$0 \to \vartheta(D) \to \Phi \to \Phi/\vartheta(D) \to 0,$$

and the cokernel $\Phi/\vartheta(D)$ is isomorphic to the direct sum $\bigoplus \mathbb{Z}/e(i)\mathbb{Z}$. As all $e(i)$ divides 12, the assertion follows. □

We next sketch the description of the set $\mathcal{I} = \Sigma(M)$ of supersingular points, that is of supersingular enhanced elliptic curves, in terms of the arithmetic of quaternion algebras. We start by fixing a supersingular elliptic curve $\mathbf{E}_0$ and keep track of the isomorphism classes of enhanced elliptic curves gotten by isogenies from $\mathbf{E}_0$. This is possible, since all supersingular elliptic curves (without considering further structure) are isogenous.

Remark 3.1.11. Recall that for a given ring R its *adelization* is defined to be

$$R_f := R \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}},$$

where $\widehat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$ is the profinite completion of $\mathbb{Z}$.

Definition 3.1.12. For each enhanced elliptic curve $\mathbf{E} = (E, C_M)$ over $\overline{\mathbb{F}}_q$ define the *q-adelic* TATE *module* by

$$T(\mathbf{E}) = T_q(E) \times \prod_{\ell \neq q} T_\ell(E), \tag{3.4}$$

where $T_q(E)$ is the DIEUDONNÉ *module* of E.

By definition, the TATE-adelic module associated to an enhanced elliptic curve is unique.

Remark 3.1.13. This distinction is necessary in characteristic q, since the classical TATE module, i.e. with respect to êtal cohomology, is just defined over primes not equal to the field characteristic. Elsewise, one has to make the construction via DE RHAM cohomology. We will not go into details, but accept these vague hints pointing to [29, §3].

Since we started with an enhanced elliptic curve $\mathbf{E} = (E, C_M)$, there is a distinguished cyclic subgroup of $T(\mathbf{E})/MT(\mathbf{E})$ which we call again C_M. For our fixed elliptic curve $\mathbf{E}_0 = (E_0, B_M)$ define

$$R = \mathrm{End}(\mathbf{E}_0) \quad \text{and} \quad H = R \otimes_{\mathbb{Z}} \mathbb{Q},$$

and let R_f respectively H_f be their adelizations (as rings). For an arbitrary supersingular enhanced elliptic curve $\mathbf{E}$, one can select a non-trivial element $\lambda \in \mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$, which can be written as $\lambda = \tilde{\lambda} \otimes \frac{r}{s}$ with a non-zero fraction $\frac{r}{s}$, since the tensor product is $\mathbb{Z}$-bilinear. We define $\lambda\left(T(\mathbf{E})\right) := T\left(\tilde{\lambda}(\mathbf{E})\right) \otimes \frac{r}{s}$. Per definitionem, $\lambda(\mathbf{E}) \subset \mathbf{E}_0$ is an elliptic curve. This justifies the definition of $T\left(\lambda(\mathbf{E})\right)$ and the definition above makes sence. What is more, λ identifies $T(\mathbf{E})$ with the sublattice $T\left(\tilde{\lambda}(\mathbf{E})\right) \otimes \frac{r}{s}$ of

$$V(\mathbf{E}_0) := T(\mathbf{E}_0) \otimes_{\mathbb{Z}} \mathbb{Q}\,. \tag{3.5}$$

From the definition of the adelic TATE module, it is clear that for the two sublattices $T(\mathbf{E})$ and $T(\mathbf{E}_0)$ of $V(\mathbf{E}_0)$ there should be an element $g \in H_f^*$, such that

$$gT(\mathbf{E}) \cong T(\mathbf{E}_0). \tag{3.6}$$

If there are two such elements g_1 and g_2 satisfying equation (3.6), then $g_1^{-1}T(\mathbf{E}_0) = g_2^{-1}T(\mathbf{E}_0)$ and this is equivalent to $g_1^{-1}g_2 \in R_f^*$. By consequence, there is a unique $g \in H_f^*/R_f^*$ such that (3.6) holds. This means that $gT(\mathbf{E})$ and $T(\mathbf{E}_0)$ coincides as sublattices of $V(\mathbf{E}_0)$ and that the induced morphism

$$g : T(\mathbf{E})/MT(\mathbf{E}) \cong T(\mathbf{E}_0)/MT(\mathbf{E}_0)$$

carries C_M to B_M. So we have got an equality of enhanced sublattices. However, because of the ambiguity in the choice of λ – indeed, two distinct λ's in $\mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$ give rise to the same sublattice $\lambda\left(T(\mathbf{E})\right)$ in $V(\mathbf{E}_0)$, if and only if they differ by an element of $\left(\mathrm{End}(T(\mathbf{E}_0) \otimes_{\mathbb{Z}} \mathbb{Q})\right)^* \cong H^*$ – g is well defined only in

$$H^* \backslash H_f^* / R_f^*.$$

Proposition 3.1.14. *There is a bijection $\Phi_{\mathbf{E}_0}$ from the set $\Sigma(M)$ of supersingular points of $X_0(M)_{\overline{\mathbb{F}}_q}$ to the coset space $H^*\backslash H_f^*/R_f^*$.*

Proof: The desired bijection comes from the construction above. First, every element $\mathbf{E} \in \Sigma(M)$ corresponds to a unique adelic Tate module $T(\mathbf{E})$ (3.4), which in turn, corresponds to a sublattice of $V(\mathbf{E}_0)$ unique up to a $\mathbb{Q}$-automorphism of $\mathbf{E}_0$. As we have seen, this sublattice is uniquely determined by $g \in H^*\backslash H_f^*/R_f^*$. □

Remark 3.1.15. There is a nice variant of this proposition proven by Vignéras in [48, p.87]: *The set $\Sigma(M)$ is naturally isomorphic to the set of right ideal classes of the* Eichler *order R of level M in H.*

Now we can deduce the main result of this section. Let B and B' be maximal orders of a quaternion algebra of discriminant q, such that the intersection $S = B \cap B'$ is an Eichler order of level M in B.

Definition 3.1.16. For an enhanced elliptic curve $\mathbf{E}$ over $\overline{\mathbb{F}}_q$, a homomorphism $(S, B) \to (\mathrm{End}(\mathbf{E}), \mathrm{End}(E))$ is a homomorphism $B \to \mathrm{End}(E)$ carrying S to $\mathrm{End}(\mathbf{E})$. Let $\kappa : (S, B) \to (\mathrm{End}(\mathbf{E}), \mathrm{End}(E))$ and $\kappa' : (S, B) \to \big(\mathrm{End}(\mathbf{E}'), \mathrm{End}(E')\big)$ be two homomorphisms. We say that $(\mathbf{E}, \kappa)$ and $(\mathbf{E}', \kappa')$ are isomorphic, if there is an isomorphism $\iota : \mathbf{E} \to \mathbf{E}'$ for which the induced isomorphism of rings $\iota : \mathrm{End}(\mathbf{E}) \to \mathrm{End}(\mathbf{E}')$ satisfies $\kappa'\iota = \kappa$.

Proposition 3.1.17. *Taking S and B as defined, there exists an enhanced supersingular elliptic curve $\mathbf{E}$ over $\overline{\mathbb{F}}_q$ and an isomorphism*

$$\kappa : (S, B) \to (\mathrm{End}(\mathbf{E}), \mathrm{End}(E))\,.$$

Moreover, they are unique in the following sense: let $\mathbf{E}'$ be a second elliptic curve of this form and $\kappa' : (S, B) \to (\mathrm{End}(\mathbf{E}), \mathrm{End}(E))$ an isomorphism. Then the pair $(\mathbf{E}', \kappa')$ is isomorphic to either of $(\mathbf{E}, \kappa)$ or $(\mathbf{E}^{(q)}, \kappa^{(q)})$.

Proof: As before, fix an enhanced supersingular elliptic curve $\mathbf{E}_0$ and set

$$R = \mathrm{End}(\mathbf{E}_0)\,, \qquad A = \mathrm{End}(E_0)\,, \qquad H = R \otimes_{\mathbb{Z}} \mathbb{Q}\,.$$

Because of the above mentioned uniqueness of quaternion algebras of the form (3.2), one can choose and fix an isomorphism $B \otimes_{\mathbb{Z}} \mathbb{Q} \cong H$.

The argumentation is now performed in four steps. To start, we establish a one-one correspondence between $H_f^*/(R_f^*\,\mathbb{Q}^*)$ and the set of isomorphism classes of pairs $(\mathbf{E}, \kappa)$, where κ is an injection $\mathrm{End}(\mathbf{E}) \otimes \mathbb{Q} \hookrightarrow H$. In the second step, we establish a necessary and sufficient global condition, that κ maps $\mathrm{End}(\mathbf{E})$ to R and $\mathrm{End}(E)$ to A to make up the required isomorphism. Afterwards, we verify this condition locally for three disjoint sets of primes. Drawing global conclusions from these local results, we see that there are two isomorphism classes of pairs $(\mathbf{E}, \kappa)$ such that $(\mathrm{End}(\mathbf{E}), \mathrm{End}(E))$ is isomorphic to (S, B) via κ.

Consider all pairs $(\mathbf{E}, \kappa)$ consisting of an enhanced elliptic curve and an injection into H (after tensoring with $\mathbb{Q}$). A priori, they do not map $\mathrm{End}(\mathbf{E})$ to S and $\mathrm{End}(E)$ to B. For each non-zero element $\lambda \in \mathrm{Hom}(E, E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$, we obtain such an injection

$$\kappa_\lambda : \mathrm{End}(\mathbf{E}) \otimes \mathbb{Q} \to H\,, \quad e \mapsto \lambda e \lambda^{-1}.$$

This is clearly well defined (although $0 \neq \lambda \in \mathrm{Hom}(E, E_0)$ may not be invertible over $\mathbb{Z}$, it is after tensoring with $\mathbb{Q}$) and an injection (sending id to id). By the Skolem-Noether Theorem, every κ is of the form κ_λ. Indeed, with $A = \mathrm{End}(\mathbf{E}) \otimes \mathbb{Q}$, $B = H$, $f = \kappa_\lambda$ and $g = \kappa$, there is, for a fixed $\lambda \neq 0$, $h \in H$ such that for all $e \in \mathrm{End}(\mathbf{E}) \otimes \mathbb{Q}$,

$$\begin{aligned} \kappa(e) &= h\kappa_\lambda(e)h^{-1} \\ &= h\lambda e\lambda^{-1}h^{-1} \\ &= \kappa_{h\lambda}(e), \end{aligned}$$

where $h\lambda$ is in fact in $\mathrm{Hom}(E, E_0)\otimes\mathbb{Q}$. What is more, the choice of λ is unique up to multiplication by a non-zero element in $\mathbb{Q}$: $\lambda \in \mathrm{Hom}(E, E_0) \otimes \mathbb{Q}$ and $\lambda' \in \mathrm{Hom}(E', E_0) \otimes \mathbb{Q}$ give isomorphic pairs $(\mathbf{E}, \kappa)$ and $(\mathbf{E}', \kappa')$ if and only if there is an isomorphism $\iota : \mathbf{E} \cong \mathbf{E}'$ such that $\kappa'\iota = \kappa$. This means, $\lambda e\lambda^{-1} = \lambda'\iota e\iota^{-1}\lambda^{-1}$ for $e \in \mathrm{End}(\mathbf{E}) \otimes \mathbb{Q}$, and hence λ and $\lambda'\iota$ differ by an element of $\mathbb{Q}^*$. We have just seen, that each $\lambda \in \mathrm{Hom}(E, E_0) \otimes_\mathbb{Z} \mathbb{Q}$ identifies $T(\mathbf{E})$ with a sublattice of $V(\mathbf{E}_0)$ and determines $g \in H_f^*/R_f^*$ uniquely. In other words, the construction

$$(\mathbf{E}, \lambda) \mapsto (T(\mathbf{E}) \subset V(\mathbf{E}_0))$$

furnishes a one-to-one correspondence between the set of isomorphism classes of pairs $(\mathbf{E}, \lambda)$ and the set H_f^*/R_f^* of "enhanced" lattices in $V(\mathbf{E}_0)$. After all, we have to divide by $\mathbb{Q}^*$ on both sides to receive a one-one correspondence between the set of isomorphism classes of pairs $(\mathbf{E}, \kappa)$, where $\mathbf{E}$ is an elliptic curve and κ an injection $\mathrm{End}(\mathbf{E}) \otimes \mathbb{Q} \hookrightarrow H$, and the set $H_f^*/(R_f^*\,\mathbb{Q}^*)$.

Select $g \in H_f^*$ and consider the associated pair $(\mathbf{E}, \kappa)$. By definition of κ as conjugation by an element $\lambda \in \mathrm{Hom}(E, E_0)\otimes_\mathbb{Z}\mathbb{Q}$, which corresponds to g, the image of $\mathrm{End}(\mathbf{E})$ under κ is the order $H \cap (gR_fg^{-1})$, that of $\mathrm{End}(E)$ is $H \cap (gA_fg^{-1})$. We look for an injection κ that maps $\mathrm{End}(\mathbf{E})$ to S and $\mathrm{End}(E)$ to B. With the above fixed isomorphism $B \otimes_\mathbb{Z} \mathbb{Q} \cong H$, we see that κ satisfies these conditions if and only if the following equalities hold:

$$gR_fg^{-1} = S_f\,, \qquad gA_fg^{-1} = B_f. \tag{3.7}$$

To verify these conditions, it suffices to verify them locally at every prime ℓ for the occuring rings tensored with $\mathbb{Z}_\ell$ instead of $\widehat{\mathbb{Z}}$. For g now in $H_\ell^* = H^* \otimes_\mathbb{Z} \mathbb{Z}_\ell$, we verify for which g's, if any, the equalities

$$gR_\ell g^{-1} = S_\ell\,, \qquad gA_\ell g^{-1} = B_\ell \tag{3.8}$$

hold. (3.7) holds, if and only if (3.8) holds for every prime ℓ. For this purpose it makes sense to split the set of all primes into three disjoint sets.

When $\ell = q$, there is no condition on g. Indeed, for the unique quaternion algebra H_q over $\mathbb{Q}_q$, we can apply what VIGNÉRAS stated for local fields in [48, Lemme 1.5, p.34] and see that H_q over $\mathbb{Q}_q$ has a unique maximal order, namely B_q. Thus trivially conjugation with any $g \in H_q^*$ takes A_q to B_q and R_q to S_q. By the way, there are two classes in $H_q^*/(R_q^*\,\mathbb{Q}_q^*)$. We have a valuation on H_q^* extending $\nu_q^{\mathbb{Q}_q}$ on $\mathbb{Q}_q$. By definition of discrete valuation rings, $R_q^* = \left\{a \in H_q^* \,\middle|\, \nu_q^{H_q}(a) = 0\right\}$ is the kernel of $\nu_q^{H_q}$ and it makes sense to divide it out: $\overline{\nu}_q^{H_q} : H_q^*/R_q^* \to \mathbb{Z}$ in order to obtain an isomorphism

$$H_q^*/R_q^* \cong \mathbb{Z}\,.$$

$\mathbb{Z}_q$ is ramified in R_q, more precisely, there exists $\pi \in R_q$ such that $\pi^2 = \pm q$, i.e. $\nu_q^{H_q}(q) = 2 \equiv 0$ mod 2. Thence, $\nu_q^{H_q}(\mathbb{Q}_q^*) = 2\,\mathbb{Z}$, and $\overline{\nu}_q^{H_q}$ induces an isomorphism

$$H_q^*/(R_q^*\,\mathbb{Q}_q^*) \cong \mathbb{Z}\,/2\,\mathbb{Z}\,.$$

When ℓ is prime to qM, A and R, as well as B and S, coincide over ℓ. So the two equalities of (3.8) melt into one. As we have seen in (3.2), this is the case $H_q \cong \mathbf{M}_2(\mathbb{Q}_\ell)$. According to [48, Théorèm 2.3, p.38], all maximal orders of $\mathbf{M}_2(\mathbb{Q}_\ell)$ are conjugate, and so the equality can be satisfied. Further, the g satifying the equation build one class in $H_q^*/(R_q^*\,\mathbb{Q}_q^*)$, because the normaliser of $\mathbf{M}_2(\mathbb{Z}_\ell)$ in $\mathbf{GL}_2(\mathbb{Q}_\ell)$ is $\mathbf{GL}_2(\mathbb{Z}_\ell)\,\mathbb{Q}_\ell^*$.

Remains the case when ℓ divides M. Again $H_\ell \cong \mathbf{M}_2(\mathbb{Q}_\ell)$. Let $n > 0$ be the valuation of M at ℓ, that is the largest power of ℓ dividing M. A lemma due to Hijikata, stated in [48, Lemme 2.4, p.39] giving conditions for an order to be Eichler, shows that the two Eichler orders R_ℓ and S_ℓ are each intersections of a unique pair of maximal orders

$$S_\ell = B_\ell \cap B'_\ell \text{ and } R_\ell = A_\ell \cap A'_\ell,$$

where A' is the endomorphism ring gotten by dividing E by the enhancing subgroup of order M. By consequence, we can substitute the first equality of (3.8) by

$$gA'_\ell g^{-1} = B'_\ell.$$

As short excurse note, that for any prime p there is a notion of a tree $\mathcal{T}$ of $\mathbf{PGL}_2(\mathbb{Q}_p)$ associated to the set $\mathcal{L}$ of homothety classes of lattices in $\mathbb{Q}_p^2$, the Bruhat-Tits *tree*. The vertices of $\mathcal{T}$ are simply the elements of $\mathcal{L}$. Given two such elements $\overline{L}_1$, $\overline{L}_2$ we may assume that, after lifting them to real lattices L_1 and L_2 and multiplying L_2 by a suitable minimal power of p, $L_1 \supset L_2$. Now $\#(L_1/L_2) = p^n$ for some $n \in \mathbb{N}_0$. We call n the distance *between* $\overline{L}_1$ and $\overline{L}_2$. $\overline{L}_1$ and $\overline{L}_2$ are said to be connected by an edge, if their distance is equal to 1. As any lattice in $\mathbb{Q}_p^2$ is isomorphic to $\mathbb{Z}_p^2$, there are exactly $\#\,\mathbb{P}^1(\mathbb{Z}\,/p\,\mathbb{Z}) = p+1$ sublattices of index p. Consequently, there are exactly $(p+1)$ vertices which are at a distance of 1 from $\mathbb{Z}_p^2$. Contrariwise, every vertex of $\mathcal{T}$ is connected to $(p+1)$ other vertices by means of edges. A well studied (see for example [42, Chapitre II, §1]) case of Bruhat-Tits trees is the tree Δ attached to $\mathbf{SL}_2$ which will occure again in Chapter 4.

We may regard A_ℓ, B_ℓ, A'_ℓ and B'_ℓ as vertices a, b, a', b' of the tree Δ associated to $\mathbf{SL}_2$ over $\mathbb{Q}_\ell$ – for details see [42, Chapitre II]. The vertices of Δ are the lattices in $\mathbb{Q}_\ell^2$ taken modulo homothety. By [48, p.41], there is a one-to-one correspondence between the vertices of Δ and the maximal orders in $\mathbf{M}_2(\mathbb{Q}_\ell)$ sending a lattice L to $\mathrm{End}(L)$. Since R and S are Eichler of level M with $\nu_\ell(M) = n > 0$, the vertices a and b, as well as a' and b' are at distance n from each other. The Elementary Divisor Theorem allows us to choose a basis e_1, e_2 of $\mathbb{Q}_\ell^2$, such that a is represented by the lattice $\mathbb{Z}_\ell\, e_1 \oplus \mathbb{Z}_\ell\, e_2$ and b by $\mathbb{Z}_\ell\, e_1 \oplus \ell^n\, \mathbb{Z}_\ell\, e_2$. Similarly, we can find f_1, f_2 for a' and b'. If $g \in \mathbf{GL}_2(\mathbb{Q}_\ell)$ maps e_i to f_i, then g conjugates A_ℓ to B_ℓ and A'_ℓ to B'_ℓ. This shows existence. If h is a second such element, then $h^{-1}g$ is in the normalizer of A_ℓ and A'_ℓ and hence

$$h^{-1}g \in N(A_\ell) \cap N(A'_\ell) = (A_\ell^*\, \mathbb{Q}_\ell^*) \cap ({A'}_\ell^*\, \mathbb{Q}_\ell^*) = (A_\ell^* \cap {A'}_\ell^*)\, \mathbb{Q}_\ell^* = R_\ell^*\, \mathbb{Q}_\ell *.$$

It follows, that there is again a single class of conjugating g's in $H_q^*/(R_q^*\, \mathbb{Q}_q^*)$.

We can now bring together all this local information and conclude that the $g \in H_f^*$, which conjugate A_f to B_f and R_f to S_f form exactly two classes in $H_f^*/(R_f^*\, \mathbb{Q}_f^*)$. In accordance with our argumentation in the local case $\ell = q$, these classes can be interchanged by left multiplication by any idèle, i.e. any element of H_f^*, trivial outside q and of odd valuation at q. A standard fact, which we will not prove, is that this multiplication corresponds to the Frobenius map. This shows the claimed uniqueness. □

3.2 The Hecke Algebra and the Modular Curve of Level qM

In section 1.4.4 we established in concrete terms the action of the Hecke algebra on modular forms and on cusp forms. Now we want to persue a rather abstract way defining them as correspondences on modular curves. This allows us to define these objects over $\mathbb{Q}$ acting in a compatible way on modular forms, modular Jacobians and homology groups.

3.2.1 Hecke Operators as Correspondences

We can only give an introductory overview of correspondences. Whoever wants to go into details, is referred to [44].

Definition 3.2.1. Let C_1 and C_2 be curves. A *correspondence* $C_1 \rightsquigarrow C_2$ is a triple (C, α, β), where C is a curve and $\alpha : C \to C_1$ and $\beta : C \to C_2$ are non-constant morphisms. One represents a correspondence by a diagram

$$\begin{tikzcd} & C \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ C_1 & & C_2. \end{tikzcd} \tag{3.9}$$

Given a correspondence $C_1 \rightsquigarrow C_2$, the dual correspondence $C_2 \rightsquigarrow C_1$ is obtained by looking at the diagramm in a mirror.

To get a inition into the theory, we will focus on the simple case, when the modular curve is $X_0(N)$ and the Hecke operator is T_p, with $p \nmid N$. To see T_p as correspondence $X_0(N) \rightsquigarrow X_0(N)$, we have to find a curve C and two non-constant morphisms α and β fitting into a diagramm of the form (3.9). It turns out, that $C = X_0(pN)$ and that α and β are degeneracy maps which forget data. To define them, we come back to view $X_0(N)$ as classifying isomorphism classes of pairs $\mathbf{E} = (E, C_N)$ of enhanced elliptic curves. We will not worry about what happens on the cusps, since any rational map on the nonsingular locus of a curve extends uniquely to a morphism. Since p and N are relatively prime and the enhancing subgroups are cyclic, the points of $X_0(pN)$ are the isomorphism classes $(E, C_N \oplus C_p) = (E, C_N, C_p)$. The map α forgets the subgroup C_p of order p and β quotients out by C_p:

$$\begin{tikzcd} & X_0(pN) \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ X_0(N) & & X_0(N), \end{tikzcd}$$

with

$$\begin{array}{rcl} \alpha : (E, C_N \oplus C_p) & \mapsto & (E, C_N) \\ \beta : (E, C_N \oplus C_p) & \mapsto & (E/C_p, (C_N \oplus C_p)/C_p). \end{array} \tag{3.10}$$

Using the language of complex analysis, α and β induce pullback maps on differentials

$$\alpha^*, \beta^* : \mathrm{H}^0\left(X_0(N), \Omega^1\right) \to \mathrm{H}^0\left(X_0(pN), \Omega^1\right),$$

which are nonconstant holomorphic maps. By first pulling back, then pushing forward, we obtain induced maps on differentials

$$\mathrm{H}^0\left(X_0(N), \Omega^1\right) \xrightarrow{\alpha^*} \mathrm{H}^0\left(X_0(pN), \Omega^1\right) \xrightarrow{\beta_*} \mathrm{H}^0\left(X_0(N), \Omega^1\right).$$

We may consider just as well the dual correspondence and obtain a map $\alpha_* \circ \beta^*$ instead of $\beta_* \circ \alpha^*$.

Recalling the identification (1.25) of $\mathcal{S}_2(N)$ with $\mathrm{H}^0\left(X_0(N), \Omega^1\right)$, we obtain two maps

$$\alpha^*, \beta^* : \mathcal{S}_2(N) \to \mathcal{S}_2(pN),$$

and recover the action of T_p on modular forms defined in 1.4.4 (where T_n was denoted by $\mathrm{T}_2(n)$).

We will now see how correspondences induce maps on JACOBIANS of curves via their action on divisor groups. Consider a correspondence (3.9), where α is of degree $d \geq 1$. View $\alpha^{-1}(P)$ as a divisor of C, i.e. the formal sum of points lying over P counted with multiplicities. Then $\beta\left(\alpha^{-1}(P)\right)$ is a divisor on C_2. We therefore obtain maps

$$\mathrm{Div}^n(C_1) \xrightarrow{\beta\circ\alpha^{-1}} \mathrm{Div}^{dn}(C_2),$$

on the divisor groups of degree n. We want to apply this construction to T_p. With α and β defined as in (3.10), the induced map is

$$\beta_* \circ \alpha^* : (E, C_N) \mapsto \sum_{C_p} (E, C_M \oplus C_p) \mapsto \sum_{C_p} \left(E/C_p, (C_M \oplus C_p)/C_p\right), \tag{3.11}$$

where the sums are taken over all subgroups of order p in E. Thus we have a map $\mathrm{T}_p : \mathrm{Div}(X_0(N)) \to \mathrm{Div}(X_0(N))$. Since the PICARD group can be obtained from the divisors by dividing out the principle divisors, we are at the same time provided with a map T_p on $\mathrm{Pic}(X_0(N))$ and what is important on $\mathrm{Pic}^0(X_0(N))$, which can be identified with the JACOBIAN $J_0(N)$.

Coming from PICARD functoriality, this is a contravariant association $X \to J(X)$. By autoduality of the JACOBIAN, there is a covariant association $X \to J(X)$ coming from ALBANESE functoriality, so that a correspondence induces two maps on the JACOBIAN and it can be confusing to decide which duality to use. Fortunately, for T_p with p prime to N, it does not matter which choice we make. However, it matters a lot, if $p \mid N$, since then we have non-commuting confusable operators. We denote the map induced via ALBANESE functoriality ξ_p. For an arbitrary $n > 0$, we have

$$\mathrm{T}_n = \xi_n^\vee\,, \qquad \xi_n = \mathrm{T}_n^\vee,$$

where $^\vee$ is the ROSATI involution on $\mathrm{End}(J_0(N))$.

We just mention without precise definition and proof, that one can get out of it with the help of ATKIN-LEHNER operators. Let $w = w_N$ be the standard ATKIN-LEHNER involution of $X_0(N)$ (cf. (1.24)). Write again w for the induced involution on the JACOBIAN $J_0(N)$. This is not ambigous since an involution on a curve induces the same endomorphism of its JACOBIAN via PICARD and ALBANESE functoriality. We then have

$$wT_nw = \xi_n\,, \qquad w\xi_nw = \mathrm{T}_n\,. \tag{3.12}$$

Consider the subalgebras Ξ_N and $\mathbf{T}_N$ of $\mathrm{End}(J_0(N))$ generated by the ξ_n and T_n respectively. The ROSATI as well as the ATKIN-LEHNER involution induces an isomorphism of these subalgebras. Ξ and $\mathbf{T}_N$ may each be identified with the algebra generated by the classical HECKE operators T_n on the space $\mathcal{S}_2(N)$ as defined in Section 1.4.4. This algebra is a free finitely generated $\mathbb{Z}$-module of rank equal to the dimension of the abelian variety $J_0(N)$, that means to the dimension of $\mathcal{S}_2(N)$.

Once the HECKE operators on $J_0(N)$ have been defined over $\mathbb{Q}$, they act also on the NÉRON model of $J_0(N)$ and of course on the fibers at each prime dividing N.

3.2.2 Action of HECKE Operators on the Torus attached to $X_0(qM)$

Let in this section $N = qM$, where as before M is a positive integer and $q \nmid M$ is a prime. We can assume that M is squarefree. Consider the abelian variety $J_0(N)$ over $\mathbb{Q}_p$ and imagine the problem of reducing $J_0(N)$ modulo q. In general, the variety $J_0(N)$ has bad reduction at q, which is to say that its NÉRON model (its "best possible reduction") over $\mathbb{F}_q$ is not necessarily an abelian variety over $\mathbb{F}_q$. This reduction has, however, a maximal toric subgroup T – more precisely, T is the toric part in the fiber at q of the NÉRON model $\mathcal{N}(J_0(qM))$ of the JACOBIAN and we will show that $J_0(N)$ has semistable reduction at q. As we have just asserted, the T_n induce as endomorphisms of $J_0(qM)$ endomorphisms of this torus and act by Hom-functoriality on the character group X of T. Inspired by the connection induced by this functoriality, we propose to investigate this latter action of the HECKE algebra. We will see that the group $T = \mathrm{Hom}(X, \mathbf{G}_\mathrm{m})$ naturally extends to a finite flat group scheme over $\mathbb{Z}_q$.

It turns out that the canonical isomorphism in equation (2.1)

$$X \cong \mathrm{H}_1(\mathcal{G}, \mathbb{Z})$$

is very helpful, in particular, because it induces a canonical inclusion $X \hookrightarrow \mathbb{Z}^{\mathcal{I}}$, where $\mathcal{I} = \Sigma(M)$ is the set of isomorphism classes of supersingular enhanced elliptic curves of level M over $\overline{\mathbb{F}}_q$. It is therefore natural to relate the HECKE action on X to the correspondences induced by the T_n in the previous section, though we have to keep at the back of our minds, that the inclusion map $X \hookrightarrow \mathbb{Z}^{\mathcal{I}}$ depends on our having oriented each edge $i \in \mathcal{I}$.

In the case where n is prime to q, there is no inversion of an orientation to take into account, as T_n preserves the components of $X_0(qM)$. The T_n satisfy on $\Sigma(M)$ the same modular rules as over $\mathbb{Q}$ exposed in the Theorem 1.4.22 of HECKE. Let $\mathbf{E} = (E, C_M)$ be an enhanced elliptic curve. For a prime number $r \neq q$ which is also prime to M, we have the expression

$$\mathrm{T}_r(\mathbf{E}) = \sum_{C_r} \mathbf{E}/C_r, \tag{3.13}$$

where the sum goes over all $r+1$ subgroups of order r in E according to (3.11). However, if r divides M, one has to be more careful: the enhancement of E by C_M provides E with a subgroup D of order r which has to be ignored in the sum

$$\mathrm{T}_r(\mathbf{E}) = \sum_{C_r \neq D} \mathbf{E}/C_r. \tag{3.14}$$

The hole story turns out to be a little more complicated if $r = q$. Now there are in fact inversions of orientation, having to do with the choice of PICARD respectively ALBANESE functoriality. Here comes the ATKIN-LEHNER involution $w = w_q$ on $X_0(N)$ into play. In modular terms, it is defined by regarding the points of $X_0(N)$ as triples (E, C_M, C_q). We have

$$w_q : X_0(N) \to X_0(N)\,, \quad (E, C_M, C_q) \mapsto (E/C_q, (C_M \otimes C_q)/C_q, E[q]/C_q)\,. \tag{3.15}$$

See also Section 1.4.5. The involution w_q acts via the above described functoriality also on the torus T and on its character group X. As we have seen in the first chapter (especially Section 1.4.5) the ATKIN-LEHNER involution helps to define the space of cusp forms in so called old forms and new forms. We will come back to this more precisely in the next section. Meanwhile, we give an identity, which exploits the fact, that T pertains to cusp forms of level qM which are q-new.

Proposition 3.2.2. *The identity $w_q = -\mathrm{T}_q$ holds on the torus T.*

PROOF: Consider the two degeneracy maps $\alpha, \beta : X_0(qM) \to X_0(M)$ of the form (3.10) defined over $\mathbb{Q}$. Pushing forward the one and pulling back the other on divisors, we get the following maps

$$\begin{aligned} \alpha^* \quad &: \quad \mathrm{Div}\,(X_0(M)) \to \mathrm{Div}\,(X_0(qM))\,,\ (E, C_M) \mapsto \sum_{C_q} (E, C_M \oplus C_q), \\ \beta_* \quad &: \quad \mathrm{Div}\,(X_0(qM)) \to \mathrm{Div}\,(X_0(M))\,,\ (E, (C_M \oplus C_q)) \mapsto (E/C_q, (C_M \oplus C_q)/C_q)\,. \end{aligned}$$

Those maps induce an endomorphism of the JACOBIAN $\alpha^*\beta_* : J_0(qM) \to J_0(qM)$ by

$$(E, (C_M \oplus C_q)) \mapsto (E/C_q, (C_M \oplus C_q)/C_q) \mapsto \sum_{D_q} (E/C_q, ((C_M \oplus C_q)/C_q \oplus D_q)),$$

where the sum goes over subgroups of order q of E/C_q. In this expression, we split the sum to derive an identification with

$$\begin{aligned}\sum_{D_q \neq C_q} (E/D_q, (C_M \oplus D_q)/D_q) \quad + \quad (E/C_q, (C_M \oplus C_q)/C_q, E[q]/C_q) = \\ \mathrm{T}_q\,(E, (C_M \oplus C_q)) + w_q\,(E, (C_M \oplus C_q)),\end{aligned}$$

where the sum goes over all subgroups of order q of E not equal to C_q. This calculation shows, that the endomorphism $w_q + \mathrm{T}_q$ of $J_0(qM)$ factors through $\beta_* : J_0(qM) \to J_0(M)$. Considering the fibers at q of the corresponding NÉRON models and restricting to the torus T, we see that $w_q + \mathrm{T}_q$ factors through a map

$$T \to J_0(M).$$

However, all such maps are trivial, i.e. the zero map, since T is a torus and $J_0(M)$ an abelian variety. This shows that $w_q + \mathrm{T}_q$ is zero on T which proofs the assertion. □

Remark 3.2.3. According to [4, Chapter V, §1], the involution w_q permutes the two components of $X_0(qM)_{\mathbb{F}_q}$. What is more, it acts on the set of singular points of $X_0(qM)_{\mathbb{F}_q}$ as the FROBENIUS morphism.

Corollary 3.2.4. *The action of* T_q *on the character group* X *is the restriction to* X *of the map on* $\mathbb{Z}^{\Sigma(M)}$ *induced by the* FROBENIUS *automorphism of* $\Sigma(M)$. *In fact, this restriction is the* FROBENIUS *automorphism of* X.

PROOF: By Proposition 3.2.2 w_q and T_q are equal on T and by Hom-functoriality also on X. Therefore, the first assertion follows from the remark, since w_q combines the FROBENIUS automorphism of $\Sigma(M)$ with an inversion of the two vertices of the graph $\mathcal{G}$. The second statement is then a consequence from the fact, that the two components of $X_0(qM)_{\mathbb{F}_q}$ are rational as explained in [23, Appendix, §3] □

Having taken into account all possible inversions, this concludes our description of the HECKE operation on the torus T. As promised, we will now enlarge upon the old and new subspace of $\mathcal{S}_2(qM)$.

3.2.3 Old and New Subspace of $\mathcal{S}_2(qM)$

As a consequence of the introductory discussion of HECKE correspondences, we can consider the subring $\mathbf{T}_{qM}$ of the endomorphism ring of the JACOBIAN $J_0(qM)$ generated by all HECKE operators. Recall that, as mentioned in Section 3.2.1, taking the cotangent space of the dual of $J_0(qM)_{\mathbb{C}}$ identifies $\mathbf{T}_{qM}$ with a subring of $\mathrm{End}\,(\mathcal{S}_2(qM))$. What is more, this action derived by functoriality coincides with the classical HECKE action as described in 1.4.4.

Let α and β be as hitherto.

Definition 3.2.5. The *q-old subspace* of $\mathcal{S}_2(qM)$ is defined to be the direct sum

$$\mathcal{S}_2(qM)^{\mathrm{old}} = \alpha^*\,(\mathcal{S}_2(M)) \oplus \beta^*\,(\mathcal{S}_2(M))$$

of two distinguished copies of $\mathcal{S}_2(M)$. The corresponding *q-new space* is the orthogonal complement $\mathcal{S}_2(qM)^{\mathrm{new}}$ with respect to the PETERSSON inner product.

The maps induced by α and β on cusp spaces are the maps

$$\alpha^* : \mathcal{S}_2(M) \to \mathcal{S}_2(qM),\ f(\tau) \mapsto f(\tau)$$

and

$$\beta^* : \mathcal{S}_2(M) \to \mathcal{S}_2(qM),\ f(\tau) \mapsto f(q\tau).$$

This agrees with the examples and the definition in Section 1.4.4. We have already seen there, that the old and new subspace of $\mathcal{S}_2(qM)$ are $\mathbf{T}_{qM}$-stable subspaces.

Definition 3.2.6. The images $\mathbf{T}_{qM}^{\mathrm{old}}$ and $\mathbf{T}_{qM}^{\mathrm{new}}$ of $\mathbf{T}_{qM}$ in the endomorphism rings of the q-old and q-new subspace respectively are called the *q-old* and the *q-new quotient* of $\mathbf{T}_{qM}$.

Via the product map

$$\mathbf{T}_{qM} \to \mathbf{T}_{qM}^{\mathrm{old}} \times \mathbf{T}_{qM}^{\mathrm{new}},$$

we identify $\mathbf{T}_{qM}$ with a subring of finite index of $\mathbf{T}_{qM}^{\mathrm{old}} \times \mathbf{T}_{qM}^{\mathrm{new}}$.

We consider again the fiber over q of the NÉRON model of $J_0(qM)$. According to MAZUR in [23, Appendix], the group of connected components of this $\mathbb{F}_q$-group scheme is finite abelian and $\mathcal{N}\left(J_0(qM)\right)_q$ itself has a canonical decomposition

$$\mathcal{N}\left(J_0(qM)\right)_q = J_q^0 \times C,$$

where J_q^0 is the connected component of the fiber at $\mathbb{F}_q$ and C is a cyclic group generated by the class of divisor $(0) - (\infty)$ (cf. [23, Theorem A.1 and Remarks]). MAZUR also connects results of RAYNAUD and DELIGNE-RAPOPORT to obtain a short exact sequence

$$1 \to T \to J_q^0 \to J_0(M) \times J_0(M) \to 0, \tag{3.16}$$

where T is our usual torus. This sequence turns out to be of central interest for our further calculations. By definition of the NÉRON model, all endomorphisms of $J_0(qM)$ defined over $\mathbb{Q}$ are defined on its NÉRON model and so via (3.16) on T and $J_0(M) \times J_0(M)$. The resulting action of $\mathbf{T}_{qM}$ on T corresponds to the already discussed action of HECKE operators on X respectively T. As for the action of $\mathbf{T}_{qM}$ on $J_0(M) \times J_0(M)$, there is just one dubious point, namely the endomorphism arising from T_q. Contrariwise to the other HECKE operators, it coincides not necessarily with the diagonal action of $\mathrm{T}_q \in \mathbf{T}_M$.

Remark 3.2.7. The surjective map $J_q^0 \to J_0(M) \times J_0(M)$ occuring in (3.16) is deduced by PICCARD functoriality from two maps $X_0(M) \to X_0(qM)$ which exist naturally in characteristic q only. It may not identified with the map $J_q^0 \to J_0(M) \times J_0(M)$ derived by ALBANESE functoriality from the two degeneracy maps α, $\beta : X_0(qM) \to X_0(M)$ in characteristic 0.

We will now examine the action of $\mathbf{T}_{qM}$ on T and on $J_0(M) \times J_0(M)$.

Theorem 3.2.8. *An element t of $\mathbf{T}_{qM}$ is 0 on T, if and only if it is 0 on the q-new subspace $\mathcal{S}_2(qM)^{new}$.*

PROOF: The degeneracy maps α and β combine to produce by PICARD functoriality a map

$$\rho : J_0(M) \times J_0(M) \to J_0(qM).$$

Denote by A the image and Q the cokernel of ρ, such that we obtain a short exact sequence of abelian varieties

$$0 \to A \to J_0(qM) \to Q \to 0. \tag{3.17}$$

If we regard these varieties over $\mathbb{C}$, dualizing and applying the cotangent functor we obtain a short exact sequence of $\mathbb{C}$-vector spaces

$$0 \to \mathcal{S}_2(qM)^{\mathrm{old}} \to \mathcal{S}_2(qM) \to \mathcal{S}_2(qM)^{\mathrm{new}} \to 0. \tag{3.18}$$

This is why one often refers to A as *q-old subvariety* and to Q as *q-new quotient*. This correspondence of sequences shows, that $t \in \mathbf{T}_{qM}$ is 0 on $\mathcal{S}_2(qM)^{\text{new}}$, i.e. maps to 0 in $\mathbf{T}_{qM}^{\text{new}}$, if and only if it acts as 0 on Q.

The fiber of A at q is again an abelian variety, that means A has good reduction at q, since $J_0(M)$ is an abelian variety and $q \nmid M$. On the other hand, this implies that Q has purely toric reduction. Moreover, the dimension of Q and T coincides, which can be seen comparing the reduction of ρ at q with the short exact sequence over $\mathbb{F}_q$ (3.16). Hence, the connected component of 0 in the fiber at q of the NÉRON model $\mathcal{N}(Q)$ is a torus U of the same dimension as T. It is known, that in this case of an abelian variety with purely toric reduction, the action of $\text{End}_{\mathbb{Q}}(Q)$ on U is faithful, i.e. for any two distinct $g, h \in \text{End}_{\mathbb{Q}}(Q)$ there is $u \in U$, such that $gx \neq hx$. In particular $t \in \mathbf{T}_{qM}$ acts as 0 on U, if and only if t acts as 0 on Q, or equivalently, as we have just seen, t acts as 0 on $\mathcal{S}_2(qM)^{\text{new}}$.

Now look at the quotient map $\pi : J_0(qM) \to Q$ of the short exact sequence (3.17) and take the same functorial way as before; that means, we take the connected component of 0 at the q-fibers of the NÉRON models. Herefrom, we obtain a homomorphism $\pi_* : J_q^0 \to U$. Restricting to the torus T via the inclusion of T in J_q^0 in (3.16), results in a map $\pi_* : T \to U$ which is $\mathbf{T}_{qM}$-equivariant, because T and U are tori of the same dimension. It is possible to choose a map of abelian varieties $\eta : Q \to J_0(qM)$, which complement π to an isogeny of Q. By the same procedure as before, we get a map $\eta_* : U \to T$ in characteristic q and $\pi_*\eta_*$ is an isogeny of tori. However, each of them is an isogeny on its own, by means that T and U have the same dimensions. Hence, π_* is a $\mathbf{T}_{qM}$-equivariant isogeny and this shows, that $t \in \mathbf{T}_{qM}$ acts as 0 on T if and only if it acts as 0 on U. By the above said, this shows the claim. □

Another way to express the assertion of the theorem, is to say, that the action $\mathbf{T}_{qM}$ on T cuts out the q-new quotient $\mathbf{T}_{qM}^{\text{new}}$. A similar observation can be made for the q-old quotient $\mathbf{T}_{qM}^{\text{old}}$.

Theorem 3.2.9. *An element $t \in \mathbf{T}_{qM}$ is 0 on $J_0(M) \times J_0(M)$ if and only if it is 0 on the q-old subspace $\mathcal{S}_2(qM)^{old}$.*

PROOF: We consider the same exact sequences (3.17) and (3.18) as in the proof of Theorem 3.2.8. By the same argumentation, $t \in \mathbf{T}_{qM}$ is 0 on $\mathcal{S}_2(qM)^{\text{old}}$, if and only if it acts as 0 on A.

In the next step, the proof differs from that of Theorem 3.2.8. Since A has good reduction at q, as we have mentioned, the inclusion of A in $J_0(qM)$ of the exact sequence (3.17) induces a map $A \to J_q^0$ at the fiber of q. We have to view A simply as a variety over $\mathbb{F}_q$, whereas we had to manage before with the auxiliary torus U. Since A is the image of $J_0(M) \times J_0(M)$ under ρ, the composition of this map with the surjective map $J_q^0 \to J_0(M) \times J_0(M)$ of (3.16) is a homomorphism $J_q^0 \to A$ which induces an isogeny $A \to J_0(M) \times J_0(M)$. Therefore, $t \in \mathbf{T}_{qM}$ acts as 0 on A, if and only if t acts as 0 on $J_0(M) \times J_0(M)$. This completes the proof. □

3.2.4 HECKE Operators on the Group of Connected Components

The aim of this section is to prove, that the group of connected components Φ of the fiber at q of the NÉRON model of $J_0(qM)$ is "EISENSTEIN" in the sense of [23, II, §9].

Definition 3.2.10. The EISENSTEIN *ideal* $\mathfrak{I} \in \mathbf{T}_N$ is the ideal generated by the elements $1+\ell-\text{T}_\ell$ ($\ell \neq N$) and $1 + w_N$. A prime ideal $\mathfrak{P} \in \mathbf{T}_N$ in the support of the EISENSTEIN ideal is called an EISENSTEIN *prime*. A subgroup Δ of $J_0(N)$ is called EISENSTEIN, if the HECKE operator T_r operates by multiplication by $1 + r$ for all primes $r \nmid N$.

Remark 3.2.11. Consider the maps on the JACOBIANS $\alpha_*, \beta_* : J_0(rN) \to J_0(N)$ and $\alpha^*, \beta^* : J_0(N) \to J_0(rN)$ induced by ALBANESE and PICARD functoriality from the degeneracy maps α and β. Since the initial degeneracy maps are coverings of curves of degree $r + 1$ (there are $r + 1$ subgroups of an elliptic curve having order r), the composition of the pull-backs and pushing-forwards are

$$\alpha_*\alpha^* = \beta_*\beta^* = r + 1.$$

At the same time, we have by the geometric definition of the HECKE operators

$$\alpha_*\beta^* = \beta_*\alpha^* = \mathrm{T}_r$$

on $J_0(N)$. In particular, suppose that Δ is a subgroup of $J_0(N)$, on which $\alpha^* = \beta^*$. By the above formulas, we deduce that $\mathrm{T}_r = r+1$. Moreover, if the relation $\alpha^* = \beta^*$ is satisfied for each prime r not dividing N, then the group Δ is EISENSTEIN in the sense of MAZUR. See [36]

Recall the description of Φ given in Chapter 2. In our special case, where $C = X_0(qM)$, denote Λ the free abelian group $\mathbb{Z}^{\mathfrak{I}}$ of the set of supersingular points of $X_0(M)_{\overline{\mathbb{F}}_q}$. Let X again be the character group of the torus T associated with $X_0(qM)$, i.e. the toric part in the fiber at q of the NÉRON model of $J_0(qM)$. Quoting Proposition 2.2.7, we know that X is the subgroup of Λ consisting of elements of degree 0. As described in Section 3.1.1 the set $\mathfrak{I}$ is the set $\Sigma(M)$ of $\overline{\mathbb{F}}_q$-isomorphism classes of enhanced supersingular elliptic curves $(\mathbf{E}, C_M)$. Define for each $i \in \mathfrak{I}$ the integers $e(i)$ as above, which admittes a diagonal pairing on Λ. This pairing furnishes an embedding

$$\kappa : \Lambda \to \mathrm{Hom}(\Lambda, \mathbb{Z}) =: \Lambda^\vee,\ i \mapsto e(i, \cdot), \tag{3.19}$$

where $e(i,j) = \begin{cases} e(i) & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$. Restricting the pairing to the degree-0 subgroup X, we obtain similarly the embedding

$$\iota : X \to X^\vee.$$

The Theorems 2.2.9 and 2.3.3 give us an isomorphism

$$\Phi \cong \mathrm{Coker}(\iota)$$

at hand.

The action of HECKE operators T_n on the target $X^\vee$ of ι is the action induced by the discussed standard action of T_n on X via contravariant Hom-functoriality. However, one has to be careful with the action of T_n on the source X of ι. The source of ι is naturally the character group which occures if we establish $J_0(qM)$ via ALBANESE functoriality. Anyway, ATKIN-LEHNER or ROSATI involution translates the action of T_n on the ALBANESE to the action of ξ_n on the JACOBI variety. These subtleties seem to be confusing, but they do not really intervene in our analysis, because with regard on the definition of Φ being EISENSTEIN, we are just interested in HECKE operators T_r for prime numbers $r \nmid qM$ and in this case $\mathrm{T}_r = \xi_r$, since the ATKIN-LEHNER involution w_{qM} commutes with those HECKE operators as we have seen at the end of Section 1.4.5, and $w_{qM} T_r w_{qM} = \xi_r$ by (3.12). For such r, we define a correspondence

$$\eta_r := \mathrm{T}_r - (r+1)$$

on $X_0(qM)$ and take it by functoriality to Φ.

Lemma 3.2.12. *If $\eta_r(\Lambda^\vee) \subset \Lambda$, then we have the stronger inclusion $\eta_r(X^\vee) \subset X$.*

PROOF: Let $\zeta \in \Lambda^\vee$. Since κ, which is used here to embed Λ into $\Lambda^\vee$, has finite cokernel, we have $e\zeta \in \Lambda$ for $e = [\Lambda^\vee : \Lambda]$; further, it is obvious, that $\eta_r(\Lambda) \subseteq X$. Indeed, for any generator $(E, C_M) \in \Sigma(M)$ we have

$$\eta_r(E, C_M) = \sum_{C:\mathrm{ord}(C)=r} (E/C, (C_M \oplus C)/C) - (r+1)(E, C_M),$$

which means $\deg(\eta_r(E, C_M)) = \sum_{i=1}^{r+1} 1 - (r+1) = 0$. Thus $\eta_r(E, C_M) \in X$. As a consequence,

$$e\eta_r(\zeta) = \eta_r(e\zeta) \in \eta_r(\Lambda) \subset X.$$

By assumption, $\eta_r(\zeta)$ is an element of Λ for which there exists an integer e, such that $e\eta_r(\zeta) \in X$, i.e. $e\eta_r(\zeta)$ is 0 in Λ/X. But this quotient can be bijectively identified with the torsion free group $\mathbb{Z}$ via the degree map. Therefore, $\eta_r(\zeta)$ lies already in X. So we have the inclusion

$$\eta_r(\Lambda^\vee) \subset X.$$

With $\eta_r(X^\vee) \subset \Lambda$ the desired inclusion follows. □

To prove the main result of this section, we need the following

Lemma 3.2.13. *Let $i \in \mathcal{I}$. The coefficient of $i \neq j \in \mathcal{I}$ in $\mathrm{T}_r(i)$ is divisible by $e(i)$.*

Proof: Fix such a $j \in \mathcal{I}$ and let (E, B_M) and (F, D_M) be enhanced elliptic curves representating the isomorphism classes of i and j respectively. According to (3.3), $e(i)$ is the cardinality of the finite group $\mathrm{Aut}(\mathbf{E})/\pm 1$. As $\mathrm{T}_r(\mathbf{E}) = \sum_{\mathrm{ord}(H)=r} \mathbf{E}/H$ and because we want to find the coefficient of $\mathbf{F}$ in this sum, it is now our task to determine the number of subgroups H of E having order r, for which $\mathbf{E}/H \cong \mathbf{F}$.

There is an evident action of $\mathrm{Aut}(\mathbf{E})/\pm 1$ on the set of such subgroups H. If this action is free, we can quotient it out, which means, that the number of H's is divisible by $e(i) = \#\left(\mathrm{Aut}(\mathbf{E})/\pm 1\right)$. Thus for our purpose, it suffices to show that this action is free.

Assume the contrary. Then there is H with $\mathbf{E}/H \cong \mathbf{F}$ and $\alpha \in \mathrm{Aut}(\mathbf{E})$ not equal to ± 1, such that $\alpha(H) = H$. By Proposition 3.1.10, we know, that the order of α must divide 24. Since it may be regarded as a unit in some imaginary quadratic field, one can even say, that α has order 3, 4, or 6. Changing the sign if necessary, we may assume that it has order 4 or 6.

Denote by R the subring of $\mathrm{End}(\mathbf{E})$ generated by α over $\mathbb{Z}$, such that

$$R \cong \begin{cases} \mathbb{Z}[i] & \text{if } \mathrm{ord}(\alpha) = 4 \\ \mathcal{O}\left(\mathbb{Q}(\sqrt{-3})\right) & \text{if } \mathrm{ord}(\alpha) = 6. \end{cases}$$

Since we are in characteristic r, H is an R-submodule of the free R/rR-module $E[r]$ of rank 1. Such submoduls are in one-to-one correspondence with the ideals $\mathfrak{P}$ of R containing the ideal generated by r. Because the ring R is a principle ideal domain, there is some π dividing r in R such that $\mathfrak{P} = (\pi)$. Then H is the kernel of the multiplication by $\frac{r}{\pi}$ on E. This endomorphism of $\mathbf{E}$ then induces an isomorphism $\mathbf{E}/H \cong \mathbf{E}$, which means that $\mathbf{F}$ and $\mathbf{E}$ are in the same isomorphism class – this is a contradiction to our assumption that $i \neq j$. □

Theorem 3.2.14. *The group Φ is annihilated by η_r for all primes r not dividing qM.*

Proof: Fix such a prime r. The action of T_r on Λ is derived by linearity from the usual map (3.13). This action comes by functoriality with an action on the subgroup X and the duals $X^\vee$ and $\Lambda^\vee$. In view that $\mathrm{T}_r = \xi_r$, the embeddings κ and ι commute with these actions:

$$\mathrm{T}_r \circ \kappa = \kappa \circ \xi_r = \kappa \circ \mathrm{T}_r$$

and the same for ι.

Using ι to embed X in $X^\vee$, we have $\Phi = X^\vee/X$. So we have to show $\eta_r(X^\vee) \subset X$. By Lemma 3.2.12 it suffices to show

$$\eta_r(\Lambda^\vee) \subset \Lambda. \tag{3.20}$$

We will show this on a basis. Let $\{i^\vee\}$ be the basis of $\Lambda^\vee$ dual to the basis $\mathcal{I} = \{i\}$ of Λ. A priori, $\eta_r(i^\vee)$ is just in $\Lambda^\vee$ and we have to find an element $\lambda \in \Lambda$, such that $\eta_r(i^\vee)(j) = \langle \lambda, j \rangle_X$, where $\langle \lambda, j \rangle_X = \kappa(\lambda)(j)$ indicates the pairing induced by the $e(i)$. Since $\eta_r(i^\vee)(j) = \langle i, \eta_r(j) \rangle_{\mathrm{eukl}}$, and $\eta_r(j) = \sum_k \langle k, \eta_r(j) \rangle_{\mathrm{eukl}}\, k$, $\eta_r(i^\vee)(j)$ represents the coefficient of i in $\eta_r(j)$. We may write this number as

$$\begin{aligned}\langle i, \eta_r(j)\rangle_{\mathrm{eukl}} &= \frac{1}{e(i)}\,\langle i, \eta_r(j)\rangle_X \\ &= \frac{1}{e(i)}\,\langle e(i)i, \eta_r(j)\rangle_{\mathrm{eukl}} \\ &= \frac{1}{e(i)}\,\langle e(j)j, \eta_r(i)\rangle_{\mathrm{eukl}} \\ &= \frac{1}{e(i)}\,\langle j, \eta_r(i)\rangle_X\,,\end{aligned}$$

where we have used the η_r-equivariance of the pairing.

We have therefore a good candidate for λ: If $\eta_r(i) \in e(i)\Lambda$, we may take

$$\lambda = \frac{\eta_r(i)}{e(i)}.$$

So it suffices to show, that the coefficient of each k in $\eta_r(i)$ is divisible by $e(i)$. We have seen in the proof of Lemma 3.2.12, that the degree of $\eta_r(i)$ is 0, i.e. the sum of those coefficients is 0. Consequently we have done, if we have shown this divisibility for $k \neq i$. For these k however the coefficients in $\eta_r(i)$ coincide with the coefficients in $\mathrm{T}_r(i)$ – since the action of $(r+1)$ is diagonal. This was the result of Lemma 3.2.13. □

Before we finish this section, we want to state a supplementary proposition.

Proposition 3.2.15. *For each prime number r not dividing qM, the map $\eta_r : \Lambda^\vee \to X$ deduced in Lemma 3.2.12 induces an injection*

$$\Phi \hookrightarrow X/\eta_r(X).$$

Proof: We have the following (from linear algebra) evident identity:

$$\Phi \cong X^\vee/X \cong \Lambda^\vee/(X \oplus X^\perp),$$

where $X^\perp$ is the “orthogonal complement” of X in the sense, that it is the subgroup of $\Lambda^\vee$ consisting of linear forms on Λ which vanish on X. We have seen, that η_r preserves X and hence at the same time $X^\perp$. However, as a subgroup of $\Lambda^\vee$, $X^\perp$ is sent to X according to Lemma 3.2.12, and this means

$$\eta_r(X^\perp) \subseteq X^\perp \cap X = 0.$$

Consequently, $\eta_r(X \oplus X^\perp) = \eta_r(X)$, and since $\eta_r(\Lambda^\vee) \subseteq X$, this means, that there is a well defined map of quotients

$$\sigma : \Phi \to X/\eta_r(X).$$

Stating Weil's Riemann Hypothesis, we may deduce, that η_r is an isogeny on the curve $J_0(qM)$. In particular, it is surjective (since non-trivial). So by functoriality, it acts injectively on X, which means that the cokernel of η_r is a finite group. Furthermore, the kernel of $\eta_r : \Lambda^\vee \to X$ is $X^\perp$. Indeed, $X^\perp$ is in the kernel. And it is the whole story, since, just as Λ/X, $\Lambda^\vee/X^\perp$ is torsion free.

Finally to prove injectivity, let $\eta_r(\zeta_1) = \eta_r(\zeta_2)$ for ζ_1, $\zeta_2 \in \Lambda^\vee$. We may assume without loss of generality that $\zeta_1 = \zeta \in \Lambda^\vee$ and $\zeta_2 = x \in X$, and show that $\zeta - x \in X^\perp$. But this is evident from the above said. This gives lastly the injectivity of the map σ as wanted. □

3.3 Comparison with $X_0(pqM)$

3.3.1 The Character Group associated with $X_0(pqM)_{\overline{\mathbb{F}}_q}$

We will now go a step farther and examine what happens, if we extend the original curve to $X_0(pqM)$ where p is a prime not dividing qM. Let thereby L be the analogue of our previous X, i.e. consider the toric part of the fiber at q (not at p!) of the NÉRON model of the JACOBIAN $J_0(pqM)$ and take the character group of this torus. As before, Proposition 2.2.7 brings out L as a group of degree-0 divisors on the set $\Sigma(pM)$ of supersingular points of $X_0(pM)_{\overline{\mathbb{F}}_q}$, onward in terms of supersingular pM-enhanced elliptic curves.

Lemma 3.3.1. *Supersingular elliptic curves enhanced by cyclic subgroups of order pM may be seen as p-isogenies*

$$\mathbf{E}_1 \to \mathbf{E}_2,$$

where E_1 and E_2 are enhanced of order M as before.

PROOF: Let $(E, C_M \oplus C_p)$ be such an object. We relate to it the two enhanced elliptic curves of cyclic order M

$$\mathbf{E}_1 = (E, C_M) \text{ and } \mathbf{E}_2 = (E/C_p, (C_M \oplus C_p)/C_p)\,,$$

and the projection map

$$\mathsf{proj}_p : (E, C_M) \to (E/C_p, (C_M \oplus C_p)/C_p)\,.$$

This is evidently surjective and even an isogeny of order p - indeed its inversion is ramified of order p. □

Remark 3.3.2. Whenever we talk of "enhanced elliptic curves", we mean enhanced of order M.

There are again our two natural degeneracy maps

$$\alpha, \beta : X_0(pqM) \rightrightarrows X_0(qM)$$

unless q is replaced by p. There is no risk to mix up the two pairs of maps, so that we continue to denote them α and β. These induce two maps of character groups

$$\alpha_*, \beta_* : L \rightrightarrows X$$

which are by means of Lemma 3.3.1 and the definition of α and β in 3.10 realized by sending the maps $\mathbf{E}_1 \to \mathbf{E}_2$ to either $\mathbf{E}_1$ or $\mathbf{E}_2$. The two maps combine to make up a single degeneracy map

$$\delta : L \to (X \oplus X).$$

A quite surprising result of this section is, that this map is surjective. The proof is based on results concerning the arithmetic of EICHLER orders which we deduced from [48].

Lemma 3.3.3. *Let $\mathbf{E}$ be an enhanced supersingular elliptic curve over $\mathbb{F}_q$. There is a non-zero endomorphism of $\mathbf{E}$, whose degree is an odd power of p.*

PROOF: Let again be $R = \mathrm{End}(\mathbf{E})$, maximal order in the unique quaternion algebra $H = R \otimes_{\mathbb{Z}} \mathbb{Q}$. As defined at the beginning of [48], the reduced norm of an element of a quaternion algebra is given by multiplicating the element with its conjugate. Recall, that in the case of H, conjugation means dualizing by the ROSATI involution. Thus, the degree of $x \in R$, $\deg(x) = x\hat{x}$ coincides with the reduced norm. According to [48, p.80, Théorème 4.1] the set K_H of rational numbers which are positive at infinite places and ramified in H coincides with the image of H under the reduced norm. Combining this with [48, p.90, Corollaire 5.9], we see that for every EICHLER order $\mathcal{O}$,

$$\mathrm{Norm}(\mathcal{O}) = K_H \cap R = \mathrm{Norm}(H) \cap R.$$

Take the EICHLER order $\mathcal{O} = R[p^{-1}]$. By the above said, there is $x \in R[p^{-1}]$, such that

$$\mathrm{Norm}(x) = x\hat{x} = p.$$

By eventually multiplying x with a positive power of p, we make sure, that the resulting endomorphism $x' = p^k x$ is in R. The reduced norm of this x' is

$$\mathrm{Norm}(x') = x'\hat{x}' = p^{2k} x\hat{x} = p^{2k+1},$$

an odd power of p and the claim is showed. □

Lemma 3.3.4. *Let $\mathbf{E}_1$ and $\mathbf{E}_2$ be enhanced elliptic curves. There is an isogeny $\mathbf{E}_1 \to \mathbf{E}_2$ whose degree is a power of p.*

PROOF: Let $R = \mathrm{End}(\mathbf{E}_1)$ and $T = \mathrm{Hom}(\mathbf{E}_1, \mathbf{E}_2)$ over $\mathbb{Z}$. It is clear, that T is a right R-module. What is more, it is locally free of rank one. Indeed, for any non-trivial isogeny $\gamma \in \mathrm{Hom}_{\mathbb{F}_r}(\mathbf{E}_1, \mathbf{E}_2)$ for a prime r, every other isogeny can be derived by combining γ with an endomorphism of $\mathbf{E}_1$ over $\mathbb{F}_r$.

Further, for $0 \neq x \in T$ we have the identity

$$\deg^2(x) = [T : xR].$$

We apply now [48, p.89 Théorème 5.7] stated by VIGNERAS save that we deal with a right module instead of a left ideal and replace the reduced norm by the degree. With $S = \mathbb{Z}\backslash\{p\}$ (which verifies the condition of EICHLER in the sense of [48, p.81, Définition]), the R-right-module $T' = T \otimes \mathbb{Z}[p^{-1}]$ is free of rank one, if and only if $\deg(T') = (\deg(t')|T' \in T')_R$ is a principle ideal in $\mathrm{Norm}(H)$. But this is the case, since all positive rational numbers, in particular p^{-1}, are in $\mathrm{Norm}(H)$, as we have seen in Lemma 3.3.3. Thus we know, that once the prime p is inverted T becomes a free R-module of rank 1 generated by an element $x' = x \cdot \frac{1}{p^k}$ where x is in T.

By the above identity,

$$\deg^2(x') = [T' : x'R] = 1,$$

in particular $\deg(x') = 1$ and as a consequence $\deg(x) = p^{2k}$. □

Now we have all tools at hand to prove

Theorem 3.3.5. *The map $\delta : L \to (X \oplus X)$ is surjective.*

PROOF: We only have to show that for two enhanced elliptic curves of order M, denote them $\mathbf{E}$ and $\mathbf{E}'$, the two elements $(\mathbf{E} - \mathbf{E}', 0)$ and $(0, \mathbf{E} - \mathbf{E}')$ of $X \oplus X$ are in the image of δ. Since the two curves were chosen arbitrarily, the assertion of the theorem follows then by linearity.

By Lemma 3.3.4 there is an isogeny $\phi : \mathbf{E} \to \mathbf{E}'$ whose degree is a power of p. If this power is even, there is nothing to modify. However, if this power is odd, we combine the isogeny ϕ with the endomorphism of $\mathbf{E}$ from Lemma 3.3.3 of degree an odd power of p. So without loss of generality we may assume, that the degree of ϕ is an even power of p, say p^{2i}.

Set $\mathbf{E} = \mathbf{E}_0$ and $\mathbf{E}' = \mathbf{E}_{2i}$. By the field theoretic approach of elliptic curves, there is a factorization of $\phi : \mathbf{E} \to \mathbf{E}'$ into a product of $2i$ isogenies of degree p:

$$\phi : \mathbf{E}_0 \xrightarrow{\phi_0} \mathbf{E}_1 \xrightarrow{\phi_1} \mathbf{E}_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_{2i-2}} \mathbf{E}_{2i-1} \xrightarrow{\phi_{2i-1}} \mathbf{E}_{2i}\,.$$

Now form the element

$$\lambda = \phi_0 - \hat{\phi}_1 + \phi_2 - \hat{\phi}_3 + \cdots + \phi_{2i-2} - \hat{\phi}_{2i-1},$$

where the hat denotes as usual the dual isogeny. This element is a degree zero divisor of p-isogenies of enhanced elliptic curves of order M, and thence an element of L. After all,

$$\begin{aligned}
\delta(\lambda) &= \delta(\phi_0) - \delta(\hat{\phi}_1) + \cdots + \delta(\phi_{2i-2}) - \delta(\hat{\phi}_{2i-1}) \\
&= (\mathbf{E}_0, \mathbf{E}_1) - (\mathbf{E}_2, \mathbf{E}_1) + (\mathbf{E}_2, \mathbf{E}_3) - \cdots - (\mathbf{E}_{2i-2}, \mathbf{E}_{2i-3}) + (\mathbf{E}_{2i-2}, \mathbf{E}_{2i-1}) - (\mathbf{E}_{2i}, \mathbf{E}_{2i-1}) \\
&= (\mathbf{E}_0 - \mathbf{E}_{2i}, 0) \\
&= (\mathbf{E} - \mathbf{E}', 0)
\end{aligned}$$

and just as well

$$\delta(\hat{\lambda}) \quad = \quad (0, \mathbf{E} - \mathbf{E}').$$

This is the desired result. □

3.3.2 The action of Hecke on L

For all positive integers n, we can equivalently to the previous section consider the Hecke correspondences T_n on $X_0(pqM)$. Again the T_n induce operators on the Jacobian $J_0(pqM)$ and on the character group L. Via our surjective degeneracy map δ, we compare these operators with the Hecke operators on X arising from correspondences on $X_0(qM)$.

Provided that $\gcd(n,p) = 1$, δ is by Bézout's lemma equivariant under action of T_n on L and on $X \oplus X$. Contrariwise, the Hecke operator T_p of L induces an operator on $X \oplus X$ such that it commutes with δ, which must be distinguished from the operator τ coming from the p^{th} Hecke correspondence on $X_0(qM)$. Let w_p be the Atkin-Lehner involution to the divisor p of pqM (see Section 1.4.5). With the kernel $Y = \mathrm{Ker}(\delta)$, we obtain a short exact sequence

$$0 \to Y \to L \to X \oplus X \to 0. \tag{3.21}$$

The action of T_p and the connection to τ can then be described in the following way.

Theorem 3.3.6. *The operator T_p of L preserves Y. We have the formula*

$$\mathrm{T}_p = -w_p$$

on Y. The endomorphism of $X \oplus X$ given by T_p is the map

$$(x, y) \mapsto (\tau(x) - y, px).$$

Proof: With the definitions (3.10) and (3.15), we observe that the composition

$$\begin{aligned}
\alpha w_p \quad : \quad & X_0(pqM) \to X_0(pqM) \to X_0(qM), \\
& (E, C_{qM}, C_p) \mapsto (E/C_p, (C_{qM} \oplus C_p)/C_p, E[p]/C_p) \mapsto (E/C_p, (C_{qM} \oplus C_p)/C_p)
\end{aligned}$$

coincides with β and

$$\begin{aligned}
\beta w_p \quad : \quad & X_0(pqM) \to X_0(pqM) \to X_0(qM), \\
& (E, C_{qM}, C_p) \mapsto (E/C_p, (C_{qM} \oplus C_p)/C_p, E[p]/C_p) \mapsto \\
& \mapsto ((E/C_p)/(E[p]/C_p), ((C_{qM} \oplus C_p)/C_p \oplus E[p]/C_p)\,/(E[p]/C_p)) \cong (E, C_{qM})
\end{aligned}$$

equals α. These facts imply, that w_p preserves the kernel Y of δ. Indeed, let $y \in Y$. We use the diagonal map Δ to describe δ and obtain

$$0 = \delta(y) = (\alpha_* \oplus \beta_*) \circ \Delta(y).$$

For the image of y under the ATKIN-LEHNER involution, this means

$$\begin{aligned}\delta\left(w_p(y)\right) &= (\alpha_* \oplus \beta_*) \circ \Delta\left(w_p(y)\right)\\ &= (\alpha_* \circ w_p) \oplus (\beta_* \circ w_p)) \circ \Delta(y)\\ &= (\beta_* \oplus \alpha_*) \circ \Delta(y) = 0,\end{aligned}$$

and $w_p(y)$ is again in the kernel of δ. By this means, the two identities induce, since δ is surjective, a map on $X \oplus X$ which simply interchanges the coefficients.

We proceed to the operator $\mathrm{T}_p + w_p$, which is, simultanously to the proof of Proposition 3.2.2, obtained by composing $\alpha_* : L \to X$ (derived from $\alpha : X_0(pqM) \to X_0(qM)$ by JACOBIAN functoriality) with $\beta^* : X \to L$ (derived from $\beta : X_0(pqM) \to X_0(qM)$ by ALBANESE functoriality). For Y is a subgroup of the kernel of α_*, i.e.

$$Y = \mathrm{Ker}(\delta) = \mathrm{Ker}(\alpha_*) \cap \mathrm{Ker}(\beta_*) \subseteq \mathrm{Ker}(\alpha_*) \subseteq \mathrm{Ker}(\beta^*\alpha_*) = \mathrm{Ker}(\mathrm{T}_p + w_p),$$

$\mathrm{T}_p + w_p$ vanishes on Y, which is the first part of the assertion.

In Remark 3.2.11 we have already established the identities

$$\tau = \beta_*\alpha^* = \alpha_*\beta^*$$

and

$$p + 1 = \alpha_*\alpha^* = \beta_*\beta^*$$

on X. Consequently, the map $\mathrm{T}_p + w_p = \beta^*\alpha_*$ on L induces via δ on $X \oplus X$ the map

$$\phi : (x, y) \mapsto (\tau x, (p + 1)x)\,,$$

which can be seen as follows:

$$\begin{aligned}\delta \circ (\mathrm{T}_p + w_p) &= (\alpha_* \oplus \beta_* \circ \Delta) \circ \beta^*\alpha_*\\ &= ((\alpha_*\beta^*)\alpha_* \oplus (\beta_*\beta^*)\alpha_*)\,\Delta\\ &= (\tau\alpha_* \oplus (p + 1)\alpha_*)\\ &= \phi \circ (\alpha_* \oplus \beta_* \circ \Delta).\end{aligned}$$

It remains to subtract w_p to obtain the formula for T_p. As we have already seen, w_p inverts the coefficients of $X \oplus X$. So the final formula for T_p is

$$(x, y) \mapsto (\tau x - y, (p + 1)x - x) = (\tau x - y, px)$$

as stated. □

We continue our study by considering the HECKE algebra $\mathbf{T}_{pqM}$, the subring of End $(J_0(pqM))$ generated by all T_n. Analogously to above, we define the p-old, p-new, q-old and q-new quotients of $\mathbf{T}_{pqM}$ with help of the pull-backs of the appropriate degeneracy maps. In addition, we define the pq-new quotient $\mathbf{T}_{pqM}^{pq\text{-new}}$ of $\mathbf{T}_{pqM}$. The space of level-2 cusp forms $\mathcal{S}_2(pqM)$ contains as described two subspaces whose intersection is not necessarily trivial. They are isomorphic to

$$\mathcal{S}_2(qM) \oplus \mathcal{S}_2(qM),$$

which belongs to the p-old subspace, and

$$\mathcal{S}_2(pM) \oplus \mathcal{S}_2(pM),$$

belonging to the q-old subspace.

Definition 3.3.7. The (not necessarily direct) sum of these two subspaces is the *pq-old subspace* of $\mathcal{S}_2(pqM)$, denoted by $\mathcal{S}_2(pqM)^{pq\text{-old}}$. Its orthogonal complement with respect to the PETERSSON inner product is the *pq-new subspace* $\mathcal{S}_2(pqM)^{pq\text{-new}}$. The image of $\mathbf{T}_{pqM}$ in the endomorphism rings of these spaces are the pq-old and pq-new quotients $\mathbf{T}_{pqM}^{pq\text{-old}}$ and $\mathbf{T}_{pqM}^{pq\text{-new}}$.

In the previous theorem, we have seen, that the kernel Y of δ is a $\mathbf{T}_{pqM}$-module. Now we examine this action more closely and state an analogon to Theorem 3.2.8 – also the proofs are alike.

Theorem 3.3.8. *An element $t \in \mathbf{T}_{pqM}$ is 0 on Y, if and only if it acts as 0 on the pq-new subspace $\mathcal{S}_2(pqM)^{pq\text{-new}}$. One says that Y cuts out $\mathbf{T}_{pqM}^{pq\text{-new}}$.*

PROOF: Replace the q-new quotient Q of $J_0(qM)$ in Theorem 3.2.8 by the pq-new quotient $J_0(pqM)/\operatorname{Im}(\rho) =: R$, where $\rho : J_0(qM)\times J_0(qM)\times J_0(pM)\times J_0(pM) \to J_0(pqM)$ is the natural degeneracy map induced by the appropriate α's and β's. Then by the same argumentation as in 3.2.8 it is clear, that a fixed $t \in \mathbf{T}_{pqM}$ is 0 on $\mathcal{S}_2(pqM)^{pq\text{-new}}$, if and only if it is 0 on R. This quotient R is evidently a quotient of the q-new quotient Q of $J_0(pqM)$ (quotient out consecutively the images of the different degeneracy maps belonging to p and q) which already has purely toric reduction in characteristic q (see Theorem 3.2.8). So the same holds for R. Let then V be the torus $\left(\mathcal{N}(R)_{\mathbb{F}_q}\right)^0$, i.e. the connected component of the fiber at q of the NÉRON model of R. (The analogue in Theorem 3.2.8 would be U.) Per definitionem the analogous torus for $J_0(pqM)$ is $\operatorname{Hom}(L,\mathbb{G}_m)$, while it was $T = \operatorname{Hom}(X,\mathbb{G}_m)$ for $J_0(qM)$.

The quotient map

$$\pi : J_0(pqM) \to R,$$

which is trivial on the image of $J_0(qM)\times J_0(qM)$ in $J_0(pqM)$, induces by functoriality a map of tori

$$\operatorname{Hom}(L,\mathbb{G}_m) \to V,$$

which is trivial on the image of $\operatorname{Hom}(X,\mathbb{G}_m)\times\operatorname{Hom}(X,\mathbb{G}_m)$ in $\operatorname{Hom}(L,\mathbb{G}_m)$. Since Y is the kernel of $\delta : L \to X \oplus X$, this induces a map of tori

$$\lambda : \operatorname{Hom}(Y,\mathbb{G}_m) \to V.$$

These two tori have the same dimension. Indeed, with help of the degeneracy map the dimension of L can be described as

$$\dim(L) = \dim\left(J_0(pqM)\right) - 2\dim\left(J_0(pM)\right).$$

Taking the cotangent spaces of the duals, this becomes equal to

$$\dim\left(\mathcal{S}_2(pqM)\right) - 2\dim\left(\mathcal{S}_2(pM)\right)$$

and equivalently

$$\dim(X) = \dim\left(\mathcal{S}_2(qM)\right) - 2\dim\left(\mathcal{S}_2(M)\right).$$

Combining these results, we obtain

$$\begin{aligned}\dim(Y) &= \dim(L) - 2\dim(X)\\ &= \dim\left(\mathcal{S}_2(pqM)\right) - 2\dim\left(\mathcal{S}_2(pM)\right)\\ &\quad -2\dim\left(\mathcal{S}_2(qM)\right) + 4\dim\left(\mathcal{S}_2(M)\right).\end{aligned}$$

Following the reasoning of 3.2.8, we have the two equalities

$$\dim(V) = \dim(R) = \dim\left(\mathcal{S}_2(pqM)^{pq\text{-new}}\right)$$

and the latter one is equal to $\dim(\mathcal{S}_2(pqM)) - \dim(\mathcal{S}_2(qM) \oplus \mathcal{S}_2(qM)) - \dim(\mathcal{S}_2(pM) \oplus \mathcal{S}_2(pM)) +$ $\dim(\mathcal{S}_2(qM) \oplus \mathcal{S}_2(qM) \cap \mathcal{S}_2(pM) \oplus \mathcal{S}_2(pM))$. The intersection in this expression is isomorphic to the direct sum of four copies of $\mathcal{S}_2(M)$ and so the whole expression is equal to $\dim(Y)$.

For the $\mathbf{T}_{pqM}$-equivariant map λ of tori of the same dimension we find a map $\eta : V \to \operatorname{Hom}(Y, \mathbb{G}_m)$ such that $\lambda\eta$ is an isogeny of V. By reasons of dimension, λ is already an isogeny. Consequently, $t \in \mathbf{T}_{pqM}$ acts as 0 on $\operatorname{Hom}(Y, \mathbb{G}_m)$, respectively on Y, if and only if t acts as 0 on V. For R has purely toric reduction over q, this is equivalent to say, that t acts as 0 on R. This completes the proof. □

View $X \oplus X$ as a $\mathbf{T}_{pqM}$-module via the short exact sequence (3.21). To study this action, we introduce the following quotient of $\mathbf{T}_{pqM}$.

Definition 3.3.9. Consider the intersection $\mathcal{S}_2(pqM)^{q\text{-new}/p\text{-old}}$ of the q-new and the p-old subspaces of $\mathcal{S}_2(pqM)$. The image of $\mathbf{T}_{pqM}$ in the endomorphismring of this intersection is called the *q-new/p-old quotient of* $\mathbf{T}_{pqM}$ and denoted by $\mathbf{T}_{pqM}^{q\text{-new}/p\text{-old}}$.

Theorem 3.3.10. *The* HECKE *algebra $\mathbf{T}_{pqM}$ acts on $X \oplus X$ through its quotient $\mathbf{T}_{pqM}^{q\text{-new}/p\text{-old}}$, which acts faithfully on $X \oplus X$.*

PROOF: In the proof of Theorem 3.2.8 we have seen, that the torus T with character group X is isogenous to the torus U (which was the connected component of 0 in the fiber at q of the NÉRON model of the q-new quotient of $J_0(qM)$). We can confer this upon the associated character groups and obtain, that the group $X \oplus X$ is naturally isogenous to the character group of the torus arising from the reduction at q of the q-new quotient of $J_0(qM) \times J_0(qM)$. On the other hand, $J_0(qM) \times J_0(qM)$ is isogenous to the p-old subvariety of $J_0(pqM)$, that is the image of the p-degeneracy map. Thus, the q-new quotients of these two spaces are as well isogenous. The cotangent space of the dual of this subquotient is isomorphic to the intersection $\mathcal{S}_2(pqM)^{q\text{-new}/p\text{-old}}$. By the above said, this shows the assertion. □

In our discussion of $J_0(qM)_{\mathbb{F}_q}$ we studied the group of connected components Φ of the fiber at q of the NÉRON model of $J_0(qM)$ and showed that it is EISENSTEIN. Let Θ be the analogous group for $J_0(pqM)_{\mathbb{F}_q}$. The p-degeneracy map

$$J_0(qM) \times J_0(qM) \to J_0(pqM)$$

induces a map of finite groups

$$\vartheta : \Phi \times \Phi \to \Theta.$$

We establish an exact sequence (which is not a short exact sequence) by taking the kernel K and the cokernel C of ϑ

$$0 \to K \to \Phi \times \Phi \to \Theta \to C \to 0. \tag{3.22}$$

We will now take advantage of this sequence to describe further the action of $\mathbf{T}_{pqM}$ on $X \oplus X$.

Theorem 3.3.11. *The group K contains the image of Φ in $\Phi \times \Phi$ under the antidiagonal embedding $f \mapsto (f, -f)$.*

PROOF: Per definitionem, the map ϑ is induced by the dual of $\delta : L \to X \oplus X$ and therefore the combination of $\alpha_*, \beta_* : \Phi \rightrightarrows \Theta$ induced by the degeneracy maps $\alpha, \beta : X_0(pqM) \rightrightarrows X_0(qM)$. Consider by Hom-functoriality the map

$$\eta = \operatorname{Hom}(\alpha^* - \beta^*, \mathbb{Z}) : X^\vee \to L^\vee,$$

that is the dual of $\alpha^* - \beta^* : L \to X$. We will show, that $\operatorname{Im}(\eta) \subseteq \operatorname{Im}(\iota_L)$, where ι_L is the embedding (3.19) for L.

Let $\phi \in X^\vee$ and lift it to a linear form on $\Lambda = \mathbb{Z}^{\Sigma(M)}$, where $\Sigma(M)$ is the set of supersingular points of the fiber $X_0(M)_{\overline{\mathbb{F}}_q}$, i.e. $\phi \in \Lambda^\vee$. The divisor D on supersingular points $\Sigma(pM)$ of $X_0(pM)_{\overline{\mathbb{F}}_q}$, defined by

$$D := \sum_{i \in \Sigma(pM)} \phi(\alpha^* i - \beta^* i) \cdot i$$

has degree

$$\sum_{i \in \Sigma(pM)} \phi(\alpha^* i) - \sum_{i \in \Sigma(pM)} \phi(\beta^* i).$$

However, the two sums are equal, since $\alpha \cdot w_p = \beta$ according to the proof of Theorem 3.3.6 and since w_p is just a permutation of $\Sigma(pM)$. Therefore, D has degree 0, which is to say, that it is an element of L. (Recall, that L can be seen as degree-0 divisors on $\Sigma(pM)$ equivalent to X by Proposition 3.1.4.) Furthermore, one has the embeddings $\iota_X : X \hookrightarrow X^\vee$ and $\iota_L : L \hookrightarrow L^\vee$ defined by the diagonal pairings $(e(i))_{i \in \Sigma(M)}$ and $(e(i))_{i \in \Sigma(pM)}$.

We want to establish the equality

$$\iota_L(D) = \eta(\phi),$$

which means, we have to show, that for any two elements $i_1, i_2 \in \Sigma(pM)$, i.e. $\deg(i_1 - i_2) = 0$,

$$\langle D, i_1 - i_2 \rangle_L = \eta(\phi)(i_1 - i_2).$$

The left-hand side is easily computed by taking the ${i_1}^{\text{th}}$ and ${i_2}^{\text{th}}$ coefficient to be

$$\phi(\alpha^* i_1 - \beta^* i_1) e(i_1) - \phi(\alpha^* i_2 - \beta^* i_2) e(i_2).$$

The right-hand side is

$$\phi \circ (\alpha^* - \beta^*)(i_1 - i_2) = \phi(\alpha^* i_1 - \beta^* i_1) - \phi(\alpha^* i_2 - \beta^* i_2).$$

Suppose, that $e(i) > 1$ for $i \in \Sigma(pM)$, then $\alpha^* i - \beta^* i = 0$. Indeed, let i be the isomorphism class of (E, C_M, C_p). Since $e(i) = \frac{\#\operatorname{Aut}(E, C_M, C_p)}{2}$, there is a non-trivial automorphism of E preserving both C_p and C_M. But we have already argued in the proof of Lemma 3.2.13, that in this case $(E, C_M) \cong (E/C_p, (C_M \oplus C_p)/C_p)$, in other words $\alpha^* i = \beta^* i$. So we have the desired equality.

Finally this shows that $\operatorname{Im}(\eta : X^\vee \to L^\vee) \subseteq \operatorname{Im}(\iota_L : L \to L^\vee)$. Consequently, the induced map

$$X^\vee \to L^\vee$$

is trivial. Since $\Phi = \operatorname{Coker}(\iota_X) = X^\vee / X$ and $\Theta = \operatorname{Coker}(\iota_L) = L^\vee / L$, the triviality of this latter map can be conferred on

$$\alpha_* - \beta_* : \Phi \to \Theta,$$

such that α_* and β_* are equal. That $(f, -f)$ is in the kernel of

$$\vartheta : \Phi \times \Phi \to \Theta, \quad (x, y) \mapsto \alpha_*(x) + \beta_*(y),$$

is straightforward. □

Remark 3.3.12. This theorem may be viewed as a refinement of Theorem 3.2.14 in the following way: combine the map $\vartheta : \Phi \times \Phi \to \Theta$ with the map $\Theta \to \Phi \times \Phi$ coming from Albanese functoriality of Jacobians to derive an endomorphism μ of $\Phi \times \Phi$. In terms of the p^{th} Hecke operator τ of $J_0(qM)$ the map μ is given by the formula

$$\mu : (x, y) \to ((p + 1)x + \tau y, \tau x + (p + 1)y),$$

since on Jacobians we have combined the maps

$$(x,y) \mapsto \alpha^*(x) + \beta^*(y) \mapsto (\alpha_*\alpha^*(x) + \alpha_*\beta^*(y), \beta_*\alpha^*(x) + \beta_*\beta^*(y))$$

and by the proof of Theorem 3.3.6 this latter expression equals

$$((p+1)x + \tau y, \tau x + (p+1)y)\,.$$

Clearly $\mathrm{Ker}(\vartheta) \subseteq \mathrm{Ker}(\mu)$, so, by the latter theorem, the image of Φ in $\Phi\times\Phi$ under the antidiagonal embedding is contained in the kernel of μ. This implies, that for all $x \in \Phi$

$$(0,0) = \mu(x,-x) = ((p+1)x - \tau x, \tau x - (p+1)x)\,,$$

and thus $(\tau - (p+1))\,(x) = 0$ for all $x \in \Phi$. For the prime p can be chosen arbitrarily coprime to qM we get the statement of 3.2.14. However, in both proofs, we made use of (parts of) Lemma 3.2.13.

The map $\vartheta : \Phi \times \Phi \to \Theta$ can be seen to be induced by the dual of the degeneracy map $\delta : L \to X \oplus X$ as well as by the map

$$\sigma : X \oplus X \to L,$$

which arises from the two degeneracy maps $\alpha, \beta : X_0(pqM) \rightrightarrows X_0(qM)$ via ALBANESE functoriality of JACOBIANS. From the remark it follows that the composite $\delta\sigma : X \oplus X \to X \oplus X$ is the endomorphism given by the 2×2 matrix $\mu = \begin{pmatrix} p+1 & \tau \\ \tau & p+1 \end{pmatrix}$. Let $Y^\vee$ be the linear dual $\mathrm{Hom}(Y,\mathbb{Z})$ of the kernel of δ. Restricting the above mentioned pairing on L to Y, we obtain an embedding $\iota_Y : Y \hookrightarrow Y^\vee$.

Proposition 3.3.13. *There is a natural exact sequence*

$$0 \to K \to (X \oplus X)/\mu(X \oplus X) \to Y^\vee/Y \to C \to 0.$$

PROOF: Let us start with the natural exact sequence coming from the embedding ι_L

$$0 \to L \to L^\vee \to L^\vee/L \to 0.$$

Dividing out Y, which is contained in L gives

$$0 \to L/Y \to L^\vee/Y \to \Theta \to 0,$$

since $(L^\vee/L)/Y = L^\vee/L = \Theta$. On the other hand, we have the exact sequence coming from ι_X

$$0 \to X \to X^\vee \to X^\vee/X \to 0,$$

which doubled results in

$$0 \to X \oplus X \to X^\vee \oplus X^\vee \to \Phi \times \Phi \to 0,$$

since $X^\vee/X = \Phi$. With Y coming as kernel of δ, we can combine the two exact sequences to a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & X \oplus X \arrow[r] \arrow[d, "\sigma"] & X^\vee \oplus X^\vee \arrow[r] \arrow[d, "\delta^*"] & \Phi \times \Phi \arrow[r] \arrow[d, "\vartheta"] & 0 \\
0 \arrow[r] & L/Y \arrow[r] & L^\vee/Y \arrow[r] & \Theta \arrow[r] & 0.
\end{tikzcd}$$

We know that $\mathrm{Coker}(\delta^*) = \mathrm{Ker}(\delta)^\vee$, more precisely $L^\vee/(X^\vee \oplus X^\vee) = Y^\vee$. In particular, the cokernel of the middle vertical map δ^* is $Y^\vee/Y$. Since the pairing on Y is positive definite (as restriction of the positive definite pairing on L), the latter group is finite. Further we know that $X^\vee \oplus X^\vee$ and $L^\vee/Y$ have the same rank over $\overline{\mathbb{F}}_q$ since Y is the kernel of δ, which thus identifies L/Y with $X \oplus X$. These two statements imply that δ^* is injective. Again identifying L/Y with $X \oplus X$ via δ, the cokernel of the first vertical map σ becomes $(L/Y) / (\sigma(X \oplus X)) \cong (\delta(L/Y)) / (\delta\sigma(X \oplus X)) = X \oplus X/\mu(X \oplus X)$. With the cokernel C and the kernel K of ϑ as introduced above, we obtain the following diagram

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & 0 \arrow[d] & 0 \arrow[d] & K \arrow[d] & \\
0 \arrow[r] & X \oplus X \arrow[r] \arrow[d, "\sigma"] & X^\vee \oplus X^\vee \arrow[r] \arrow[d, "\delta^*"] & \Phi \times \Phi \arrow[r] \arrow[d, "\vartheta"] & 0 \\
0 \arrow[r] & L/Y \arrow[r] \arrow[d] & L^\vee/Y \arrow[r] \arrow[d] & \Theta \arrow[r] \arrow[d] & 0 \\
 & (X \oplus X)/\mu(X \oplus X) \arrow[d] & Y^\vee/Y \arrow[d] & C \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

The application of the Snake Lemma to this diagram now gives the desired exact sequence. □

Remark 3.3.14. The exact sequence of the proposition is compatible with the action of the Hecke algebra, although care must be taken with two points. Firstly, as was already pointed out during our discussion, the p^{th} Hecke operator used on $J_0(qM)^2$ is not induced by the p^{th} Hecke operator of $J_0(qM)$. The second point is caused by the ambiguity of Albanese and Picard functoriality. The correspondences T_n of $X_0(pqM)$ lead, depending on which functoriality one takes, to two $\mathbf{T}_{pqM}$-module structures on L, which are isomorphic since they are interchanged by the Atkin-Lehner involution.

As we have seen, the endomorphism of $\Theta = L^\vee/L$ (and similarly of $\Phi = X^*/L$) induced by T_n is the combination of $(\mathrm{T}_n)^* = \mathrm{Hom}(\mathrm{T}_n, \mathrm{id})$ on $L^\vee$ and ξ_n on L. Consequently, the exact sequence of Proposition 3.3.13, as constructed by the Snake Lemma, is an exact sequence of $\mathbf{T}_{pqM}$-modules via Picard functoriality on all groups save $(X \oplus X)/\mu(X \oplus X)$, where we have to take Albanese functoriality. On the other hand, the $\mathbf{T}_{pqM}$-module structures derived by the different functorialities are again isomorphic, intertwining with an involution corresponding to w_{pqM}. It is induced by the Atkin-Lehner operator $w_{qM} \in \mathrm{Aut}(X)$ diagonally taken on $X \oplus X$. More precisely, it is the interchanging map $(x, y) \mapsto (y, x)$ on $X \oplus X$. Thus, the assertion of Proposition 3.3.13 is correct as it is, even if all groups are equipped with the more usual Picard $\mathbf{T}_{pqM}$-module structure. So, in the following parts we will choose this structure systematically.

Proposition 3.3.15. *Let* $\gamma = (\mathrm{T}_p)^2 - 1 \in \mathbf{T}_{pqM}$. *Then*

$$\mu(X \oplus X) = \gamma(X \oplus X).$$

Proof: The map λ defined on $X \oplus X$ by

$$(x, y) \mapsto (-x, \tau x - y)$$

is an automorphism for its determinant is non-zero. In particular,

$$\lambda(X \oplus X) = X \oplus X.$$

We compute the composition $\mu\lambda : X \oplus X \to X \oplus X \to X \oplus X$ as

$$\begin{aligned}(x,y) \mapsto (-x, \tau x - y) \quad &\mapsto \quad \big(-(p+1)x + \tau x^2 - \tau y, -\tau x + (p+1)\tau x - (p+1)y\big) \\ &= \big(\big(\tau^2 - (p+1)\big)\, x - \tau y, p\tau x - (p+1)y\big)\,.\end{aligned}$$

On the other hand, $\gamma : X \oplus X \to X \oplus X$ is, according to Theorem 3.3.6, given as

$$\begin{aligned}(x,y) \quad \mapsto \quad & \mathrm{T}_p(\tau x - y, px) - (x,y) \\ &= (\tau^2 x - \tau y - px, p\tau x - py) - (x,y) \\ &= \big((\tau^2 - p - 1)x - \tau y, p\tau x - (p+1)y\big)\,.\end{aligned}$$

Comparing the expressions shows that the two maps coincide on $X \oplus X$ and we have $\gamma(X \oplus X) = \mu\lambda(X \oplus X) = \mu(X \oplus X)$ as desired. □

Chapter 4

Bad Reduction of SHIMURA Curves

This chapter exploits well known results of CEREDNIK-DRINFELD stated e.g. in [17]; more precisely, we are interested in the reduction at p of SHIMURA curves. The goal is to deduce some relations between SHIMURA curves and the modular curves $X_0(qM)$ and $X_0(pqM)$ studied in Chapter 3.

4.1 SHIMURA Curves

4.1.1 Idea and Definition

For an indefinite rational quaternion division algebra H there is a (not necessarily unique) indentification of $H \otimes_{\mathbb{Q}} \mathbb{R}$ with $\mathbf{M}_2(\mathbb{R})$. Choose a maximal order $\mathfrak{M}$ of H. Upon the mentioned identification, we can view the group of positive units of $\mathfrak{M}$, denoted by Γ, as a subgroup of $\mathbf{SL}_2(\mathbb{R})$. The group Γ is then a FUCHSIAN group of the first kind and the RIEMANN surface $\Gamma\backslash\mathfrak{H} =: C_H$ is closed (thus compact) which was proven by SHIMURA. (Thinking of the case $H \cong \mathbf{M}_2(\mathbb{Q})$ and $\Gamma \cong \mathbf{SL}_2(\mathbb{Z})$ one obtains the classical modular curves over $\mathbb{C}$ which are not compact.) SHIMURA made the observation that these curves C_H parametrize abelian surfaces with multiplication by $\mathfrak{M} \subseteq H$. From this he was able to show that C_H admits a canonical model V_H over $\mathbb{Q}$ and to prove the EICHLER-SHIMURA relations which serve to describe the HASSE-WEIL L-function of V_H.

Now we will construct SHIMURA curves in a more concrete setting. Let $D = p_1 \cdots p_{2m}$ be the product of an even number of (finite) distinct primes in $\mathbb{Z}$. The unique quaternion algebra H_D over $\mathbb{Q}$ of Section 3.1.2 satisfies $H_D \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbf{M}_2(\mathbb{R})$. So, picking a maximal order $\mathcal{O}_D$ in H_D, one gets an injection

$$\mathcal{O}_D^+ \hookrightarrow \mathcal{O}_D^* \hookrightarrow (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Q})^* = H_D^* \hookrightarrow (H_D \otimes_{\mathbb{Q}} \mathbb{R})^* \cong \mathbf{GL}_2(\mathbb{R}).$$

We write $\mathcal{O}_D^+$ for the inverse image of $\mathbf{GL}_2^+(\mathbb{R})$ in $\mathcal{O}_D^*$ of the composed maps $\mathcal{O}_D^* \hookrightarrow \mathbf{GL}_2^+(\mathbb{R})$, where $\mathbf{GL}_2^+(\mathbb{R})$ is the set of matrices in $\mathbf{GL}_2(\mathbb{R})$ with positive discriminant. Thus we get an inclusion $\mathcal{O}_D^+ \hookrightarrow \mathbf{GL}_2^+(\mathbb{R})$. We denote the composition of the above maps $\mathcal{O}_D^+ \hookrightarrow \mathbf{GL}_2(\mathbb{R})$ by ι.

Definition 4.1.1. Consider the RIEMANN surface $\iota(\mathcal{O}_D^+)\backslash\mathfrak{H}$, where $\mathfrak{H}$ is the POINCARÉ upper half plane. It is compact as we have already mentioned. We define the SHIMURA *curve* $C_D/\mathbb{C}$ *associated to* H_D to be this compact RIEMANN surface.

It has the following modular interpretation: it parametrizes principally polarized abelian surfaces whose ring of endomorphisms contains a maximal order in the quaternion algebra H_D. We denote by V_D the canonical model of C_D over $\mathbb{Q}$. Due to DELIGNE-RAPOPORT respectively CEREDNIK-DRINFELD it is known that C_D has also a model over $\mathbb{Z}[\frac{1}{D}]$ and even over $\mathbb{Z}$.

Remark 4.1.2. As a variation we define $\mathcal{O}_D^\circ(N)$ for N coprime to D to be the set of $x \in \mathcal{O}_D$, for which, upon identifying $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ with $\mathbf{M}_2(\mathbb{Z}_\ell)$ for $\ell \nmid D$, one gets $x \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod \ell^n$ for all $\ell \nmid D$ and $\ell \parallel N$. Again in the same way as above one builds a curve $C_D^0(N)$ over $\mathbb{C}$ and establishes a model $V_D^0(N)$ over $\mathbb{Q}$, which we will call a SHIMURA *curve of discriminant D and level N.*

We note as a fact that the JACOBIAN of $V_D^0(N)$ over $\mathbb{Q}$ is isomorphic to the D-new quotient of $J_0(DN)$.

4.1.2 Our Setting

Let p and q again be distinct primes and M an integer coprime to both. Let further B be an indefinite quaternion division algebra over $\mathbb{Q}$ of discriminant pq uniquely determined up to isomorphism by property (3.2). Let $\mathcal{O}$ be an EICHLER order of level M in B as defined in Section 3.1.2. Let Γ_∞ be the subgroup of $\mathcal{O}$ of elements with reduced norm 1. As mentioned, we can fix an embedding

$$B \to \mathbf{M}_2(\mathbb{R}),$$

which provides in particular an embedding

$$\Gamma_\infty \to \mathbf{SL}_2(\mathbb{R}).$$

Hence, we can consider the action of Γ_∞ on the POINCARÉ upper half plane $\mathfrak{H}$ according to Lemma 1.4.1. Let C be the standard canonical model over $\mathbb{Q}$ of the compact RIEMANN surface $\Gamma_\infty \backslash \mathfrak{H}$ and let J be its JACOBIAN $\mathrm{Pic}^0(C)$. Akin to modular curves (see Section 3.2.1), the curve C is furnished with HECKE correspondences T_n for positive integers n. We write again T_n for the endomorphism of the JACOBIAN induced by it via PICARD functoriality and ξ_n for that one induced via ALBANESE functoriality.

Denote by $\mathcal{C}$ a model for C over $\mathbb{Z}_p$ of the type we considered in Section 2.3, i.e. an admissible model of $C_{\mathbb{Q}_p}$. It follows from the work of SEREDNIK and DRINFELD that J has purely toric reduction at p. Let Z be the character group of the torus $(J_{\mathbb{F}_p})^0$ and Ψ the group of connected components of $J_{\mathbb{F}_p}$. Equivalently to our discussion in Chapter 2 we know that there is a natural bilinear pairing on Z which embeds Z in $Z^\vee$ and the analogue of Theorem 2.2.9 tells us that the group Ψ is the cokernel of this pairing, thus $\Psi \cong Z^\vee/Z$. Later (see Proposition 4.2.8) we will see that this pairing is diagonal and we are to compute its entries.

Let $\widetilde{\mathbf{T}}_{pqM}$ be the formal polynomial ring generated by commuting indeterminates T_n, $n \in \mathbb{N}$, over $\mathbb{Z}$. There are as usual two actions of $\widetilde{\mathbf{T}}_{pqM}$ on J. We denote the action derived via PICARD functoriality by T_n and the ALBANESE action by ξ_n for every n. We shall consider both actions on Z, but only the standard (PICARD) action on Ψ. The standard action of $\widetilde{\mathbf{T}}_{pqM}$ on $\Psi = Z^\vee/Z$ arises from PICARD action of $\widetilde{\mathbf{T}}_{pqM}$ on $Z^\vee$ together with the ALBANESE action of $\widetilde{\mathbf{T}}_{pqM}$ on the submodule $Z \subseteq Z^\vee$.

The aim of this chapter is to relate Z and Ψ to the objects Y and Φ of the previous chapter. Note in particular that every $\mathbf{T}_{pqM}$-module is naturally a $\widetilde{\mathbf{T}}_{pqM}$-module since the HECKE operators T_n of $J_0(pqM)$ turn $\mathbf{T}_{pqM}$ in a quotient of the free $\mathbb{Z}$-module $\widetilde{\mathbf{T}}_{pqM}$ with their relations.

4.2 SHIMURA Curves and their Dual Graphs

4.2.1 The Theorem of CEREDNIK-DRINFELD

To draw a connection between the two character groups Y and Z we summarize results due to CEREDNIK-DRINFELD which were published in [8, §4] and taken on in [17]. They furnish a model $\mathcal{C}$ for C over $\mathbb{Z}_p$.

We first mention without going into details some properties listed at the beginning of [17, §4] of the p-adic upper half plane $\mathcal{P}$, which will be of central interest in the construction of the model. Firstly, the formal scheme $\mathcal{P}$ is flat and locally of finite type over $\mathbb{Z}_p$. It is regular and irreducible, and admits a natural action by $\mathbf{PGL}_2(\mathbb{Q}_p)$. Secondly, the special fiber $\mathcal{P}_0$ of $\mathcal{P}$ is reduced and geometrically connected. All its components are smooth projective rational curves intersecting transversally. All components and their points of intersection are rational over $\mathbb{F}_p$. Finally, the dual graph of the special fiber, with the induced action of $\mathbf{PGL}_2(\mathbb{Q}_p)$ is canonically identified with the BRUHAT-TITS tree Δ of $\mathbf{SL}_2(\mathbb{Q}_p)$, i.e. $\mathbf{PGL}_2(\mathbb{Q}_p)/\,\mathbf{PGL}_2(\mathbb{Z}_p)$, which occured already in the proof of 3.1.17.

Definition 4.2.1. Let $\mathbb{Z}_p^{\mathrm{unr}}$ be a strict henselization of $\mathbb{Z}_p$ and let $\mathsf{Frob} : \mathbb{Z}_p^{\mathrm{unr}} \to \mathbb{Z}_p^{\mathrm{unr}}$ be the FROBENIUS map. Set

$$\mathcal{P}^{\mathrm{unr}} = \mathcal{P} \times_{\mathrm{Spf}\,\mathbb{Z}_p} \mathrm{Spf}\,\mathbb{Z}_p^{\mathrm{unr}}$$

viewed as a formal scheme over $\mathbb{Z}_p$. Define an action of $\mathbf{GL}_2(\mathbb{Q}_p)$ on $\mathcal{P}^{\mathrm{unr}}\,/\,\mathbb{Z}_p$ as follows: For an element $\gamma \in \mathbf{GL}_2(\mathbb{Q}_p)$ denote by $[\gamma]$ the element represented by γ in $\mathbf{PGL}_2(\mathbb{Q}_p)$. Then define

$$\gamma : \mathcal{P}^{\mathrm{unr}} \to \mathcal{P}^{\mathrm{unr}} \quad , \quad (x,u) \mapsto ([\gamma]x, \mathsf{Frob}^{-\operatorname{ord}_p(\det\gamma)}\,u).$$

This is well defined since $[\gamma]$ acts on x via its natural action.

Remark 4.2.2. We use the term of *formal schemes* as introduced in [11, Chapitre 1, §4] seeing them as covariant k-functors from the category of finite k-rings to the category of sets, where k is an arbitrary commutative ring. More precisely, a formal k-functor X is called a formal k-scheme if there is a profinite k-ring A such that there is an equivalence of functors $X \cong \mathrm{Spf}_k(A)$, where $\mathrm{Spf}_k A$ is the formal k-functor defined as follows: for every finite k-ring R, $\mathrm{Spf}_k A(R) = \mathrm{Hom}_k^{\mathrm{cont}}(A,R)$ is the set of morphisms of profinite k-rings from A to R; for every morphism of finite k-rings $\xi : R \to S$, $\mathrm{Spf}_k A(\xi)$ maps $x : A \to R$ to $\xi \circ x : A \to S$.

For a quaternion algebra H of discriminant q over $\mathbb{Q}$, which we will determine later, let K be the product of the multiplicative groups of the completions away from p of a certain EICHLER order $R \subset H$ of level M. Roughly spoken, K is the group of "prime-to-p idèles" of H arising from R. The major result on the bad reduction of SHIMURA curves is the following theorem explained in [17, Theorem 4.3].

Theorem 4.2.3. *The associated formal scheme of the model $\mathcal{C}$ over $\mathbb{Z}_p$ is the quotient*

$$\mathbf{GL}_2(\mathbb{Q}_p)\backslash(\mathcal{P}^{unr} \times X). \tag{4.1}$$

The notations remind us of Chapter 3 and we will see that there is more than one analogy. The ring R in the CEREDNIK-DRINFELD theorem is analogously to the EICHLER orders $\mathrm{End}(\mathbf{E})$ obtained by fixing over $\overline{\mathbb{F}}_p$ a two dimensional abelian variety A. As for the enhancement we fix an embedding $L \subset \mathrm{End}(A)$ of a maximal order L in the quaternion algebra B and a subgroup D of $A[M]$ which is of order M^2 and cyclic over L. By $A[M]$ we denote as usual the M-division points on the variety. Note that our choice of a subgroup of order M^2 is perfectly justified as we deal with a variety of dimension two this time instead with a curve. Further, it comes along with an $L \otimes \mathbb{Z}_p$-isomorphism ι between the formal group of A and a certain "standard" formal modul Φ. The ring R is finally the commutant of L in $\mathrm{End}(\mathbf{A})$, where $\mathbf{A} = (A, D)$ denotes the enhanced variety. This means we have an identification

$$R = \mathrm{End}_L(\mathbf{A}).$$

The ring R is by construction an EICHLER order of level M in the quaternion algebra $H = R \otimes \mathbb{Q}$ given explicitly as the intersection of the two maximal orders $\mathrm{End}_L(A/D)$ and $\mathrm{End}_L(A)$ of H.

Remark 4.2.4. One may ask whether one can override the maximal order $L \subset B$ as it has no counterpart in the theory linking EICHLER orders $\mathrm{End}(\mathbf{E})$ and modular curves as developed in the previous chapter (see in the first instance Section 3.1.2). However, this gives the connection to our initial SHIMURA curve and assures that R has discriminant qM and furthermore H is a quaternion algebra of discriminant q over $\mathbb{Q}$. Indeed, H is the definite quaternion algebra obtained from B by interchanging local invariants at p and ∞; its discriminant is $\frac{\mathsf{Disc}(B)}{p} = q$.

The isomorphism ι mentioned above furnishes by Hom-functoriality an isomorphism

$$R \otimes \mathbb{Z}_p \cong \mathbf{M}_2(\mathbb{Z}_p)$$

which in return induces an isomorphism $H \otimes \mathbb{Q}_p \cong \mathbf{M}_2(\mathbb{Q}_p)$.

The space $X = K \backslash H_f^* / H^*$ can be seen by functoriality as the space of isomorphism classes of two dimensional abelian varieties A' over $\overline{\mathbb{F}}_p$ which are given with the following data: an action of L as to imbed L in $\mathrm{End}(A)$, an enhancement $D' \subset A[M]$ of order M^2 and an isomorphism between Φ and the formal group of A'. More precisely, given an abelian variety A', we choose an isogeny $A' \to A$ which is compatible with the actions of L on either of them. This isogeny identifies the adelic TATE module $T(A') = T_p(A') \times \prod_{\ell \neq p} T_\ell(A')$ with a sublattice of $V(A) = T(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. We may find $g \in H_f^*$ such that

$$T(A') = g^{-1} T(A),$$

and whose image in X classifies A' uniquely with its accompanying data. In principle with little more information, we can now determine the singular points of $\mathcal{C}$ as classes of quadruples.

4.2.2 The Dual Graph Attached to the Special Fiber of $\mathcal{C}$

We will now focus on the dual graph attached to the special fiber of the model $\mathcal{C}$ of our SHIMURA curve over p to compare it with the dual graph of the modular curve $X_0(qM)_{\overline{\mathbb{F}}_p}$. Denote by $\mathbf{GL}_2(\mathbb{Q}_p)^+$ the kernel of the map

$$\nu : \mathbf{GL}_2(\mathbb{Q}_p) \to \mathbb{Z}/2\mathbb{Z} \quad , \quad \gamma \mapsto \mathrm{ord}_p(\det \gamma) \bmod 2,$$

i.e. $\mathbf{GL}_2(\mathbb{Q}_p)^+$ consists of the matrices whose determinants contain an even power of p. The argumentation in [17, §4] result in a geometric EICHLER-SHIMURA relation concerning the dual graph $\mathcal{G}$ attached to the special fiber of $\mathcal{C}$ ([17, Theorem 4.4]):

Theorem 4.2.5. *There is an isomorphism of pairs*

$$(\mathcal{G}, \mathsf{Frob}_{\mathcal{G}}) \cong \left(\mathbf{GL}_2(\mathbb{Q}_p)^+ \backslash (\Delta \times X), \mathfrak{w}_p\right),$$

where $\mathsf{Frob}_{\mathcal{G}}$ *is the induced* FROBENIUS *automorphism of graphs and* $\mathfrak{w}_p$ *may be represented by an element of* L *of norm* p *which coincides with its inverse.* Δ *is the well-known tree attached to* $\mathbf{SL}_2$ *(cf. [42, Chapitre II §1]).*

Recall ([48, p.39]) that for every ring of integers R of a local field K of residue character p with uniformizer π, there is an evident EICHLER order of level π^n in $\mathbf{M}_2(R)$ to which every other EICHLER order of the same level is conjugate. It is given by

$$\mathbf{M}_2(R) \cap \begin{pmatrix} R & \pi^{-n}R \\ \pi^n R & R \end{pmatrix} = \begin{pmatrix} R & R \\ \pi^n R & R \end{pmatrix}.$$

Let $S \subset R$ be the EICHLER order of level Mp in H gotten by intersecting the EICHLER order R of level M with the EICHLER order of level p in $\mathbf{M}_2(\mathbb{Z}_p)$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{M}_2(\mathbb{Z}) \,\middle|\, p \nmid c \right\}.$$

Let $\mathcal{V}$ be the set of isomorphism classes of locally free rank-1 left R-modules, and $\mathcal{E}$ the set of isomorphism classes of locally free rank-1 left S-modules. According to [48, p.87] we have canonically

$$\mathcal{V} = R_f^* \backslash H_f^* / H^*$$

and

$$\mathcal{E} = S_f^* \backslash H_f^* / H^*.$$

The inclusion of S in R defines a projection or degeneracy map

$$\alpha : \mathcal{E} \to \mathcal{V}\,.$$

To maintain the analogy to modular curves, we aim for a second degeneracy map

$$\beta : \mathcal{E} \to \mathcal{V}\,.$$

It is obtained by considering the EICHLER order T of H, which is of level M, contains S and is distinct from R but agrees with R locally at all places except at p. We can think adelically of T as $mR_f m^{-1}$, where m is trivial except at p – it can for instance be chosen as the diagonal matrix $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. Analogously to α there is a projection map

$$\mathcal{E} \to (mR_f^* m^{-1}) \backslash H_f^* / H^*.$$

Since R and T – like all EICHLER orders of the same level – are conjugate, we may identify this last space with $\mathcal{V}$ via multiplication with m^{-1} on H_f^*. The two maps combine to β which therefore maps the class of x in the double coset space defining $\mathcal{E}$ to the class of $m^{-1}x$ in the double coset space defining $\mathcal{V}$.

Proposition 4.2.6. *The set of edges of $\mathcal{G}$ is canonically the set $\mathcal{E}$. The set of vertices of $\mathcal{G}$ is the disjoint union $\mathcal{V} \times \{1, 2\}$ of two copies of $\mathcal{V}$. A given edge $e \in \mathcal{E}$ connects the vertex $(\alpha(e), 1)$ with the vertex $(\beta(e), 2)$.*

PROOF: First note that the quotient $\mathbf{GL}_2(\mathbb{Q}_p)^+ \backslash X$ is trivial because of strong approximation. To specify, for any two enhanced abelian varieties $\mathbf{A}$ and $\mathbf{A}'$ there is – analogously to Lemmas 3.3.3 and 3.3.4 in the case of enhanced elliptic curves – an isogeny $\mathbf{A} \to \mathbf{A}'$ whose degree (or determinant) is an even power of p. For X is the space of isomorphism classes of abelian varieties over $\overline{\mathbb{F}}_p$ with additional data, this means that the quotient is trivial. Hence the set of vertices of $\mathcal{G}$ is the quotient

$$\mathbf{GL}_2(\mathbb{Q}_p)^+ \backslash \left(\mathcal{V}_\Delta \times X \right),$$

where $\mathcal{V}_\Delta$ is the set of vertices of the tree Δ. We refere to [42, Chapitre II, §1] on trees, to state that this set is given by

$$\mathcal{V}_\Delta = \mathbf{PGL}_2(\mathbb{Q}_p) / \mathbf{PGL}_2(\mathbb{Z}_p) = H_p^* / R_p^* \, \mathbb{Q}^*\,.$$

There are two orbits of $\mathcal{V}_\Delta$ under the action of $\mathbf{GL}_2(\mathbb{Q}_p)^+$ namly

$$\mathcal{V}_{\Delta^+} = \mathbf{PGL}_2(\mathbb{Q}_p)^+ / \mathbf{PGL}_2(\mathbb{Z}_p)$$

and its complement in $\mathcal{V}_\Delta$, which we denote by $\mathcal{V}_{\Delta^-}$, depending, whether the discriminant of an element in $\mathbf{PGL}_2(\mathbb{Q}_p)$ contains an even or an odd power of p. Hence the set

$$\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash(\mathcal{V}_{\Delta^+}\times X)$$

is a quotient of X. Two pairs $(1,x)$ and $(1,y)\in\mathcal{V}_{\Delta^+}$ represent the same class in this quotient if and only if x and y have the same image in $\mathbf{GL}_2(\mathbb{Z}_p)\backslash X$. This is clear, since X is defined over $\mathbb{Q}_p$. But recall that $X=K\backslash H_f^*/H^*$ and that K is the product of the multiplicative groups of the completions of R away from p. Thus

$$\mathbf{GL}_2(\mathbb{Z}_p)\backslash\left(K\backslash H_f^*/H^*\right)\cong R_f^*\backslash H_f^*/H^*=\mathcal{V}\,.$$

This shows that

$$\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\,(\mathcal{V}_{\Delta^+}\times X)\cong\mathcal{V}$$

and we have obtained the first copy of $\mathcal{V}$ in $\mathcal{G}$.

Secondly, we study $\mathcal{V}_{\Delta^-}$. Analogously to the previous case, consider

$$\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\,(\mathcal{V}_{\Delta^-}\times X)\,.$$

An arbitrary matrix $m\in\mathbf{GL}_2(\mathbb{Q}_p)$, which is not in $\mathbf{GL}_2(\mathbb{Q}_p)^+$, i.e. whose determinant contains an odd power of p, for instance the diagonal matrix $\begin{pmatrix}1&0\\0&p\end{pmatrix}$, induces a bijection

$$\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\,(\mathcal{V}_{\Delta^+}\times X)\to\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\,(\mathcal{V}_{\Delta^-}\times X)$$

sending the class of $(1,x)$ to the class of (m,mx). So the isomorphism $\mathcal{V}\cong\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\,(\mathcal{V}_{\Delta^-}\times X)$ follows easily, which finally gives us our two desired copies of $\mathcal{V}$ and the set of vertices of $\mathcal{G}$ is naturally a disjoint union of two copies of $\mathcal{V}$.

The set of edges of $\mathcal{G}$ is

$$\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\,(\mathcal{E}_\Delta\times X)$$

where $\mathcal{E}_\Delta$ is the set of edges of the tree Δ. This latter set is isomorphic to the quotient group $\mathbf{GL}_2(\mathbb{Q}_p)^+/S_p^*\,\mathbb{Q}^*$, S_p^* defined as above. The map

$$X\to\mathcal{E}_\Delta\times X\quad,\quad x\mapsto(1,x)$$

identifies $\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\,(\mathcal{E}_\Delta\times X)$ with $S_p^*\backslash X$ via $S_p^*\backslash X\to\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\left(\mathbf{GL}_2(\mathbb{Q}_p)^+/S_p^*\,\mathbb{Q}^*\times X\right)$. It is well defined, since for $x=y$ modulo S_p^* there is $s\in S_p^*$, such that $sx=y$. By choice, s is in the same class as 1 in $\mathbf{GL}_2(\mathbb{Q}_p)^+/S_p^*\,\mathbb{Q}^*$, i.e. in the same class in $\mathcal{E}_\Delta$. So (s,sx) is in the same class modulo $\mathbf{GL}_2(\mathbb{Q}_p)^+$ as $(1,y)$. Injectivity follows in an analogue way and surjectivity is clear. However,

$$S_p^*\backslash X=S_p^*\left(K\backslash H_f^*/H^*\right)\cong S_f^*\backslash H_f^*/H^*=\mathcal{E}\,.$$

Now proceed to the second statement. Take $x\in\mathbf{GL}_2(\mathbb{Q}_p)^+$. The image of x in $\mathcal{E}_\Delta=\mathbf{GL}_2(\mathbb{Q}_p)^+/S_p^*\,\mathbb{Q}^*$ is the edge of Δ, which joins the vertices in $\mathcal{V}_\Delta$ represented by x and xm in $\mathbf{GL}_2(\mathbb{Q}_p)$. The corresponding edge of $\mathcal{G}$ is the class of $(x,1)\equiv(1,x^{-1})$ in $\mathbf{GL}_2(\mathbb{Q}_p)^+\backslash\,(\mathcal{E}_\Delta\times X)$. According to the above said, it maps to the class x^{-1} in the double coset space $\mathcal{E}$. The vertices $(x,1)$ and $(xm,1)$ joined by this edge may be rewritten by the classes of $(1,x^{-1})$ and (m,x^{-1}). The first arises from the class of x^{-1} in the first copy of $\mathcal{V}$. The second arises from the class of $m^{-1}x^{-1}$ in the second copy of $\mathcal{V}$. Comparing this result with the image of the two degeneracy maps $\alpha:\mathcal{E}\to\mathcal{V}$ and $\beta:\mathcal{E}\to\mathcal{V}$ we see indeed that these two elements of $\mathcal{V}$ are obtained from the class of x^{-1} in $\mathcal{E}$ via them. □

Consider the sets of divisors on $\mathcal{E}$ and $\mathcal{V}$. Writing $(\mathbb{Z}^{\mathcal{E}})_0$ and $(\mathbb{Z}^{\mathcal{V}})_0$ for the group of degree-0 divisors over $\mathcal{E}$ and $\mathcal{V}$ respectively we formulate the following

Corollary 4.2.7. *The character group Z is the kernel of the degeneracy map*

$$\omega : (\mathbb{Z}^{\mathcal{E}})_0 \to (\mathbb{Z}^{\mathcal{V}})_0 \times (\mathbb{Z}^{\mathcal{V}})_0$$

induced by (α, β).

Proof: To say that an element $\varepsilon = \sum n_e e \in \mathbb{Z}^{\mathcal{E}}$ is in the kernel of the map

$$\omega : \mathbb{Z}^{\mathcal{E}} \to \mathbb{Z}^{ver} \times \mathbb{Z}^{\mathcal{V}}$$

induced by $(\alpha, \beta) : \mathcal{E} \to \mathcal{V} \times \mathcal{V}$ by linearity amount to the same as to say that every point of $\mathcal{V} \times \{1\}$ respectively $\mathcal{V} \times \{2\}$ is joint by an even number of edges – two of different signs (every vertex is left and joint by the same number of edges). This means, there is no free-end and ε is a loop. By definition of Z as a character group, it is according to Proposition 2.2.6 the homology group $\mathrm{H}_1(\mathcal{G}, \mathbb{Z})$ thus the set of loops of $\mathcal{G}$. So we have seen that Z is the kernel of ω. Since the degeneracy maps are linear, an element $\varepsilon = \sum n_e e \in \operatorname{Ker} \omega$ visibly has divisor degree 0. □

As explained in Section 2.2.3, there is a bilinear pairing on Z coming from the geometry of the Cerednik-Drinfeld model $\mathcal{C}$. We even know that it is the restriction to Z of a diagonal pairing on $\mathbb{Z}^{\mathcal{E}}$ whose value $o(e)$ on an edge $e \in \mathbf{GL}_2(\mathbb{Q}_p)^+ \backslash (\mathcal{E}_\Delta \times X)$ we can compute. For that purpose take a representative $\widetilde{e}$ of e in $\mathcal{E}_\Delta \times X$, and let $\Gamma \subset \mathbf{GL}_2(\mathbb{Q}_p)^+$ be the stabilizer of $\widetilde{e}$ in $\mathbf{GL}_2(\mathbb{Q}_p)^+$. Then $o(e)$ is the order of the image of Γ in $\mathbf{PGL}_2(\mathbb{Q}_p)$ which is independent of the choice of $\widetilde{e}$.

Fix e and let W be a locally free left S-module whose class in

$$\mathcal{E} = S_f^* \backslash H_f^* / H^*$$

is the edge e. The following proposition reminds us of Proposition 3.1.10.

Proposition 4.2.8. *We have*

$$o(e) = \frac{\#(\operatorname{Aut}_S(W))}{2}.$$

Proof: Let $x = (x_\nu) \in H_f^*$ be an adelic representative of e. We may take W to be the S-submodule of H whose completions at the finite places ν of $\mathbb{Q}$ are the S-modules $S_\nu \cdot x_\nu$. Then obviously the S-automorphisms of W are the stabilizer in H^* of the class of x in $S_f^* \backslash H_f^*$. But we can reverse the assertion: if $a \in H^*$ stabilizes x in $S_f^* \backslash H_f^*$, i.e. $xa \in S_f^* x$, then we have by definition $s \in S_f^*$ such that

$$sx = xa.$$

So s is in the stabilizer in S_f^* of the class of x in H_f^*/H^*. Playing the game the other way round, we see that we obtain a bijection between the two stabilizers, that is

$$\operatorname{Aut}_S(W) \cong \mathsf{stab}_{H^*}(S_f^* x) \cong \mathsf{stab}_{S_f^*}(xH^*).$$

We have to determine the stabilizer Γ of the representative $\widetilde{e} = (1, x)$ in $\mathbf{GL}_2(\mathbb{Q}_p)^+$ which is the stabilizer of $x \in X$ under the action of S_p^* on X (recall the map $X \to \mathcal{E}_\Delta \times X$, $x \mapsto (1, x)$ identifying $\mathbf{GL}_2(\mathbb{Q}_p)^+ \backslash (\mathcal{E}_\Delta \times X)$ with $S_p^* \backslash X = \mathcal{E}$). The projection

$$\mathsf{proj}_p : S_f^* \to S_p^*$$

of S_f^* onto the component at p identifies the stabilizer in S_f^* of the class of x in H_f^*/H^* with the stabilizer in S_p^* of the class of x in $X = K \backslash H_f^* / H^*$. Indeed, just as s and a of the previous paragraph determine each other, for $s_p \in S_p^*$ in the equation

$$s_p x = \kappa x a$$

a is determined by s_p and x (more precisely through its component at p) and κ is determined by s_p, x and a. This equation shows the existence of κ and a.

The discussion shows that Γ is isomorphic to the group $\mathrm{Aut}_S(W)$ and it remains to show that $\Gamma \cap \mathbb{Q}_p^*$ is the group of two elements $\{\pm 1\}$ as we have $o(e) = \#\Gamma\big|_{\mathbf{PGL}_2(\mathbb{Q}_p)}$ and

$$\Gamma\big|_{\mathbf{PGL}_2(\mathbb{Q}_p)} = \Gamma/(\Gamma \cap \mathbb{Q}_p^*).$$

Hereto suppose that $s_p \in \Gamma \cap \mathbb{Q}_p^* = \mathbb{Z}_p^*$. Then there is $\kappa \in K$ and $a \in H^*$ such that $s_p x = \kappa x a$. Then a is a rational number, which agrees with s_p at p (i.e. $(a \mod p, a \mod p^2, ...) = s_p$). On the other hand, the prime-to-p part of a coincides with κ^{-1}. Therefore a is a unit locally at each finite place of $\mathbb{Q}$, which means that $a = \pm 1$. Consequently, $s_p = \pm 1$. □

As announced, we begin our comparison of the character groups Z and Y. The latter one, which was defined at the beginning of Section 3.3.2, is the kernel of the natural degeneracy map $\delta : L \to X \oplus X$, where L and X are the degree-0 divisors on $\Sigma(Mp)$ and $\Sigma(M)$, the sets of supersingular points of $X_0(Mp)$ and $X_0(M)$ over q. As we have just seen in Corollary 4.2.7 the group Z has an analogous description with $\mathcal{E}$ instead of $\Sigma(Mp)$ and $\mathcal{V}$ instead of $\Sigma(M)$. So it suggests itself to look for further parallels. And in fact, taking first $M = Mp$ and then $M = M$ in Proposition 3.1.14, we see that $\Sigma(Mp)$ and $\Sigma(M)$ are of a similar structure as double coset spaces as are $\mathcal{E}$ and $\mathcal{V}$, only that S and R are replaced by orders of the form $\mathrm{End}(\mathbf{E}_0, C_p)$ and $\mathrm{End}(\mathbf{E}_0)$ for a supersingular curve E_0 enhanced of order M and a cyclic subgroup C_p of order p. To compare the pairs $(\mathcal{E}, \mathcal{V})$ and $(\Sigma(Mp), \Sigma(M))$ we seek for $(\mathbf{E}_0, C_p)$ such that there are identifications of orders

$$\mathrm{End}(\mathbf{E}_0, C_p) \cong S \quad \text{and} \quad \mathrm{End}(\mathbf{E}_0) \cong R.$$

For the following statement of existence let $\mathcal{M}$ denote the maximal order $\mathrm{End}_L(A)$ of H. Thus R and S are EICHLER orders of level M and pM in $\mathcal{M} \subset H$.

Proposition 4.2.9. *There is an enhanced supersingular elliptic curve $\mathbf{E}_0 = (E_0, C_M)$, a cyclic subgroup C_p of E_0, and an isomorphism $\kappa : \mathrm{End}(E_0) \to \mathcal{M}$ such that R corresponds to $\mathrm{End}(\mathbf{E}_0)$ and S to $\mathrm{End}(\mathbf{E}_0, C_p)$ under κ.*

PROOF: Apply Proposition 3.1.17 to the maximal orders $B = \mathcal{M}$ and $B' = \mathrm{End}_L(A/D)$ such that the intersection $B \cap B'$, denoted S in 3.1.17 is R in our setting. This provides us with an enhanced elliptic curve $\mathbf{E}_0 = (E_0, C_M)$ and an isomorphism $\kappa : (R, \mathcal{M}) \xrightarrow{\cong} (\mathrm{End}(\mathbf{E}_0), \mathrm{End}(E_0))$. In order to construct the subgroup C_p such that $\kappa(\mathrm{End}(\mathbf{E}_0, C_p)) = S$, we examine S and R locally at p identifying via κ $S \otimes \mathbb{Z}_p$ and $R \otimes \mathbb{Z}_p$ with subrings of

$$\mathrm{End}(E_0) \otimes \mathbb{Q}_p = \mathrm{End}(V_p(E_0)),$$

where $V_p(E_0)$ arises from the p-adic TATE module $T_p(E_0)$ by tensoring with $\mathbb{Q}$; by the way $\mathrm{End}(T_p(E_0))$ is a maximal order in $\mathrm{End}(V_p(E_0))$. Since $R = \mathrm{End}_L(\mathbf{A})$ and $\mathcal{M} = \mathrm{End}_L(A)$ agree locally at p, given that p and M are relatively prime to each other, $R \otimes \mathbb{Z}_p$ may be identified with

$$\mathrm{End}(T_p(E_0)).$$

The ring S is an EICHLER order of level p in the maximal order $\mathrm{End}(T_p(E_0))$. We constructed S by intersecting R and an "evident" EICHLER order of $\mathbf{M}_2(\mathbb{Z}_p)$. Consequently, $S \otimes \mathbb{Z}_p$ can be written as an intersection

$$\mathrm{End}(T_p(E_0)) \cap \mathrm{End}(U),$$

for some lattice $U \subseteq V_p$. According to the Lemma of BÉZOUT it is possible to scale U such that it is contained in $T_p(E_0)$ but not in $pT_p(E_0)$. Thus the group $T_p(E_0)/U$ is of order p, as is the image C_p of U in $E_0[p] = T_p/pT_p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by projection. By construction, an endomorphism of $T_p(E_0)$ preserves C_p in $T_p(E_0)/pT_p(E_0)$ if and only if it preserves U. Hence, we found C_p with the property

$$\begin{aligned} S \otimes \mathbb{Z}_p &= \operatorname{End}(T_p(E_0)) \cap \operatorname{End}(U) \\ &\cong \operatorname{End}(T_p(E_0), U) \\ &\cong \operatorname{End}(T_p(E_0)) \cap \operatorname{End}(T_p(E_0)/U) \\ &\cong \operatorname{End}(T_p(E_0)/pT_p(E_0)) \cap \operatorname{End}(C_p) \otimes \mathbb{Z}_p \\ &= \operatorname{End}(E_0, C_p) \otimes \mathbb{Z}_p\,. \end{aligned}$$

This shows the claim locally at p. Outside p, S agrees with R and $\operatorname{End}(\mathbf{E}_0, C_p)$ with $\operatorname{End}(\mathbf{E}_0)$. So we have the global result $S = \operatorname{End}(\mathbf{E}_0, C_p)$. □

Lemma 4.2.10. *There are bijections*

$$\iota : \Sigma(Mp) \to \mathcal{E} \qquad \textit{and} \qquad \lambda : \Sigma(M) \to \mathcal{V}\,.$$

PROOF: The proof is a constructive one, where we will use the enhanced elliptic curve $\mathbf{E}_0$ and its subgroup C_p given in Proposition 4.2.9, but we will surpress the isomorphism κ to simplify matters and consider $S = \operatorname{End}(\mathbf{E}_0, C_p)$ and $R = \operatorname{End}(\mathbf{E}_0)$.

Start with a given supersingular elliptic curve E over $\overline{\mathbb{F}}_q$ together with a cyclic subgroup C_{pM} of order pM in E. As in the proof of Proposition 3.1.14 consider the adelic TATE module $T(E)$ of E. There is a distinguished sublattice $T'(E)$ of $T(E)$ defined by C_{pM} which contains $pM \cdot T(E)$ and is of such a type that $T'(E)/pM \cdot T(E)$ is cyclic of order pM. Note that consequently $T(E)/T'(E)$ is cyclic of order pM. There is an analogous sublattice $T'(E_0)$ of $T(E_0)$ defined by the enhancement of order M of E_0 and by the cyclic subgroup C_p. The latter two lattices a priori and the first two ones after fixing a non-trivial homomorphism $E \to E_0$ may be regarded as contained in $V(E_0) = T(E_0) \otimes \mathbb{Q}$. As in the proof of Proposition 3.1.14 we can choose an element $g \in H_f^*$ such that the equations

$$T(E) = g^{-1}T(E_0) \qquad \text{and} \qquad T'(E) = g^{-1}T'(E_0)$$

are simultanously fullfilled. What is more, the class of g in the double coset space $\mathcal{E} = S_f^* \backslash H_f^* / H^*$ depends only on E and its given cyclic subgroup. We define the value of ι on (E, C_{pM}) to be the class of g and this is well defined. Replacing the cyclic subgroups of order Mp by such ones of order M, we can define λ straight forward in the same manner. Note that the g of λ differs from the g of ι only by a multiple in R_f^*. To see that the two maps are bijective means to copy the argumentation of 3.1.14 with the difference that the completed EICHLER order and the quaternion algebra have switched places in the double-coset representation because we use g^{-1} defining ι and λ whereas g^{+1} is used in Section 3.1.2. □

We will now study the relation between the two degeneracy maps

$$\alpha, \beta : \mathcal{E} \rightrightarrows \mathcal{V}$$

defined above and the degeneracy maps

$$\alpha, \beta : \Sigma(Mp) \rightrightarrows \Sigma(M)$$

defined in the previous chapter to legitimate their analogue nomenclatur.

Proposition 4.2.11. *We have*

$$\lambda\alpha = \alpha\iota \qquad \textit{and} \qquad \lambda\beta = \beta\iota.$$

Proof: Let $T(E)$ and $T'(E)$ be lattices as introduced above, with cyclic quotient $T(E)/T'(E)$ of order pM. Applying $\beta : \Sigma(MP) \to \Sigma(M)$ on the enhanced elliptic curve (E, C_M, C_p) means to divide out the cyclic subgroup C_p and derive a new elliptic curve F. For M and p are relatively prime by assumption, we may translate this one-to-one on the adelic Tate modules. Thus, if we apply β on $T(E)$ we obtain the unique lattice $T(F)$ between $T'(E)$ and $T(E)$ for which $T(F)/T'(E)$ is cyclic of order M. It will turn out to be essential that $T'(E)$ can be seen as a sublattice of $T(F)$ associated to the cyclic subgroup of order M in F.

Let $m \in H_f^*$ again be the idélic matrix which is trivial locally except at p, where it is the diagonal matrix $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. As in the lemma, we have $T(E_0)$ and a sublattice $T'(E_0)$ associated with the cyclic subgroup of order pM in E_0. We know that $T'(E_0)/pM \cdot T(E_0)$ is cyclic of order pM and so is $T(E_0)/T'(E_0)$. By construction of S as intersection of R and a second evident order, $m^{-1}T'(E_0)/pM \cdot T(E_0)$ and $T(E_0)/m^{-1}T'(E_0)$ are cyclic of order M. This shows that $m^{-1}T'(E_0)$ is the sublattice of $T(E_0)$ attached to the cyclic subgroup of order M in E_0. On the other hand, $mT(E_0)$ is the sublattice of $T(E_0)$ associated with the cyclic subgroup of order p in E_0.

To examine the image of λ on $\Sigma(M)$, after we have already applied $\beta : \Sigma(Mp) \to \Sigma(M)$, we have to find an element $x \in H_f^*$ for the couple $(T(F), T'(E))$ such that

$$T(F) = x^{-1}T(E_0) \qquad \text{and} \qquad T'(E) = x^{-1}(m^{-1}T'(E_0)),$$

according to the recipe of Lemma 4.2.10. Take $x = m^{-1}g$, where g comes from the definition of λ in the lemma. This will do it. Indeed,

$$\begin{aligned} x^{-1}m^{-1}T'(E_0) &= g^{-1}mm^{-1}T'(E_0) \\ &= g^{-1}T'(E_0) \\ &= T'(E) \end{aligned}$$

and

$$\begin{aligned} x^{-1}T(E_0) &= g^{-1}mT(E_0) \\ &= T(F). \end{aligned}$$

Consequently, the composition $\lambda \circ \beta$ is given by

$$\Sigma(pM) \to \Sigma(M) \to \mathcal{V}, \qquad (E, C_p \oplus C_m) \to (E/C_p, (C_p \oplus C_M)/C_p) \cong (F, C_M) \to m^{-1}g.$$

On the other hand, $\beta : \mathcal{E} \to \mathcal{V}$ is induced by multiplication by m^{-1} on H_f^*. So $\beta \circ \iota$ is the map

$$\Sigma(pM) \to \mathcal{E} \to \mathcal{V}, \qquad (E, C_p \oplus C_M) \to g \to m^{-1}g.$$

This shows the compatibility of λ and ι concerning β.

The compatibility involving α is quite straightforward. Applying α to $\Sigma(pM)$ simply means to forget about the structure of the subgroup of order p. As for the Tate modules, $T(E)$ remains, but the sublattice $T'(E)$ attached to the cyclic subgroup of order pM is replaced by the sublattice $T''(E)$ attached to the cyclic subgroup of order M. Now use the recipe of Lemma 4.2.10 with M to obtain an element $g \in H_f^*$ to which (E, C_M) is associated via λ. So $\lambda \circ \alpha$ is given by

$$\Sigma(pM) \to \Sigma(M) \to \mathcal{V}, \qquad (E, C_p \oplus C_M) \to (E, C_M) \to g.$$

The degeneracy map $\alpha : \mathcal{E} \to \mathcal{V}$ maps the class of an element x in $\mathcal{E}$ to its class in $\mathcal{V}$. So $\alpha \circ \iota$ is just given by

$$\Sigma(pM) \to \mathcal{E} \to \mathcal{V}, \qquad (E, C_p \oplus C_M) \to g \to g.$$

In both cases, we mean by g its class in the respective double-coset space. We wrote g in both cases, although the g's might not be the same, however their classes in $R_f^* \backslash H_f^* / H^*$ are, and this is what counts. So we showed the second compatibility. □

4.3 Relation between Shimura Curves and Modular Curves

The previous section gave us tools at hand to prove the main theorem of this chapter.

Theorem 4.3.1. *There is a $\widetilde{\mathbf{T}}_{pqM}$-isomorphism $Z \cong Y$ under which the bilinear pairing on Z corresponds to the restriction to Y of the natural pairing on L*

Proof: Because Y and Z are kernels of degeneracy maps coming from the respective α and β, the bijection $\iota : \Sigma(pM) \to \mathcal{E}$ of Lemma 4.2.10 induces in view of Proposition 4.2.11 an isomorphism $Y \cong Z$, which is also denoted by ι. Indeed, we have the commutative diagramm of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & Y \arrow[r] \arrow[d, "\iota"] & \mathbb{Z}_0^{\Sigma(pM)} \arrow[r, "\delta"] \arrow[d, "\iota"] & \mathbb{Z}_0^{\Sigma(M)} \oplus \mathbb{Z}_0^{\Sigma(M)} \arrow[r] \arrow[d, "\lambda"] & 0 \\
0 \arrow[r] & Z \arrow[r] & \mathbb{Z}_0^{\mathcal{E}} \arrow[r, "\delta"] & \mathbb{Z}_0^{\mathcal{V}} \oplus \mathbb{Z}_0^{\mathcal{V}} \arrow[r] & 0.
\end{tikzcd}$$

To prove the theorem completely we have to establish a compatibility of $\iota : Y \to Z$ with the natural pairings and the action of Hecke operators on these two modules.

Lemma 4.3.2. *The isomorphism $\iota : Y \to Z$ is compatible with the natural diagonal pairings on Y and Z respectively.*

Proof: As we have mentioned in Section 3.3.2 the module Y inherits from $\mathbb{Z}^{\Sigma(Mp)}$ the diagonal pairing whose value on an enhanced-of-order-pM elliptic curve $\underline{\mathbf{E}} = (E, C_{pM})$ is according to Proposition 3.1.10 the integer $\frac{\#\operatorname{Aut}(\underline{E})}{2}$. Write $\underline{\mathbf{E}}_0$ for the enhanced elliptic curve of order pM appearing as output of Proposition 4.2.9 such that $S = \operatorname{End}(\underline{\mathbf{E}}_0)$. As in the proof of Lemma 3.3.4 consider the locally free rank-1 left S-module $W = \operatorname{Hom}(\underline{\mathbf{E}}, \underline{\mathbf{E}}_0)$ whose class in $\mathcal{E}$ is the edge $e := \iota(\underline{E})$. Akin to the discussion in Section 4.2.1 we may see $W = \operatorname{Hom}(\underline{\mathbf{E}}, \underline{\mathbf{E}}_0)$ as the adélic Tate module $T(\underline{\mathbf{E}})$. As a consequence of Tate's theorem on endomorphisms of abelian varieties over finite fields (cf. [47]) we have locally

$$\operatorname{End}_{\operatorname{End}(\underline{\mathbf{E}}_0)}(T_\ell(\underline{\mathbf{E}})) \cong \mathbb{Z}_\ell \otimes \operatorname{End}(\underline{\mathbf{E}}),$$

which means globally

$$\operatorname{End}_S(W) = \operatorname{End}_{\operatorname{End}(\underline{\mathbf{E}}_0)}(\operatorname{Hom}(\underline{\mathbf{E}}, \underline{\mathbf{E}}_0)) \cong \operatorname{End}(\underline{\mathbf{E}}),$$

i.e. $\operatorname{End}(\underline{\mathbf{E}})$ is the commutant of W. In particular, we have

$$\operatorname{Aut}(\underline{\mathbf{E}}) = \operatorname{Aut}_S(W).$$

Hence by Propositions 4.2.8 and 3.1.10 there is an accordance

$$o(e) = \frac{\#\operatorname{Aut}_S(W)}{2} = \frac{\#\operatorname{Aut}(\underline{\mathbf{E}})}{2} = e(i),$$

where $e(i)$ is the value of the pairing on $\mathbb{Z}^{\Sigma(pM)}$ associated to $\underline{\mathbf{E}}$. □

We conclude with an examination of the Hecke operators.

Lemma 4.3.3. *The isomorphism $\iota : Y \to Z$ is compatible with the p^{th} Hecke operator T_p.*

Proof: The unramified p-adic upper half plane appearing in the model $\mathbf{GL}_2(\mathbb{Q}_p)\backslash(\mathcal{P}^{\mathrm{unr}} \times X)$ over $\mathbb{Z}_p$ of C is a formal scheme, more precisely it represents a functor involving formal groups, which is furnished with a natural action of the group $\mathbf{GL}_2(\mathbb{Q}_p) \times D^*$, where D is the (up to isomorphism) unique quaternion division algebra over $\mathbb{Q}_p$ (see [48, Chapitre II, Théorème 1.3]).

Drinfeld establishes the induced action on $\mathcal{P}^{\mathrm{unr}}$ explicitly in [8, §2, Main Theorem]. In our context, it suffices to know that the involution T_p of $\mathbf{GL}_2(\mathbb{Q}_p)\backslash(\mathcal{P}^{\mathrm{unr}} \times X)$ is induced by the element $1 \times \pi \in \mathbf{GL}_2(\mathbb{Q}_p) \times D^*$, where π is a uniformizer of D, which exists since we are over a local field. In particular, this element acts as the inverse Frobenius automorphism Frob^{-1} on $\mathcal{P}^{\mathrm{unr}}$. Consequently, T_p induces the Frobenius automorphism on $\mathcal{C}_{\mathbb{F}_p}$. The induced involution on the dual graph $\mathcal{G} = \mathbf{GL}_2(\mathbb{Q}_p)^+\backslash(\Delta \times X)$ is denoted by $\mathfrak{w}_p$ in Theorem 4.2.5. This involution is represented by any element $m \in \mathbf{GL}_2(\mathbb{Q}_p)$ which does not belong to $\mathbf{GL}_2(\mathbb{Q}_p)$. The resulting automorphism of $\Delta \times X$ induces an involution τ of $\mathcal{G}$ which is obviously independent of the choice of m.

To examine the action of τ on $\mathcal{G}$ start with the edges $\mathcal{E}$. Take $x \in X$ and denote by e the image of $1 \times x \in \mathcal{E}_\Delta \times X$ modulo $\mathbf{GL}_2(\mathbb{Q}_p)^+$. By construction, τe is represented by $(m \cdot 1, mx)$. However, we can choose m in a way such that τe has a representative of the form $(1, mx)$. Indeed, to give a representative of τe of this form, choose $u \in \mathbf{GL}_2(\mathbb{Q}_p)^+$ such that $um \cdot 1 = 1$ in $\mathcal{E}_\Delta$. Note that then the determinant of um has again odd p-power order. Then τe is the class of umx in $\mathcal{E} = S_p^*\backslash X$. So τ may be viewed as the involution of $S_p^*\backslash X$ induced by the non-trivial multiplication of $n = um$ on X. Since S is per constructionem the intersection of R and the Eichler order $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{M}_2(\mathbb{Z}) \,\middle|\, p \mid c\right\}$, we see easily that $nS_p^*n^{-1} \subseteq S_p^*$. This means, that it is an element of the normalizer of S_p^* in $\mathbf{GL}_2(\mathbb{Q}_p)$ which is not in S_p^* – a description which characterises τ completely. Without loss of generality, we may take

$$n = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix},$$

which recalls the Atkin-Lehner involution (1.24) of $\Sigma(pN)$. Indeed, let g be the image of (E, C_M, C_p) under ι; by the same argumentation as in Proposition 4.2.11 $ng = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$ accords to the same triple save that C_p is divided out; so by functoriality the image of $\tau : \mathcal{E} \to \mathcal{E}$ under $\iota : \Sigma(pM) \to \mathcal{E}$ is the map

$$\iota^{-1}\tau\iota : \Sigma(pM) \to \mathcal{E} \to \mathcal{E} \to \Sigma(pM)$$

given by

$$(E, C_M, C_p) \mapsto g \mapsto ng \mapsto (E/C_p, (C_M \oplus C_p)/C_p, E[p]/C_p)$$

and this is the Atkin-Lehner involution (3.15). However, the action of τ on the character group $Z \subset \mathbb{Z}^{\mathcal{E}}$ is the negative of the automorphism induced by this involution on $\mathcal{E}$. In fact, the map τ on the graph $\mathcal{G}$ changes the orientation of each edge $e \in \mathcal{E}$ since it maps vertices in the first copy of $\mathcal{V}$ to vertices in the second one and vice versa, as do all maps whose determinant contains an odd power of p as we have seen in the proof of Proposition 4.2.6.

On the other hand, the Atkin-Lehner involution of $X_0(pqM)_{\mathbb{F}_q}$ preserves the two components of $X_0(pqM)_{\mathbb{F}_q}$ such that the induced map of the associated character group $L \subset \mathbb{Z}^{\Sigma(pM)}$ is simply the restriction to L of the involution of $\mathbb{Z}^{\Sigma(pM)}$ induced by w_p on $\Sigma(pM)$; this holds equally for $Y \subset L$. Hence the action of w_p on Y corresponds to the negative action of τ on Z under the isomorphism $\iota : Y \to Z$. Equivalently, the action of T_p on Z corresponds to the map $-w_p$ on Y. But by Theorem 3.3.6 we have the formula $\mathrm{T}_p = w_p$ on Y. This completes our discussion of the Hecke operator T_p. □

The Hecke operators T_r with $r \neq p$ operate on the graph $\mathcal{G}$ through a operation on X, which is already visible on the space $K\backslash H_f^*$ of L-stable lattices of the form $T(A')$ in $V(A)$. The operator T_r applied to the adélic Tate module $T(A')$ affects only the r^{th} component of the product leaving the other factors untouched. In the language of correspondences, this mentioned modification in fact involves replacing $T_r(A')$ by a sum of several lattices in $V_r(A)$. This sum contains $r + 1$ terms save for r dividing Mq in which case it contains only r.

Since the operators T_r act on the set of vertices of $\mathcal{G}$ via their action on X, the proof of Proposition 4.2.6 tells us that it preserves in particular the decomposition of this set as a disjoint union of two copies of $\mathcal{V}$. Consequently, in contrast to the action induced by T_p, the action of T_r on Z is the restriction to Z of its action on $\mathbb{Z}^{\mathcal{E}}$.

Lemma 4.3.4. *The isomorphism $\iota : Y \to Z$ is compatible with the q^{th}* Hecke *operator T_q.*

Proof: The operator T_q replaces an $L \otimes \mathbb{Z}_q$-stable lattice $T \subset V_q(A)$ by the unique $L \otimes \mathbb{Z}_q$-stable lattice $T' \supseteq T$ for which $[T' : T] = q^2$. (It suffices to consider this case because only the q^{th} factor is affected by T_q.) Suppose that T is given in the form $g^{-1}T_q(A)$ according to Lemma 4.2.10, with $g \in H_q^*$, where

$$H_q = \mathrm{End}_{L \otimes \mathbb{Q}_q}(V_q(A)).$$

Since H_q is a quaternion algebra over a local field of residue characteristic q, we have for any uniformizer π of the ring of integers of H_q

$$T' = g^{-1}\pi^{-1}T_q(A).$$

Hence replacing T by T' means to send g to πg and the action of T_q on $\mathcal{E} = S_f^* \backslash H_f^* / H^*$ is induced by left-multiplication by π on H_f^* where π now denotes the idèle, which is a uniformizer at q and 1 elsewhere. With help of the bijection $\Sigma(pM) \cong \mathcal{E}$ this map can be identified as the Frobenius automorphism of $\Sigma(pM)$. According to the Corollary 3.2.4 of Proposition 3.2.2, applied with Mp instead of M, this automorphism induces the Hecke operator T_q on Y. □

Lemma 4.3.5. *The isomorphism $\iota : Y \to Z$ is compatible with the r^{th}* Hecke *operator T_r with a prime number r relatively prime to pqM.*

Proof: A lattice $T \subset V_r(A)$ is replaced by the formal sum of $L \otimes \mathbb{Z}_r$-stable lattices with $[T' : T] = r^2$. In analogy to the proof of Lemma 3.3.3 we construct these lattices by considering the set of elements of H_r^* which have reduced norm r. We may write this set as

$$\coprod_{i=1}^{r+1} R_r^* a_i,$$

with $a_i \in H_r^*$. As above describe T as $g^{-1}T_r(A)$ with $g \in H_r^*$. Applying T_r on T means then

$$\mathrm{T}_r(T) = \sum_{i=1}^{r+1} g^{-1}a_i^{-1}T_r(A).$$

Thus the induced map on $\mathcal{E} = S_f^* \backslash H_f^* / H^*$ sends $g \in H_f^*$ to the degree of the above divisor $\sum a_i g$. Again the a_i in this latter sum are the idèles given through the natural inclusion of H_r^* in H_f^*. The identification of $\mathcal{E}$ and $\Sigma(pM)$ via ι brings again forward the standard description (3.13) of T_r in the elliptic modular case. □

Lemma 4.3.6. *The isomorphism $\iota : Y \to Z$ is compatible with the r^{th}* Hecke *operator T_r with a prime number $r \mid M$.*

Proof: The argumentation is exactly the same as for Lemma 4.3.5 save that the coproduct and sum have only got r elements instead of $r + 1$ so as to result in the description (3.14) for T_r in the case $r \mid M$. □

These lemmas finally complete the proof of the theorem. □

On the one hand, we understand the action of $\widetilde{\mathbf{T}}_{pqM}$ on Z and on Y here to be the Picard action. On the other hand, we can deduce the following corollary.

Corollary 4.3.7. *The modules Z and Y are isomorphic with the* Albanese *action of $\widetilde{\mathbf{T}}_{pqM}$.*

PROOF: This follows from the fact that T_n and ξ_n are adjoint operators on L and Z respectively under the pairings $L \times L \to \mathbb{Z}$ and $Z \times Z \to \mathbb{Z}$. □

In Definition 3.3.7 $\mathbf{T}_{pqM}^{pq-\mathrm{new}}$ was introduced as the pq-new quotient of the HECKE algebra $\mathbf{T}_{pqM}$, i.e. the quotient of $\mathbf{T}_{pqM}$ cut out by the space $\mathcal{S}_2(pqM)^{pq-\mathrm{new}}$ of forms on $\Gamma_0(pqM)$ which are new relative to p and q with respect to the PETERSON-inner product. As we have compared Z and Y this far it is of interest to recall that $\mathbf{T}_{pqM}^{pq-\mathrm{new}}$ is also the quotient of $\mathbf{T}_{pqM}$ cut out by Y (see Theorem 3.3.8).

Corollary 4.3.8. *There is a unique injection $\mathbf{T}_{pqM}^{pq-new} \to \mathrm{End}(J)$ mapping the n^{th} HECKE operator in $\mathbf{T}_{pqM}^{pq-new}$ to the n^{th} HECKE operator on J.*

PROOF: We know that $t \in \mathbf{T}_{pqM}^{pq-\mathrm{new}}$ is 0 if and only if it acts as 0 on Y. According to Theorem 4.3.1, Z and Y are $\widetilde{\mathbf{T}}_{pqM}$-isomorphic. Thus, t acts as 0 on Y, if and only if it acts as 0 on Z. By a well known property of abelian varieties with purely toric reduction – and this is the case with J – which we already used in the proof of Theorem 3.2.8, the action of $\mathrm{End}_{\mathbb{Q}}(J)$ on Z is faithful. Therefore, t maps to 0 in $\mathrm{End}_{\mathbb{Q}}(J)$ if and only if it acts as 0 on Z. These arguments give the desired injection. □

Now take again $\gamma = (\mathrm{T}_p)^2 - 1$ as in Proposition 3.3.15. A variant of the main result of this chapter is the following

Theorem 4.3.9. *There is an exact sequence of $\mathbf{T}_{pqM}$-modules*

$$0 \to K \to (X \oplus X)/\gamma(X \oplus X) \to \Psi \to C \to 0,$$

in which K and C are the groups introduced in the exact sequence 3.22.

PROOF: In Proposition 3.3.13 we have established the natural exact sequence

$$0 \to K \to (X \oplus X)/\mu(X \oplus X) \to Y^\vee/Y \to C \to 0,$$

which by means of Proposition 3.3.15 turns into

$$0 \to K \to (X \oplus X)/\gamma(X \oplus X) \to Y^\vee/Y \to C \to 0.$$

Now we have learned that Y and Z are isomorphic. It is important that this isomorphism agrees with the action of the HECKE algebra. Indeed, Corollary 4.3.8 guarantees that $\widetilde{\mathbf{T}}_{pqM}$ operates on Y through its quotient $\mathbf{T}_{pqM}^{pq-\mathrm{new}}$ which is itself a quotient of $\mathbf{T}_{pqM}$. So it is legitimate to describe $\Psi = Z^\vee/Z$ as a $\mathbf{T}_{pqM}$-module and to replace $Y^\vee/Y$ in the sequence by Ψ in order to get the announced exact sequence. □

Chapter 5

Modular Representations of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

5.1 Modular Representations

5.1.1 The Čebotarev Density and Brauer-Nesbitt Theorems

This chapter is dedicated to a deeper study of modular Galois representations as introduced in Section 1.5. There are some famous results which we apply without proof. We begin by recalling the Čebotarev Density Theorem which is stated in [42, p. I-7].

Definition 5.1.1. Let K be a number field and denote by Σ_K the set of all finite places of K, i.e. the set of all normalized discrete valuations of K. Let P be a subset of Σ_K. For every integer n, let $a_n(P)$ be the number of places $\nu \in P$ such that $\operatorname{Norm}_{K/\mathbb{Q}}(\nu) \leq n$. If there is a real number a such that

$$\lim_{n\to\infty} \frac{a_n(P)}{a_n(\Sigma_K)} = a,$$

one says that P has *density* a.

Theorem 5.1.2. *Let L be a finite* Galois *representation of the number field K. Let X be a normal subset of the* Galois *group $\operatorname{Gal}(L/K)$. Let P_X be the set of places $\nu \in \Sigma_K$, unramified in L, such that the class of the* Frobenius *element Frob_ν is contained in X. Then P_X has density equal to $\frac{\#X}{\#\operatorname{Gal}(L/K)}$.*

This theorem has two important corollaries that both will be referred to as Čebotarev Density Theorem.

Corollary 5.1.3. *For every $g \in \operatorname{Gal}(L/K)$, there exist infinitely many unramified places $w \in \Sigma_L$ such that $\mathsf{Frob}_w = g$.*

For infinite extensions, we have:

Corollary 5.1.4. *Let L be a* Galois *extension of K, which is unramified outside a finite set S.*

1. *The set of* Frobenius *elements of the unramified places of L is dense in $\operatorname{Gal}(L/K)$.*
2. *Let X be a normal subset of $\operatorname{Gal}(L/K)$. Assume that the boundary of X has measure 0 with respect to the normalized* Haar *measure μ of X. Then the set of places $\nu \notin S$ such that $\mathsf{Frob}_\nu \subseteq X$ has a density equal to $\mu(X)$.*

The other result, which we will use is the BRAUER-NESBITT Theorem. In [3] one version is stated as Theorem 30.16.

Theorem 5.1.5. *Let K be a number field and G a finite group. Let M, N be KG-modules affording matrix representations $\mathbf{M}$ and $\mathbf{N}$ respectively. Suppose there exists an extension field L of K such that L is a splitting field for G and with the property that if V is a completely reducible (or semi-simple) KG-module, then $V \otimes L$ is a completely reducible LG-module (we may take $L = K$ if K is already a splitting field). Then M and N have the same composition factors if and only if for all $g \in G$ the matrices $\mathbf{M}(g)$ and $\mathbf{N}(g)$ have the same characteristic roots (counted according to their multiplicity).*

Particularly in the third part of this section the mentioned theorems will play an important role to identifiy certain representations.

5.1.2 Results due to RAYNAUD

We will need information about vector space schemes and group schemes of type $(p, \ldots, p)$ covered by RAYNAUD in [32].

In Section 3.3 of his article he treats prolongation of vector space schemes. Let R be a discrete valuation ring of field of fractions K and residue field $\mathbb{F}$ of characteristic p. Let $\mathcal{G}$ be a finite flat R-scheme whose generic fiber G is an $\mathbb{F}$-vector space scheme. In general the action of $\mathbb{F}$ on G does not extend to $\mathcal{G}$. But if G is ètale (respectively of multiplicative type) there exists among the diverse possible prolongations of G to R one, denoted by $\mathcal{G}^+$ (respectively $\mathcal{G}^-$), which is maximal (respectively minimal). It is a technical formality to verify that any automorphism of G prolongs to $\mathcal{G}^+$ and $\mathcal{G}^-$. In particular, the structure of G as $\mathbb{F}$-vector space scheme extends to $\mathcal{G}^+$ and $\mathcal{G}^-$. So we have the following proposition:

Proposition 5.1.6. *Suppose that R is of inequal characteristic, and let $\mathcal{G}$ be a finite flat R-group scheme, whose generic fiber is an $\mathbb{F}$-vector space scheme. Then the $\mathbb{F}$-vector space structur extends to the maximal and minimal prolongation of G.*

In the following we suppose that R is of inequal characteristic and that $\mathbb{F}$ is a finite field with $\mathrm{char}(\mathbb{F})^r$ elements. The following proposition is part 2° and 3° of [32, Proposition 3.3.2]:

Proposition 5.1.7. *Let G be an $\mathbb{F}$-vector space scheme over K of rank q which admits a finite flat prolongation $\mathcal{G}$ over R.*

1. *If $e = \nu(p) < \mathrm{char}(\mathbb{F}) - 1$, where e is the absolute ramification index of K, then $\mathcal{G}$ is up to isomorphism the unique prolongation of G on R and this is an $\mathbb{F}$-vector space scheme.*
2. *If $e = \mathrm{char}(\mathbb{F}) - 1$, and if G is simple and R henselian, then either $\mathcal{G}$ is the unique prolongation of G or there are two prolongations of G, one étale and one of multiplicative type. In all cases the prolongations are $\mathbb{F}$-vector space schemes.*

Corollary 5.1.8. *Suppose $e < \mathrm{char}(\mathbb{F}) - 1$ and let $\mathcal{G}$ and $\mathcal{H}$ be commutative finite flat R-group schemes, which are annihilated by a power of $\mathrm{char}(\mathbb{F})$. Denote by G and H their generic fibers respectively.*

1. *Every morphism $G \to H$ prolongs uniquely to an R-morphism $\mathcal{G} \to \mathcal{H}$. Furthermore, its kernel and cokernel are flat over R.*
2. *The natural map $Ext_{R-gr}(\mathcal{G}, \mathcal{H}) \to Ext_{K-gr}(G, H)$ is injective.*

Remark 5.1.9. The condition $e < p - 1$ is called a *limited-ramification situation.*

5.1.3 An Existence Theorem

Let N be a positive integer and $\mathbf{T}_N$ the ring of HECKE operators with their action on the space $\mathcal{S}_2(N)$ of cusp forms of weight 2 and level N. Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}_N$ and denote by k the residue field $\mathbf{T}_N\,/\,\mathfrak{m}$. We intend to prove the existence of certain GALOIS representations. A much more general result has been stated by DELIGNE and SERRE in [5, Théorème 6.7].

Definition 5.1.10. We say that f is a modular form of type (k,ε) over $\Gamma_0(N)$ for a positive integer k and a DIRICHLET character $\varepsilon : (\mathbb{Z}\,/N\,\mathbb{Z})^* \to \mathbb{C}^*$ if it is a modular form of weight k with respect to $\Gamma_1(N)$ with the additional property that $f|_k\gamma = \varepsilon(d)f$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

Let $K \subset \mathbb{C}$ be an algebraic number field, λ a finite place of K, $\mathcal{O}_\lambda$ the corresponding valuation ring, $\mathfrak{m}_\lambda$ its maximal ideal, $k_\lambda = \mathcal{O}_\lambda\,/\,\mathfrak{m}_\lambda$ its residue field with characteristic ℓ. By misuse of notation, we write $\bmod\,\lambda$ instead of $\bmod\,\mathfrak{m}_\lambda$.

Definition 5.1.11. Let f be a modular form of type (k,ε) over $\Gamma_0(N)$. The form f is said to be *integral* at λ if the coefficients of its q-expansion $f_\infty(q)$ at ∞ belong to $\mathcal{O}_\lambda$. Further, we write $f \equiv 0(\bmod\,\lambda)$ if the coefficients of $f_\infty(q)$ lie in $\mathfrak{m}_\lambda$.

Suppose that f is integral for λ; then f is an eigenvector of $\mathrm{T}_p \bmod \lambda$ of eigenvalue $a_p \in k_\lambda$ if

$$f|T_p - a_p f \equiv 0(\bmod\,\lambda).$$

Theorem 5.1.12. *Let f be a modular form of type (k,ε) over $\Gamma_0(N)$, $k \geq 1$, with coefficients in K. Suppose that f is integral at λ, that $f \not\equiv 0(\bmod\,\lambda)$ and that f is an eigenvector for $\mathrm{T}_r \bmod_\lambda$, for $r \nmid N\ell$, of eigenvalue $a_r \in k_\lambda$. Denote by k_f the subfield of k_λ generated by the a_r and the $(\bmod\,\lambda)$-reductions of the $\varepsilon(r)$. Then there is a semi-simple* GALOIS *representation*

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q}) \to \mathbf{GL}_2(k_f), \tag{5.1}$$

which is unramified outside $N\ell$ and for these primes, i.e.primes r with $r \nmid N\ell$, it satisfies the relations

$$\mathrm{tr}\,(\rho(\mathsf{Frob}_r)) = a_r \qquad \textit{and} \qquad \det(\rho(\mathsf{Frob}_r)) = \varepsilon(r)r^{k-1}(\bmod\,\lambda).$$

PROOF: A nice and traceable proof can be found in [5, Théorème 6.7]. □

Our actual result is a variant of this theorem as we are to see.

Corollary 5.1.13. *There is a unique semi-simple representation*

$$\rho_\mathfrak{m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q}) \to \mathbf{GL}_2(k),$$

satisfying

$$\mathrm{tr}\,(\rho_\mathfrak{m}(\mathsf{Frob}_r)) = \mathrm{T}_r(\bmod\,\mathfrak{m}) \qquad \textit{and} \qquad \det(\rho_\mathfrak{m}(\mathsf{Frob}_r)) = r(\bmod\,\mathfrak{m}),$$

outside $\mathfrak{m}\,N$. The representation is unramified at all primes coprime to $\mathfrak{m}\,N$.

PROOF: Let $\mathcal{L}$ be the space of cusp forms of weight 2 and level N whose q-expansions at the standard cusp ∞ have integral coefficients such that we may consider the q-expansion map

$$\mathcal{L} \to \mathbb{Z}[[q]]\,, \qquad f \mapsto f_\infty. \tag{5.2}$$

Hence $\mathcal{L}$ is a free $\mathbb{Z}$-module. On the one hand, it follows from [5, Proposition 2.7.1] that the rank of $\mathcal{L}$ over $\mathbb{Z}$ coincides with the dimension of $\mathcal{S}_2(N)$ over $\mathbb{C}$. On the other hand, SHIMURA has proven in [44, Theorem 3.45] (see [33, p.444]) that the rank of $\mathbf{T}_N$ as $\mathbb{Z}$-module coincides with the dimension of the abelian variety $J_0(N)$, i.e. with the dimension of $\mathcal{S}_2(N)$. Hence,

$$\mathrm{rank}_{\mathbb{Z}}(\mathcal{L}) = \mathrm{rank}_{\mathbb{Z}}(\mathbf{T}_N) =: d.$$

The q-expansion map (5.2) induces an analogous map

$$\mathcal{L} \otimes_{\mathbb{Z}} k \to k[[q]], \tag{5.3}$$

which is injective since the cokernel of (5.2) is torsion free. Indeed, suppose there is $n \in \mathbb{N}$ and $\sum b_i q^i \in \mathbb{Z}[[q]]$ such that $n \cdot \overline{\sum b_i q^i} = 0$ in $\mathrm{Coker}(\mathcal{L} \to \mathbb{Z}[[q]]) = \mathbb{Z}[[q]]/\mathcal{L}$, or equivalently $n \sum b_i q^i \in \mathcal{L}$. Since all $b_i \in \mathbb{Z}$, this is equivalent to $\sum b_i q^i \in \mathcal{L}$. It follows that the cokernel of (5.2) is actually torsion free. By the fundamental theorem on homomorphisms the map (5.2) and the induced map (5.3) have both trivial kernel.

Now consider the bilinear pairing

$$(LM \otimes_{\mathbb{Z}} k) \times (\mathbf{T}_N \otimes_{\mathbb{Z}} k) \to k \ , \qquad (f, \mathrm{T}) \mapsto \mathrm{q}(f|\,\mathrm{T}),$$

which takes (f, T) to the coefficient $\mathrm{q}(f|\,\mathrm{T})$ of q in the q-expansion of $f|\,\mathrm{T}$. The sets $\mathcal{L} \otimes_{\mathbb{Z}} k$ and $\mathbf{T}_N \otimes_{\mathbb{Z}} k$ are k-vector spaces of dimension d and so is $\mathrm{Hom}_{\mathbb{Z}}(\mathbf{T}_N, k)$ by Hom-functoriality. Therefore, the pairing may be viewed as a homomorphism

$$\mathcal{L} \otimes_{\mathbb{Z}} k \to \mathrm{Hom}_{\mathbb{Z}}(\mathbf{T}_N, k) \ , \qquad f \mapsto \mathrm{q}(f|\cdot)$$

between k-vector spaces of dimension d. To show that this is an isomorphism it suffices to show injectivity. Let hereto f with $f_\infty = \sum a_n q^n$ be in the kernel. This means that $\mathrm{q}(f|\cdot)$ is the zero-map, or equivalently that the coefficient of q in the q-expansion of $f|\,\mathrm{T}$ is 0 for all $\mathrm{T} \in \mathbf{T}_N$. Since $\mathbf{T}_N$ is generated by the HECKE operators T_n, it suffices to claim $\mathrm{q}(f|\,\mathrm{T}_n) = 0$ for all n. But by (1.27) the coefficient of q in $f|\,\mathrm{T}_n$ is the n^{th} coefficient of the q-expansion of f. So $f_\infty = 0$ and the injectivity of the q-expansion map shows that $f = 0$.

Considering now the canonical projection map

$$\mathbf{T}_N \to \mathbf{T}_N \,/\, \mathfrak{m} = k \ , \qquad \mathrm{T} \mapsto \mathrm{T}(\mathrm{mod}\, \mathfrak{m})$$

in $\mathrm{Hom}_{\mathbb{Z}}(\mathbf{T}_N, k)$, we find an element $f \in \mathcal{L} \otimes_{\mathbb{Z}} k$ whose q-expansion $f_\infty = \sum t_n q^n$ has the coefficients

$$t_n = \mathrm{T}_n(\mathrm{mod}\, \mathfrak{m}).$$

It is easy to see that f is an eigenform for the HECKE operators T_n with eigenvalues t_n. According to (1.27) $(f|\,\mathrm{T}_p)_\infty$ for a prime p is given by

$$(f|\,\mathrm{T}_p)_\infty = \begin{cases} \sum_{n=0}^{\infty} \mathrm{T}_{pn}(\mathrm{mod}\, \mathfrak{m}) q^n + p \sum_{n=0}^{\infty} \mathrm{T}_n(\mathrm{mod}\, \mathfrak{m}) q^{pn} & \text{if } p \text{ is prime to } N; \\ \sum_{n=0}^{\infty} \mathrm{T}_{pn}(\mathrm{mod}\, \mathfrak{m}) q^n & \text{if } p \text{ divides } N. \end{cases}$$

In the latter case, it follows from Theorem 1.4.22 that

$$\begin{aligned} (f|\,\mathrm{T}_p)_\infty &= \sum_{n=0}^{\infty} \mathrm{T}_{pn}(\mathrm{mod}\, \mathfrak{m}) q^n \\ &= \mathrm{T}_p(\mathrm{mod}\, \mathfrak{m}) \sum_{n=0}^{\infty} \mathrm{T}_n(\mathrm{mod}\, \mathfrak{m}) q^n \\ &= t_p f_\infty. \end{aligned}$$

In the former case, we rearrange the sum as follows to apply Theorem 1.4.22:

$$\begin{aligned}
(f|\,\mathrm{T}_p)_\infty &= \sum_{n=0}^{\infty} \mathrm{T}_{pn}(\operatorname{mod}\mathfrak{m})q^n + p\sum_{n=0}^{\infty}\mathrm{T}_n(\operatorname{mod}\mathfrak{m})q^{pn} \\
&= \sum_{p\nmid k}\mathrm{T}_{pk}(\operatorname{mod}\mathfrak{m})q^k + \sum_{p|k}\mathrm{T}_{pk}(\operatorname{mod}\mathfrak{m})q^k + p\sum_{n=0}^{\infty}\mathrm{T}_n(\operatorname{mod}\mathfrak{m})q^{pn} \\
&= \sum_{p\nmid k}\mathrm{T}_{pk}(\operatorname{mod}\mathfrak{m})q^k + \sum_{n=0}^{\infty}\mathrm{T}_{p^2n}(\operatorname{mod}\mathfrak{m})q^{pn} + p\sum_{n=0}^{\infty}\mathrm{T}_n(\operatorname{mod}\mathfrak{m})q^{pn} \\
&= \mathrm{T}_p(\operatorname{mod}\mathfrak{m})\sum_{p\nmid k}\mathrm{T}_k(\operatorname{mod}\mathfrak{m})q^k + \sum_{n=0}^{\infty}(\mathrm{T}_{p^2n} + p\,\mathrm{T}_n)(\operatorname{mod}\mathfrak{m})q^{pn} \\
&= \mathrm{T}_p(\operatorname{mod}\mathfrak{m})\sum_{p\nmid k}\mathrm{T}_k(\operatorname{mod}\mathfrak{m})q^k + \sum_{n=0}^{\infty}(\mathrm{T}_p\,\mathrm{T}_n)(\operatorname{mod}\mathfrak{m})q^{pn} \\
&= \mathrm{T}_p(\operatorname{mod}\mathfrak{m})(\sum_{p\nmid k}\mathrm{T}_k(\operatorname{mod}\mathfrak{m})q^k + \sum_{p|k}\mathrm{T}_k(\operatorname{mod}\mathfrak{m})q^k) \\
&= t_p f_\infty.
\end{aligned}$$

Now we tend to apply Theorem 5.1.12. For this we have to verify that f is a cusp form mod ℓ, where ℓ is the characteristic of k, in the sense that $f_\infty = \sum t_n q^n$ is the $(\operatorname{mod}\lambda)$-reduction of the q-expansion of a cusp form whose coefficients lie in a number field $K \subset \mathbb{C}$ and which are integral at a prime $\lambda \mid \ell$ of K. We may choose a number field K and a prime λ over ℓ such that the residue field $\mathcal{O}_{K,\lambda}\,/\,\mathfrak{m}_\lambda = k_\lambda$ – where $\mathcal{O}_{K,\lambda}$ is the valuation ring of K at λ and $\mathfrak{m}_\lambda$ the corresponding maximal ideal – contains a subfield isomorphic to k. Fix an embedding $k \hookrightarrow k_\lambda$ in order to view f inside $\mathcal{L}\otimes_{\mathbb{Z}} k_\lambda$. By choosing adequate representatives of the q-expansion coefficients, we lift f to an element $\tilde{f}$ of $\mathcal{L}\otimes_{\mathbb{Z}}\mathcal{O}_{K,\lambda}$. The image of $\tilde{f}$ in $\mathcal{S}_2(N)$ is then a cusp form with coefficients in $\mathcal{O}_{K,\lambda}$ whose q-expansion $(\operatorname{mod}\lambda)$ coincides with that of f,

$$\tilde{f}_\infty(\operatorname{mod}\lambda) = \sum \tilde{t}_n(\operatorname{mod}\lambda)q^n \equiv \sum t_n(\operatorname{mod}\lambda)q^n = f_\infty(\operatorname{mod}\lambda).$$

Now $\tilde{f}$ is a cusp form of type $(k = 2, \varepsilon = \mathrm{triv})$ which is integral at λ but non-zero $(\operatorname{mod}\lambda)$ and which is an eigenform for $\mathrm{T}_r(\operatorname{mod}\lambda)$ for $r \nmid N\ell$ (actually for all n) with eigenvalue

$$a_r = \tilde{t}_r(\operatorname{mod}\lambda) \equiv \mathrm{T}_r(\operatorname{mod}\lambda) \equiv \mathrm{T}_r(\operatorname{mod}\mathfrak{m}).$$

The existence part of the corollary follows now easily with Theorem 5.1.12.

A consequence of the ČEBOTAREV Density Theorem is that all elements of the image of $\rho_\mathfrak{m}$ are conjugate to the FROBENIUS elements $\rho_\mathfrak{m}(\mathsf{Frob}_r)$. Thus the trace and the determinant of $\rho_\mathfrak{m}$ are completely determined by the given data. Furthermore, a two-dimensional semi-simple representation is determined by its trace and determinant up to isomorphism. This shows uniqueness. □

We say that $\rho_\mathfrak{m}$ is the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q})$ attached to $\mathfrak{m}$. By definition, the cyclotomic character (see for example [40, I.1.2])

$$\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q}) \to k$$

sends the FROBENIUS elements Frob_r to $r(\operatorname{mod}\mathfrak{m})$. Again the ČEBOTAREV Density Theorem tells us that the condition on $\det(\rho_\mathfrak{m})$ in the corollary implies that the determinant of $\rho_\mathfrak{m}$ is the mod ℓ cyclotomic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q})$. Since χ_ℓ acts in particular on the set μ_ℓ of ℓ^{th} roots of unity, this shows that $\rho_\mathfrak{m}$ is self-CARTIER-dual, that is autodual with respect to the functor $\mathrm{Hom}(\cdot, \mu_\ell)$.

Example 5.1.14. Let E be a modular elliptic curve of conductor N and let $f \in \mathcal{S}_2(N)$ be a cusp form that is an eigenform for T_p with eigenvalue $a_p = \big(p+1-\#E_{\mathbb{F}_p}(\mathbb{F}_p)\big) \in \mathbb{Z}$ for all primes p prime to N. The action of $\mathbf{T}_N$ on f is given by the homomorphism $\varphi : \mathbf{T}_N \to \mathbb{C}$ which takes $\mathrm{T} \in \mathbf{T}_N$ to the eigenvalue of f under T. This homomorphism is in fact $\mathbb{Z}$-valued. Let ℓ be a prime number and consider the maximal ideal $\mathfrak{m} = \varphi^{-1}((\ell))$. Then the attached representation $\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\mathbb{F}_\ell)$ is the semisimplification ρ^{ss} of a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[\ell])$. This semisimplification is defined to be the direct sum of the JORDAN-HÖLDER factors of ρ, i.e. it is the direct sum of two one-dimensional representations if ρ is not semi-simple while ρ and ρ^{ss} coincides if ρ is already semi-simple. In the latter case $\rho_m \cong \rho$.

Definition 5.1.15. Suppose that

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\mathbb{F})$$

is a continuous homomorphism, where $\mathbb{F}$ is a finite field of characteristic ℓ. We say that ρ is a *modular representation of level* N, if the determinant of ρ is the $\bmod\,\ell$ cyclotomic character and if there is a homomorphism

$$\omega : \mathbf{T}_N \to \overline{\mathbb{F}}$$

such that

$$\mathrm{tr}\,(\rho(\mathsf{Frob}_r)) = \omega(\mathrm{T}_r)$$

for almost all primes r.

This is equivalent to Definition 1.5.6 in Section 1.5. Indeed, given ρ as in the definition, set $\mathfrak{m} = \mathrm{Ker}(\omega)$ to obtain an embedding $\omega : \mathbf{T}_N / \mathfrak{m} \hookrightarrow \overline{\mathbb{F}}$. Then the semisimplifications of ρ and $\rho_{\mathfrak{m}}$ are defined over subfields of $\overline{\mathbb{F}}$ and they are even isomorphic over $\overline{\mathbb{F}}$ since their determinant and trace (with respect to the embedding ω) coincide:

$$\Big(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho} \mathbf{GL}_2(\mathbb{F}) \hookrightarrow \mathbf{GL}_2(\overline{\mathbb{F}})\Big) \cong \Big(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{\mathfrak{m}}} \mathbf{GL}_2(k) \xrightarrow{\omega} \mathbf{GL}_2(\overline{\mathbb{F}})\Big).$$

For the other direction, it suffices to show the existence of a homomorphism ω with the desired property, as we already know that the determinant and the traces of ρ and $\rho_{\mathfrak{m}}$ coincide with respect to the embeddings $\iota : k \hookrightarrow \overline{\mathbb{F}}$ and $\mathbb{F} \hookrightarrow \overline{\mathbb{F}}$. Set $\omega = \iota \circ \mathsf{proj} : \mathbf{T}_N \to \mathbf{T}_N / \mathfrak{m} = k \to \overline{\mathbb{F}}$. Then

$$\mathrm{tr}_{\overline{\mathbb{F}}}(\rho(\mathsf{Frob}_r)) = \mathrm{tr}_{\overline{\mathbb{F}}}(\rho_{\mathfrak{m}}(\mathsf{Frob}_r)) = \iota(\mathrm{T}_r(\bmod\,\mathfrak{m})) = \omega(\mathrm{T}_r).$$

5.1.4 The Kernel of $\mathfrak{m}$ on $J_0(N)$

We consider along with $\rho_{\mathfrak{m}}$ the group W of elements of $J_0(N)(\overline{\mathbb{Q}})$ which are annihilated by all elements of $\mathfrak{m}$,

$$W := J_0(N)[\mathfrak{m}] = \bigcap_{\alpha \in \mathfrak{m}} J_0(N)[\alpha].$$

This group is a subgroup of the finite group $J_0(N)[\ell]$ of ℓ-division points of $J_0(N)$, where ℓ is the residue characteristic of $k = \mathbf{T}_N / \mathfrak{m}$, and carries a natural commuting action of k and of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus W is a $k\,\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module and a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-submodule of $J_0(N)[\ell]$.

Theorem 5.1.16. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}_N$ such that $\rho_{\mathfrak{m}}$ is irreducible.*

1. *The $k\,\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module W is non-zero. Its semisimplification is isomorphic to a product $V \times \cdots \times V$, where V is the unique $k\,\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module – up to isomorphism – which makes up the representation $\rho_{\mathfrak{m}}$.*

2. *Assume that ℓ is prime to $2N$. Then we have $W \cong V$. That is, the product given in (1.) has only one factor.*

3. *Let S be a finite set of primes. Let $\mathfrak{J} \subset \mathbf{T}_N$ be the ideal generated by the elements $\eta_r = 1 + r - \mathrm{T}_r$, with r prime and not in S. Then the ideals $\mathfrak{m}$ and $\mathfrak{J}$ are relatively prime.*

PROOF: To prove (1.) we first note the action of $\mathbf{T}_N$ on $J_0(N)$ is faithful because $\mathbf{T}_N$ is a subalgebra of $\mathrm{End}\,(J_0(N))$. Hence W is non-zero. Form the direct sum

$$D := W \oplus \mathrm{Hom}(W, \mu_\ell)$$

of W and its CARTIER dual. Let n be the dimension of W over k. We get JORDAN-HÖLDER blocks of height 2, and the characteristic polynomial of $\rho_{\mathfrak{m}}(\mathsf{Frob}_r)$ for primes $r \nmid N\ell$ is then

$$x^2 - \mathrm{tr}(\rho_{\mathfrak{m}}(\mathsf{Frob}_r))x + \det(\rho_{\mathfrak{m}}(\mathsf{Frob}_r)) = x^2 - \mathrm{T}_r(\mathrm{mod}\,\mathfrak{m}) + r(\mathrm{mod}\,\mathfrak{m}).$$

Actually, the quadratic factors of this polynomial coincide with the characteristic polynomial of Frob_r in V. Since we deal with two-dimensional semi-simple (even irreducible) representations which are determined by their trace and determinant, they are, according to the ČEBOTAREV Density Theorem, determined by the trace and determinant of the FROBENIUS elements. By the BRAUER-NESBITT Theorem, two representations have the same composition factors if and only if they have the same characteristic roots. This shows that the semisimplification of W is just V^n. Since V is non-zero, this gives (1.).

To prove (2.), we choose a minimal (non-zero) $k\,\mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q})$-submodule of W. In (1.) we have shown that this submodule must be isomorphic to V. That means there is an inclusion $V \subset W$ and we must proof equality. Considering $X_0(N)$ over $\mathbb{F}_\ell$ we take advantage of the fact that N and ℓ are relatively prime. Recall that $\mathrm{H}^0(X_0(N)/\,\mathbb{F}_q, \Omega^1) \cong \mathcal{S}_2(N)$ over $\mathbb{F}_q$ (cf. (1.25)). Hence we have the injective q-expansion map

$$\mathrm{H}^0(X_0(N)/\,\mathbb{F}_q, \Omega^1) \to \mathbb{F}_\ell[[q]].$$

Arguments that MAZUR gave in [23, Chapter II, §9], in particular Proposition 9.3, show that $\mathrm{H}^0(X_0(N)/\,\mathbb{F}_q, \Omega^1)[\mathfrak{m}]$ is of k-dimension ≤ 1.

Since $J_0(N)$ is the PICARD variety of $X_0(N)$, we compute by functoriality over $\mathbb{F}_\ell$ that

$$\mathrm{H}^1(J_0(N), \mathcal{O}_{J_0(N)})/\,\mathfrak{m}\,\mathrm{H}^1(J_0(N), \mathcal{O}_{J_o(N)})$$

is also of k-dimension ≤ 1 according to [28, p.40].

Let $\mathcal{N}(J_0(N))$ be the NÉRON model of $J_0(N)$ over $\mathbb{Q}_\ell$, such that $\mathcal{N}(J_0(N))$ is an abelian scheme over $\mathbb{Z}_\ell$. Consider the modules V and W (which actually lie in $J_0(N)$) as subsets of this NÉRON model and denote by $\mathcal{V}$ and $\mathcal{W}$ the ZARISKI closures of V and W in $\mathcal{N}(J_0(N))$ respectively. Since V and W are by definition in the kernel of the multiplication by ℓ on $J_0(N)$, $\mathcal{V}$ and $\mathcal{W}$ are in the kernel $\mathcal{N}(J_0(N))[\ell]$ of the multiplication-by-ℓ map on $\mathcal{N}(J_0(N))$. Taking into account that $\mathcal{N}(J_0(N))$ is an abelian variety, $\mathcal{N}(J_0(N))[\ell]$ is finite and flat over $\mathbb{Z}_\ell$ – in fact, according to [28, p.39] it has the structure $\mathcal{N}(J_0(N))[\ell] \cong (\mathbb{Z}/\ell\,\mathbb{Z})^i$ where i can take any value in the range $0 \leq i \leq \dim\,(\mathcal{N}(J_0(N)))$. Hence $\mathcal{V}$ and $\mathcal{W}$ are, as closed subsets, finite and flat as well.

Remember that the ideal in $\mathbb{Z}_\ell$ lying over $\ell\,\mathbb{Z}$ is $\ell\,\mathbb{Z}_\ell$ and so the absolute ramification index e of $\mathbb{Q}_\ell$ (over $\mathbb{Q}$) is 1 according to [38, p.25]. Thus, ℓ being prim to $2N$, in particular $\ell > 2$, induces that $\ell - 1 > 1 = e$. Therefore we can apply Proposition 5.1.7(1.) and conclude that $\mathcal{V}$ and $\mathcal{W}$ are again k-vector space schemes. But we have more: By Corollary 5.1.8(1.) the injection $V \hookrightarrow W$ prolongs to a morphism over $\mathbb{Z}_\ell$ such that $\mathcal{V}$ is a subgroup of $\mathcal{W}$ and that its cokernel $\mathcal{W}/\,\mathcal{V}$ is finite and flat.

Therefore the following conditions are equivalent:

1. $V = W$,

2. $\mathcal{V} = \mathcal{W}$,

3. $\mathcal{V}_{\mathrm{s}} = \mathcal{W}_{\mathrm{s}}$,

where $\mathcal{V}_{\mathrm{s}}$ and $\mathcal{W}_{\mathrm{s}}$ are the special fibers of $\mathcal{V}$ and $\mathcal{W}$ respectively. All of them are k-vector space schemes over $\mathbb{Q}_\ell$, $\mathbb{Z}_\ell$ and $\mathbb{F}_\ell$ respectively. In particular, the second assertion of the proposition means that the inclusion $\mathcal{V}_{\mathrm{s}} \subset \mathcal{W}_{\mathrm{s}}$ is an equality, or equivalently that the quotient $\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}$ is trivial.

Since $\mathcal{V}$, $\mathcal{W}$ and $\mathcal{W} / \mathcal{V}$ are finite and flat, $\mathcal{V}_{\mathrm{s}}$, $\mathcal{W}_{\mathrm{s}}$ and $\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}$ inherit particular properties of V, W and W/V. So $\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}$ is certainly a successive extension of copies of $\mathcal{V}_{\mathrm{s}}$ and $\mathcal{V}_{\mathrm{s}}$ is auto CARTIER-dual.

Here we make use of the contravariant DIEUDONNÉ module functor $\mathcal{D}$ as MAZUR does in [23, pp.116-117] whose results we will mostly cite without proof. Recall also Remark 3.1.13. We will apply $\mathcal{D}$ to finite flat group schemes of type $(\ell, \ldots, \ell)$ over $\mathbb{F}_\ell$ and obtain finite-dimensional $\mathbb{F}_\ell$-vector space schemes equipped with a FROBENIUS map Frob_ℓ and a Verschiebung Ver_ℓ. These maps are commuting $\mathbb{F}_\ell$-vector space homomorphisms and their composites $\mathsf{Frob}_\ell \circ \mathsf{Ver}_\ell = \mathsf{Ver}_\ell \circ \mathsf{Frob}_\ell = [\ell]$ are 0 over $\mathbb{F}_\ell$.

As mentioned in [23, p.116], we have a canonical isomorphism

$$\mathcal{D}(J_0(N)_\ell[\ell]) \cong \mathrm{H}^1_{\mathrm{deRham}}(J_0(N)_\ell / \mathbb{F}_\ell),$$

where $J_0(N)_\ell$ denotes the reduction of $J_0(N)$ modulo ℓ. Moreover, the quotient $\mathcal{D}(J_0(N)_\ell[\mathsf{Ver}])$ of $\mathcal{D}(J_0(N)_\ell[\ell])$ corresponds to the quotient $\mathrm{H}^1\left(J_0(N)_\ell, \mathcal{O}\right)$ of $\mathrm{H}^1_{\mathrm{deRahm}}\left(J_0(N)_\ell / \mathbb{F}_\ell\right)$. Since $W = J_0(N)[\mathfrak{m}]$, we obtain by functoriality

$$\mathcal{D}(\mathcal{W}_{\mathrm{s}}[\mathsf{Ver}_\ell]) = \mathrm{H}^1\left(J_0(N)_\ell, \mathcal{O}\right) / \, \mathfrak{m}\, \mathrm{H}^1\left(J_0(N)_\ell, \mathcal{O}\right),$$

which is of dimension ≤ 1 over k as we have seen above. Furthermore, the CARTIER auto-duality of $\mathcal{V}_{\mathrm{s}}$ induces an auto-duality of $\mathcal{D}(\mathcal{V}_{\mathrm{s}})$ which interchanges the two maps Frob_ℓ and Ver_ℓ. This fact implies that the ranks of these maps as endomorphisms of the 2-dimensional k-vector space $\mathcal{D}(\mathcal{V}_{\mathrm{s}})$ coincide. Since their composition vanishes, this rank is either 0 or 1.

Now $\mathrm{Coker}(\mathsf{Ver}_\ell) = \mathcal{D}(\mathcal{V}_{\mathrm{s}}) / \mathsf{Ver}_\ell\left(\mathcal{D}(\mathcal{V}_{\mathrm{s}})\right) = \mathcal{D}(\mathcal{V}_{\mathrm{s}}[\mathsf{Ver}_\ell])$ – a similar fact was already used above. For the k-dimension of $\mathcal{D}(\mathcal{V}_{\mathrm{s}})$ is 2 and that of $\mathsf{Frob}_\ell\, \mathcal{D}(\mathcal{V}_{\mathrm{s}})$ is the rank of Ver_ℓ, namely 0 or 1, we know that $\mathcal{D}(\mathcal{V}_{\mathrm{s}}[\mathsf{Ver}_\ell])$ has k-dimension 1 or 2. However, being a quotient of $\mathcal{D}(\mathcal{W}_{\mathrm{s}}[\mathsf{Ver}_\ell])$, $\mathcal{D}(\mathcal{V}_{\mathrm{s}}[\mathsf{Ver}_\ell])$ has at most rank 1. So we conclude that both of them have rank 1 and that the groups $\mathcal{V}_{\mathrm{s}}[\mathsf{Ver}_\ell]$ and $\mathcal{W}_{\mathrm{s}}[\mathsf{Ver}_\ell]$ are equal and in particular non-trivial.

We claim that $\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}[\mathsf{Ver}_\ell]$ is 0, i.e. that Frob_ℓ is an automorphism of $\mathcal{D}(\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}})$, because the fact that $\mathcal{D}(\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}[\mathsf{Ver}_\ell]) = \mathcal{D}(\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}) / \mathsf{Ver}_\ell\, \mathcal{D}(\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}) = 0$ is equivalent to the fact that $\mathsf{Ver}_\ell\, \mathcal{D}(\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}) = \mathcal{D}(\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}})$. Recalling that $\mathcal{D}$ is a contravariant functor, we have a short exact sequence

$$0 \to \mathcal{D}(\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}) \to \mathcal{D}(\mathcal{W}_{\mathrm{s}}) \to \mathcal{D}(\mathcal{V}_{\mathrm{s}}) \to 0,$$

to which we apply [23, Lemma (14.6)] what is possible since the cokernel $\mathcal{D}(\mathcal{W}_{\mathrm{s}}[\mathsf{Ver}_\ell])$ of Ver_ℓ on $\mathcal{D}(\mathcal{W}_{\mathrm{s}})$ is of dimension 1 over k and Frob_ℓ is non-trivial on $\mathcal{D}(\mathcal{V}_{\mathrm{s}})$ (in fact it is of degree 1 just as Ver_ℓ). By the lemma, Ver_ℓ is an isomorphism of $\mathcal{D}(\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}})$ as we claimed.

We are now able to conclude that $\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}$ is trivial. Indeed, suppose the contrary, $\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}} \neq 0$. In this case, we could find an inclusion $\mathcal{V}_{\mathrm{s}} \subset \mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}$ since $\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}$ is a successive extension of copies of $\mathcal{V}_{\mathrm{s}}$, as remarked above. This is a contradiction to the fact that $\mathcal{W}_{\mathrm{s}} / \mathcal{V}_{\mathrm{s}}[\mathsf{Ver}_\ell]$ is 0, whereas $\mathcal{V}_{\mathrm{s}}[\mathsf{Ver}_\ell]$ is not.

This finally shows that $V = W$.

To prove (3.) assume the contrary, i.e. $\mathfrak{m}$ and $\mathfrak{J}$ are not relatively prime and since $\mathfrak{m}$ is maximal, this means that $\mathfrak{J} \subseteq \mathfrak{m}$. Thus the generators $\{1 + r - \mathrm{T}_r \mid r \notin S\}$ of $\mathfrak{J}$ satisfy the relation

$$1 + r - \mathrm{T}_r \equiv 0 (\operatorname{mod} \mathfrak{m})$$

hence

$$\mathrm{T}_r \equiv 1 + r (\operatorname{mod} \mathfrak{m})$$

for almost all primes r. So $\mathrm{tr}(\rho_{\mathfrak{m}}(\mathsf{Frob}_r)) = \mathrm{T}_r (\mathrm{mod}\, \mathfrak{m}) \equiv 1 + r(\mathrm{mod}\, \mathfrak{m})$ and the characteristic polynomial of Frob_r is given by

$$x^2 - (1+r)(\mathrm{mod}\, \mathfrak{m})x + r(\mathrm{mod}\, \mathfrak{m}) = (x-1)(x-r)(\mathrm{mod}\, \mathfrak{m}).$$

As a consequence of the ČEBOTAREV Density Theorem, the characteristic polynomial of ρ_m is given by

$$(x-1)(x-\chi_\ell),$$

which is the characteristic polynomial of the direct sum of the one-dimensional trivial representation and the one-dimensional cyclotomic representation. With the BRAUER-NESBITT theorem we conclude that $\rho_{\mathfrak{m}}$ has the same simplification as this direct sum. This contradicts the hypothesis that $\rho_{\mathfrak{m}}$ is irreducible. □

The following complement to Theorem 5.1.16(2.) is the main result of [25].

Theorem 5.1.17. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}_N$ for which $\rho_{\mathfrak{m}}$ is absolutely irreducible. Suppose that the residue characteristic ℓ of $\mathfrak{m}$ is an odd prime which divides N exactly. Assume further that the representation $\rho_{\mathfrak{m}}$ is not modular of level $\frac{N}{\ell}$. Then the group $J_0(N)[\mathfrak{m}]$ is of dimension 2 over $k = \mathbf{T}_N \,/\, \mathfrak{m}$.*

In the notations of Theorem 5.1.16, we have $W \cong V$ in this case.

5.2 A Theorem due to Mazur

Now we are in the position to give arguments leading to the Main Theorem, beginning with a result of Mazur which corresponds to the Main Theorem in the case $p \not\equiv 1 (\mathrm{mod}\, \ell)$.

Fix a positive integer M and a prime p not dividing M and let $N = pM$. Consider as usual the Hecke ring $\mathbf{T}_N$ of level N. Farther, let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}_N$ and $k = \mathbf{T}_N / \mathfrak{m}$ its residue field. Let V be the $k\,\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module given by the attached representation $\rho_\mathfrak{m}$ discussed in the previous section. In this section we impose the following hypotheses on $\rho_\mathfrak{m}$:

1. The representation $\rho_\mathfrak{m}$ is irreducible.
2. The residue characteristic ℓ of $\mathfrak{m}$ is odd.
3. The representation $\rho_\mathfrak{m}$ is finite at p.

We have already mentioned finiteness of representations in Remark 1.3.9. The restriction of the representation $\rho_\mathfrak{m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(k)$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ defines an étale k-vector space scheme over $\mathbb{Q}_p$. One can ask if it can be extended to a finite flat k-vector space scheme over $\mathbb{Z}_p$; if this is the case, we say that $\rho_\mathfrak{m}$ is finite (cf. [39, p.189]). For $p \neq \ell$ this means simply that $\rho_\mathfrak{m}$ is unramified at p.

According to Theorem 5.1.16(1.) we can choose an inclusion of $k\,\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules $V \subseteq W$, where $W = J_0(N)[\mathfrak{m}]$. Fix such an inclusion to view it as a map $\iota : V \to J_0(N)$. Since we assumed $\rho_\mathfrak{m}$ to be finite, V extends to a finite flat k-vector space scheme $\mathcal{V}$ over $\mathbb{Z}_p$.

Lemma 5.2.1. *The map ι prolongs to a map $\mathcal{V} \to \mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)$ over $\mathbb{Z}_p$, where $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)$ is the Néron model of $J_0(N)_{\mathbb{Q}_p}$.*

Proof: First we treat the case $p \neq \ell$, where we can use the Néron mapping property of Definition 2.1.1. Since $\mathcal{V}$ is a smooth $\mathbb{Z}_p$-scheme, ι extends uniquely to a $\mathbb{Z}_p$-morphism $\mathcal{V} \to \mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)$.

Things become more complicated when $p = \ell$. In this case $p > 2$ by the second hypothesis on $\rho_\mathfrak{m}$. Therefrom, the absolute ramification index e of $\mathbb{Q}_p$ over $\mathbb{Q}$, which is 1 as mentioned in the previous section, satisfies the condition $e < p - 1$ of Corollary 5.1.8(1.). Note farther that $J_0(N)_{\mathbb{Q}_p}$ has semistable reduction as we have shown in Section 3.2 for p divides N exactly that is $p^2 \nmid N$.

In particular, because of the semistable reduction, the multiplication by p map is surjective (a non-zero isogeny). According to [14, Lemme 2.2.1] this is a condition that for all $\nu > 0$ the kernels $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p^\nu]$ are quasi-finite, seperated and flat group schemes over $\mathbb{Z}_p$ and form a projective system of group schemes with faithfully flat morphisms

$$\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p^{\nu'}] \to \mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p^\nu], \qquad x \mapsto p^{\nu'-\nu}x.$$

By reason that $\mathbb{Z}_p$ is henselian, we know, as exposed in [14, 2.2.3], that $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]$ as quasi-finite seperated scheme decomposes canonically into a sum

$$\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p] = \mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]^\mathrm{f} \sqcup \mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]',$$

where $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]^\mathrm{f}$ is finite over $\mathbb{Z}_p$ and the special fiber $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]'_\mathrm{s} = \emptyset$, which means that $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]'$ is reduced to its generic fiber. Hence $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]^\mathrm{f}$ has the same special fiber as $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]$. Since this decomposition is evidently functorial, we conclude that $\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]^\mathrm{f}$ is a finite flat subgroup scheme and that the quotient

$$\mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p] / \mathcal{N}\left(\mathrm{J_0(N)_{\mathbb{Q}_p}}\right)[p]^\mathrm{f}$$

is étale, quasi-finite and has trivial special fiber.

Moreover, the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}(\overline{\mathbb{Q}}_p)$ is unramified which we see applying results of [14, 11.6], if we replace $\mathbb{Q}_p$ by its maximal unramified extension K and $\mathbb{Z}_p$ by the ring of integers of K. Then the GALOIS group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ is the inertia group at p of the according representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, whereas $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is the decomposition group. Analogously to Definition 1.3.4 we have to show that this inertia group acts trivially on $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}(\overline{\mathbb{Q}}_p)$. The group $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}$ becomes a quotient of the group scheme ${}_p\Psi$ appearing in [14, 11.6.6], whose generic fiber can be identified with a quotient M/pM by [14, 11.6.7], where M is a certain constant group scheme. Unfortunately, it would go beyond the scope of this work to exploit the details of these arguments. However, they show that the generic fiber $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}_K$ is constant, which means that the inertia group $\mathrm{Gal}(K/\overline{\mathbb{Q}}_p)$ of the GALOIS group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts trivially on $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}(\overline{\mathbb{Q}}_p)$.

We may express $\mathcal{V}$ in the usual way as an extension

$$0 \to \mathcal{V}^0 \to \mathcal{V} \to \mathcal{V}^{\text{ét}} \to 0$$

of an étale group scheme $\mathcal{V}^{\text{ét}}$ by a connected group scheme $\mathcal{V}^0$ which are both finite flat group schemes over $\mathbb{Z}_p$ and write $\mathcal{V}^{\text{ét}}_\eta$ and $\mathcal{V}^0_\eta$ for the respective generic fibers. Just as for the quotient $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}(\overline{\mathbb{Q}}_p)$ we see that, as a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module, $\mathcal{V}^{\text{ét}}_\eta$ is the largest unramified quotient of V.

Moreover, we have the extension

$$0 \to \mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f} \to \mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p] \to \mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f} \to 0.$$

It follows that the image of $\mathcal{V}^0_\eta$ under ι lands in the generic fiber $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}_\eta$ of $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}$, since $\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}$ is unramified. By Corollary 5.1.8(1.) the induced map of generic fibers

$$\mathcal{V}^0_\eta \to \mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}_\eta$$

prolongs uniquely to a map

$$u : \mathcal{V} \to \mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)[p]^\mathrm{f}.$$

Finally, we obtain the desired prolongation $\mathcal{V} \to \mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)$ of $\iota : V \to J_0(N)$ via [14, Lemme 5.9.2] with $G = \mathcal{V}$, $G' = \mathcal{V}^0$, $G'' = \mathcal{V}^{\text{ét}}$, $A = \mathcal{N}\left(\mathrm{J}_0(\mathrm{N})_{\mathbb{Q}_\mathrm{p}}\right)$, $v_\eta = \iota$ and $u = u$. □

Remark 5.2.2. The result [14, Lemme 5.9.2] which we applied at the end of our proof says the following:

Let S be a smooth scheme, A a néronian group scheme over S,

$$1 \to G' \to G \to G'' \to 1$$

an extension of group schemes over S, where G'' is smooth,

$$u : G' \to A$$

a morphism of groups and

$$v_\eta : G_\eta \to A_\eta$$

a morphism prolonging u to generic fibers. Suppose that the extension of G'' by A via u is representable. Then there is a unique morphism of groups

$$v : G \to A$$

extending v_η and u.

We now introduce some notation which is essentially that of Chapter 3, except that p will play the role of the prime q in Chapter 3. Denote by J_{s} the special fiber of the NÉRON model $\mathcal{N}(J_0(N))$ and J_{s}^0 the connected component of 0 in J_{s}. Considering work of MAZUR, RAYNAUD and DELIGNE-RAPOPORT we have obtained the exact sequence (3.16) which shows that J_{s}^0 is an extension

$$1 \to T \to J_{\mathrm{s}}^0 \to J_0(M) \times J_0(M) \to 0$$

of the product $J_0(M) \times J_0(M)$ by a torus T. Let X be the character group T. Let Φ be the group of connected components of J_{s}. In the proof of Theorem 5.1.16(2.) we have seen, that $\mathcal{V}$ is finite and flat. Further, V is contained in $J_0(N)[\ell]$. So we may use the map $\mathcal{V} \to \mathcal{N}(J_0(N))$ of Lemma 5.2.1 to identify $\mathcal{V}$ with a subgroup of the largest finite flat subgroup H of $\mathcal{N}(J_0(N))[\ell]$. Write $\mathcal{V}_{\mathrm{s}}$ for the special fiber of $\mathcal{V}$.

Coming from $J_0(N)$ via an exact sequence of the form (3.16) T is defined over $\mathbb{Q}_p$, but we may lift it to the torus

$$\underline{T} = \mathrm{Hom}(X, \mathbb{G}_{\mathrm{m}})$$

over $\mathbb{Z}_p$. Retracing the explanation of GROTHENDIECK in [14, 5.1] we see easily that $\underline{T}$ embeds into the formal completion of $\mathcal{N}(J_0(N))$ along its special fiber (see in particular (5.1.3) of [14, 5.1]). Due to the fact that $\underline{T}$ is finite and flat, the same holds for the kernels $\underline{T}[\ell^\nu]$ for all $\nu \geq 0$. This implies that $\underline{T}[\ell]$ is naturally a finite flat subgroup of H, too.

Lemma 5.2.3. *If $\rho_{\mathfrak{m}}$ is not modular of level $M = \frac{N}{p}$, then the group $\mathcal{V}$ is a subgroup of $\underline{T}[\ell]$.*

PROOF: Recall that J_{s} is the extension of its group of connected components Φ by its connected component of 0. As we have seen in Theorem 3.2.14, Φ is annihilated by the elements $\eta_r = 1 + r - \mathrm{T}_r$ with $r \nmid N = pM$, i.e. all primes up to finitely many. The ideal $\mathfrak{J}$ generated by these elements is by Theorem 5.1.16(3.) relatively prime to $\mathfrak{m}$. This means that $J_{\mathrm{s}}[\mathfrak{m}]$ is contained in J_{s}^0. And in particular the subgroup $\mathcal{V}_{\mathrm{s}}$ of $J_{\mathrm{s}}[\mathfrak{m}]$ is contained in J_{s}^0.

In view of the sequence (3.16) we obtain a map $\mathcal{V}_{\mathrm{s}} \to J_0(M) \times J_0(M)$. If the image of this map is non-trivial, the maximal ideal $\mathfrak{m}$, which annihilates $\mathcal{V}_{\mathrm{s}}$, acts by functoriality as zero on $J_0(M) \times J_0(M)$. Thus by Theorem 3.2.9 it is contained in the p-old quotient $\mathbf{T}_N^{\mathrm{old}}$ of $\mathbf{T}_N$. What is more, $\mathfrak{m}$ arises from a maximal ideal of $\mathbf{T}_N^{\mathrm{old}}$. Considering the definition of the p-old subspace we recognize that we have lowered the level to $M = \frac{N}{p}$ and this implies that $\rho_{\mathfrak{m}}$ is modular of level M. Therefore our assumption that $\rho_{\mathfrak{m}}$ is **not** modular of level M implies that $\mathcal{V}_{\mathrm{s}}$ is not contained non-trivially in $J_0(M) \times J_0(M)$ but in T – and so evidently in $T[\ell]$.

To prove that $\mathcal{V}$ is a subgroup of $\underline{T}[\ell]$, we consider the composite ν of the injection

$$\mathcal{V} \hookrightarrow H$$

and the canonical projection

$$H \twoheadrightarrow H/\underline{T}[\ell].$$

The map ν has finite flat kernel. This is clear in the case $p \neq \ell$ since $\mathcal{V}$ is a finite flat subgroup of H over $\mathbb{Z}_p$. In the case $p = \ell$, we have as before $p > 2$, so the condition $p - 1 > 1 = e$, for the absolute ramification index e, holds and we can apply Corollary 5.1.8(1.), which affirms that the kernel is flat (finiteness is trivial). By what we have derived before, $\mathcal{V}_{\mathrm{s}}$ is contained in the lifting $\underline{T}[\ell]$ of $T[\ell]$, that is to say in the kernel of ν, i.e.

$$\mathcal{V}_{\mathrm{s}} \subseteq \mathrm{Ker}(\nu) \subseteq \mathcal{V}\,.$$

It follows that the kernel is the whole group $\mathcal{V}$ and this proves the assertion. □

The announced theorem claims the following:

Theorem 5.2.4. *Assume that the three hypotheses on $\rho_{\mathfrak{m}}$ listed at the beginning of the section are satisfied. Suppose further that we have*

$$p \not\equiv 1 (\mathrm{mod}\, \ell).$$

Then the representation $\rho_{\mathfrak{m}}$ is modular of level $M = \frac{N}{p}$.

Proof: We think of $D_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ as the decomposition group at p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We will effect a contradiction assuming the contrary of the assertion. Take for granted that $\rho_{\mathfrak{m}}$ is not modular of level M. From Lemma 5.2.3 we obtain by tensoring with $\overline{\mathbb{Q}}_p$ the inclusion of kD_p-modules

$$V \subset \underline{T}[\mathfrak{m}](\overline{\mathbb{Q}}_p) = \mathrm{Hom}(X/\mathfrak{m}\, X, \mu_\ell),$$

where the last equality follows from $\underline{T} = \mathrm{Hom}(X, \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})_{\mathrm{m}})$ since ℓ is the residue characteristic attached to $\mathfrak{m}$.

The action of D_p on $X/\mathfrak{m}\, X$ is unramified (in the case $p \neq \ell$ this is clear; in the case $p = \ell$ this follows from the fact that $\mathcal{N}\left(\mathrm{J_0(N)}_{\mathbb{Q}_\mathrm{p}}\right)[p]/\mathcal{N}\left(\mathrm{J_0(N)}_{\mathbb{Q}_\mathrm{p}}\right)[p]^{\mathrm{f}}(\overline{\mathbb{Q}}_p)$ is unramified as explained in the proof of Lemma 5.2.1 and the fact that $T[\ell]$ is contained in $\mathcal{N}(J_0(N))[\ell]$), hence the related inertia group is trivial and, by the theory exploited in Section 1.3.2, D_p is generated by the Frobenius automorphism Frob_p of X (coming from the fact that T is defined over $\mathbb{F}_p$). According to Corollary 3.2.4 the Frobenius automorphism of X coincides with the Hecke operator T_p. This operator is an involution, more precisely, the negative Atkin-Lehner involution w_p as deduced in Proposition 3.2.2. But since $\mathbf{T}_N/\mathfrak{m} = k$ is a field, the action of D_p on $X/\mathfrak{m}\, X$ is given by $+1$ or -1. By Cartier functoriality, the action of D_p on $\mathrm{Hom}(X/\mathfrak{m}\, X, \mu_\ell)$ is given by the character

$$\varepsilon\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell,$$

where ε is an unramified quadratic character and χ_ℓ is the cyclotomic character of ℓ. This implies that D_p acts also on the kD_p-submodule V of $\mathrm{Hom}(X/\mathfrak{m}\, X, \mu_\ell)$ by the character $\varepsilon\chi_\ell$.

In particular, the determinant of the action of D_p on V induced by the representation $\rho_{\mathfrak{m}}$ is

$$\varepsilon^2\chi_\ell^2 = \chi_\ell^2.$$

Contrariwise, the determinant of the representation $\rho_{\mathfrak{m}}$, from which after all V is deduced, is χ_ℓ. Comparing these two expressions for the determinant, we are forced to conclude that χ_ℓ is trivial on $\mathbb{F}_p$, which is equivalent to the congruence $p \cong 1(\mathrm{mod}\, \ell)$. This is a contradiction to the supposition, which finally shows the theorem. □

Here is a variant of this theorem.

Theorem 5.2.5. *Assume that* $\mathfrak{m}$ *is a maximal ideal of* $\mathbf{T}_N$ *which satisfies the first two conditions on* $\rho_{\mathfrak{m}}$. *Assume further that the residue characteristic* ℓ *of* $\mathfrak{m}$ *is prime to* $pM(p-1)$. *Then the* $k = \mathbf{T}/\mathfrak{m}$*-vector space* $X/\mathfrak{m} X$ *is of dimension* ≤ 1.

Proof: Since ℓ is prime to N and by hypothesis odd, Theorem 5.1.16(2.) implies that the module $V = J_0(N)[\mathfrak{m}]$ is a two-dimensional k-vector space giving the representation $\rho_{\mathfrak{m}}$. Since $\mathrm{Hom}(X/\mathfrak{m}\, X, \mu_\ell)$ considered as kD_p-module is a subspace of $J_0(N)[\ell] = V$, $X/\mathfrak{m}\, X$ is of dimension ≤ 2. If it was of dimension 2, we would get the equality

$$V = \mathrm{Hom}(X/\mathfrak{m}\, X, \mu_\ell).$$

Now the argumentation follows the same pattern as above and we get the congruence $p \cong 1(\mathrm{mod}\, \ell)$ which is contrary to our assumption about ℓ. □

5.3 Changing the Modular Level

5.3.1 Raising the Level

As we made plain in Section 1.6 our actual object is to decrease the modular level of certain ℓ-adic GALOIS representations. However, we have to go an indirect way and study foremost the increasing-level-case. In this section and the following one, we make use of various results of Sections 3.2 and 3.3 with p and q interchanged.

Consider as in Section 3.3 two distinct primes p and q and a positive integer M which is relatively prime to both of them. The ring of HECKE operators $\mathbf{T}_{pM}$ of level pM is a subring of the endomorphismring $\operatorname{End}(\mathcal{S}_2(pM))$. It operates diagonally on the direct sum

$$\mathcal{S}_2(pM) \oplus \mathcal{S}_2(pM).$$

On the other hand recall that we have defined the q-old subspace of $\mathcal{S}_2(pqM)$ according to Definition 3.2.5 where M has to be replaced by pM by

$$\mathcal{S}_2(qpM)^{q\text{-old}} = \alpha^*\left(\mathcal{S}_2(pM)\right) \oplus \beta^*\left(\mathcal{S}_2(pM)\right),$$

where α and β are the degeneracy maps defining T_q. The ring $\mathbf{T}_{pqM}$ operates faithfully on $\mathcal{S}_2(pqM)$ and preserve the q-old subspace (see hereto Section 3.2.3). The image of $\mathbf{T}_{pqM}$ in the endomorphism ring $\operatorname{End}(\mathcal{S}_2(pqM)^{q\text{-old}})$ is the q-old quotient of $\mathbf{T}_{pqm}^{q\text{-old}}$ of $\mathbf{T}_{pqM}$.

We may identify these two spaces as subspaces of $\mathcal{S}_2(pqM)$, but we have to be careful with the HECKE action. The two subrings $\mathbf{T}_{pM}$ and $\mathbf{T}_{pqM}^{q\text{-old}}$ of $\operatorname{End}(\mathcal{S}_2(pM) \oplus \mathcal{S}_2(pM))$ are essentially identical – the only crucial point is the q^{th} HECKE operator. More precisely, $\mathbf{T}_{pM}$ and $\mathbf{T}_{pqM}^{q\text{-old}}$ share a common subring R generated by the T_n with n prime to q and we have

$$\mathbf{T}_{pM} = R[\tau_q] \qquad \text{and} \qquad \mathbf{T}_{pqM}^{q\text{-old}} = R[T_q],$$

where τ_q and T_q are the q^{th} HECKE operators in level pM and pqM respectively. In Theorem 3.3.11 we studied the connection of the two operators when operating on $X \oplus X$, where X is the character group associated with the toric part of the reduction of $J_0(pM)$ at the prime p, with the result that T_q is given by

$$(x, y) \mapsto (\tau_q x - y, qx).$$

Consequently, we have

$$\begin{aligned}
(\mathrm{T}_q^2 - \mathrm{T}_q\,\tau_q + q)\,(x, y) &= \mathrm{T}_q\,(\tau_q x - y, qx) - \mathrm{T}_q\,(\tau_q x, \tau_q y) + (qx, qy) \\
&= ((\tau_q - q)x - \tau_q y, \tau_q q x - qy) - \left(\tau_q^2 x - \tau_q y, \tau_q q x\right) + (qx, qy) \\
&= 0.
\end{aligned}$$

Thus the operators are connected by the quadratic equation

$$\mathrm{T}_q^2 - \mathrm{T}_q\,\tau_q + q = 0, \tag{5.4}$$

not only on $X \oplus X$ but by functoriality this is a general connection of T_q and τ_q.

Evidently, the two HECKE operators commute with each other and every other element in R. Moreover, they both lie in the commutative subring $\mathcal{R} = R[\tau_q, \mathrm{T}_q]$ of $\operatorname{End}(\mathcal{S}_2(pM)^2)$.

Definition 5.3.1. We say that two maximal ideals $\mathfrak{m}_{pM}$ of $\mathbf{T}_{pM}$ and $\mathfrak{m}_{pqM}^{q\text{-old}}$ of $\mathbf{T}_{pqM}^{q\text{-old}}$ are *compatible* if there is a maximal ideal of $\mathcal{R}$ which contains both of them. Identifying the set of maximal ideals of the quotient $\mathbf{T}_{pqM}^{q\text{-old}}$ with an appropriate subset of the set of maximal ideals of $\mathbf{T}_{pqM}$, we say that a maximal ideal of $\mathbf{T}_{pqM}$ is q-old if it arises from a maximal ideal of $\mathbf{T}_{pqM}^{q\text{-old}}$.

In other words, two respective maximal ideals are compatible if and only if their intersections with R coincide.

Proposition 5.3.2. *Every representation which is modular of level pM is modular of level pqM.*

Proof: Suppose that $\mathfrak{m}_{pM}$ is a maximal ideal of $\mathbf{T}_{pM}$. Then $\mathfrak{m}_{pM} \cap R$ is a maximal ideal of R. By using Nakayama's Lemma or the going-up theorem of Cohen-Seidenberg, we may find a maximal ideal $\mathfrak{m}_{pqM}^{q\text{-old}}$ of $\mathbf{T}_{pqM}^{q\text{-old}}$ whose intersection with R is $\mathfrak{m}_{pM} \cap R$. So every $\mathfrak{m}_{pM}$ is compatible with at least one $\mathfrak{m}_{pqM}^{q\text{-old}}$ and by the above said, we may see the latter one as a maximal ideal $\mathfrak{m}_{pqM}$ of $\mathbf{T}_{pqM}$. Then the representations $\rho_{\mathfrak{m}_{pM}}$ and $\rho_{\mathfrak{m}_{pqM}}$ are easily seen to coincide in the following strong case: the residue fields of $\mathfrak{m}_{pqM}$, $\mathfrak{m}_{pM} \cap R$ and $\mathfrak{m}_{pM}$ are all identical, and the representations $\rho_{\mathfrak{m}_{pM}}$ and $\rho_{\mathfrak{m}_{pqM}}$ are equivalent representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q})$ over this finite field. This shows the assertion. □

Finally recall a concept which was already used in Theorem 3.3.10. Suppose that $\mathfrak{m}_{pM}$ is p-new, i.e. that it arises from the quotient $\mathbf{T}_{pM}^{p\text{-new}}$ of $\mathbf{T}_{pM}$ which is associated with the Petersson-orthogonal complement of $\alpha^*(\mathcal{S}_2(M)) \oplus \beta^*(\mathcal{S}_2(M)) \cong \mathcal{S}_2(M) \oplus \mathcal{S}_2(M)$ in $\mathcal{S}_2(pM)$. (Similarly to the above procedure in the q-old case, we may identify the set of maximal ideals of $\mathbf{T}_{pM}^{p\text{-new}}$ with a subset of the set of maximal ideals of $\mathbf{T}_{pM}$.) Then there are maximal ideals $\mathfrak{m}_{pqM}$ of $\mathbf{T}_{pqM}$ which are p-new and compatible with $\mathfrak{m}_{pM}$ – in fact they are p-new and q-old. This can be seen by working in the p-new subspace of $\mathcal{S}_2(pqM)$ rather than in $\mathcal{S}_2(pqM)$ itself.

Lemma 5.3.3. *Let p and M be given, and let $\mathfrak{m}_{pM}$ be a maximal ideal of $\mathbf{T}_{pM}$. Then there exist infinitely many prime numbers q, prime to $pM\,\mathfrak{m}_{pM}$, for which $\rho_{\mathfrak{m}_{pM}}(\mathsf{Frob}_q)$ has trace 0 and determinant -1.*

Proof: Let $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\,\mathbb{Q})$ be a complex conjugation in $\overline{\mathbb{Q}} \subset \mathbb{C}$. By elementary considerations (the matrix of the complex conjugation on the two-dimensional $\mathbb{R}$-vector space $\mathbb{C}$ is $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$) the matrix $\rho_{\mathfrak{m}_{pM}}(c)$ has trace 0 and determinant -1. By the Corollary 5.1.3 of the Čebotarev Density Theorem, there are infinitely many primes q for which $\rho_{\mathfrak{m}_{pM}}(\mathsf{Frob}_q)$ is conjugate to $\rho_{\mathfrak{m}_{pM}}(c)$. Such a q satisfy the desired condition. □

Remark 5.3.4. By construction (see Corollary 5.1.13) the determinant of $\rho_{\mathfrak{m}_{pM}}(\mathsf{Frob}_q)$ is q modulo λ, that is q modulo ℓ if ℓ is the residue characteristic of $\mathfrak{m}_{pM}$. Hence $\rho_{\mathfrak{m}_{pM}}$ has determinant -1 in $k = \mathbf{T}_{pM} \,/\, \mathfrak{m}_{pM}$ if and only if we have $q \equiv -1 (\mathrm{mod}\, \ell)$.

Lemma 5.3.5. *Let p and M be given as usual, and let $\mathfrak{m}_{pM}$ be a maximal ideal of $\mathbf{T}_{pM}$ which is p-new. Let q be a prime number relatively prime to $pM\,\mathfrak{m}_{pM}$ for which $\rho_{\mathfrak{m}_{pM}}(\mathsf{Frob}_q)$ has trace 0 and determinant -1. Let further $\mathfrak{m}_{pqM}$ be a q-new maximal ideal of $\mathbf{T}_{pqM}$ which is compatible with $\mathfrak{m}_{pM}$. Then one has*

$$\mathrm{T}_q^2 - 1 \in \mathfrak{m}_{pqM}\,.$$

Proof: Consider the commutative subring $\mathcal{R}$ of $\mathrm{End}(\mathcal{S}_2(pM)^2)$ generated by $\mathbf{T}_{pM}$ and $\mathbf{T}_{pqM}^{q\text{-old}}$. In view of the fact that $\mathfrak{m}_{pM}$ and $\mathfrak{m}_{pqM}$ are compatible, there is a maximal ideal $\mathfrak{J}$ of $\mathcal{R}$ containing $\mathfrak{m}_{pM}$ and $\mathfrak{m}_{pqM}$. According to equation (5.4) we have the equality

$$\mathrm{T}_q^2 - 1 = \tau_q \, \mathrm{T}_q - (q+1).$$

Since τ_q and $q+1$ are obviously elements of $\mathfrak{m}_{pM}$ (elsewise it would not be maximal), the equation shows that $\mathrm{T}_q^2 - 1$ is an element of $\mathfrak{J}$. However, we know that $\mathrm{T}_q^2 - 1$ is in $\mathbf{T}_{pqM}^{q\text{-old}}$ and $\mathfrak{J} \cap \mathbf{T}_{pqM}^{q\text{-old}} = \mathfrak{m}_{pqM}$. This shows the Lemma. □

The outcome of this Lemma is the following theorem which will be needed in the last section to prove the main result.

Theorem 5.3.6. *Assume the same hypotheses as in Lemma 5.3.5. Assume further that $\rho_{\mathfrak{m}_{pM}}$ is irreducible. Then $\mathfrak{m}_{pqM}$ is pq-new, i.e. $\mathfrak{m}_{pqM}$ arises from a maximal ideal of the pq-new quotient $\mathbf{T}_{pqM}^{pq\text{-}new}$ of $\mathbf{T}_{pqM}$.*

Proof: The principle of the proof is that $\mathfrak{m}_{pqM}$ is in the support of a pq-new group.

Consider again the character group X associated with the toric part of the reduction of $J_0(pM)$ at the prime p. As we have deduced in Theorem 3.3.10, T_{pqM} acts faithfully on the direct sum $X \oplus X$ via its q-old/p-new quotient $\mathbf{T}_{pqM}^{q\text{-old}/p\text{-new}}$ which is as in Definition 3.3.9 the image of $\mathbf{T}_{pqM}$ in the endomorphism ring of the intersection $\mathcal{S}_2(pqM)^{q\text{-new}/p\text{-old}}$ of the q-new and the p-old subspaces of $\mathcal{S}_2(pqM)$.

Since $\mathfrak{m}_{pqM}$ is by hypothesis p-new and q-old, it follows that it belongs to this quotient and therefore in view of the faithfulness to the support of the $\mathbf{T}_{pqM}$-module $X \oplus X$, i.e. the localization $(X \oplus X)_{\mathfrak{m}_{pqM}}$ does not vanish. Due to the fact that $\mathrm{T}_q^2 - 1$ is in $\mathfrak{m}_{pqM}$ (cf. Lemma 5.3.5), $\mathfrak{m}_{pqM}$ is even in the support of

$$(X \oplus X)/(\mathrm{T}_q^2 - 1)(X \oplus X).$$

This reminds us the quotient $(X \oplus X)/\gamma(X \oplus X)$ of the exact sequence

$$0 \to K \to (X \oplus X)/\gamma(X \oplus X) \to \Psi \to C \to 0$$

in Theorem 4.3.9, where Ψ is the group of connected components associated with the reduction at p of the Shimura curve C – the analogue to Φ of Chapter 3. The group Ψ acts as the mentioned pq-new group and we will show that after localizing at $\mathfrak{m}_{pqM}$ Ψ and $(X \oplus X)/(\mathrm{T}_q^2 - 1)(X \oplus X)$ are isomorphic.

By definition of K and C in the sequence (3.22), they are kernel and cokernel of a degeneracy map on the component groups coming from $J_0(pM)$ and $J_0(pqM)$ respectively. As shown in Section 3.2.4 especially in Theorem 3.2.14, component groups of this type are Eisenstein, i.e. the Hecke operators T_r (up to the finitely many, where r divides the modular level) act as multiplication by $r+1$. In particular, the ideal generated by the elements $\eta_r = \mathrm{T}_r - (1+r)$ for all primes, which are coprime to pM (respectively to pqM) is part of the annihilator of the respective component group. Without loss of generality, we take $\mathfrak{J}$ to be the ideal generated by the elements $\eta_r = \mathrm{T}_r - (1+r)$ for all primes which are coprime to pqM. It follows that $\mathfrak{J}$ is in the annihilator of K and C. Now it comes into play that $\rho_{\mathfrak{m}_{pM}}$ is irreducible, as it enables us to apply Theorem 5.1.16(3.) to $\mathfrak{J}$, which is therefore relatively prime to $\mathfrak{m}_{pM}$ and then naturally to $\mathfrak{m}_{pqM}$ since the two maximal ideals are compatible. This shows, that $\mathfrak{m}_{pqM}$ is not in the support of K and C. Indeed, if it was in the support of K, we would get inclusions

$$\mathfrak{J} \subset \mathrm{ann}(K) \subset \mathrm{rad}(\mathrm{ann}(K)) = \bigcap_{\mathfrak{P} \in \mathrm{supp}(K)} \mathfrak{P} \subset \mathfrak{m}_{pqM},$$

which is a contradiction, since $\mathfrak{J}$ and $\mathfrak{m}_{pqM}$ are relatively prime. This shows that after localizing at m_{pqM} the groups K and C vanish and Ψ and $(X \oplus X)/(\mathrm{T}_q^2 - 1)(X \oplus X)$ are isomorphic.

However, according to the proof of Theorem 4.3.9, $\mathbf{T}_{pqM}$ acts on Ψ through its pq-new quotient $\mathbf{T}_{pqM}^{pq\text{-new}}$. By the above said, $\mathfrak{m}_{pqM}$ can be seen as ideal of $\mathbf{T}_{pqM}^{pq\text{-new}}$, which is not the unit ideal. This proves the claim. □

Remark 5.3.7. On the one hand, $\mathfrak{m}_{pqM}$ is obviously q-old (as compatible ideal for $\mathfrak{m}_{pM}$). On the other hand, it is q-new because it is already pq-new (recall Definition 3.3.7). Although this might seem paradoxical, it is possible for an ideal of $\mathbf{T}_{pqM}$ to be q-new and q-old at the same time. This reflects the fact that newforms and oldforms may be congruent modulo ℓ. Mazur brought up the terminology to call $\mathfrak{m}_{pqM}$ an *ideal of fusion* between the q-old and the q-new subspace of $\mathcal{S}_2(pqM)$.

5.3.2 Lowering the Level

In this section we consider again two distinct primes p and q and a natural number M prime to both of them. Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}_{pqM}^{pq\text{-new}}$ and let ℓ be the residue characteristic of $\mathfrak{m}$. Assume in addition that ℓ is odd and the attached representation $\rho_{\mathfrak{m}}$ irreducible. We are up to show how to lower the modular level of this representation under certain assumptions from pqM to qM.

Theorem 5.3.8. *Suppose that ℓ is prime to qM and that $\rho_{\mathfrak{m}}$ is finite at p. Assume that q does not satisfy the congruence $q \equiv 1(\operatorname{mod} \ell)$. Then $\rho_{\mathfrak{m}}$ is modular of level qM.*

PROOF: In the case when $p \not\equiv 1(\operatorname{mod} \ell)$ this is Theorem 5.2.4 and the point of the theorem is that it's true also if q is not congruent to $1 \operatorname{mod} \ell$. This is slightly surprising, but it follows from the p-q switch that results from a comparison between the Jacobians of Shimura curves and classical modular forms. So we may without loss of generality assume that $p \equiv 1(\operatorname{mod} \ell)$. In particular, ℓ and p are relatively prime, so that with the hypothesis ℓ is prime to pqM. Let C be the SHIMURA curve introduced in Section 4.1.2 which is associated to the subgroup of units of reduced norm 1 of an EICHLER order of level M in the unique (up to isomorphism) quaternion algebra over $\mathbb{Q}$ of discriminant pq. Denote by $J = \operatorname{Pic}^0(C)$ the JACOBIAN variety of C.

Because of the established relation between modular curves and SHIMURA curves, it suggests itself to consider the $k\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module

$$W = J(\overline{\mathbb{Q}})[\mathfrak{m}],$$

where $k = \mathbf{T}_{pqM}/m$. Due to the EICHLER-SHIMURA relations for J, which resulted in the analogy between the JACOBIANS of Shimura and modular curves brought up in Theorem 4.3.1, the proof of Theorem 5.1.16(1.) shows that W is a successive extension of copies of the $k\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module V coming from the representation $\rho_{\mathfrak{m}}$.

The idea of the proof is to view the representation in characteristic p and to see where it lands in the NERON model of the JACOBIAN of the SHIMURA curve. Either it will encounter the component group of the reduction mod p of the Neron model or it will stay entirely in the connected component (which is a torus).

Recall that the pq-new quotient $\mathbf{T}_{pqM}^{pq\text{-new}}$ is the quotient of $\mathbf{T}_{pqM}$ cut out by the module Y as explained in Theorem 3.3.8 which is as $\mathbb{Z}[\ldots, \mathrm{T}_n, \ldots] = \widetilde{\mathbf{T}}_{pqM}$-module isomorphic to the character group Z of the torus $(J_{\mathbb{F}_p})^0$. This shows, together with the fact that there is, by Corollary 4.3.8, a unique injection $\mathbf{T}_{pqM}^{pq\text{-new}} \hookrightarrow \operatorname{End}(J)$, that W as kernel of the $\mathbf{T}_{pqM}^{pq\text{-new}}$-ideal $\mathfrak{m}$ is non-zero. Thus, there is an embedding of $k\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules $V \subseteq W$.

Fixing such an embedding of (initially only) $\overline{\mathbb{Q}}$-schemes, we take advantage of the hypothesis that V is via the representation $\rho_{\mathfrak{m}}$ finite at p (which is, as $\gcd(p, \ell) = 1$, the same as to say that V is unramified at p) to identify V with a subgroup of $J(\overline{\mathbb{F}}_p)$. This injection is compatible with the natural actions of the HECKE algebra $\mathbf{T}_{pqM}$ and the FROBENIUS map $\mathsf{Frob}_p \in \operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on V and $J(\overline{\mathbb{F}}_p)$ respectively. Let Ψ be again the group of connected components and Z the character group mentioned in the previous paragraph. We will distinguish two cases.

The first case is that the image of V in Ψ is non-zero. Since V is annihilated by $\mathfrak{m}$, $\mathfrak{m}$ belongs to the support of V. Hence, it belongs to the support of Ψ. As our discussion in the proof of Theorem 5.3.6 has shown, the localization at $\mathfrak{m}$ of Ψ and $(X \oplus X)/(\mathrm{T}_q^2 - 1)(X \oplus X)$ are isomorphic, where X is again the character group associated with the toric part of the reduction of $J_0(qM)$ at the prime q. Further we know that $\mathrm{T}_q^2 - 1$ belongs to $\mathfrak{m}$ by Lemma 5.3.5 and therefore the localization at $\mathfrak{m}$ of $X \oplus X$ is non trivial if this holds for $(X \oplus X)/(\mathrm{T}_q^2 - 1)(X \oplus X)$ and Ψ. This shows that $\mathfrak{m}$ belongs to the support of the $\mathbf{T}_{pqM}$-module $X \oplus X$. According to Theorem 3.3.10, which states that $\mathbf{T}_{pqM}$ acts on $X \oplus X$ through its quotient $\mathbf{T}_{pqM}^{q\text{-new}/p\text{-old}}$, this implies that $\mathfrak{m}$ is q-new/p-old. So it can be considered as a maximal ideal in $\mathbf{T}_{pqM}^{p\text{-old}}$. Using again the going-up theorem of COHEN-SEIDENBERG mirror-inverted as in Proposition 5.3.2, we can find a maximal ideal $\mathfrak{m}_{qM}$ of $\mathbf{T}_{qM}$ which is compatible with $\mathfrak{m}$ in the sense of Definition 5.3.1 and the two associated representations $\rho_{\mathfrak{m}}$ and $\rho_{\mathfrak{m}_{qM}}$ are isomorphic. Consequently, $\rho_{\mathfrak{m}}$ is of level qM.

It remains to treat the second case, where the image of V in Ψ is zero. Since Ψ is isomorphic to the quotient $Z^\vee/Z$ (c.f. Section 4.1.2), where $Z^\vee = \mathrm{Hom}(Z, \mathbb{Z})$, and V is in the kernel of $\mathfrak{m}$, this means that V is contained in the group $\mathrm{Hom}(Z/\mathfrak{m}\,Z, \mu_\ell)$. Given that the representation $\rho_{\mathfrak{m}}$ is two-dimensional, i.e. V is two dimensional over k, the group $\mathrm{Hom}(Z/\mathfrak{m}\,Z, \mu_\ell)$ has k-dimension at least 2 and by functoriality

$$\dim_k(Z/\mathfrak{m}\,Z) \geq 2.$$

Under the isomorphism $Z \cong Y$ of Theorem 4.3.1, where Y is the $\mathbf{T}_{pqM}$-module defined in the sequence (3.21) as kernel of the degeneracy map $L \to X \oplus X$, L being the character group associated to the toric part of the reduction at q of $J_0(pqM)$, we have

$$\dim_k(Y/\mathfrak{m}\,Y) \geq 2.$$

If $\mathfrak{m}$ belongs to the support of $X \oplus X$, proceed as in the case above to get hold of the conclusion. So we may cut down the conditions to the case that $\mathfrak{m}$ does not belong to the support of $X \oplus X$, which means that the localization $(X \oplus X)_{\mathfrak{m}}$ vanishes. In view of the short exact sequence (3.21),

$$0 \to Y \to L \to X \oplus X \to 0,$$

we obtain an isomorphism

$$Y/\mathfrak{m}\,Y \cong L/\mathfrak{m}\,L$$

giving finally the statement

$$\dim_k(L/\mathfrak{m}\,L) \geq 2.$$

Since $\mathfrak{m}$ is a maximal ideal of $\mathbf{T}_{pqM}$ satisfying the first two conditions of Section 5.2, the residue characteristic ℓ of $\mathfrak{m}$ is prime to $pqM(p-1)$. We are free to apply Theorem 5.2.5 with p replaced by q, M replaced by pM and X replaced by L. It states that

$$\dim_k(L/\mathfrak{m}\,L) \leq 1,$$

which is a contradiction such that the case that $\mathfrak{m}$ does not belong to the support of $X \oplus X$ can not occure. This concludes our reasoning. □

At last, the hardest part is done and we are ready to prove the main theorem.

Main Theorem (Ribet) 5.3.9. *Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\mathbb{F})$ be an irreducible* $\bmod \ell$ *modular representation of level $N = Mp$, where p is a prime not dividing M. Assume that ρ is finite at p. Assume further that at least one of the following conditions holds:*

1. *The prime ℓ is not a divisor of M.*
2. *We do not have $p \equiv 1(\bmod \ell)$.*

Then ρ is modular of level M.

Proof: By Definition 5.1.15 and 1.5.6, ρ is isomorphic to a representation $\rho_{\mathfrak{m}_{pM}}$ for some maximal ideal $\mathfrak{m}_{pM}$ of $\mathbf{T}_{pM}$. Theorem 5.2.4 covered the case if $p \not\equiv 1(\bmod \ell)$, i.e. if (2.) holds. Therefrom we may assume that $p \equiv 1(\bmod \ell)$, and particularly that p and ℓ are different.

Consider first the case when $\mathfrak{m}_{pM}$ is p-old, i.e. it can be considered as maximal ideal of $\mathbf{T}_{pM}^{p\text{-old}}$. In this case, we can again make use of our Cohen-Seidenberg argument: let R be the common subring of $\mathbf{T}_M$ and $\mathbf{T}_{pM}^{p\text{-old}}$ such that $\mathbf{T}_M = R[\tau_p]$ and $\mathbf{T}_{pM}^{p\text{-old}} = R[T_p]$ where τ_p and T_p are the respective p^{th} Hecke operators. The intersection $\mathfrak{m}_{pM} \cap R$ is a maximal ideal in R. By the going-up theorem we may find a maximal ideal $\mathfrak{m}_M$ of $\mathbf{T}_M$ such that $\mathfrak{m}_M \cap R = \mathfrak{m}_{pM} \cap R$. By the above said, the two maximal ideals are compatible and the associated representations are isomorphic. In particular $\rho_{\mathfrak{m}_{pM}}$ is modular of level M.

Since the p-old and p-new subspace of $\mathcal{S}_2(pM)$ are PETERSSON-orthogonal, a maximal ideal which does not arise from the p-old quotient of $\mathbf{T}_{pM}$ arises automatically from its p-new quotient. So we can secondly consider this case. Choose a prime number q prime to $pM\,\mathfrak{m}_{pM}$ for which $\rho_{\mathfrak{m}_{pM}}(\mathsf{Frob}_q)$ has trace 0 and determinant -1, whose existence was settled in Lemma 5.3.3. As we have already pointed out, there are p-new maximal ideals of $\mathbf{T}_{pqM}$ which are compatible with $\mathfrak{m}_{pM}$. Choose one of them. This maximal ideal $\mathfrak{m}_{pqM}$ is by Theorem 5.3.6 even pq-new.

Since ℓ is odd as assumed at the beginning of this section, we have, if (1.) holds, in fact $q \equiv -1 (\operatorname{mod} \ell)$ and not $q \equiv 1 (\operatorname{mod} \ell)$ accordingly to Remark 5.3.4. So we are in the position to apply Theorem 5.3.8. It shows that $\rho_{\mathfrak{m}_{pqM}}$ and at the same time ρ is modular of level qM which means that we have interchanged p and q. We finish the proof applying Theorem 5.2.4 with p replaced by q. Indeed, this is possible, for $\rho_{\mathfrak{m}_{pqM}}$ satisfies the three conditions at the beginning of Section 5.2 and farther $q \not\equiv 1 (\operatorname{mod} \ell)$. We deduce that ρ is modular of level M. □

Bibliography

[1] Artin, Michael: *Néron Models* in Cornell, Gary; Silverman, Joseph H. eds., *Arithmetic Geometry.* Springer-Verlag, New York, (1986).

[2] Bosch, Siegfried; Lütkebohmert, Werner; Raynaud, Michel: *Néron Models.* Ergebnisse der Mathematik und ihrer Grenzgebiete **3.Folge, Band 21**, A Series of Modern Surveys in Mathematics, Springer-Verlag, Berlin Heidelberg, (1990).

[3] Curtis, Charles W.; Reiner, Irving: *Representation Theory of Finite Groups and Associative Algebras.* Pure and applied mathematics **XI**, John Wiley & Sons inc., (1962).

[4] Deligne, Pierre; Rapoport, Michael: *Les schémas de module de courbe elliptique.* Lecture Notes in Mathematics **349**, pp. 143-316, Springer-Verlag, Berlin-Heidelberg-New York, (1973).

[5] Deligne, Pierre; Serre, Jean-Pierre: *Formes modulaires de poids* 1. Annales Scientifiques de l'École Normale Supérieure, **IV** Ser. **7**, pp. 507-530, (1974).

[6] Deuring, Max: *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abhandlung Mathematischer Seminare **14**, pp. 197-272, Universität Hamburg, (1941).

[7] Diamond, Fred; Shurman, Jerry: *A First Course in Modular Forms.* Graduate Texts in Mathematics **228**, Springer-Verlag, New York, (2005).

[8] Drinfeld, Vladimir G.: *Coverings of p-adic symmetric regions.* Functional Analysis and its Applications **10**, pp. 107-115, Springer-Verlag, New York, (1976).

[9] Edixhoven, Bas: *L'action de l'algébre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein".* Courbes modulaires et courbes de Shimura, Astérisque **196-197**, pp. 59-70, (1991).

[10] Faltings, Gerd: *Finiteness Theorems for Abelian Varieties over Number Fields* in Cornell, Gary; Silverman, Joseph H. eds., *Arithmetic Geometry.* Springer-Verlag, New York, (1986).

[11] Fontaine, Jean-Marc: *Groupes p-divisibles sur les corps locaux.* Astérisque **47-48**, Société Mathématique de France, (1977).

[12] Frey, Gerhard: *Links between Stable Elliptic Curves and Certain Diophantine Equations.* Annales Universitatis Saraviensis, Series Mathematicae **1**, pp. 1-40, (1986).

[13] Frey, Gerhard: *Links between solutions of $A - B = C$ and Elliptic Curves.* Lecture Notes in Mathematics **1380**, pp. 31-62, Springer-Verlag, Berlin-Heidelberg-New York, (1986).

[14] Grothendieck, Alexander: *SGA 7 I, Exposé IX.* Lecture Notes in Mathematics **288**, pp. 313-523, Springer-Verlag, Berlin-Heidelberg-New York, (1972).

[15] HARTSHORNE, ROBIN: *Algebraic Geometry.* Graduate Texts in Mathematics **52**, Springer-Verlag, New York, (1977).

[16] HUSEMÖLLER, DALE: *Elliptic Curves.* Graduate Texts in Mathematics **111**, Springer-Verlag, New York, (1987).

[17] JORDAN, BRUCE; LIVNÉ, RON A.: *Local diophantine properties of Shimura curves.* Mathematische Annalen **270**, pp. 235-248, (1985).

[18] JORDAN, BRUCE; LIVNÉ, RON A.: *On the Néron Model of Jacobians of Shimura Curves.* Compositio Mathematica **60** n°2, pp. 227-236, (1986).

[19] KATZ, NICHOLAS M.; MAZUR, BARRY: *Arithmetic Moduli of Elliptic Curves.* Annals of Mathematical Studies **108**, Princeton University Press, Princeton, (1985).

[20] KNAPP, ANTHONY W.: *Elliptic Curves.* Mathematical Notes **40**, Princeton University Press, Princeton, (1993).

[21] LIU, QING: *Algebraic Geometry and Arithmetic Curves.* Oxford Graduate Texts in Mathematics **6**, Oxford University Press, Oxford-New York, (2002).

[22] MAZUR, BARRY: *Number Theory as Gadfly.* The American Mathematical Monthly **98**, No. 7, pp. 593-610, Mathematical Association of America, (August-September 1991).

[23] MAZUR, BARRY: *Modular Curves and the Eisenstein Ideal.* Publ. Math. I.H.E.S. **47**, pp. 33-186, (1977).

[24] MAZUR, BARRY; SERRE, JEAN-PIERRE: *Points rationnels des courbes modulaires* $X_0(N)$. Séminaire N.Bourbaki **27e année** 1974/75, exposé 469, pp. 238-255, (1975).

[25] MAZUR, BARRY; RIBET, KENNETH A.: *Two-dimensional representations in the arithmetic of modular curves.* Astérisque **196-197**, pp. 215-255, S.M.F., (1991).

[26] MILNE, JAMES S.: *Jacobian Varieties* in CORNELL, GARY; SILVERMAN, JOSEPH H. eds., *Arithmetic Geometry.* Springer-Verlag, New York, (1986).

[27] MORIKAWA, HISASI: *On Theta Functions and Abelian Varieties over Valuation Fields of Rank One.* Nagoya Mathematical Journal **21**, pp. 231-250, (1962).

[28] MUMFORD, DAVID: *Abelian Varieties.* Tata Institute of Fundamental Research Studies in Mathematics, Oxford University Press, (1974).

[29] ODA, TADAO : *The first de Rham cohomology group and Dieudonné modules.* Annales Scientifiques de l'École Normale Supérieure IV **2**, pp. 63 - 135, (1969).

[30] OESTERLÉ, JOSEPH: *Nouvelles approches du "théorèm" de Fermat.* Séminaire N.Bourbaki 1987/88, exposé 694, Astérisque **161-162**, S.M.F., pp. 385-437, (1988).

[31] OGG, ANDREW P.: *Elliptic curves and wild ramification.* American Journal of Mathematics **89**, No. 1, pp. 1-21, The Johns Hopkins University Press, (1967).

[32] RAYNAUD, MICHEL: *Schémas en groupes de type* $(p, \ldots, p)$. Bulletin de la Société Mathématique de France **102**, pp. 241-280, (1974).

[33] RIBET, KENNETH A.: *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Inventiones mathematicae **100**, pp. 431-476, Springer-Verlag, Berlin-Heidelberg-New York, (1990).

[34] Ribet, Kenneth A.: *From the Taniyama-Shimura Conjecture to Fermat's Last Theorem.* Annales de la Faculté des Sciences de Toulouse, Sér. **5**, **11** no.**1**, pp. 116-139, (1990).

[35] Ribet, Kenneth A.: *p-adic L-functions attached to characters of p-power order.* Séminaire Delange-Pisot-Poitou, Théorie des nombres **19** 1, exposé 9, pp. 1-8, (1977/78).

[36] Ribet, Kenneth A.: *On the Component Groups and Shimura Subgroup of* $J_0(N)$. Séminaire de Théorie des Nombres de Bordeaux **16**, exposé 6, pp. 1-10, (1987).

[37] Ribet, Kenneth A.; Stein, William A.: *Modular Forms, Hecke Operators and Abelian Varieties.* (2003).

[38] Serre, Jean-Pierre: *Corps Locaux.* Publications de l'institut de mathématique de l'université de Nancago **VIII**, Hermann, Paris, (1968).

[39] Serre, Jean-Pierre: *Sur les représentations modulaire de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Mathematica Journal **54**, pp. 179-230, (1987).

[40] Serre, Jean-Pierre: *Abelian l-adic Representations and Elliptic Curves.* McGill University Lecture Notes, W.A.Benjamin Inc., New York and Amsterdam, (1968).

[41] Serre, Jean-Pierre: *Propriété galoisiennes des points d'ordre fini des courbes elliptiques.* Inventiones mathematicae **15**, pp.259-331, Springer-Verlag, (1972).

[42] Serre, Jean-Pierre: *Arbres, Amalgames,* $\mathbf{SL}_2$. Astérisque **46**, Société Mathématique de France, (1977).

[43] Serre, Jean-Pierre: *Points rationnels des courbes modulaires* $X_0(N)$. Séminaire N.Bourbaki **30e année** 1977/78, exposé 511, pp. 89-100, (1977).

[44] Shimura, Goro: *Introduction to the Arithmetic Theory of Automorphic Functions.* Mathematical Notes , Princeton University Press, Princeton, (1971).

[45] Silverman, Joseph H.: *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics **106**, Springer-Verlag, New York, (1986).

[46] Tate, John T.: *The Arithmetic of Elliptic Curves.* Inventiones mathematicae **23**, pp. 179-206, Springer-Verlag, Berlin-Heidelberg-New York, (1974).

[47] Tate, John T.: *Endomorphisms of Abelian Varieties over Finite Fields.* Inventionens mathematicae **2**, pp. 134-144, (1966).

[48] Vigneras, Marie-France: *Arithmétique des Algèbres de Quaternions.* Lecture Notes in Mathematics **800**, Springer-Verlag, Berlin-Heidelberg-New York, (1980).

Erklärung

Hiermit versichere ich, dass ich diese Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Unterammergau, den 31. Juli 2009