Contents

0.1 Introduction

This thesis aims to give a motivated account of Galois representations and étale cohomology, all with the purpose of giving a precise statement of the historically important Fontaine-Mazur conjecture.

0.2 Some history and motivation

The Fontaine-Mazur conjecture, in its modern incarnation, sits at the confluence of two winding threads in number theory: the classical program of understanding arithmetic problems via extensions of fields, and the more recent program of associating arithmetic objects to so-called "automorphic" ones. From the nineteenth century onwards, one may trace a steady movement from explicit analytic results to a a more structural one, consisting more of geometry and representation theory. Beginning with Dirichlet's theorem on arithmetic progressions, number theorists studied L-functions attached to characters, which were secretly certain *one-dimensional* representations of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Later work of Kronecker, Weber, Hilbert, and Tagaki paved the way for class field theory, which aimed to classify abelian extensions of a number field K in terms of the arithmetic of K. This theory would go through many changes over the 20th century, but once again, the story begins with certain L-functions related to number fields, and moves to something more akin to relating *automorphic* objects to the representation theory of $G_{\mathbb{Q}}$.

A parallel, *geometric* strand emerged in the attempt to understand the L-functions attached not to number fields but to algebraic varieties. The *Weil conjectures,* proposed André Weil, proposed a striking set of analogies between the zeta function of a smooth projective variety over a finite field, and the cohomology of a topological manifold. These conjectures predicted that somehow, there should exist some kind of a cohomology theory for varieties over finite fields with the same formal properties as cohomology over $\mathbb{C}$, including the existence of an analogue of the Lefschetz fixed point formula. Alexander Grothendieck's advent of *étale cohomology* provided precisely such a theory; however, such a theory required a complete reformulation of the foundations of algebraic geometry (including the advent of *schemes*), and many years of hard work.

The theory of étale cohomology, in fact, gave a concrete and powerful way to go from geometric objects (i.e., varieties over fields) to arithmetic ones: l-adic Galois representations. However, going the other direction happens to be significantly trickier. It is thus reasonable to ask: given a Galois representation

$$\rho : G_K \to GL(V),$$

does this representation "come from" the étale cohomology of some variety? The Fontaine-Mazur conjecture aims to answer this question precisely. Currently, the con-

jecture is only known for the GL_1 case and parts of the GL_2 case, the latter requiring incredibly sophisticated machinery which is far beyond the scope of this thesis. It turns out that, in each case, the major tools used are again "automorphic" in nature, and so the program of relating automorphic objects to Galois theoretic ones remains a central philosophical tenet, and one which we attempt to emphasize here, though only in heavily restricted cases.

0.3 Outline of the thesis

We will assume that the reader is familiar with the basic theory of schemes and the major theorems of class field theory, although we require no familiarity with cohomology.

Chapter 1 focuses on some background related to elliptic curves and modular/automorphic forms. Chapter 2 moves straight into briefly developing the theory of étale cohomology, and mentioning some relations to the objects in Chapter 1. Chapter 3 introduces Galois representations and gives examples, coming from both geometry and from automorphic representations. Chapter 4 develops the necessary theory for p-adic representations to finally give a precise statement of the conjecture, and explain a relation to the Modularity theorem. Finally, Chapter 5 looks at a restricted case of modularity (originally due to Shimura), with the hope of giving the reader something concrete which can be seen as evidence for the conjecture.

Chapter 1

Some background on elliptic curves and modular forms

We start by recalling some basic definitions about elliptic curves, abelian varieties, and modular forms. We end by briefly sketching some facts about automorphic forms in number theory. This section is particularly light on formal proofs, and we instead refer the reader to standard references where appropriate.

1.1 Elliptic curves and Abelian Varieties

We begin by giving an overview of the theory of elliptic curves. We will start with the general situation, and then give some more specifics for elliptic curves over certain fields.

Definition 1.1. Let k be a field (not necessarily algebraically closed) with $\operatorname{char} k \neq 2, 3$. An *elliptic curve* $E(k)$ over k is a smooth projective curve of genus one defined over k, along with a specified k-rational point O, called the *base point.*

Every such curve can be written as the zero locus in $\mathbb{P}^2_k$ of a cubic ("Weierstrass") equation

$$y^2 = x^3 + ax + b,$$

with $a, b \in k$ with nonzero discriminant, i.e., $4a^3 + 27b^2 \neq 0$. In this case, we have that $O = (0 : 1 : 0)$. If the base field is unambiguous, we may just denote a particular elliptic curve by E. We can extend this definition to an arbitrary base scheme S. An elliptic curve E over S is a pair (E, O) of a proper smooth curve $f : E \to S$ with geometrically connected fibers of genus one, and a section $O : S \to E$.

One of the most important properties of elliptic curves is that they are *abelian varieties,* i.e., they have the structure of an abelian group. Recall that for a scheme X, the *Picard group* $\operatorname{Pic}(X)$ to be the group of isomorphism classes of line bundles (i.e.,invertible $\mathcal{O}_X$-modules; see [Har77], II.6), with the group operation being the tensor

product. Note that for X a smooth proper curve over k, the Picard group is isomorphic to the divisor class group of closed points of X modulo principal divisors.

Now recall that, given a proper morphism $f : X \to Y$ of k-schemes, we can define the *degree* of f to be $\deg(f) := [k(X) : k(Y)]$. If X is a proper, integral curve over k, then taking degrees gives a group homomorphism $\deg : \mathrm{Pic}(X) \to \mathbb{Z}$. In general, the pullback f^* of f (or inverse image sheaf, see [Har77], II.5) gives a homomorphism $f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$, and making the Picard group a functor from $\mathsf{Sch} \to \mathsf{Ab}$.

We now define the relative Picard functor, which upgrades the Picard group to a functor $\mathsf{Sch} \to \mathsf{Set}$. Given a scheme $f : X \to S$ over a scheme S, note that line bundles pull back to line bundles (see [Har77], exercise III.12.4), we can define the following:

Definition 1.2. Let $f_T^* : \mathrm{Pic}(T) \to \mathrm{Pic}(X)$ be the pullback map. The *relative Picard functor* $\mathrm{Pic}_{X/S} : \mathsf{Sch}_S \to \mathsf{Set}$ is defined by sending

$$T \mapsto \mathrm{Pic}(X \times_S T)/f_T^*\mathrm{Pic}(T)$$

Since we have a nice functor to Set, it is natural to ask whether or not this functor is representable by a scheme. In the case of elliptic curves, this is true due to the following theorem ([BLR90],Theorem 8.2.1)

Theorem 1.3. *Let $f : X \to S$ be projective, finitely presented, flat, and the geometric fibers of f are reduced and irreducible. Then $Pic_{X/S}$ is representable by a separated S-scheme which is locally of finite presentation over S.*

Then we call this unique scheme representing the relative Picard functor $\mathrm{Pic}_{E/S}$ of an elliptic curve the *Picard scheme* of E, and denote it by $\underline{\mathrm{Pic}}_{E/S}$.

We now wish to state an important result about the group structure of elliptic curves, known as *Abel's theorem.* Let E be an elliptic curve over a scheme S, and let T be an S-scheme. For notational convenience, let $E_T := E \times_S T$. For an $\mathcal{O}_{E_T}$-module $\mathcal{L}$, we can define its degree $\deg \mathcal{L}$ to be the locally constant function $T \to \mathbb{Z}$ defined by setting $\deg \mathcal{L}(t) = \deg(\mathcal{L}|_{\mathcal{E}_T})$. Hence we get a more general degree map $\deg : \mathrm{Pic}(E_T) \to \mathbb{Z}(T) := \mathrm{Hom}_{\mathsf{Set}}(T, \mathbb{Z})$. Now define the *degree 0 part* of the Picard group, $\mathrm{Pic}^0_{E/S}$, to be the subgroup of $\mathrm{Pic}_{E/S}(T)$ of isomorphism classes of invertible sheaves on E_T which are (fiber-by-fiber) degree zero. It turns out that $\mathrm{Pic}(E_T)$ decomposes as $\mathbb{Z}(T) \oplus \mathrm{Pic}(T) \oplus \mathrm{Pic}^0_{E/S}(T)$, and hence $\mathrm{Pic}^0_{E/S}$ defines a functor $\mathsf{Sch}_S \to \mathsf{Sch}$. We can naturally view E as a functor $\mathsf{Sch}_S \to \mathsf{Sch}$ as well in the obvious way, and so we define a natural transformation $E \to \mathrm{Pic}^0_{E/S}$ by sending $P \in E(T)$ to the image of $[\mathcal{O}_{E_T}(P)]$ in $\mathrm{Pic}_{E/S}(T)$. We have the following theorem (see [KM85], Theorem 2.1.2 for a proof):

Theorem 1.4. ***(Abel's Theorem)*** *The natural transformation $E \to Pic^0_{E/S}$ is an isomorphism of functors.*

Since $\mathrm{Pic}^0_{E/S}$ is also an abelian group, this shows that E has the structure of an abelian variety.

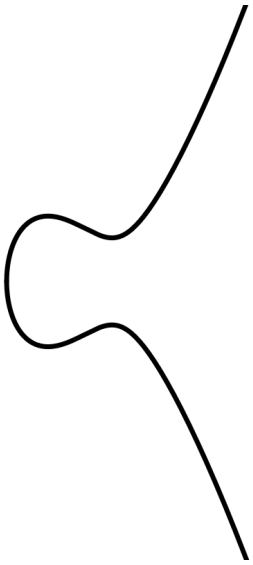


Figure 1.1: The curve $y^2 = x^3 - x + 1$

If k is algebraically closed, we can say even more. In this case, if X is a nonsingular projective curve of genus g over k, $\mathrm{Pic}(X)$ is isomorphic to the group of zero-cycles modulo rational equivalence, i.e., the dimension zero part of the Chow group A^0X. The kernel of the degree homomorphism is an abelian variety $\mathrm{Jac}(X)$ over k of dimension g, called the *Jacobian variety* of X. In the case that $X = E$, an elliptic curve, $\mathrm{Jac}(E)$ is an elliptic curve isomorphic to E.

This gives the group law on an elliptic curve in as much generality as we need, but may not be very instructive or intuitive at a first glance. Luckily, if we are working over a field, we can talk about this group law in a much more explicit manner via some basic geometry.

1.1.1 Elliptic curves over fields

We return back to earth for the time being. Going back to out first definition of an elliptic curve, let k be a field of characteristic $\neq 2, 3$. In this case, we don't have to deal much with the scheme-theoretic formalism, and the situation is much more intuitively geometric. For some examples, the affine curves given by Weierstrass equations can be easily visualized as curves in $\mathbb{R}^2$, which can be seen in Figures 1.1 and 1.2.

In this case, the group operation on elliptic curves can be described purely geometrically, at the level of high school algebra. Given an elliptic curve E in $\mathbb{P}^2$, and a line L in $\mathbb{P}^2$, one can see that L intersects E in exactly three points, given that the defining equation has degree three (this is a special case of Bézout's theorem, if one likes). We define an "addition" rule on E as follows:
1) Given two points $P, Q \in E$, form the line L_1 through P and Q (in the case $P = Q$, take the tangent line to E at P).

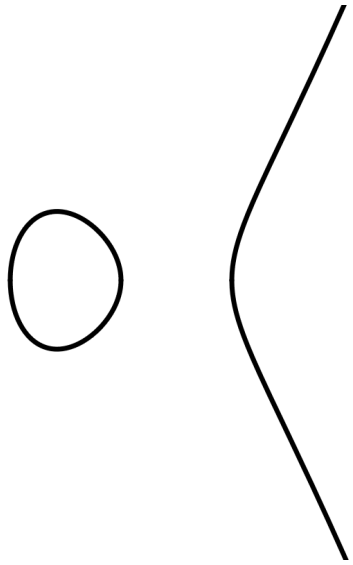


Figure 1.2: The curve $y^2 = x^3 - x$

2) Let $-(P+Q)$ be the third point of intersection of L_1 with E.
3) Let L_2 be the line passing through $-(P+Q)$ and O. This again intersects E at a third point, which we denote by $P+Q$.

It is almost obvious that this defines a group structure on E : clearly $P+O=P$ for any point $P \in E$; commutativity is clear, and given a point P, taking the line L through P and O gives a third point, $-P$, such that $P+(-P)=O$. Associativity is less obvious, but Abel's theorem tells us that this works.

An important point is that certain points on the curve have finite order, i.e., they have *torsion.* For example, doubling the point P in Figure 1.5 yields O, so P has order 2. We will denote the subgroup of points of order $n \in \mathbb{Z}$ by $E[n]$, the n-torsion subgroup. Putting all these together, we arrive at the *torsion subgroup of* E,

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

1.1.2 Elliptic curves over $\mathbb{C}$

The theory of elliptic curves really started with a *complex analytic* theory, which we now give a brief part of. The full story, however, must wait until we discuss *modular curves.*

Let E be an elliptic curve over $\mathbb{C}$. Given a lattice $\Lambda \subseteq \mathbb{C}$, we define the quantities

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda} \frac{1}{\omega^4}$$
$$g_3(\Lambda) = 140 \sum_{\omega \in \Lambda} \frac{1}{\omega^6}.$$

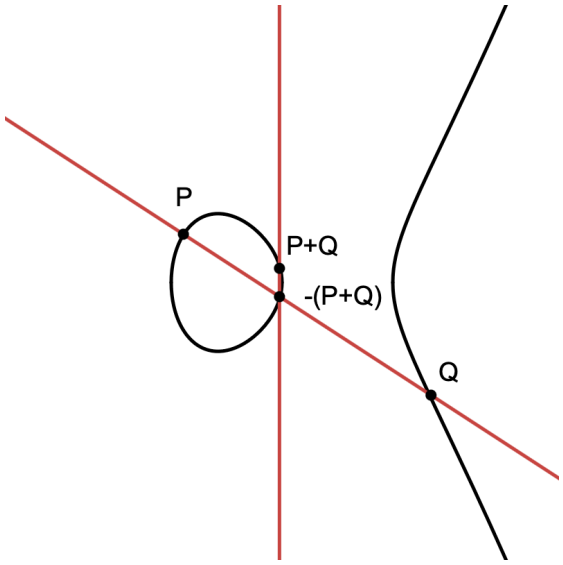


Figure 1.3: Point addition on $E : y^2 = x^3 - x$

Then it turns out:

Proposition 1.5. *There exists a lattice $\Lambda \subseteq \mathbb{C}$ such that E is defined by $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$.*

Proof. see [DS05], Proposition 1.4.3. □

Thus, we can associate to any elliptic curve over $\mathbb{C}$ a *complex torus,* given by $\mathbb{C}/\Lambda$. It also turns out that the converse is true: given any complex lattice Λ, there is a corresponding elliptic curve. Given a lattice Λ, define the *Weierstrass $\wp$-function* to be

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \Big)$$

for $z \notin \Lambda$ in $\mathbb{C}$, where the sum is taken over all *nonzero* $\omega \in \Lambda$.

Proposition 1.6. *The functions $\wp$ and $\wp'$ satisfy the nonsingular equation*

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

by letting $x = \wp(z)$ and $y = \wp'(z)$.

Proof. see [DS05] Proposition 1.4.1 □

Hence we get a *bijection*

$$(\wp, \wp') : \{\text{complex tori}\} \xrightarrow{\sim} \{\text{(isomorphism classes of) elliptic curves over } \mathbb{C}\},$$

and the two objects can be identified.

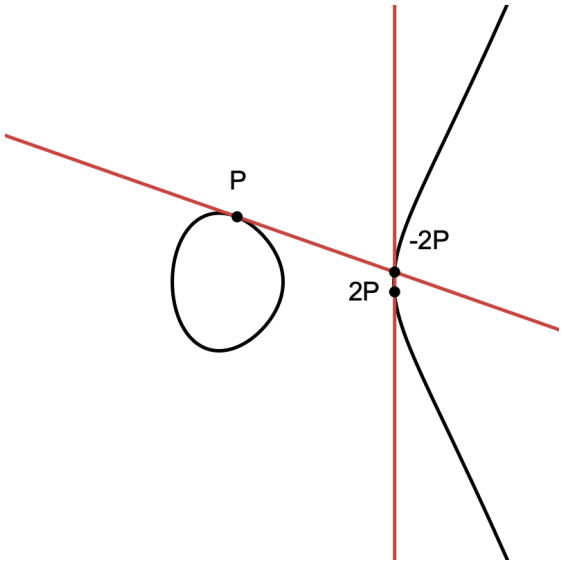


Figure 1.4: Point doubling on $E : y^2 = x^3 - x$

Isogenies of Elliptic Curves

Let E_1 and E_2 be two elliptic curves over a field k.

Definition 1.7. An *isogeny* from E_1 to E_2 is a morphism $\varphi : E_1 \to E_2$ such that $\varphi(O) = O$.

Two elliptic curves E_1 and E_2 are called *isogenous* is there exists a nontrivial isogeny $E_1 \to E_2$. We will denote

$$\mathrm{Hom}(E_1, E_2) := \{\text{isogenies } E_1 \to E_2\}.$$

Further, we define the *endomorphism ring*

$$\mathrm{End}(E) := \mathrm{Hom}(E, E),$$

with addition defined in the obvious way.

The major example of an endomorphism is the *multiplication-by-n* isogeny

$$[n] : E \to E,$$

sending $P \to [m]P = \underbrace{P + P + \cdots + P}_{(n \text{ times})}$.

One other topic worth mentioning is that of *complex multiplication,* which will play a major role at the end of this thesis. Again, let E be an elliptic curve over $\mathbb{C}$, (or possibly any other field of characteristic 0). The "multiplication by n" maps $[n] : E \to E$ are group endomorphisms of E, so we can define a map

$$[-] : \mathbb{Z} \to \mathrm{End}(E),$$

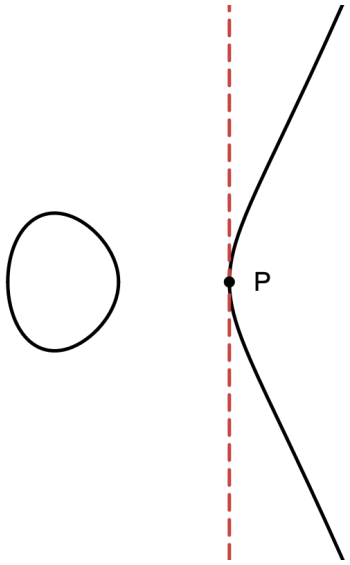


Figure 1.5: $2P = O$, i.e., *torsion* point

where $\mathrm{End}(E)$ is the ring of endomorphisms of E over $\mathbb{C}$. Typically, in characteristic 0, this is all that one gets: this map is usually an isomorphism. But, if E contains *other* endomorphisms, and is strictly *larger* than $\mathbb{Z}$, we say that E has complex multiplication (often abbreviated "E has CM").

As an example, let E be the elliptic curve

$$E : y^2 = x^3 - 11.$$

This has the order three automorphism $(x, y) \mapsto (e^{2\pi i/3} \cdot x, y)$, and we have $\mathrm{End}(E) \cong \mathbb{Z}[e^{2\pi i/3}] \neq \mathbb{Z}$!

1.2 Modular forms and modular curves

We now turn to modular forms, which will be our other major source of abelian varieties in this thesis. We will give three different definitions of a modular form, which will each highlight some different aspect of the theory.

1.2.1 Modular Forms, Classically

We begin with a classical, garden-variety definition of a modular form. The study of modular forms is really quite old, going back as far as Gauss around the year 1800. For some time, the concept of a modular form was thought of as lying squarely in the study of complex analysis, albeit with some applications elsewhere. We begin with this analytic story.

Definition 1.8. A subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if there is an integer $N \geq 1$ such that $\Gamma \subseteq \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$.

Two particularly important such subgroups are $\Gamma_1(N)$ and $\Gamma_0(N)$, given explicitly by

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv 1, c \equiv 0 \bmod N \right\}$$
$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

Note that in fact $\Gamma_1(N) \subseteq \Gamma_0(N)$, and $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. We define two actions of $\mathrm{SL}_2(\mathbb{Z})$, one on the upper half plane $\mathbb{H}$, and the other on modular forms. The first is defined by letting

$$\gamma(z) = \frac{az+b}{cz+d}$$

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$. For a holomorphic function f on the upper half plane, we can also define the *weight-k* operator $[\gamma]_k$ on modular forms, by setting for f a holomorphic function f on $\mathbb{H}$

$$f[\gamma]_k(z) = (cz+d)^{-k} f(\gamma(z)).$$

Definition 1.9. Let Γ be a congruence subgroup and $k \geq 2$ be an integer. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form* of weight k with respect to Γ if

1. $f[\gamma]_k = f$ for all $\gamma \in \Gamma$ 2. For each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $f[\gamma]_k$ is holomorphic.

f is called a *cusp form* if its first Fourier coefficient is 0. For Γ a congruence subgroup, we write $S_k(\Gamma)$ for the space of cusp forms, and $M_k(\Gamma)$ for the space of modular forms.

As an example, the functions g_2 and g_3 from the complex theory of elliptic curves were normalized versions of *Eisenstein series,* which for $k \in \mathbb{Z}$ even, $k \geq 4$, is defined by

$$G_k(z) := \sum_{0 \neq m,n \in \mathbb{Z}} \frac{1}{(mz+n)^k}.$$

These series are modular forms of weight k.

1.2.2 Modular Forms From Curves

Through a bit of work (see [DS05], Theorem 1.5.1]), one finds that there is a bijection between lattices in $\mathbb{C}$ and the quotient space $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. Then from the complex-analytic theory for elliptic curves, every point of $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ corresponds to an isomorphism class of elliptic curves. In this sense, $Y(1)(\mathbb{C}) := \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$, called the *modular curve of level 1,* is a *moduli space* for elliptic curves. Similarly, for the congruence subgroups $\Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$, the quotient $Y_1(N)(\mathbb{C}) := \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ is called the modular curve of level $\Gamma_0(N)$, and there is a bijection

$Y_1(N)(\mathbb{C}) \to \{\cong$ classes of elliptic curves E with a chosen point $P \in E(\mathbb{C})$ of order $N\}$

We now define the *universal elliptic curves* over the modular curves $Y_1(N)$ (for $N \geq 4$). Consider the semi-direct product $\Gamma_1(N) \ltimes \mathbb{Z}^2$ with respect to the left action by ${}^t\gamma^{-1}$. Let R be the set of $(z_1, z_2) \in \mathbb{C}^2$ such that $\mathrm{Im}(z_1/z_2) > 0$. Define an action of $\mathbb{C}^\times \times \Gamma_1(N) \ltimes \mathbb{Z}^2$ as follows: given $c \in \mathbb{C}^\times$, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, and $m, n \in \mathbb{Z}$, set

$$\begin{aligned} c \cdot ((z_1, z_2), z) &= ((cz_1, c_z 2), cz), \\ \gamma((z_1, z_2), z) &= ((az_1 + bz_2, cz_1 + dz_2), z), \\ (m, n)((z_1, z_2), z) &= ((z_1, z_2), z + mz_1 + nz_2). \end{aligned}$$

Taking the quotient, we get

$$E_{Y_1(N)} := (\mathbb{H} \times \mathbb{C})/(\Gamma_1(N) \ltimes \mathbb{Z}^2) \to \mathbb{H}/\Gamma_1(N) = Y_1(N).$$

Then fiber at each $\tau \in \mathbb{H}$ is the elliptic curve $\mathbb{C}/(\mathbb{Z} \otimes \tau\mathbb{Z})$.

A remarkable fact is that we can view modular forms as sections of a certain *line bundle* on a modular curve. Let $O : Y_1(N) \to E_{Y_1(N)}$ be the zero-section of the universal elliptic curve. Then we have (see [DR73])

$$\{f \text{ holomorphic and weight } k\text{-invariant}\} = \Gamma(Y_1(N), O^*\Omega_{E_{Y_1}(N)}/Y_1(N))$$

1.2.3 Jacobians of Curves

Following Abel's theorem, we want to look at the representability of the functor $\mathrm{Pic}^0_{X/S}$, in the case that $f : X \to S$ is a proper smooth curve with geometrically connected fibers of genus g. Then we get a distinguished case of Theorem 1.3:

Theorem 1.10. *[BLR90] The functor $Pic^0_{X/S}$ is representable by a proper smooth scheme $Jac_{X/S}$ with geometrically connected fibers of dimension g, called the Jacobian of X.*

For ease of notation, for the modular curve $X_1(N)$, we will write $J_1(N) = \mathrm{Jac}_{X_1(N)/\mathbb{C}}$.

1.2.4 The Abelian Variety of a Newform

Let $f = \sum a_n(f)q^n \in \mathcal{S}_2(\Gamma_1(N_f))$ be a newform of weight 2 and level N_f. Let K_f be the number field generated by the Fourier coefficients of $a_n(f)$ of f. Letting $\mathbb{T}_\mathbb{Z}$ denote the Hecke algebra, we will denote by λ_f the homomorphism $\mathbb{T}_\mathbb{Z} \to \mathbb{C}$ sending f to the eigenvalue of T acting on f. Denote its kernel by

$$I_f = \ker(\lambda_f).$$

The map λ_f induces an isomorphism at the level of abelian groups from the quotient $\mathbb{T}_\mathbb{Z}$ to $\mathbb{Z}[\{a_n(f)\}]$. The Hecke algebra $\mathbb{T}_\mathbb{Z}$ acts on the Jacobian variety $J_1(N_f)$, making $J_1(N_f)$ a $\mathbb{T}_\mathbb{Z}$-module, allowing us to speak of the subgroup $I_f J_1(N_f)$ of $J_1(N_f)$.

Definition 1.11. The *abelian variety* of f is the quotient

$$A_f = J_1(N_f)/I_f J_1(N_f).$$

1.3 A little bit about automorphic forms

We will depart somewhat from the geometric characterizations of modular forms and instead talk about a purely group-theoretic way to define them. To start, note that the upper-half plane $\mathbb{H}$ can be identified with the quotient $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$, and hence given a group structure.

Definition 1.12. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and let $k \in \mathbb{Z}$. A function $f : \mathbb{H} \to \hat{\mathbb{C}}$ is called an *automorphic form of weight k* for Γ if

(a) f is meromorphic

(b) f is weight-k invariant under Γ

(c) $f[\alpha]_k$ is meromorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Then we can view such automorphic forms as certain functions

$$f : \Gamma \setminus \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \longrightarrow \mathbb{C}.$$

Further we can lift these to functions on $\Gamma \setminus \mathrm{GL}_2(\mathbb{R})$: define

$$\widetilde{f}(\gamma) := (\det \gamma)^{k/2} j(\gamma, i)^{-k} f(\gamma \cdot i),$$

where $j(\gamma, z) = cz + d$ is the factor of automorphy, and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Although modular forms aren't quite functions on $\Gamma \setminus \mathbb{H}$, and instead are only sections of a certain line bundle as we noted previously, these can also be lifted to functions on $\Gamma \setminus \mathrm{GL}_2(\mathbb{R})$ in a similar manner. Geometrically, this line bundle is becoming trivial after pulling back.

Let us briefly recall the adèles of $\mathbb{Q}$. The ring of *finite adèles* $\mathbb{A}_f$ is defined to be the restricted product of all the fields $\mathbb{Q}_p$, i.e., the subring of $\prod \mathbb{Q}_p$ consisting of all (a_p) such that $a_p \in \mathbb{Z}_p$ for all but finitely many primes p. Then the full ring of adèles is defined as

$$\mathbb{A} := \mathbb{Q}_\infty \times \mathbb{A}_f = \mathbb{R} \times \mathbb{A}_f.$$

In other words, this is a certain product over all the completions of $\mathbb{Q}$. Then it turns out that things can be transferred further to get functions

$$F : \mathrm{GL}_2(\mathbb{Q}) \setminus \mathrm{GL}_2(\mathbb{A}) \to \mathbb{C}.$$

For instance, if $\Gamma = \Gamma_0(N)$, and we let

$$K_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : c \equiv 0 \mod N \right\}.$$

Then there is a natural isomorphism (see [Boo15])

$$\Gamma_0(N) \setminus \mathrm{GL}_2(\mathbb{R})^+ \cong \mathrm{GL}_2(\mathbb{Q}) \setminus \mathrm{GL}_2(\mathbb{A})/K_0(N),$$

where $\mathrm{GL}_2(\mathbb{R})^+$ is the subgroup of $\mathrm{GL}_2(\mathbb{R})$ consisting of matrices with positive determinant. There is also a way to lift modular forms to functions on $\mathrm{GL}_2(\mathbb{Q}) \setminus \mathrm{GL}_2(\mathbb{A})$, though we will not give that construction here (again, see [Boo15]).

In more generality, an *adelic automorphic form for* $\mathbb{Q}$ consists of:

1. a function $\varphi : \mathrm{GL}_n(\mathbb{Q}) \setminus \mathrm{GL}_n(\mathbb{A}) \to \mathbb{C}$,
2. a character $\omega : Z(\mathbb{A})/\mathbb{Q}^\times \to \mathbb{C}^\times$,
3. a maximal compact subgroup $K \subseteq \mathrm{GL}_n(\mathbb{A})$,

satisfying the following conditions:

1) for all $z \in Z(\mathbb{A})$,

$$\varphi(zg) = \omega(z)\varphi(g),$$

2) φ is smooth in the archimedean variable g_∞, and locally constant in the finite adelic variable g_f,

3) the space spanned by right translates $\{\varphi(gk) : k \in K\}$ is finite-dimensional,

4) φ is finite under the action of the center of the universal enveloping algebra $\mathfrak{U}(\mathfrak{gl}_n(\mathbb{R}))$.

Definition 1.13. A (discrete) *automorphic representation* of $\mathrm{GL}_n(\mathbb{Q})$ will be a direct summand of

$$L^2(\mathrm{GL}_n(\mathbb{Q}) \setminus \mathrm{GL}_n(\mathbb{A})/\mathbb{R}^\times)$$

which, under the right regular representation, defines an irreducible representation of $\mathrm{GL}_n(\mathbb{A})$.

The definition over any number field goes similarly. We are merely including these definitions for completeness, but for the remainder of the thesis, we will primarily be concerned with automorphic forms for GL_1. In a nice turn of events, these objects will turn out to just be characters of $\mathbb{A}^\times/\mathbb{Q}^\times$, which via class field theory, correspond to Galois-theoretic objects. That this situation should generalize in an appropriate way for all n is the content of the so-called *Langlands program,* and offers a major insight into the Fontaine-Mazur conjecture.

Chapter 2

Étale cohomology

Now that we have some background out of the way, we proceed for now in a somewhat different direction. Here we aim to give a rough account of the theory of l-adic cohomology, and we end with a note about its relationship to the Tate modules constructed before.

If V is an algebraic variety over $\mathbb{C}$, one can view V with the complex topology, and it makes sense to look at the cohomology groups $H^i(V, \mathbb{Q})$. However, in general, say over a field k, there is no "nice" topological cohomology theory for the *Zariski* topology on the variety V. However, a key insight of André Weil was that certain phenomena, such as the number of points on varieties, behaved as if the theory *did* indeed exist, even if $\operatorname{char} k = p > 0$.

The usual sheaf cohomology on the Zariski topology is far too coarse: for a smooth affine curve $X/\mathbb{F}_q$, its "Zariski" cohomology with constant coefficients vanishes in degree > 0. Further, Weil predicts a "Lefschetz formula" in terms of the geometric Frobenius morphism, which counts the number of points on the variety over $\mathbb{F}_q$. However, Frobenius is not a continuous map on spaces, but an arithmetic, Galois-theoretic one lying in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, and classical sheaf cohomology has no mechanism to account for this. Thus, some other theory, with coefficients in $\mathbb{Q}_\ell$, ends up being necessary.

2.1 Preliminaries on sites and sheaves

2.1.1 Derived functors

We will also need to talk a bit about derived functors before giving a proper definition of cohomology later on. Recall that a category C is called *additive* if each hom set $\mathrm{Hom}_{\mathsf{C}}(A, B)$ has the structure of an abelian group, with bilinear compositions

$$\mathrm{Hom}_{\mathsf{C}}(A, B) \times \mathrm{Hom}_{\mathsf{C}}(B, C) \to \mathrm{Hom}_{\mathsf{C}}(A, C),$$

and it has a zero object and direct sums.

If C is an additive category, we will call a sequence

$$0 \to A \to B \xrightarrow{\alpha} C$$

in C *exact* if for all objects T in C, the sequence of abelian groups

$$0 \to \mathrm{Hom}(T, A) \to \mathrm{Hom}(T, B) \to \mathrm{Hom}(T, C)$$

is exact. In this case, A is called the *kernel* of α. Likewise, a sequence

$$A \xrightarrow{\beta} B \to C \to 0$$

is exact if

$$0 \to \mathrm{Hom}(C, T) \to \mathrm{Hom}(B, T) \to \mathrm{Hom}(A, T)$$

is exact for all T in C, and C is called the *cokernel* of β.

Suppose C is a category in which every morphism has both a kernel and a cokernel, and let $\alpha : A \to B$ be a morphism in C. We will call the kernel of the cokernel of α is called the *image* of α, $\mathrm{im}(\alpha)$, and the cokernel of the kernel of α the *co-image* of α, $\mathrm{coim}(\alpha)$ There is always a canonical morphism $\mathrm{coim}(\alpha) \to \mathrm{im}(\alpha)$.

The category C is called *abelian* if it is additive, all kernels and cokernels exist, and for all morphisms f in C, the canonical map $\mathrm{Coim}(f) \to \mathrm{Im}(f)$ is an isomorphism. For the time being, we will assume all our categories are abelian.

If C is an abelian category, we will call an object I of C *injective* if the hom functor $\mathrm{Hom}_{\mathsf{C}}(-, I)$ is exact (recall this is automatically left exact, so one just has to check exactness at one place). We say C *has enough injectives* if for every object A of C, there is a monomorphism $A \to I$ into an injective object I of C. Now let $F : \mathsf{C} \to \mathsf{D}$ be a left exact functor (again with both categories being abelian). So, given a short exact sequence

$$0 \to A \to B \to C \to 0$$

in C, we get an exact sequence $0 \to F(A) \to F(B) \to F(C)$ in D. Since we are trying to do (co)homology, it might be nice to try extending that last sequence to a long exact sequence. For an object A of C, an *injective resolution* of A is a long exact sequence

$$0 \to A \to I^0 \xrightarrow{d^0} I^1 \to \cdots \to I^r \xrightarrow{d^r} I^{r+1} \to \cdots,$$

with each of the I^r's an injective object of C. For short hand, we will denote this complex by $A \to I^\bullet$. The following lemma shows that, in fact, injective resolutions always exist in abelian categories with enough injectives.

Lemma 2.1. *If A is an object of C, and C has enough injectives, then there exists an injective resolution $A \to I^\bullet$.*

Proof. C has enough injectives, so in particular, there is some injective object I^0 admitting a monomorphism $A \to I^0$. In other words, we automatically have an exact sequence

$$0 \to A \to I^1.$$

Now let $C^1 = \operatorname{coker}(M \to I^0)$. Again, since C has enough injectives, we have a monomorphism

$$0 \to C^1 \to I^1,$$

where I^1 is injective. Now we have an exact sequence

$$0 \to A \to I^0 \to I^1.$$

Now we just continue inductively by letting $C^n = \operatorname{coker}(B^{n-1} \to I^{n-1})$, and continuing in this way proves the lemma. □

Given a left exact functor $F : \mathsf{C} \to \mathsf{D}$ of abelian categories and an injective resolution $A \to I^\bullet$, applying F gives rise to a new complex

$$F(I^0) \xrightarrow{d^0} F(I^1) \xrightarrow{d^1} F(I^2) \to \cdots,$$

which we denote by $F(I^\bullet)$. This may no longer be exact, so it would be nice to have some way to measure the "failure" of exactness at a particular place in the sequence. We define the ith cohomology of the sequence to be

$$H^i(F(I^\bullet)) := \ker(F(d^i))/\operatorname{im}(F(d^{i-1})),$$

and given that the sequence might not be exact, these group may be nonzero. The following lemma will finally allow us to define derived functors:

Lemma 2.2. *Let A and B be objects of a category C, and let $A \to I^\bullet$ and $B \to J^\bullet$ be injective resolutions. Given a morphism $\varphi : A \to B$ in C, there is an extension to a map of complexes*

$$\begin{array}{ccc} A & \longrightarrow & I^\bullet \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi^\bullet} \\ B & \longrightarrow & J^\bullet \end{array}$$

Further, given a left exact functor $F : \mathsf{C} \to \mathsf{D}$, the morphism

$$H^i(F(\varphi^\bullet)) : H^i(F(I^\bullet)) \to H^i(F(J^\bullet))$$

is independent of the choice of $\varphi^\bullet$.

Proof. The first part is essentially just a diagram chase. We have maps $A \to I^0$ and $B \to J^0$, which are both monomorphisms, so in particular each has a left inverse. Then we can extend φ to a map $\varphi^0 : I^0 \to J^0$ by composing with the $B \to J^0$ and the left inverse of $A \to I^0$. Now, this induces a map on cokernels $\text{coker}(I^0 \to I^1) \to \text{coker}(J^0 \to J^1)$, and since J^1 is injective, this extends to a map $\varphi^1 : I^1 \to J^1$. Repeating inductively proves the first part.

For the second part, we first want to check that the objects $H^i(F(I^\bullet))$ are well-defined. By the first part (or the previous lemma), given two injective resolutions $A \to I^\bullet$ and $A \to J^\bullet$, there is a morphism $\text{id}^\bullet$ extending the identity map $\text{id} : A \to A$, and the maps $H^i(F(I^\bullet)) \to H^i(F(J^\bullet))$ on cohomology it defines are isomorphisms, independent of the choice of $\text{id}^\bullet$. Now for each object A of C, fix an injective resolution. For objects A and B, say the resolutions are $A \to I^\bullet$ and $B \to J^\bullet$. Then given a morphism $\varphi : A \to B$ this gives rise to a well-defined morphism of complexes $H^i(F(I^\bullet)) \to H^i(F(J^\bullet))$.

Now it remains to show that this morphism is independent of choice of resolutions. We call two morphisms $\alpha^\bullet, \beta^\bullet : I^\bullet \to J^\bullet$ of complexes *homotopic* if there exists a *homotopy* between them, i.e., a family of morphisms $k^r : I^r \to J^{r-1}$ such that for all i,

$$\alpha^i - \beta^i = d^{i-1} \circ k^i + k^{i+1} \circ d^i$$

(the name "homotopy" for such a family comes from algebraic topology). Now note that, for any $x \in \ker(d^i)$, $\alpha^i(x) - \beta^i(x) = d^{i-1}(k^i(x))$, and so is in $\text{im}(d^{i-1})$. Hence $\alpha(x)$ and $\beta(x)$ have the same image in $H^i(J^\bullet)$, so homotopic morphisms induce the same morphism on cohomology. □

The proof showed that taking the cohomology $H^i(F(I^\bullet))$ is a functor, and is independent of choice of injective resolution up to isomorphism. So, given a left exact functor $F : \mathsf{C} \to \mathsf{D}$, we define the *right derived functor* of F (after choosing injective resolutions) for an object A of C and injective resolution $A \to I^\bullet$ to be

$$(R^i)(A) := H^i(F(I^\bullet)).$$

2.1.2 Étale morphisms

An apparently large goal of this thesis is to introduce the theory of étale cohomology, although we have yet to mention whatsoever what "étale" even means. We first introduce étale morphisms geometrically in the context of varieties over an algebraically closed field k. Let W, V be nonsingular algebraic varieties over k.

Definition 2.3. A regular morphism $f : W \to V$ is called *étale* at a point $P \in W$ if the induced map $df : T_P(W) \to T_{f(P)}(V)$ on tangent spaces is an isomorphism. f is étale if it is étale at every point of W.

By this definition, it is clear that an étale morphism should be something like an

algebraic analogue a local isomorphism of manifolds (it will turn out that they are also analogous to unramified extensions of number fields). Of course, we would like to extend this definition to at least include arbitrary varieties over k. Recall that given a local ring $\mathcal{O}$ with maximal ideal $\mathfrak{m}$, one can associate a graded ring via the filtration $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots$ ([Eis95]) by

$$\mathrm{gr}_{\mathfrak{m}}\mathcal{O} := (\mathcal{O}/\mathfrak{m}) \oplus (\mathfrak{m}/\mathfrak{m}^2) \oplus \cdots .$$

Any local homomorphism of local rings $A \to B$ then also induces a homomorphism of associated graded rings $\mathrm{gr}_{\mathfrak{m}_A}(A) \to \mathrm{gr}_{\mathfrak{m}_B}(B)$.

Proposition 2.4. *Let $A \to B$ be a local homomorphism. Then the induced map on associated graded rings $gr_{\mathfrak{m}_A}(A) \to gr_{\mathfrak{m}_B}(B)$ is an isomorphism if and only if the induced map on completions $\hat{A} \to \hat{B}$ is an isomorphism.*

Proof. Recall that the completions of A and B are defined by taking inverse limits over the same filtration that was used to define the associated graded ring. For instance,

$$\hat{A} = \varprojlim_k A/\mathfrak{m}_A^k.$$

For the converse, note that $\mathrm{gr}_{\mathfrak{m}}(A) = \mathrm{gr}_{\mathfrak{m}}(\hat{A})$. Then for the forward direction, we just need to show that for each i, $A/\mathfrak{m}_A^i \cong B/\mathfrak{m}_B^i$. Now note that since we have an isomorphism of graded rings, the degree i parts of each graded ring is also an isomorphism, i.e.,

$$\mathfrak{m}_A^i/\mathfrak{m}_A^{i+1} \xrightarrow{\sim} \mathfrak{m}_B^i/\mathfrak{m}_B^{i+1}$$

via the degree-i component map.

We will proceed by induction. For $i = 0$, we get that $A/\mathfrak{m}_A \cong B/\mathfrak{m}_B$. Assume by induction that for all $i > 0$, $A/\mathfrak{m}_A^i \cong B/\mathfrak{m}_B^i$. For each $i \geq 0$, there is a commutative diagram of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{m}_A^i/\mathfrak{m}_A^{i+1} & \longrightarrow & A/\mathfrak{m}_A^{i+1} & \longrightarrow & A/\mathfrak{m}_A^i & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{m}_B^i/\mathfrak{m}_B^{i+1} & \longrightarrow & B/\mathfrak{m}_B^{i+1} & \longrightarrow & B/\mathfrak{m}_B^i & \longrightarrow & 0
\end{array}$$

Since the vertical map $\mathfrak{m}_A^i/\mathfrak{m}_A^{i+1} \xrightarrow{\sim} \mathfrak{m}_B^i/\mathfrak{m}_B^{i+1}$ is an isomorphism. By induction, the map $A/\mathfrak{m}_A^i \xrightarrow{\sim} B/\mathfrak{m}_B^i$ is an isomorphism as well. Then by the five lemma, the middle vertical map $A/\mathfrak{m}_A^{i+1} \to B/\mathfrak{m}_B^{i+1}$ is an isomorphism as well. Hence by induction, $A/\mathfrak{m}_A^i \cong B/\mathfrak{m}_B^i$ for all i. Passing to inverse limits, we get the result. □

For general varieties over k, we can take the following definition:

Definition 2.5. A regular map $f : W \to V$ *étale* at $P \in W$ if the map $\hat{\mathcal{O}}_{V,f(P)} \to \hat{\mathcal{O}}_{W,P}$ on completed local rings induced by f is an isomorphism.

By the last proposition, this is equivalent to checking the isomorphism on tangent cones. For nonsingular varieties, this definition thus agrees with the old one. For varieties over an arbitrary field k, we say that $f : W \to V$ is *étale* at $P \in W$ if for some algebraic closure $\overline{k}$ of k, the map $\overline{f} : W_{\overline{k}} \to V_{\overline{k}}$ is étale at the points of $W_{\overline{k}}$ mapping to P.

For general schemes, we will have to translate everything to commutative algebra. Recall that an A-algebra $A \to B$ is *flat* if the functor $B \otimes_A -$ is exact.

Definition 2.6. A morphism $f : X \to Y$ of schemes is called *flat* if the local homomorphisms $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ are flat for all $x \in X$.

The main idea (geometrically) behind flat morphisms is that the fibers of points should not "jump" in dimension. If f is flat, then in fact we have that $\dim f^{-1}(y) = \dim X - \dim Y$ for all closed $y \in Y$ for which the fiber is nonempty (see [CITE Milne étale cohomology book]). If $f : \operatorname{Spec} B \to \operatorname{Spec} A$ is a map of affine schemes, the condition of being flat says that $\dim_{A/\mathfrak{m}} B/\mathfrak{m}B$ is independent of choice of maximal ideal $\mathfrak{m} \subseteq A$.

Definition 2.7. A local homomorphism $f : A \to B$ of local rings is called *unramified* if $f(\mathfrak{m}_A) = \mathfrak{m}_B$ and $B/\mathfrak{m}_B$ is a finite, seperable extension of $A/\mathfrak{m}_A$.

In particular, this agrees with the definition of ramification in algebraic number theory through the lens of discrete valuation rings. Similarly to the situation for flatness, we will call a morphism $f : X \to Y$ of schemes *unramified* if the homomorphisms $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ are unramified for all $x \in X$. If $f : X \to Y$ is of finite type, it turns out that f is unramified if and only if the tangent sheaf $\Omega_{X/Y}$ is zero.

Now we can define étale morphisms for any scheme we want.

Definition 2.8. We will call a morphism $f : X \to Y$ of schemes *étale* if it is both flat and unramified.

For varieties, this definition agrees with the old one.

Proposition 2.9. *Let $f : X \to Y$ be a morphism of varieties over an algebraically closed field k. Then the "geometric" and "algebraic" definitions of étale coincide.*

Proof. See [Mil80] □

2.1.3 Sites and Sheaves

In order to properly define a theory of étale cohomology on schemes, it is necessary to obtain a finer topology on schemes than the Zariski topology which is standard in algebraic geometry. In effect, we will relax the condition that a covering should consist of subsets of a scheme.

Definition 2.10. Let C be a category, and for each object U of C, suppose we have a set of families of maps $(U_i \to U)_{i\in I}$, which we will call the "coverings" of U. This system of coverings is called a *Grothendieck topology* if the following conditions are satisfied:

(i) for any covering $(U_i \to U)_{i\in I}$, and any morphism $V \to U$ in C, the fiber products $U_i \times_U V$ exist and together define a covering of V.

(ii) given a covering $(U_i \to U)_{i\in I}$, if for each $i \in I$, $(V_{ij} \to U_i)_{j\in J_i}$ is a covering of U_i, then the collection $(V_{ij} \to U)_{i\in I, j\in J_i}$ is also a covering of U.

(iii) for any U in C, the "identity covering" $(U \xrightarrow{\text{id}} U)$ consisting of a single map is a covering of U.

Definition 2.11. A *site* is a category C along with a Grothendieck topology on C.

If $\mathbb{T}$ is a site, then $\mathsf{Cat}(\mathbb{T})$ will denote the underlying category of $\mathbb{T}$. A *presheaf* on a site $\mathbb{T}$ is a contravariant functor $F : \mathsf{Cat}(\mathbb{T}) \to \mathsf{C}$ to some category C. Hence a presheaf on a site is not dependent on the coverings. A *sheaf* on a site $\mathbb{T}$ is a presheaf F which satisfies the sheaf condition:

(a) for every covering $(U \to U_i)_{i\in I}$, the equalizer diagram

$$F(U) \to \prod_{i\in I} F(U_i) \rightrightarrows \prod_{i,j} F(U_i \times_U U_j)$$

is exact.

As a familiar example, if X is a topological space, and $\mathsf{Open}(X)$ is the category consisting of open sets of X, then the families $(U_i \to U)$ such that $\{U_i\}$ is an open covering of U is a Grothendieck topology on $\mathsf{Open}(X)$. Hence a sheaf on this site is just the usual definition of a sheaf on a topological space X. If X is a scheme with the Zariski topology, this site is called the *Zariski site* on X, and denoted X_{zar}

Definition 2.12. Let X be a scheme. Let Et/X be the category whose objects are the étale morphisms $U \to X$ and whose arrows are the morphisms of X-schemes $U \to V$. The *étale site* X_{et} is a site on Et/X whose coverings are the surjective families of étale morphisms $(U_i \to U)$ in Et/X. This can be extended to the *big étale site* whose underlying category is Sch_X.

Note that that a sheaf F on X_{et} defines by restriction a sheaf on U_{zar} for every $U \to X$ which is étale. Then the following gives an easier way to check if a given presheaf is a sheaf on X_{et} :

Proposition 2.13. *If F is a presheaf on X_{et}, and F satisfies the the sheaf condition for Zariski open coverings and for étale open coverings $V \to U$ with V and U affine, then F is a sheaf on X_{et}.*

Proof. If F satisfies the sheaf condition for Zariski open coverings, then we immediately

get that $F(\coprod u_i) = \prod F(U_i)$. Note also that

$$(\coprod U_i) \times_U (\coprod U_i) = \coprod_{i,j \in I} (U_i \times_U U_j),$$

so the sequence in the sheaf condition is isomorphic to the sequence coming from a single morphism $(\coprod U_i \to U)$. A finite disjoint union of affine schemes is affine, so the proposition holds for finite coverings.

Let $f : U' \to U$ be the morphism $\coprod U'_j \to U$, where $(U'_j \to U)_{j \in I}$ is a covering, and write U as a union of open affine schemes U_i. Then $f^{-1}(U_i)$ is a union of open affine schemes $f^{-1}(U_i) = \bigcup U'_{ik}$. Each $f(U'_{ik})$ is open in U_i, and U_i is (quasi-)compact, so there is a finite set K_i such that $(U'_{ik} \to U_i)_{k \in K_i}$ is a covering. Continuing in this way, we can write $U = \bigcup U_i$ and $U' = \bigcup U'_{ik}$ as unions of open affine schemes such that for any i, $(U'_{ik} \to U_i)_{k \in K_i}$ is a finite covering of U_i. Consider the diagram

$$\begin{array}{ccccc}
F(U) & \longrightarrow & F(U') & \rightrightarrows & F(U' \times_U U') \\
\downarrow & & \downarrow & & \downarrow \\
\prod_i F(U_i) & \rightrightarrows & \prod_i \prod_k F(U'_{ik}) & \rightrightarrows & \prod_i \prod_{k,l} F(U'_{ik} \times_U U'_{il}) \\
\downarrow\downarrow & & \downarrow\downarrow & & \\
\prod_{i,j} F(U_i \cap U_j) & \longrightarrow & \prod_{i,j} \prod_{k,l} F(U'_{ik} \cap U'_{jl}) & &
\end{array}$$

From the Zariski condition, the two columns are exact, and from the second condition, the middle row is a product of exact sequences, and so is exact. Then $F(U) \to F(U')$ is injective. Hence the bottom row is injective, and by a diagram chase, the top row must be exact. □

Next, let's turn to some examples of sheaves on X_{et}. For any $U \to X$ which is étale, define $\mathcal{O}_{X_{\mathsf{et}}}(U) := \gamma(U, \mathcal{O}_U)$. Then by the previous proposition and Proposition 2.18 in [Mil80], $\mathcal{O}_{X_{\mathsf{et}}}$ forms a sheaf on X_{et}, called the *structure sheaf* on X_{et}.

Now let Z be an X-scheme. Then 2hom-sets give us a contravariant functor $F : \mathsf{Et}/X \to \mathsf{Set}$, given by sending $U \mapsto \mathrm{Hom}_X(U, Z)$. This is in fact a sheaf of sets on X_{et}. If $Z = \operatorname{Spec} C$ is affine, then again by Proposition 2.18 in [Mil80], the sequence

$$\mathrm{Hom}_{A-\mathsf{alg}}(C, A) \to \mathrm{Hom}_{A-\mathsf{alg}}(C, B) \rightrightarrows \mathrm{Hom}_{A-\mathsf{alg}}(C, B \otimes_A B)$$

is exact. THe sheaf condition also clearly holds for Zariski open coverings, so by Proposition 2.13, F is a sheaf.

As a last example for now, let $\mathcal{M}$ be a sheaf of coherent $\mathcal{O}_X$-modules on X_{zar}, i.e., the

usual coherent sheaves in algebraic geometry. For every étale map $f : U \to X$, pulling back gives a coherent $\mathcal{O}_U$-module $f^*\mathcal{M}$ on U_{zar}. We can form a presheaf $U \mapsto \Gamma(U, f^*\mathcal{M})$ on X_{et}, which we denote $\mathcal{M}^{\mathsf{et}}$. This is in fact a sheaf (see [Mil]).

It is also necessary to talk about stalks of an étale (pre)sheaf. Let X be a scheme and let F be a presheaf on X_{et}.

Definition 2.14. The *stalk* of F at a geometric point $x \to X$ is

$$F_x := \varinjlim_{(U,u)} F(U),$$

with the limit taken ocer all the étale neighborhoods of x.

Given a scheme X, it makes sense to talk about the category of presheaves on X_{et}; this is just the functor category between $(\mathsf{Et}/X)^{\mathsf{op}}$ to Ab, which we shall denote by $\mathsf{PreSh}(X_{\mathsf{et}})$ Strictly speaking, Et/X is not a small category, and so taking the functor category may cause certain problems (for instance, hom-sets may not actually be sets anymore, which is required for the definition of a category), but we ignore these for now. $\mathsf{PreSh}(X_{\mathsf{et}})$ is in fact an abelian category: a sequence

$$\cdots \to F \to G \to H \to \cdots$$

of functors to Ab is exact if and only if

$$\cdots \to F(U) \to G(U) \to H(U) \to \cdots$$

is exact for all U in Et/X, and since Ab is an abelian category, so is $\mathsf{PreSh}(X_{\mathsf{et}})$.

We now define the category of étale sheaves of abelian groups on X, $\mathsf{Sh}(X_{\mathsf{et}})$, to be the full subcategory of $\mathsf{PreSh}(X_{\mathsf{et}})$ whose objects are the sheaves of abelian groups on X_{et}. $\mathsf{Sh}(X_{\mathsf{et}})$ is clearly additive, but we will now show that it, like $\mathsf{PreSh}(X_{\mathsf{et}})$, is abelian. Note that a homomorphism of sheaves will just be a natural transformation of functors.

Lemma 2.15. *Let*

$$0 \to F' \to F \to F'' \to 0$$

be a sequence of sheaves of abelian groups on X_{et}. Then the sequence is exact in $\mathsf{Sh}(X_{\mathsf{et}})$ if and only if the sequence

$$0 \to F'_x \to F_x \to F''_x \to 0$$

on stalks is exact for each geometric point $x \to X$.

Proof. See [Mil], Chapter 7. □

Proposition 2.16. *The category $\mathsf{Sh}(X_{\mathsf{et}})$ is abelian.*

Proof. Let $\alpha : F \to G$ be a morphism. The lemma showed that, for any geometric point $x \to X$, the stalk functor $(-)_x : \mathsf{Sh}(X_{\mathsf{et}}) \to \mathsf{Set}$ is exact, and so preserves kernels

and cokernels. In Ab, we have that for any morphism f, $\mathrm{coim}(f) = \mathrm{im}(f)$. Hence the map from the co-image of a morphism to its image is an isomorphism because it is on stalks. $\square$

Just as in the case of usual sheaves on topological spaces, not all presheaves on a site $\mathbb{T}$ are sheaves. But, as before, there is a way to associate a sheaf to any presheaf in a unique way.

Definition 2.17. Let $\mathbb{T}$ be a site, and let $F \to F^+$ be a homomorphism from a presheaf F to a sheaf F^+ on $\mathbb{T}$. F^+ is called the *sheafification* of F if all other homomorphisms from F to a sheaf on $\mathbb{T}$ factor uniquely through $F \to F^+$. In other words, $\mathrm{Hom}(F, G) \cong \mathrm{Hom}(F^+, G)$ for all sheaves G.

To wrap up our basic discussion of étale sheaves, it is necessary to talk about direct and inverse images of sheaves.

Definition 2.18. Let $f : X \to Y$ be a morphism of schemes, and let F be a presheaf on X_{et}. For an étale morphism $U \to X$, define

$$f_*F(U) := F(U \times_Y X).$$

Since the base change of an étale morphism is étale (see [Mil] Proposition 3.3), $U \times_Y X \to X$ is étale. Hence f_*F becomes a presheaf on X_{et}.

For a scheme X over S, let $X_Y = X \times_S Y$ be the scheme over Y. Suppose F is a sheaf. Then $X \mapsto X_Y$ is a functor taking étale maps to étale maps (as well as surjective families to surjective families, and fiber products over S to fiber products over Y). Let $(U_i \to U)$ be a surjective family of étale maps in Et/S. Then from what we just said, $(U_{iY} \to U_Y)$ is also a surjective family of étale maps in Et/Y, and so the sheaf sequence

$$F(U_Y) \to \prod F(U_{iY}) \rightrightarrows \prod F(U_{iY} \times_Y U_{jY})$$

is exact. But by definition, this is just the sequence

$$(f_*F)(U) \to \prod (f_*F)(U_i) \rightrightarrows \prod (f_*F)(U_i \times_S U_j),$$

and so this is also exact, and hence f_*F satisfies the sheaf condition. Thus we have just shown that whenever F is a sheaf, so is f_*F.

The functor $f_* : \mathsf{PreSh}(X_{\mathsf{et}}) \to \mathsf{PreSh}(Y_{\mathsf{et}})$ is exact, so the restriction to $f_* : \mathsf{Sh}(X_{\mathsf{et}}) \to \mathsf{Sh}(Y_{\mathsf{et}})$ is left exact.

For inverse images of sheaves, we will define a left adjoint to the functor f_*. As before, let $f : X \to Y$ be a morphism of schemes, and let F be a presheaf on Y_{et}. For $V \to X$ étale, define

$$F'(V) := \varinjlim F(U),$$

where the limit is over diagrams

$$\begin{array}{ccc} V & \longrightarrow & U \\ \downarrow & & \downarrow \\ X & \longrightarrow & Y \end{array}$$

where $U \to X$ is étale. It is not hard to show that for any presheaf G on X,

$$\mathrm{Hom}_{X_{\mathsf{et}}}(F', G) \cong \mathrm{Hom}_{Y_{\mathsf{et}}}(F, f_* G).$$

However, F' may not be a sheaf, even if F is indeed a sheaf. Nonetheless, we can preserve the isomorphism by sheafification. Define $f^* F := F'^{+}$. Then for any sheaf G on X_{et}, we have that

$$\mathrm{Hom}_{X_{\mathsf{et}}}(f^* F, G) \cong \mathrm{Hom}_{X_{\mathsf{et}}}(F', G) \cong \mathrm{Hom}_{Y_{\mathsf{et}}}(F, f_* G),$$

and thus f^* is a left adjoint functor to $f_* : \mathsf{Sh}(X_{\mathsf{et}}) \to \mathsf{Sh}(Y_{\mathsf{et}})$.

Since we talked about derived functors earlier, and $\mathsf{Sh}(X_{\mathsf{et}})$ is an abelian category, it would be nice if it had enough injectives as well. The following proposition shows that this is indeed the case:

Proposition 2.19. *Every sheaf F on X_{et} can be embedded into an injective sheaf.*

Proof. For every $x \in X$, choose a geometric point $i_x : \overline{x} \to X$ with image x and an embedding $F_{\overline{x}} \hookrightarrow I(x)$ into an abelian group $I(x)$ (since Ab has enough injectives). For any morphism f, f^* is an exact functor, so f_* preserves injectives (see [Mil]). Hence $\mathcal{I}^X := i_{x*}(I(x))$ is injective as well, and $\mathcal{I} := \prod \mathcal{I}^x$ is an injective sheaf. □

2.1.4 The étale fundamental group

Before moving onto cohomology, we will briefly cover the *étale fundamental group*. For X a variety or scheme, this group will classify the finite étale coverings of X in an manner analogous to the way the familiar topological fundamental group classifies covering spaces of a topological space.

Recall that for X a topological space, which is assumed to be path-connected and semi-locally simply connected (see [Hat01]), with a fixed base point $x \in X$, the topological fundamental group $\pi_1(X, x)$ is the group of homotopy classes of closed paths in X based at x. A map $p : E \to X$ is a covering space is for every $x \in X$, there is an open neighborhood U such that $p^{-1}(U)$ is a disjoint union of open sets U_i which are each homeomorphic to U via p. A map of covering spaces $E \to X$ and $E' \to X$ is a map $E \to E'$ commuting in the obvious way over X. For any X, there exists a unique (up to isomorphism) simply connected covering space $\pi : \widetilde{X} \to X$ satisfying the following universal property: for a fixed $\widetilde{x}$, and any covering space $E \to X$ with point $e \in E$

mapping to $x \in X$, there exists a unique map $\widetilde{X} \to E$ sending $\widetilde{x} \mapsto e$. This $\widetilde{X} \to X$ is called the *universal covering space* of X.

If we let $\mathsf{Cov}(X)$ denote the category of covering spaces of X (with finitely many connected components), we can define a functor $F : \mathsf{Cov}(X) \to \mathsf{Set}$ sending a covering space $p : E \to X$ to the set $p^{-1}(x)$. It turns out that this functor is representable by $\widetilde{X}$, in other words that

$$F(E) \cong \mathrm{Hom}_X(\widetilde{X}, E),$$

where the isomorphism is at the level of functors. If $\mathrm{Aut}_X(\widetilde{X})$ denotes the group of automorphisms of $\widetilde{X}$ in $\mathsf{Cov}(X)$, we can let this act on $\widetilde{X}$ in the obvious way on the right. Thus it acts on $\mathrm{Hom}_X(\widetilde{X}, E)$ on the right by

$$\alpha f := f \circ \alpha$$

for $\alpha \in \mathrm{Aut}_X(\widetilde{X}), f \in \mathrm{Hom}_X(\widetilde{X}, E)$. Then F is a functor from $\mathsf{Cov}(X)$ to the category of $\mathrm{Aut}_X(\widetilde{X})$-sets.

But there is an isomorphism $\mathrm{Aut}_X(\widetilde{X}) \xrightarrow{\sim} \pi_1(X, x)$ (again, see [Hat01]). Hence the functor F defines an equivalence of categories between $\mathsf{Cov}(X)$ and the category $\pi_1(X, x) - \mathsf{Set}^{\mathsf{fin}}$ of $\pi_1(X, x)$-sets with finitely many orbits.

Unfortunately, if X is a connected scheme (or even a variety), we cannot define such a fundamental group using homotopy, as path-connectedness in the Zariski topology does not behave nicely. Instead, we try to give an algebraic analogue of the characterization of $\pi_1(X, x)$ via covering spaces. Let $\overline{x} \to X$ be a geometric point. A finite étale map $\pi : Y \to X$ is open and closed,, so it must be surjective when Y is nonempty. Given X a variety over an algebraically closed field k and $\pi : Y \to X$ finite étale, the fiber $\pi^{-1}(x)$ of each point $x \in X$ has the same number of points, as well as a neighborhood $U \to X$ such that $Y \times_X U$ is a disjoint union of open subvarieties U_i which are each isomorphic to U via $\pi \times 1$; in other words, the coverings for the étale site which we constructed previously really *are* analogous to covering spaces in topology.

Let FEt/X denote the category whose objects are the finite étale coverings of X. We can define a functor $F : \mathsf{FEt}/X \to \mathsf{Set}$ sending a covering $\pi : Y \to X$ to the set of $\overline{x}$-valued points of Y over x, so that $F(Y) = \mathrm{Hom}_X(\overline{x}, Y)$. Now, if we were to follow an exact analogy with the topological characterization, we would want to define the universal covering space of X to be the object representing F. Unfortunately for us, there usually is no such object. Instead, the functor F is what is called "pro-representable:" there is a projective system $(X_i)_{i \in I}$ of finite étale coverings of X which are indexed by a directed set I, such that

$$F(Y) = \varinjlim_{i \in I} \mathrm{Hom}(X_i, Y).$$

We thus define $\widetilde{X} := (X_i)_i$ and call it "the universal covering space of X". It is in fact

possible ot choose $\widetilde{X}$ so that each X_i has degree $|\operatorname{Aut}_X(X_i)|$, which we will call being *Galois* over X. Any map $X_j \to X_i$ with $i \leq j$ induces a homomorphism $\operatorname{Aut}_X(X_j) \to \operatorname{Aut}_X(X_i)$ in the obvious way, so we can define

$$\pi_1^{\text{et}}(X, \overline{x}) := \varprojlim \operatorname{Aut}_X(X_i).$$

The action of $\pi_1^{\text{et}}(X, \overline{x})$ on the right defines an action of $\pi_1^{\text{et}}(X, \overline{x})$ on $F(Y)$ on the left for each finite étale covering Y of X. Then finally: the functor F is an equivalence of categories between FEt/X and the category of finite discrete $\pi_1^{\text{et}}(X, \overline{x})$-sets. Hence $\pi_1^{\text{et}}(X, \overline{x})$ classifies the finite étale coverings of X in the same way as the topological fundamental group for a (nice enough) topological space.

Example 2.20. Let $\mathbb{A}^1$ be the affine line over an algebraically closed field k of characteristic 0. The finite étale coverings of $\mathbb{A}^1 \setminus \{0\}$ are the maps sending $t \to t^n$. As expected, there is no "biggest" one of these maps which would constitute a universal covering, so even in this simple case the prorepresentable characterization is needed. We have that

$$\operatorname{Aut}_X(X_i) = \mu_i(k),$$

which is the group of ith roots of unity in k. Thus

$$\pi_1^{\text{et}}(\mathbb{A}^1 \setminus \{0\}, \overline{x}) = \varprojlim \mu_i(k).$$

If we choose a compatible system of isomorphisms $\mathbb{Z}/i\mathbb{Z} \to \mu_i(k)$, we see that this is isomorphic to

$$\varprojlim \mathbb{Z}/i\mathbb{Z} \cong \hat{\mathbb{Z}}.$$

Example 2.21. Let $X = \operatorname{Spec} k$ for a field k. In this case, the étale coverings $Y \to X$ are the Spec's of finite étale k-algebras A. Hence we can just work in the (opposite) category Et/k of étale k-algebras. Choosing a geometric point of X amounts to a choice of a separably algebraically closed field K containing k. Define the functor $F : \mathsf{Et}/k \to \mathsf{Set}$ by $F(A) = \operatorname{Hom}_{k-\text{alg}}(A, K)$. Let $L := (L_i)_i$ be the projective system of all finite Galois extensions of k which are contained in K. Then

$$F(A) \cong \varinjlim \operatorname{Hom}(A, L_i).$$

Thus

$$\operatorname{Aut}_k(L) := \varprojlim \operatorname{Aut}_{k-\text{alg}}(L_i) = \varprojlim \operatorname{Gal}(L_i/k) = \operatorname{Gal}(\overline{k}/k),$$

where $\overline{k}$ is the separable algebraic closure of k in K. Further, this F defines an equivalence of categories from Et/k to the category of finite discrete $\operatorname{Gal}(\overline{k}/k) - sets$. Hence, this theory coverings contains the same information as the classical Galois theory of fields.

2.2 Cohomology

We now finally move to definitions of cohomology. The functor $\Gamma(X, -) : \mathsf{Sh}(X_{\mathsf{et}}) \to \mathsf{Ab}$ defined by $F \mapsto \Gamma(X, F)$ is left exact, so since we showed $\mathsf{Sh}(X_{\mathsf{et}})$ is an abelian category with enough injectives, we can define its derived functors. For a sheaf F, choose an injective resolution

$$0 \to F \to \mathcal{I}^0 \to \mathcal{I}^1 \to \cdots,$$

and apply the functor $\Gamma(X, -)$. Then we arrive at a complex which may no longer be exact.

Definition 2.22. The ith *étale cohomology* of X $H^i(X_{\mathsf{et}}, -)$ to be the right derived functor of $\Gamma(X, -)$. In other words, for every sheaf F, we have an abelian group $H^i_{\text{ét}}(X, F) := R^i(F)$.

For any sheaf F, we have that $H^0(X_{\mathsf{et}}, F) = \Gamma(X, F)$, which is immediate from the definition of derived functors. Also from the theory of derived functors, given a short exact sequence

$$0 \to F' \to F \to F'' \to 0$$

of sheaves, there is a corresponding (functorially) long exact sequence

$$0 \to H^0_{\text{ét}}(X, F') \to H^0_{\text{ét}}(X, F) \to H^0_{\text{ét}}(X, F'') \to H^1_{\text{ét}}(X, F') \to \cdots.$$

Now let $g : Y \to X$ be a morphism of schemes. Recall that for a sheaf F on Y_{et}, we defined the sheaf g_*F to be the sheaf on X_{et} such that

$$\Gamma(U, g_*F) = \Gamma(U \times_X Y, F).$$

The functor $g_* : \mathsf{Sh}(Y_{\mathsf{et}}) \to \mathsf{Sh}(X_{\mathsf{et}})$ is left exact, and so we can take right derived functors of it.

Definition 2.23. The *higher direct images* of F are the $R^r g_* F$, where the $R^r g_*$ are the right derived functors of g_*.

2.3 Tate modules and cohomology

In this section, we will finally relate the theory of étale cohomology to material we have seen so far. We will start with looking at the cohomology of projective curves, and eventually move on to cohomology for abelian varieties. We will begin by considering

the Kummer sequence. Let X be a scheme, and let $n \in \mathbb{Z}$ such that n is not divisible by char κ for any residue field κ of X. For instance, if X is a variety over $\mathbb{F}_p$, then p does not divide n. Define $\mathbb{G}_m$ to be the sheaf $\mathcal{O}_X^\times$; in other words, for an étale morphism $U \to X$, this is the sheaf sending $U \mapsto \Gamma(U, \mathcal{O}_U)^\times$. Now define $\mu_n := \ker(\mathbb{G}_m \overset{(-)^n}{\to} \mathbb{G}_m)$ to be the sheaf of nth roots of unity in $\mathbb{G}_m$. Then we get an exact sequence of sheaves, called the *Kummer sequence*:

$$0 \to \mu_n \to \mathbb{G}_m \overset{(-)^n}{\to} \mathbb{G}_m \to 0.$$

Proving this is indeed exact amounts to showing

$$0 \to \mu_n(\mathcal{O}_{X,x}) \to \mathcal{O}_{X,x}^\times \overset{(-)^n}{\to} \mathcal{O}_{X,x}^\times \to 0$$

is exact for every local ring $\mathcal{O}_{X,x}$ of X. This is clear except at the right end of the sequence, so we must show that every element of $\mathcal{O}_{X,x}^\times$ is an nth power. In other words, each element of $\mathcal{O}_{X,x}$ must satisfy $f(x) = x^n - 1$. But $f'(x) = nx^{n-1} \neq 0$ in the residue field of $\mathcal{O}_{X,x}$, so f splits in $\mathcal{O}_{X,x}[x]$ ([AM69]).

Let X be a complete connected nonsingular algebraic curve of genus g over an algebraically closed field k.

Theorem 2.24. $H^r_{\acute{e}t}(X, \mathbb{G}_m) = \begin{cases} \Gamma(X, \mathcal{O}_X^\times), & r = 0 \\ Pic(X), & r = 1 \\ 0 & r > 1 \end{cases}$

Proof. See [Mil] Theorem. 13.7 □

Theorem 2.25. *For any $n > 0$ such that* $\gcd(n, char\, k) = 1$, *we have*

$$H^r_{\acute{e}t}(X, \mu_n) = \begin{cases} \mu_n(k), & r = 0, \\ (\mathbb{Z}/n\mathbb{Z})^{2g}, & r = 1, \\ \mathbb{Z}/n\mathbb{Z}, & r = 2, \\ 0, & r > 0 \end{cases}$$

Proof. See [Mil] Proposition 14.3 □

Now, let us look back at the Kummer sequence, with ℓ a prime.

$$0 \to \mu_{\ell^n} \to \mathbb{G}_m \overset{(-)^n}{\to} \mathbb{G}_m \to 0.$$

Then we have a short exact sequence for cohomology:

$$0 \to H^1_{\text{ét}}(X, \mu_{l^n}) \to H^1_{\text{ét}}(X, \mathbb{G}_m) \to H^1_{\text{ét}}(X, \mathbb{G}_m) \to 0.$$

Hence we can identify

$$H^1_{\text{ét}}(X, \mu_{l^n}) \cong \text{Pic}(X)[\ell^n],$$

where the righthand side is the ℓ^n-torsion of $\text{Pic}(X)$. We also have that

$$\mu_n \cong \underline{\text{Hom}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m),$$

i.e., there is a duality between the sheaves μ_{ℓ^n} and $\mathbb{Z}/\ell^n\mathbb{Z}$. So, we get that

$$H^1_{\text{ét}}(X_{\overline{k}}, \mathbb{Z}_\ell(1)) = \varprojlim - \, H^1_{\text{ét}}(X_{\overline{k}}, \mu_{\ell^n}) \cong \varprojlim \text{Pic}(X_{\overline{k}})[\ell^n] = T_l(\text{Pic}(X_{\overline{k}})).$$

Recall that $\text{Pic}(X_{\overline{k}}) = \text{Jac(X)}$ Then by the above duality, we see that

$$H^1_{\text{ét}}(X_{\overline{k}}, \mathbb{Z}_l) \cong \text{Hom}_{\mathbb{Z}_\ell}(T_l(\text{Jac}(X)), \mathbb{Z}_\ell) = T_l(\text{Jac}(X))^\wedge.$$

Thus, taking Tate modules is essentially taking cohomology! In the case that $X = E$, an elliptic curve, Abel's theorem tells us that the 1st cohomology of E is in fact dual to $T_l(E)$ itself. A similar statement holds for Tate modules of abelian varieties, but we will not prove it here (See [Mil] Theorem 12.1 or [Rob21] for discussions and proofs).

Chapter 3

Galois representations

In this chapter, we give an introduction to Galois representations in number theory. A *Galois representation* is simply a representation of the absolute Galois group of a field k, i.e., a continuous homomorphism $\mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(V)$ for some vector space V. We will be most interested in the Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

$G_{\mathbb{Q}}$ is perhaps the most natural Galois group to study in the context of number theory, as it contains information about all number fields $K/\mathbb{Q}$. In fact, it is a profinite topological group: recall that one can define

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K/\mathbb{Q}),$$

with the inverse limit taken over finite normal subextensions of $\overline{\mathbb{Q}}/\mathbb{Q}$; topologically, a basis of open neighborhoods is given by the subgroups $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ with K running over subextensions of $\overline{\mathbb{Q}}/\mathbb{Q}$ that are finite over $\mathbb{Q}$.

The conjecture which we aim to introduce in these notes mainly concerns "global" representations, i.e., those of $G_{\mathbb{Q}}$. However, in the next chapter, we will return to study some distinguished subgroups of $G_{\mathbb{Q}_p}$, which will be important for some local conditions related to the conjecture (specifically, being "de Rham" at a prime l). For now, we will talk about some generalities of representations of profinite groups, and focus on some particular examples of representations of $G_{\mathbb{Q}}$.

3.1 Representations of Profinite Groups

Definition 3.1. A topological group G is called *profinite* if G is compact, and the identity element $1_G \in G$ has a system of neighborhoods made up of open normal subgroups.

As an obvious example, for any field k, its absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ is profinite. Further, any projective limit over a projective system of finite groups is profinite (see [Hid00] Proposition 2.1). Let PFGrp be the category of profinite groups, with morphisms being continuous group homomorphisms.

Let G be a profinite group, and let F be a field. Recall that a representation $\rho : G \to \mathrm{GL}(V)$, where V is an F-vector space, is called *reducible* if V has a proper nontrivial subspace which is invariant under G. A representation is called *irreducible* if it is not reducible. ρ is called *completely irreducible* if the induced representation $\rho_{\overline{E}} : G \to V \otimes_E \overline{E}$ is irreducible.

Let $F[G]$ denote the group ring of G over F. Consider the category of F-representations of G, $\mathsf{Rep}_F(G)$, whose objects are finite-dimensional F-vector space with a continuous action by G under the discrete topology, and whose morphisms are $F[G]$-linear maps. The *representation ring* of $\mathsf{Rep}_F(G)$, denoted $R_F(G)$, is the ring generated by $[R]$ for R an object of $\mathsf{Rep}_F(G)$, with the relation that $[R] = [R'] + [R'']$ if there is an exact sequence $0 \to R' \to R \to R'' \to 0$ of $F[G]$-modules. In fact, this is simply a particular case of a *Grothendieck group*, although we will not delve further into the general theory. It is not hard to check that this is in fact a ring with the product as the tensor product over F, i.e.,

$$[R_1] \cdot [R_2] = [R_1 \otimes_F R_2].$$

The multiplicative identity is simply the trivial G-module F, and the additive one is $[0]$, where 0 is the zero ring.

Let $H \subseteq G$ be a closed subgroup of finite index. For an object $R \in R_E(H)$, we define the *induced G-module* $\mathrm{Ind}_H^G R = \mathrm{Hom}_{F[H]}(F[G], R)$. We can regard $\mathrm{Ind}_H^G R$ as an $F[G]$-module by setting $g \cdot \phi(x) = \phi(xg)$ for $\phi \in \mathrm{Ind}_H^G R$. Thus we get a linear map $\mathrm{Ind}_H^G : R_F(H) \to R_F(G)$, as Ind_H^G preserves exact sequences. It is not hard to see that this further gives a functor $\mathrm{Ind}_H^G : \mathsf{Rep}_F(H) \to \mathsf{Rep}_F(G)$.

We can also talk about the forgetful functor $\mathrm{Res}_H^G : \mathsf{Rep}_F(G) \to \mathsf{Rep}_F(H)$. Then Ind_H^G and Res_H^G form an adjoint pair, i.e.,

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G V, W) \cong \mathrm{Hom}_H(V, \mathrm{Res}_H^G W)$$

for V in $\mathsf{Rep}_F(H)$ and W in $\mathsf{Rep}_F(G)$. This statement is one incarnation of *Frobenius reciprocity* (see [FH91]).

3.2 Class Field Theory and the GL_1 Story

To start, we will discuss one-dimensional Galois representations, which appear naturally in the context of class field theory. These will also give a nice occasion to briefly discuss the so-called *Langlands program*, which connects automorphic forms on the adele groups to certain Galois representations.

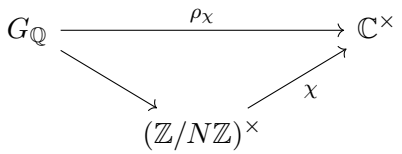
For any field k, a one dimensional Galois representation simply amounts to a homomorphism

$$G_{\mathbb{Q}} \to GL_1(k) \cong k^{\times}.$$

Recall that a *Dirichlet character* is a homomorphism

$$\chi_N : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Given that $G_\mathbb{Q}/G_{\mathbb{Q}(e^{2\pi i/N})} \cong \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/N})/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})$, this χ extends to a homomorphism



i.e., a one-dimensional Galois representation.

As another example, let p be a prime integer. By taking a projective limit, we arrive at the *p-adic cyclotomic character*

$$\chi := \varprojlim_n \chi_{p^n} : G_\mathbb{Q} \to \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Let K be a number field and let $\mathbb{A}_K$ be the ring of adèles for K. We define the *group of idèles* $I_K := \mathbb{A}_K^\times$. The *idèle class group* of K is the quotient $I_K/K^\times = \mathbb{A}_K^\times/K^\times$.

Theorem 3.2 (Artin Reciprocity (adelic version))**.** *For every number field K, there is a map*

$$\theta_K : \mathbb{A}_K^\times/K^\times \to Gal(K^{ab/K}).$$

Proof. See [Neu92] □

There is technically some information missing in the above statement, namely the exact characterization of $\ker \theta_K$; however, we won't need Artin reciprocity in its full power, at least for the time being, and just having the map θ_K suffices.

Let us briefly return to the topic of automorphic forms and representations. An automorphic form on $\mathrm{GL}_1(K)$, following our previous terse definition, should be a function $\mathrm{GL}_1(K)/K^\times \to \mathbb{C}$ satisfying some conditions. Hence an automorphic representation of $\mathrm{GL}_1(K)$ should be an irreducible subrepresentations of $\mathrm{GL}_1(\mathbb{A}_K)$ acting on the space of automorphic forms on $\mathrm{GL}_1(K)$ by right translation. $\mathrm{GL}_1(\mathbb{A}_K)$ is abelian, so a basic fact of representation theory tells us that such a representation should be one-dimensional, and thus spanned by exactly *one* nonzero automorphic form f. $\mathbb{C}f$ is invariant under right translation. So, we find that $f(xg) = \lambda_g f(x)$ for some λ_g and for all $x, g \in \mathrm{GL}_1(\mathbb{A}_K)$. Letting $x = 1$, we see that $\lambda_g f(1) = f(g)$, so

$$f(1)f(xg) = f(g)f(x).$$

Then we may simply scale things so that $f(1) = 1$, making f a homomorphism. Since f is invariant under $K^\times$, we also find that $K^\times \subseteq \ker f$.

The other properties of f being automorphic imply that f is continuous, and hence we get a continuous homomorphism

$$f : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times;$$

such a homomorphism is known as a *Hecke character,* which appear in class field theory. Thus every automorphic representation of $\mathrm{GL}_1(K)$ is spanned by a unique Hecke character, and it turns out that the converse holds as well. Hence we may identify "automorphic representations of $\mathrm{GL}_1(K)$" with "Hecke characters."

We will now show that we can get certain (compatible systems of) Galois representations from such objects, and this will be our first instance of recieving such representations from *automorphic* objects. For now, let $K = \mathbb{Q}$, and let f be a Hecke character. The restriction r of f to the finite places $\prod \mathbb{Z}_p^\times$ is a afinite order character, and the restriction of f to the Archimedean place $\mathbb{R}^+$ is of the form $x \mapsto x^a$ for some $a \in \mathbb{R}$. f is called *algebraic* if a is an integer.

Let α_∞ be the Hecke character which is trivial at the finite places and on $\mathbb{R}^+$ is given by the inclusion $\mathbb{R}^+ \hookrightarrow \mathbb{C}^\times$. Then a Hecke character is algebraic if and only if it is of the form $r\alpha_\infty^n$ for some finite order character r and some $n \in \mathbb{Z}$.

Now suppose f is a p-adic Hecke character, i.e., a continuous homomorphism $\mathbb{A}_K^\times / K^\times \to \overline{\mathbb{Q}}_p^\times$. Hence the restriction of f to $\mathbb{R}^+$ is trivial. The restriction of f to any of ther $\mathbb{Z}_p^\times$ is a continuous homomorphism $\mathbb{Z}_p^\times \to \overline{\mathbb{Q}}_p^\times$. In this situation, we call f algebraic if this restriction if of the form $x \mapsto x^n$ on a compact open subset of $\mathbb{Z}_p^\times$. Similarly to the former case, let α_p be the p-adic Hecke character that is trivial on $\mathbb{R}^+$ and $\prod_{l \neq p} \mathbb{Z}_l^\times$, and the restriction to $\mathbb{Z}_p^\times$ is the inclusion $\mathbb{Z}_p^\times \hookrightarrow \overline{\mathbb{Q}}_p^\times$. Then a p-adic Hecke character is algebraic if and only if it is of the form $r\alpha_p^n$ for some finite order character r and $n \in \mathbb{Z}$.

Now, let f be an algebraic Hecke character. Then by the above, we can write it as $f = r\alpha_\infty^n$. We can define an algebraic p-adic Hecke character by setting

$$f_p := r\alpha_p^n$$

(where we are identifiying the roots of unity in $\mathbb{C}$ and $\overline{\mathbb{Q}}_p^\times$). By the Artin map $\theta_\mathbb{Q}$, the p-adic Hecke character α_p corresponds to the cyclotomic character χ_p, and thus f_p corresponds to $r'\chi_p^n$, where r' is the character of $G_\mathbb{Q}$ corresponding to r.

Now, varying p lets us arrive at a *compatible system* of characters. In this one-dimensional case, this amounts to, for each prime p, a p-adic character ψ_p of $G_\mathbb{Q}$ such that at each place v, $\psi_p(\mathrm{Frob}_v)$ is independent of p. Given that the system of Dirichlet charactes $\{\chi_p\}_{p \text{ prime}}$ form a compatible system, so does $\{r'\chi_p^n\}_p$. Thus, as promised, starting with an automorphic representation, one can construct Galois representations. The story for general number fields is the same, but requires slightly more work, which we skip here. What we have worked out here is essentially the *global Langlands correspondence* for GL_1

3.3 Galois representations from elliptic curves

For our next example, let E be an elliptic curve over $\mathbb{Q}$ and let l be a prime integer. Recall that $E[m]$ denotes the group of m-torsion points of E. Then the multiplication by l maps on torsion,

$$E[l^{n+1}] \to E[l^n],$$

give an inverse system of groups and homomorphisms:

$$E[l] \leftarrow E[l^2] \leftarrow E[l^3] \leftarrow \cdots$$

Then we can take an inverse limit, and the result is the *Tate module* of E,

$$T_l(E) := \varprojlim_n E[l^n].$$

For any $m \in \mathbb{Z}$, we have that

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2,$$

so in particular

$$T_l(E) \cong \varprojlim_n (\mathbb{Z}/l^n\mathbb{Z})^2 = \mathbb{Z}_l \times \mathbb{Z}_l,$$

although the isomorphism depends on a choice of basis for each $E[l^n]$.

Now note that the action of $G_\mathbb{Q}$ on each $E[l^n]$ commutes with the multiplication-by-l maps: $G_\mathbb{Q}$ acts on the coordinates of E, and hence each $\sigma \in G_\mathbb{Q}$ gives an automorphism of $\mathrm{Pic}^0(E)$, by

$$\Big(\sum n_x(x)\Big)^\sigma = \sum n_x(x^\sigma).$$

Given that $E \cong \mathrm{Pic}^0(E)$ as we saw in the first chapter, the $G_\mathbb{Q}$ clearly commutes with the multiplication-by-l^n map on E for every n. Hence the actions must commute on E as well, and the $G_\mathbb{Q}$-action restricts to the torsion groups, giving homomorphisms

$$G_\mathbb{Q} \to \mathrm{Aut}(E[l^n])$$

for each n, with commuting diagrams

$$\begin{array}{ccc} & G_\mathbb{Q} & \\ \swarrow & & \searrow \\ \mathrm{Aut}(E[l^n]) & \longleftarrow & \mathrm{Aut}(E[l^{n+1}]) \end{array}$$

Thus the $G_\mathbb{Q}$-action extends to the Tate module, and $T_l(E)$ is indeed a $G_\mathbb{Q}$-module, meaning we have a homomorphism $G_\mathbb{Q} \to \mathrm{Aut}(T_l(E))$. Choosing a basis then gives a representation

$$\rho_{E,l} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_l) \subseteq \mathrm{GL}_2(\mathbb{Q}_l).$$

Another form we will use, in order to avoid the non-canonical choice of basis, is to exploit the natural map

$$\mathrm{Aut}(T_l(E)) \hookrightarrow \mathrm{Aut}(T_l(E)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l;$$

we define

$$V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

and note that $\rho_{E,l}$ extends to a homomorphism with target $\mathrm{Aut}(V_l(E))$.

Proposition 3.3. *The representation $\rho_{E,\ell}$ is irreducible.*

The proof of this statement is beyond the scope of this thesis, but it will be used later on in the next chapter. For more details, see [DS05], Chapter 9.

3.4 Representations from modular forms (weight 2)

We now briefly construct Galois representations associated to weight 2 cusp forms. The original construction is due to Shimura, although Deligne later gave a construction for $k > 2$ using étale cohomology (although we do not give it here).

Let $f \in S_2(N, \chi)$, and recall that the Hecke algebra contains the kernel of the eigenvalue map, denoted I_f, and that we defined

$$A_f = J_1(N)/I_f J_1(N)$$

Let $\mathcal{O}_f$ be the ring generated over $\mathbb{Z}$ be adjoining the Fourier coefficients of f. There is a natural isomorphism

$$\mathbb{T}_{\mathbb{Z}}/I_f \cong \mathcal{O}_f.$$

Under this, the Fourier coefficient $a_p(f)$ acts as $T_p + I_f$ on A_f. Further, $\chi(p)$ acts on A_f as $\langle p \rangle + I_f$. Taking the field of fractions of f, we get a number field which we denote by $\mathbb{K}_f$. The degree of this extension over $\mathbb{Q}$ is also the dimension d of A_f. As is the case with curves, (although we did not express Tate modules of abelian varieties in the cohomological lens), A_f has an l-adic Tate module:

$$T_\ell(A_f) = \varprojlim A_f[\ell^n] \cong \mathbb{Z}_l^{2d}.$$

Analogously to the case of elliptic curves, the action of $\mathcal{O}_f$ on A_f is defined on the ł-power torsion, and so extends to an action on the whole Tate module.

Lemma 3.4. *The map $\phi : Pic^0(X_1(N))[\ell^n] \to A_f[\ell^n]$ is surjective, and* $\ker \phi$ *is invariant under $G_{\mathbb{Q}}$.*

Proof. Multiplication by ℓ^n is surjective on $I_f J_1(N)$. Now take any $x \in A_f[\ell^n]$, and let $x = r + I_f J_1(N)$ for some $r \in J_1(N)$ such that $\ell^n r \in I_f J_1(N)$. Then by the surjectivity of multiplication by ℓ, there is some $r' \in I_f J_1(N)$ such that $\ell^n r = \ell^n r'$. Thus $r - r' \in$

$J_1(N) = \mathrm{Pic}^0(X_1(N))[\ell^n]$, and maps to x. Thus the map $\phi : \mathrm{Pic}^0(X_1(N))[\ell^n] \to A_f[\ell^n]$ is surjective.

For the second part, note that there is a containment

$$(I_f\mathrm{Pic}^0(X_1(N))[\ell^n] \subseteq (I_f J_1(N))[\ell^n],$$

since

$$\ker\phi = \mathrm{Pic}^0(X_1(N))[\ell^n] \cap I_f J_1(N) = (I_f J_1(N))[\ell^n].$$

We claim that containment this is an equality. Recall that

$$J_1(N) = S_2(\Gamma_1(N))^\wedge / H_1(X_1(N), \mathbb{Z}).$$

Then

$$\begin{aligned} I_f J_1(N) &= (I_f S_2(\Gamma_1(N))^\wedge + H_1(X_1(N), \mathbb{Z}))/H_1(X_1(N), \mathbb{Z}) \\ &\cong I_f S_2(\Gamma_1(N))^\wedge / (H_1(X_1(N), \mathbb{Z}) \cap I_f S_2(\Gamma_1(N))^\wedge) \end{aligned}$$

This is notationally quite cumbersome, so for now let $S = S_2(\Gamma_1(N))^\wedge$ and $H = H_1(X_1(N), \mathbb{Z})$. Suppose that $y \in (I_f J_1(N))[\ell^n]$. Then y is of the form $x + H$ for some $x \in I_f S$ such that $\ell^n x \in H \cap I_f S$. $H \cap I_f S$ contains $I_f H$ as a subgroup of finite index m. Then $H \cap I_f S \subseteq I_f m^{-1} H$. Thus, $\ell^n x \in I_f m^{-1} H$, and hence $x \in I_f m^{-1} l^{-1} H$. Take $x = Tx'$, with $T \in I_f$, $x' \in S$, and $m\ell^n x' \in H$. Then $y = T(x' + H)$, with $x' + H \in J_1(N)$, and $m\ell^n(x' + H) = 0$. After all this, this $y \in (I_f J_1(N)[\ell^n]$ is also in $I_f(J_1(N)[m\ell^n])$. But then

$$y \in I_f(J_1(N)[m\ell^n]) = I_f(\mathrm{Pic}^0(X_1(N))[m\ell^n]) \subseteq I_f\mathrm{Pic}^0(X_1(N)).$$

Since $\ell^n y = 0$, we further have that $y \in (I_f\mathrm{Pic}^0(X_1(N)))[\ell^n]$; thus we have the equality

$$(I_f\mathrm{Pic}^0(X_1(N))[\ell^n] = (I_f J_1(N))[\ell^n].$$

The kernel is now

$$(I_f\mathrm{Pic}^0(X_1(N))[\ell^n] = \mathrm{Pic}^0(X_1(N)) \cap I_f\mathrm{Pic}^0(X_1(N)).$$

Now note that the right hand side of the intersection is stable under the Galois action since the action preserves ℓ^n-torsion. On the other hand, the left hand side of the intersection is stable under the action since the Galois action commutes with the action of the Hecke operators on $\mathrm{Pic}^0(X_1(N))$. □

Hence $G_{\mathbb{Q}}$ acts on $A_f[\ell^n]$, and thus on $T_l(A_f)$. Thus we get a Galois representation

$$\rho_{A_f,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(V_\ell(A_f)).$$

Note that $V_\ell(A_f)$ is a module over $\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. In fact:

Lemma 3.5. *$V_\ell(A_f)$ is a rank 2 free module over $\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.*

Proof. With notation as before, let

$$R = S/I_f S$$

and

$$T = (H + I_f S)/I_f S,$$

which are both $\mathcal{O}_f$-modules. Note that

$$\begin{aligned} A_f &= J_1(N)/I_f J_1(N) \\ &\cong S/(I_f S + H) \\ &\cong (S/I_f S)/((H + I_f S)/I_f S) \\ &= R/T. \end{aligned}$$

Hence $A_f[\ell^n] \cong \ell^{-n}T/T$ for any $n \in \mathbb{Z}$. Then we get

$$T_l(A_f) = \varprojlim A_f[\ell^n] = \varprojlim \ell^{-n}T/T \cong \varprojlim T/\ell^n T \cong T \otimes \mathbb{Z}_\ell.$$

A_f has dimension d, so given that $A_f \cong R/T$, the $\mathcal{O}_f$-module T has rank $2d$ over $\mathbb{Z}$. Hence $T \otimes \mathbb{Q}$ is a free $\mathbb{K}_f$-module of rank $2d$ over $\mathbb{Q}$; its rank over $\mathbb{K}_f$ must then be 2, and so clearly $T \otimes \mathbb{Q}_\ell$ is free of rank 2 over $\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ (given that $T \otimes \mathbb{Q}_\ell = T \otimes \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$). Thus

$$V_\ell(A_f) \cong T \otimes \mathbb{Z}_\ell \otimes \mathbb{Q} \cong T \otimes \mathbb{Q}_\ell$$

as $\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-modules. Thus $V_\ell(A_f)$ also has rank 2 over $\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. □

Theorem 3.6. *Let $f \in S_2(N, \chi)$ be a normalized eigenform with number field $\mathbb{K}_f$, and fix a prime ℓ. For each maximal ideal λ of $\mathcal{O}_{\mathbb{K}_f}$ lying over ℓ, there is a 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(\mathbb{K}_{f,\lambda})$$

Proof. Note that $G_{\mathbb{Q}}$ acts $(\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$-linearly on $V_\ell(A_f)$, and by the lemma, we know that $V_\ell(A_f) \cong (\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^2$. Choose a basis of $V_\ell(A_f)$ to get a homomorphism

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{K}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell).$$

Note that there is a ring homomorphism

$$\mathbb{K} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} \mathbb{K}_{f,\lambda},$$

where the product is taken over all primes λ of $\mathbb{K}_f$ lying above ℓ, and $\mathbb{K}_{f,\lambda}$ is the λ-adic completion of $\mathbb{K}_f$. Then for each λ, composing with a projection gets a map $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{K}_{f,\lambda})$, as desired. □

3.5 Representations from l-adic cohomology

These Galois representations are all quite nice, and both would suggest taking Tate modules (for which we already have a neat cohomological characterization) of nice enough varieties allows one to get a Galois representation. However, we will show that étale cohomology lets us push this much further, and that we can actually get a fairly large class of Galois representations from the étale cohomology of *schemes*. As we will see, this construction is essentially the motivation for the Fontaine-Mazur conjecture.

Let X be a scheme, and let G be a sheaf of groups on $X_{\text{ét}}$. Let S be a sheaf of sets on which G acts on the right. S is called a *principal homogeneous space* for G if there exists an étale covering $(U_i \to X)_i$ of X such that for all i, $S(U_i)$ is nonempty, and for every $U \to X$ étale and $s \in \Gamma(U, S)$, the map $g \mapsto sg : G|_U \to S|_U$ is an isomorphism of sheaves.

Let k be a field, and let V/k be a variety. Let F be the constant sheaf associated to an abelian group H. A Galois covering of V with group H is a principal homogeneous space for F, and every principal homogeneous space here arises from a Galois covering. Recall that when V is connected, the Galois coverings are classified be the continuous homomorphisms $\pi_1^{\text{ét}}(V, \overline{x}) \to H$, where $\overline{x} \to V$ is any geometric point of V. Thus for V connected, there is a canonical isomorphism

$$H^1_{\text{ét}}(V, F) \cong \mathrm{Hom}(\pi_1(V, \overline{x}), H).$$

Now, we have the following exact sequence of groups:

$$0 \to \pi_1^{\text{ét}}(V_{\overline{k}}) \to \pi_1^{\text{ét}}(V) \to \pi_1^{\text{ét}}(\mathrm{Spec}\, k) \cong G_k \to 0.$$

By the isomorphism in the previous paragraph, this produces a Galois action on $H^1_{\text{ét}}(V_{\text{ét}}, F)$.

To get the l-adic representations from this, for each n, take F_n to be the constant sheaf associated to $\mathbb{Z}/\ell^n\mathbb{Z}$. Then

$$H^1_{\text{ét}}(V_{\text{ét}}, \mathbb{Z}/\ell^n\mathbb{Z}).$$

Then taking an inverse limit gives

$$H^1_{\text{ét}}(V_{\text{ét}}, \mathbb{Z}_\ell) := \varprojlim_n H^1_{\text{ét}}(V, \mathbb{Z}/\ell^n\mathbb{Z}).$$

Finally,

$$H^1_{\text{ét}}(V, \mathbb{Q}_\ell) := H^1_{\text{ét}}(V, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}\ell} \mathbb{Q}_\ell$$

is a finite-dimensional $\mathbb{Q}_l$-vector space with an action of G_k, and hence we can view it as a Galois representation.

In general, let X/k be a scheme. Let $\overline{k}$ be an algebraic closure of k, and let F be a sheaf on X. Let $X_{\overline{k}} = X \times_k \operatorname{Spec} k$ be the base change of X, and $r : X_{\overline{k}} \to X$ the induced morphism. Denote by $F_{\overline{k}} = r^*F$ the pullback of F to $X_{\overline{k}}$. Now let $g \in G_k$. This induces a morphism $g : X_{\overline{k}} \to X_{\overline{k}}$. Locally, i.e., if $X = \operatorname{Spec} A$, with A some k-algebra, the base change is just $\operatorname{Spec}(A \otimes_k \overline{k})$, and so $g \in G_k$ acts trivially on A and by g on $\overline{k}$:

$$\text{id} \times g : a \otimes b \mapsto a \otimes g(b).$$

Now we also have a pullback $g^*F_{\overline{k}}$, and there is a canonical isomorphism

$$g^*F_{\overline{k}} = g^*p^*F \cong p^*F = F_{\overline{k}}.$$

Thus, we have an induced action on cohomology,

$$H^i_{\text{ét}}(X_{\overline{k}}, F_{\overline{k}}) \to H^i_{\text{ét}}(X_{\overline{k}}, g^*F_{\overline{k}}) \cong H^i_{\text{ét}}(X_{\overline{k}}, F_{\overline{k}}).$$

Thus, we have a continuous action of G_k on $H^i_{\text{ét}}(X_{\overline{k}}, F_{\overline{k}})$. BY a similar procedure for the H^1 case, this allows us to construct ℓ-adic representations of G_k.

Chapter 4

The Fontaine-Mazur Conjecture

4.1 p-adic Representations

One can also study certain distinguished subgroups of $G_{\mathbb{Q}}$ Recall for a prime integer p, the p-adic valuation given by setting $|\alpha|_p = p^{-k}$, where $\alpha = p^k a/b$, with a, b, p all coprime. Completing $\mathbb{Q}$ with respect to this valuation gives the locally compact topological field $\mathbb{Q}_p$, which we have encountered previously.

Let $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. The absolute value $|\cdot|_p$ extends uniquely to an absolute value on $\overline{\mathbb{Q}}_p$. For each embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, there is a closed embedding $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$, and this embedding is determined up to conjugacy. It is worth noting that unlike the Archimedean situation (which we sketch below), the field $\overline{\mathbb{Q}}_p$ is *not* complete. We will denote by $\mathbb{C}_p$ its completion, and note that $G_{\mathbb{Q}_p}$ can be identified with the group of *continuous* automorphisms of $\mathbb{C}_p$.

We also have the familiar Archimedean absolute value on $\mathbb{Q}$ (which we think of as with respect to the prime "at infinity", and denote $|\cdot|_\infty$). Completing $\mathbb{Q}$ with respect to this absolute value gives us the familiar (complete!) field $\mathbb{R}$. Each embedding $\overline{\mathbb{Q}} \to \mathbb{C}$ gives us a closed embedding

$$G_{\mathbb{R}} := \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \hookrightarrow G_{\mathbb{Q}},$$

noting that $G_{\mathbb{R}} \cong \mathbb{Z}/2\mathbb{Z}$, with the only elements being the identity and complex conjugation.

Now, the elements of $\mathbb{Q}_p$ with absolute value ≤ 1 form the closed subring $\mathbb{Z}_p$, which we have also previously encountered in the context of cohomology. Recall that this ring can also be defined as the localization of $\mathbb{Z}$ at the prime ideal (p), so in fact this ring is local with maximal ideal $p\mathbb{Z}_p$. In the absolute value description, this maximal ideal is the ideal consisting of elements with absolute value *strictly* less than 1. Similarly, the elements of $\overline{\mathbb{Q}}_p$ form a local ring $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ with maximal ideal $\mathfrak{m}$. The field $\mathcal{O}_{\overline{\mathbb{Q}}_p}/\mathfrak{m}$ is the algebraic closure of the finite field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$, so we will denote $\overline{\mathbb{F}}_p := \mathcal{O}_{\overline{\mathbb{Q}}_p}/\mathfrak{m}$

We then get a continuous surjective homomorphism

$$G_{\mathbb{Q}_p} \twoheadrightarrow G_{\mathbb{F}_p} := \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p).$$

We define

$$I_{\mathbb{Q}_p} := \ker(G_{\mathbb{Q}_p} \twoheadrightarrow G_{\mathbb{F}_p}),$$

called the *inertia* subgroup of $G_{\mathbb{Q}_p}$. The group $G_{\mathbb{F}_p}$ has a canonical generator given by

$$\mathrm{Frob}_p^{-1}(x) = x^p,$$

called the *Frobenius element.*

A representation ρ is said to be *unramified* at a prime ℓ of $\mathbb{Q}$ if the inertia subgroup acts trivially, i.e., $\rho|_{I_{\mathbb{Q}_p}} = 1$. Equivalently, $\rho|_{G_{\mathbb{Q}_p}}$ is determined by $\rho(\mathrm{Frob}_p)$. A similar definition holds for representations of G_K, where K is a number field, with the primes ℓ replaced by places of K.

Now let K be a finite extension of $\mathbb{Q}_l$, and let ℓ be an odd prime. Let $\mathcal{O}_K$ denote the ring of integers of K. If M is a profinite $\mathcal{O}_K[G_{\mathbb{Q}_l}]$-module (which we will write as $\mathcal{O}[G_\ell]$ for short), we define the following:

Definition 4.1. M is called *good* if for every discrete quotient N of M, there is a finite flat group scheme $\mathcal{F}/\mathbb{Z}_l$ such that $N \cong F(\overline{\mathbb{Q}}_\ell)$ as $\mathbb{Z}_\ell[G_\ell]$-modules.

Definition 4.2. M is called *ordinary* if there is an exact sequence

$$0 \to M^{(-1)} \to M \to M^{(0)} \to 0$$

of profinite $\mathcal{O}[G_l]$-modules, such that $I_{\mathbb{Q}_l}$ acts trivially on $M^{(0)}$ and by the character $\epsilon : G_{\mathbb{Q}_l} \to \mathcal{O}_K^\times$.

Definition 4.3. M is called *semistable* if it is either good or ordinary.

4.2 Periods and de Rham Representations

Before stating the conjecture, there is a somewhat involved definition which we must state, namely, that of a representation being "de Rham." This will be an excessively brief overview of the material needed to for the statement, so it is worth noting that this definition is a part of a *much* larger field known as *p-adic Hodge theory,* which studies p-adic representations. An extensive account of the algebraic theory is given in [FO22], and we direct the reader there for the definition of the ring of de Rham periods B_{dR}.

In the formalism of admissable representations in [FO22], de Rham representations will simply be the B_{dR}-admissible ones. We start by defining a functor D_{dR} :

$\mathsf{Rep}_{\mathbb{Q}_p}(G_K) \to \mathsf{FinVec}_K$ by setting

$$D_{\mathrm{dR}}(V) := (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Since $B_{\mathrm{dR}}^{G_K} = K$, clearly $D_{\mathrm{dR}}(V)$ is a K-vector space for any V. Now there is also a natural B_{dR}-linear map

$$\alpha_{\mathrm{dR}}(V) : D_{\mathrm{dR}}(V) \otimes_K B_{\mathrm{dR}} \to B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$$

sending $w \otimes b \mapsto b \cdot w$. B_{dR} is a field, so this map is injective. Now $B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$ is free as a B_{dR}-module, and the domain of the above map is just the extension of scalars of $D_{\mathrm{dR}}(V)$ to B_{dR}, so it has the same dimension (recall for any field extension $L \supseteq F$, if V is a finite dimensional F-vector space, then $\dim_L(V \otimes_F L) = \dim_F V$.). Then since B_{dR} contains K which contains $\mathbb{Q}_p$, we arrive at the inequality

$$\dim_K D_{\mathrm{dR}}(V) = \dim_{B_{\mathrm{dR}}}(D_{\mathrm{dR}}(V) \otimes_K B_{\mathrm{dR}}) \leq \dim_{B_{\mathrm{dR}}}(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V) = \dim_{\mathbb{Q}_p} V.$$

Definition 4.4. If V is a representation such that the above is a *equality*, i.e., if $\dim_K D_{\mathrm{dR}}(V) = \dim_{\mathbb{Q}_p} V$, then we call V a *de Rham representation.*

4.3 The conjecture

We are now in a position to give a full, proper statement of the Fontaine-Mazur conjecture, first stated in [FM93] The main idea of the conjecture is that certain Galois representations, which we will call "geometric," happen to "come from algebraic geometry."

Definition 4.5. An l-adic representation ρ of a number field K is called *geometric* is it is unramified outside a finite set of places of K, and for each place $v|\ell$ of K, the restriction $\rho|_{G_{K_v}}$ is de Rham.

Definition 4.6. A continuous irreducible ℓ-adic representation of G_K *comes from geometry* if it is isomorphic to a subquotient of the étale cohomology $H^i_{\text{ét}}(V, \mathbb{Q}_l(r))$ for some algebraic variety V over K.

We already saw that we can construct a large class of Galois representations from geometry, so it is natural to ask exactly which Galois representations arise in this way. Fontaine-Mazur predicts that these are precisely the "geometric" Galois representations:

Conjecture 4.7 (**Fontaine-Mazur**). *An irreducible ℓ-adic representation of G_K is geometric if and only if it comes from geometry.*

Something worth noting, although we will not prove it here, is that, in fact, each representation in the compatible system of Galois characters $(\chi_\ell)_\ell$ associated to an algebraic Hecke character χ satisfies the conjecture! For a proof, see [Far06].

4.4 Fontaine-Mazur and modularity

To motivate the final section of this thesis, we will explore the relation between the FM conjecture and the famed Modularity Theorem, which was proven in [Wil95] and [Bre+01]. Before Wiles' original proof of Fermat's Last Theorem [Wil95], little was known about the FM conjecture. Indeed, we will show that modularity can be viewed as the first evidence towards the conjecture.

We call a representation ρ *modular* is for some weight 2 newform f, ρ is equivalent over K_f to ρ_f. With some mild extra assumptions (see [FM93] and [DDT07]), a special case of the conjecture is the following:

Conjecture 4.8. *If $\rho : G_{\mathbb{Q}} \to GL_2(K)$ is an absolutely irreducible l-adic representation and $\rho|_{G_{\mathbb{Q}_l}}$ is semistable, then ρ is modular.*

We will call an elliptic curve *modular* if its Galois representation $\rho_{E,l}$ is modular (although we note that there are many other equivalent formulations, and their equivalence is highly nontrivial; we take this as a definition for convenience). The following is the *Modularity theorem*:

Theorem 4.9. *All elliptic curves $E/\mathbb{Q}$ are modular.*

The proof of this fact is far beyond the scope of this thesis, and requires significantly more sophisticated techniques concerning the objects used thus far. But, from this perspective, it is not hard to see that

Proposition 4.10. *If the (modified) Fontaine-Mazur conjecture holds, then the Modularity theorem holds.*

Proof. This is immediate since $\rho_{E,\ell}$ is irreducible. □

Hence, it is reasonable to view the Modularity theorem as certain evidence for the Fontaine-Mazur conjecture. In fact, so-called "automorphy lifting" theorems are currently one of the major tools used in researching the Fontaine-Mazur conjecture, and these were first introduced to prove modularity. In the next section, we shall see that there is one case of modularity which is essentially due to "one-dimensional"/abelian information, and so we can see some concrete "evidence" for Fontaine-Mazur through this lens.

Chapter 5

A special case

Given that we showed the Fontaine-Mazur conjecture is highly related to the Modularity theorem, it is worthwhile to consider what is essentially the first triumph in the story of modularity: modularity of elliptic curves with complex multiplication. Long before the proof of the full Modularity theorem in 2001, which required deep mathematics from a vast swath of fields, in 1971 Goro Shimura proved a very special (yet historically very informative) case with essentially just complex analysis and the theory of algebraic curves. In particular, he showed that if an elliptic curve E has complex multiplication, then one can associate to it a certain modular form via some analytic methods, and it turns out that its associated abelian variety is an elliptic curve isogenous to E.

Here, we give an overview of Shimura's [Shi71b], along with a Galois-theoretic formulation of the associated Hecke character to a CM elliptic curve.

5.1 The Character of a CM Elliptic Curve

Let E be an elliptic curve over $\mathbb{C}$. From the general theory of elliptic curves, its endomorphism ring over $\mathbb{C}$, $\mathrm{End}_{\mathbb{C}}(E)$, is either isomorphic to $\mathbb{Z}$, or to an order $\mathcal{O}$ in an imaginary quadratic field K. In the second case, we say that E has *complex multiplication* by K. If E is instead an elliptic curve over $\mathbb{Q}$, we will say E has complex multiplication if $\mathrm{End}_{\mathbb{Q}}(E) := \mathrm{End}_{\overline{\mathbb{Q}}}(E) \otimes \mathbb{Q} \cong K$, where K is an imaginary quadratic field (we have to be a bit more finicky about what "having CM" means in this situation, since E really only has CM in some finite algebraic extension of $\mathbb{Q}$). We wish to show that one can associate to E an algebraic Grössencharacter. (Note that $\mathcal{O} = K \cap \mathrm{End}_{\mathbb{Q}}(E) = K \cap \mathrm{End}_L(E)$ for any field extension L/K, and hence is invariant with respect to extensions ([ST68]).) Note, in particular, that we can view E as an elliptic curve over the field K.

Let $T_l(E)$ be the l-adic Tate module of E, and define

$$V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Then $\mathcal{O}$ acts on $T_l(E)$, and by linearity, $T_l(E)$ is an $(\mathcal{O} \otimes_{\mathbb{Q}} \mathbb{Z}_l)$-module. Hence $V_l(E)$ is

a $(K \otimes_{\mathbb{Q}} \mathbb{Q}_l)$-module. For ease of notation, let $\mathcal{O}_l = \mathcal{O} \otimes_{\mathbb{Q}} \mathbb{Z}_l$ and $K_l = K \otimes_{\mathbb{Q}} \mathbb{Q}_l$

Lemma 5.1. *The K_l-module $V_l(E)$ is free of rank 1.*

Proof. By [Sil09] Theorem III.7.4, the map $\mathrm{End}(E) \otimes \mathbb{Z}_l \to \mathrm{End}T_l(E)$ is injective, and hence so is the map $\mathrm{End}(E) \otimes \mathbb{Q}_l \to \mathrm{End}(V_l(E))$. Now recall that $\mathrm{End}(E) \otimes \mathbb{Q} \cong K$, so then $\mathbb{Q}_l \otimes \mathrm{End}(E) \cong K \otimes \mathbb{Q}_l = K_l$. Hence we have an injective map $K_l \to \mathrm{End}(V_l(E))$, and so K_l acts faithfully on $V_l(E)$. Now clearly $V_l(E)$ is 2-dimensional over $\mathbb{Q}_l$. But, by definition of an order, $\mathcal{O}$ has dimension 2 over $\mathbb{Z}$. Hence after tensoring, K_l has dimension 2 over $\mathbb{Q}_l$. Since K_l acts faithfully on $V_l(E)$ and $\dim_{\mathbb{Q}_l} K_l = \dim_{\mathbb{Q}_l} V_l(E)$, counting dimensions shows that $V_l(E)$ must be free of rank 1 over K_l. □

Lemma 5.2. *The commutant of $\mathcal{O}$ in End$(V_l(E))$ is K_l.*

Proof. By the previous lemma, any element of $\mathrm{End}(V_l(E))$ which commutes with $\mathcal{O}$ also commutes with the ring $K_l = K \otimes \mathbb{Q}_l$. □

Lemma 5.3. *Let $\rho_l : G_K \to \mathrm{Aut}(V_l)$ be the l-adic representation of E (viewing E over K). Then $\mathrm{im}\,\rho_l$ is a commutative group.*

Proof. If $\sigma \in G_K$, it is clear that $\rho_l(\sigma)$ commutes with the elements of R, and so by the previous lemma, $\rho_l(\sigma)$ is contained in K_l. Hence ρ_l is a homomorphism $G_{\mathbb{Q}} \to K_l^* = (K \otimes \mathbb{Q}_l)^*$. □

Then ρ_ℓ takes its values in K_l^*, and factors through $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, where K^{ab} is the maximal abelian extension of K. Further, via Frobenius Reciprocity, the 2-dimensional representation of $G_{\mathbb{Q}}$ is the induced representation of the 1-dimensional representation of G_K

Now, mostly following the constructions in [Con11] and [Far06], we will associate to ρ_ℓ a certain character. Recall the Artin reciprocity map from class field theory (Chapter 3):

$$\theta_K : \mathbb{A}_K^\times / K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Then composing with θ_K gives an "ℓ-adic Hecke character" $\lambda = \rho_l \circ \theta_K$ on $\mathbb{A}_K^\times / K^\times$:

$$\omega_\ell = \rho_\ell \circ \theta_K : \mathbb{A}_K^\times / K^\times \xrightarrow{\theta_K} G_K \xrightarrow{\rho_\ell} K_\ell^\times \hookrightarrow \mathrm{GL}_1(\overline{\mathbb{Q}}_\ell).$$

For our purposes, however, we want to get some *Grössencharacter,* that is, an appropriate map into $\mathbb{C}$. This in fact gives us a *compatible system* of Galois characters, since for every ℓ,

$$\mathrm{tr}_{K_\ell/\mathbb{Q}_\ell}(\omega_\ell(u_{F_v})) = 1 - \#E(\kappa_v) + q_v,$$

where κ_v is the residue field of F at the place v, $q_v = \#\kappa_v$, and u_{F_v} is a uniformizer (see [Bru16]). Then from chapter 3, we see that there is a corresponding algebraic Hecke character $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$. Each of the ρ_ℓ are "locally algebraic" (any ℓ-adic

representation coming from an elliptic curve is locally algebraic; see [Con11] Lemma 1 and the following remark), i.e. there exists an open neighborhood U_ℓ of $1 \in K^*$ and a $\mathbb{Q}$-algebra homomorphism $\chi_{alg} : K^* \to \overline{\mathbb{Q}}$ such that $\rho_\ell \circ \theta_{K,\ell}|_{U_\ell} = \chi_{alg} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Then choose some prime ℓ, and define

$$\omega(x) = \rho_\ell(\theta_K(x))\chi_{alg}(x_\ell)^{-1}.$$

Then the corresponding compatible system of representations is precisely the ρ_l.

5.2 Modularity for CM elliptic curves

As in the last section, let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication, i.e., its endomorphism algebra $\mathrm{End}_{\mathbb{Q}}(E)$is isomorphic to an imaginary quadratic field K. The motivation of Shimura's original proof is noticing that the L-function of our previously-defined Hecke character (which we will refer to as a *Grössencharacter* interchangeably) is the Mellin transform of a certain cusp form. We will follow Shimura's original proof and work ideal-theoretically instead of idele-theoretically. For any finite idele $a_f \in A_{K,f}^\times$, we get a fractional ideal $\mathfrak{a} = a_f \cdot \hat{\mathcal{O}}_K \cap K$.

Let $\mathfrak{f}$ be an integral ideal of K, and let $I_\mathfrak{f}$ be the group of fractional ideals of K coprime to $\mathfrak{f}$ (i.e., a certain subgroup of I_K). Let $W_\mathfrak{f}$ be the group of elements $\alpha \in K^*$ such that $\alpha \equiv 1 \bmod \mathfrak{f}$. Then a (classical) Hecke (or Grössen-) character of K is a character $\chi : I_\mathfrak{f} \to \mathbb{C}^*$ such that

$$\chi((\alpha)) = \alpha^v$$

for every $\alpha \in W_\mathfrak{f}$, where v is a fixed integer. Denote the set of all such characters by $\Lambda_\mathfrak{f}^v$.

Given a Grössencharacter χ on a number field K, we can associate a function (which will turn out to be a modular form) $f_\chi(z)$ given by

$$f_\chi(z) := \sum_{\mathfrak{a}} \chi(\mathfrak{a}) e^{2\pi i N(\mathfrak{a}) z},$$

with the sum being taken over all integral ideals $\mathfrak{a}$ coprime to $\mathfrak{f}$. If $\mathfrak{a}$ is an integral ideal, we can choose a representative a_f with

$$a_f \cdot \hat{\mathcal{O}}_K = \mathfrak{a}.$$

Hence, given a Grössencharacter χ, we have that

$$\chi(\mathfrak{a}) = \chi_f(a_f)$$

for any a_f representing an integral ideal. Then idelically, this defintion can be written

$$f_\chi(z) = \sum_{a_f \in K^\times \backslash A_{K,f}^\times / \hat{\mathcal{O}}_K^\times} \chi_f(a_f) q^{N(a_f \hat{\mathcal{O}}_K)},$$

where the sum is taken over a set of coset representatives a_f such that a_f represents an integral ideal.

Lemma 5.4. *Let $-D$ be the discriminant of K. Suppose χ is a Grössencharacter with*

$$\chi((\alpha)) = \alpha^v$$

for every $\alpha \in W_{\mathfrak{f}}$, and set $M = D \cdot N(\mathfrak{f})$. Then $f_\chi \in S_{v+1}(M, \varepsilon)$, with $\varepsilon : (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}^\times$ given by

$$\varepsilon(a) = \Big(\frac{-D}{a}\Big) \cdot \frac{\chi((a))}{a^v}$$

for $a \in \mathbb{Z}$ coprime to M.

Proof. WE proceed by induction on $N(\mathfrak{c}^{-1}\mathfrak{m})$, where $\mathfrak{c}$ is the conductor of χ. Suppose by induction that $f_\chi \in S_{v+1}(D \cdot N(\mathfrak{n}), \varepsilon)$. Suppose $\mathfrak{c}^{-1}\mathfrak{m}$ contains a prime factor $\mathfrak{p}$, and let $\mathfrak{n} = \mathfrak{p}^{-1}\mathfrak{m}$. Note that $\Lambda_{\mathfrak{n}}^v \supseteq \Lambda_{\mathfrak{m}}^v$, and denote by μ the element of $\Lambda_{\mathfrak{n}}^v$ that, when restricted to $\Lambda_{\mathfrak{m}}^v$, coincides with χ. Let $q = N(\mathfrak{p})$. Then

$$f_\mu(qz) = \sum_{(\mathfrak{I},\mathfrak{n})=1} \mu(\mathfrak{I}) e^{2\pi i N(\mathfrak{p}\mathfrak{I})z}.$$

Note that $\mu(\mathfrak{p}) = 0$ if $\mathfrak{p}$ divides $\mathfrak{n}$. Then

$$\begin{aligned} f_\mu(z) - \mu(\mathfrak{p}) f_\mu(qz) &= \sum_{(\mathfrak{I},\mathfrak{n})=1} \mu(\mathfrak{I}) e^{2\pi i N(\mathfrak{p}\mathfrak{I})z} - \mu(\mathfrak{p}) \sum_{(\mathfrak{I},\mathfrak{n})=1} \mu(\mathfrak{I}) e^{2\pi i N(\mathfrak{p}\mathfrak{I})z} \\ &= \sum_{(\mathfrak{I},\mathfrak{n})=1} \mu(\mathfrak{I}) e^{2\pi i N(\mathfrak{p}\mathfrak{I})z} - \sum_{(\mathfrak{I},\mathfrak{n})=1} \mu(\mathfrak{p}\mathfrak{I}) e^{2\pi i N(\mathfrak{p}\mathfrak{I})z} \\ &= \sum_{(\mathfrak{I},\mathfrak{m})=1} \mu(\mathfrak{I}) e^{2\pi i N(\mathfrak{p}\mathfrak{I})z} = f_\chi(z). \end{aligned}$$

With a little extra work, one sees $f_\mu(qz) \in S_{v+1}(q \cdot D \cdot N(\mathfrak{n}), \varepsilon) = S_{v+1}(D \cdot N(\mathfrak{m}), \varepsilon)$, and hence so is f_χ. □

Then with E as in the beginning of this section, we can define a *modular form* f_χ to its associated Grössencharacter, from which we can further associate an abelian variety

$$A_\chi := A_{f_\chi}$$

to f_χ, as in the first chapter.

Let $\mathfrak{c}$ be the conductor of χ, and set $M = D \cdot N(\mathfrak{c})$. Then $f_\chi \in S_2(M, \varepsilon)$. Let $k_\chi = \mathbb{Q}(a_1, a_2, \dots)$ be the field generated by the Fourier coefficients of f_χ. By [Shi71a],

A_χ is an abelian variety of dimension $[k_\chi : \mathbb{Q}]$

Lemma 5.5. *The abelian variety A_χ is isogenous to a product of copies of an elliptic curve E with $End_{\mathbb{Q}}(E) \cong K$.*

Proof. See [Shi71b] □

Lemma 5.6. $[k_\chi : \mathbb{Q}] = 1$.

Proof. By the theory of complex multiplication (see [Sil99]), the Hasse-Weil zeta function of E coincides exactly with the L-function of χ, and so we have that

$$L(s, \chi) = \prod \left(1 - a_p p^{-s} + \varepsilon(p) p^{1-2s}\right)^{-1},$$

where here ε is the trivial character. Since E is defined over $\mathbb{Q}$, this implies a_n must be rational. □

Since $k_\chi = \mathbb{Q}$, and $\dim A_\chi = [k_\chi : \mathbb{Q}]$, we find that A_χ must be an *elliptic curve,* by virtue of Lemma 5.5.

Lemma 5.7. *E and A_χ determine the same Grössencharacter.*

Proof. By [Shi71a] Thm. 7.15, the zeta function of A_χ coincides with the L-function of χ up to finitely many Euler factors. By Lemma 5.5, $\mathrm{End}_{\mathbb{Q}}(A_\chi) \cong K$, so again by the theory of complex multiplication, the zeta function of A_χ coincides with $L(s, \mu)$ for some Grössencharacter μ of K.

Thus, $L(s, \chi)$ and $L(s, \mu)$ coincide up to finitely many factors in the Euler products. In other words, $\chi(\mathfrak{p}) = \mu(\mathfrak{p})$ or $\chi(\mathfrak{p}) = \mu(\mathfrak{p}^r)$ for almost all prime ideals $\mathfrak{p}$ in K. Now, if $\mathfrak{m}$ contains both the conductors of χ and μ, we have that $\chi((\alpha)) = \alpha = \mu((\alpha))$ for $\alpha \in K$ with $\alpha \equiv 1 \bmod \mathfrak{m}$. Thus, it must be the case that $\chi(\mathfrak{p}) = \mu(\mathfrak{p})$, and so $\chi = \mu$. □

Theorem 5.8. *A_χ is an elliptic curve isogenous to E over $\mathbb{Q}$.*

Proof. See [Shi67], Theorem 8. □

To say a bit more about the Galois-theoretic information, the Isogeny Theorem tells us that in this case, the Tate modules of E and A_χ are also isomorphic as $\mathbb{Z}_l$-modules, so in particular their associated ℓ-adic representations are the same. Hence, Galois representations coming from CM elliptic curves "come from" an automorphic object, as is predicted in many other places in number theory.

References

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Basic Books, 1969.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Neron Models*. Springer, 1990.

[Boo15] Jeremy Booher. *Viewing Modular Forms as Automorphic Representations*. `https://www.math.canterbury.ac.nz/~j.booher/expos/adelic_mod_forms.pdf`. 2015.

[Bre+01] Christophe Breuil et al. "On the modularity of elliptic curves over **Q**: wild 3-adic exercises". In: *Journal of the American Mathematical Society* (2001).

[Bru16] Peter Bruin. *Galois Representations and Automorphic Forms*. `https://pub.math.leidenuniv.nl/~bruinpj/GaloisReps.pdf`. 2016.

[Con11] Brian Conrad. *Algebraic Hecke characters*. `https://math.stanford.edu/~conrad/DarmonCM/2011Notes/algebraic%20Hecke%20characters.pdf`. 2011.

[DDT07] Henri Darmon, Fred Diamond, and Richard Taylor. *Fermat's Last Theorem*. 2007.

[DR73] Pierre Deligne and Michael Rapoport. "Les schemas de modules de courbes elliptiques". In: *Modular Functions of One Variable II*. Lecture Notes in Mathematics. Springer, 1973.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Springer, 2005.

[Eis95] David Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*. Springer-Verlag, 1995.

[Far06] Laurent Fargues. *Motives and automorphic forms: The (potentially) abelian case*. `https://webusers.imj-prg.fr/~laurent.fargues/Motifs_abeliens.pdf`. 2006.

[FH91] William Fulton and Joe Harris. *Representation Theory: A First Course*. Graduate Texts in Mathematics. Springer-Verlag, 1991.

[FM93] Jean-Marc Fontaine and Barry Mazur. *Geometric Galois Representations*. 1993.

[FO22] Jean-Marc Fontaine and Yi Ouyang. *Theory of p-adic Galois Representations*. Springer, 2022.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[Hat01] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2001.

[Hid00] Haruzo Hida. *Modular Forms and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2000.

[KM85] Nicholas Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*. Princeton University Press, 1985.

[Mil] J.S. Milne. *Lectures on Étale Cohomology*.

[Mil80] J.S. Milne. *Étale Cohomology*. Princeton University Press, 1980.

[Neu92] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1992.

[Rob21] Damien Robert. *General theory of abelian varieties and their moduli spaces*. `https://www.math.u-bordeaux.fr/~damienrobert/pro/publications/books/avtheory.pdf`. 2021.

[Shi67] Goro Shimura. "On the zeta-function of an abelian variety with complex multiplication". In: *Annals of Mathematics* (1967).

[Shi71a] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.

[Shi71b] Goro Shimura. *On Elliptic Curves with Complex Multiplication as Factors of the Jacobians of Modular Function Fields*. 1971.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[Sil99] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 1999.

[ST68] Jean-Pierre Serre and John Tate. "Good reduction of abelian varieties". In: *Annals of Mathematics* (1968).

[Wil95] Andrew Wiles. "Modular Elliptic Curves and Fermat's Last Theorem". In: *Annals of Mathematics* (1995).