

Modular curves and complex multiplication

June 7, 2018

Contents

0	Introduction	3
1	Number fields	4
1.1	Ramification	4
1.1.1	The Galois case	5
1.2	The Artin symbol	6
1.3	Artin reciprocity law	7
1.4	Completions	8
2	Complex multiplication	11
2.1	Lattices	11
2.1.1	Orders	12
2.1.2	The endomorphisms of a lattice	12
2.2	Tori	12
2.3	Elliptic curves over \mathbb{C}	13
2.4	Binary quadratic forms	15
2.4.1	The form class group is finite	16
2.4.2	Lattices, proper ideals and forms	16
2.5	$\text{cl}(\mathcal{O})$ acts on $\text{Ell}_{\mathbb{C}}(\mathcal{O})$	17
2.5.1	The action in terms of isogenies	18
2.6	The Hilbert class polynomial	18
2.7	The Galois action	19
2.8	The First Main theorem of CM	20
2.8.1	Relating $\text{cl}(\mathcal{O})$ with $\text{cl}(\mathcal{O}_K)$	21
2.8.2	Some Galois groups of ring class fields	22

3	Modular curves	23
3.1	The modular curve	23
3.2	Elliptic points	24
3.3	Cusps and $X(\Gamma)$	25
3.4	The genus of $X(\Gamma)$	26
3.5	Modular curves as algebraic curves	28
3.5.1	Algebraic curves	28
3.5.2	Automorphic forms	30
3.5.3	The modular polynomial	31
3.5.4	Properties of the modular polynomial	32
3.6	Modular curves as moduli spaces	34
4	Heegner points on $X_0(N)$	36
4.1	The modularity theorem	36
4.2	The L -function	36
4.2.1	Reduction over local fields	37
4.3	Heegner points	38
4.4	Group cohomology	38
4.4.1	The Selmer and Tate-Shafarevich groups	39
4.5	Kolyvagin's theorem	41
4.5.1	Galois action on torsion points	41
4.5.2	The Heegner points form an Euler system	42
4.5.3	Constructing cohomology classes in $H^1(K, E_p)$	43

0 Introduction

Complex multiplication is a property some elliptic curves have. An elliptic curve E can be defined to be the zero locus of a degree 3 polynomial in two variables having no singularities. Drawing an elliptic curve E on a real plane has its limitations, since the picture we obtain depends on the particular equation E verifies. If we allow complex numbers and instead embed it in the complex projective plane then E is now isomorphic to a complex torus, a genus 1 compact surface.

Moreover, one can define through a geometrical construction a law group on E making it an abelian group. In abelian groups one can consider the multiplication-by- n endomorphisms defined by $P \mapsto nP$. In the case of most elliptic curves, there are no other endomorphisms i.e. the endomorphism ring $\text{End}(E)$ is isomorphic to \mathbb{Z} . Then E has complex multiplication (CM) if $\text{End}(E)$ is strictly larger than \mathbb{Z} . The ring $\text{End}(E)$ is then also an special kind of ring i.e. an order \mathcal{O} of a quadratic imaginary field K .

There is a quantity attached to every elliptic curve that tells us whether two curves are \mathbb{C} -isomorphic or not, the j -invariant. In the case that E has CM its j -invariant is an algebraic number over \mathbb{Q} .

Every order \mathcal{O} has an associated proper ideal class group $\text{cl}(\mathcal{O})$ and a ring class field K_f , and both are constructed in terms of elliptic curves having CM by \mathcal{O} . The main theorem of CM shows that the Galois group of K_f over K is $\text{cl}(\mathcal{O})$. Since $\text{cl}(\mathcal{O})$ is abelian this is an explicit construction of infinitely many finite abelian extensions of K . This solves partially - for the quadratic imaginary case - the main problem in class field theory, which is finding all the finite abelian extensions of a number field.

All of this requires showing that the j -invariants of elliptic curves with CM are algebraic over \mathbb{Q} . This last property is proven by using the fact that the modular curve $X_0(N)$ can be defined over \mathbb{Q} and an alternative interpretation of $X_0(N)$ as a moduli space i.e. the curve $X_0(N)$ classifies the degree N isogenies between elliptic curves. However, the first definition of $X_0(N)$ is geometrical.

In the same way a complex torus $T = \mathbb{C}/\Lambda$ is the quotient space when Λ acts on the plane as a discrete group of isometries, the modular curve is also defined in geometrical terms¹. It is the quotient space $X_0(N) = \mathfrak{H}/\Gamma_0(N)$, where $\Gamma_0(N)$ is a carefully chosen finite index subgroup of $\text{SL}_2(\mathbb{Z})$.

Finally, we discuss the construction of Heegner points, which we can think of as an application of the theory of complex multiplication. Together with the Modularity theorem, Kolyvagin, Gross and Zagier gave results closely related to the Birch and Swinnerton-Dyer conjecture, an open problem concerning elliptic curves.

¹ $\text{SL}_2(\mathbb{Z})$ is also a discrete subgroup of isometries of the upper half plane \mathfrak{H} with the Poincaré metric.

1 Number fields

A *number field* is a finite extension $K \subset \mathbb{C}$ of \mathbb{Q} . The *algebraic integers* \mathcal{O}_K of K are the elements α of K for which there exists $f \in \mathbb{Z}[x]$ monic with $f(\alpha) = 0$. They form a subring of K and the field of fractions of \mathcal{O}_K is K itself. Furthermore \mathcal{O}_K is a *Dedekind domain*, that is

- \mathcal{O}_K is Noetherian
- Every prime ideal $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ is maximal
- \mathcal{O}_K is integrally closed

In a Dedekind domain, every ideal \mathfrak{a} of \mathcal{O}_K factors uniquely up to reordering as a product of prime ideals

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

A *fractional ideal* of K is a finitely generated \mathcal{O}_K -submodule of K , and it can be regarded as a generalization of ideal of \mathcal{O}_K . The set of fractional ideals $\mathcal{I}(K)$ forms a group under multiplication, and it is freely generated by the prime ideals of K . Note that the subset of principal fractional ideals $\mathcal{P}(K)$ forms a subgroup of $\mathcal{I}(K)$.

The *ideal class group* of K is the abelian group $\text{cl}(K) = \mathcal{I}(K)/\mathcal{P}(K)$. The cardinal of $h_K = |\text{cl}(K)|$ is called the *class number* of K , and it is always finite.

Another result is *Dirichlet's unit theorem* which states that the group of units \mathcal{O}_K^\times of \mathcal{O}_K verifies $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$ where r and $2s$ are respectively the number of real and complex embeddings of K in \mathbb{C} and $\mu(K)$ is the *torsion* of \mathcal{O}_K^\times , the roots of unity contained in \mathcal{O}_K .

Let L/K be a finite extension and let $\alpha \in L$, and let M_α be a matrix of the K -linear map $m_\alpha : L \rightarrow L$ in some basis of L/K . The *norm* $N_{L/K}(\alpha)$ and *trace* $\text{Tr}_{L/K}(\alpha)$ of α is the norm and trace of M_α . An *integral basis* of \mathcal{O}_L is a set $\{\beta_i\}_i$ such that $\mathcal{O}_L = \langle \beta_i \rangle_{\mathbb{Z}}$ as a \mathbb{Z} -module. The *discriminant* of L/K with respect to β_i is the determinant of the matrix $\{\text{Tr}_{L/K}(\beta_i \beta_j)\}_{i,j}$. As it depends on a choice of basis, it is defined in general up to elements in $(\mathcal{O}_K^\times)^2$.

In this section, we consulted [4, 3, 1].

1.1 Ramification

Let L/K be a finite extension of K and let \mathfrak{p} be a prime ideal of \mathcal{O}_K . One can consider the factorization of $\mathfrak{p}\mathcal{O}_L$ in \mathcal{O}_L

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \tag{1.1}$$

Here it is said that \mathfrak{P}_i *lies above* \mathfrak{p} . The coefficients e_i in (1.1) are the *ramification indices*. The *inertial degrees* of \mathfrak{p} are $f_i = [\mathbb{F}_{\mathfrak{P}_i}^L : \mathbb{F}_{\mathfrak{p}}^K]$; note that $\mathbb{F}_{\mathfrak{P}_i}^L = \mathcal{O}_L/\mathfrak{P}_i$ can be regarded as a finite Galois extension of $\mathbb{F}_{\mathfrak{p}}^K = \mathcal{O}_K/\mathfrak{p}$, because these fields are finite and $\mathfrak{p} \subset \mathfrak{P}_i$.

We say that a prime ideal \mathfrak{p} of K

- *splits* in L if $e_i = 1$ for all i
- *splits completely* in L if it splits and $f_i = 1$ for all i
- *ramifies* in L if it does not split and it is not a prime of K
- is *inert* in L if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal of L

It can be shown that if \mathfrak{p} ramifies then \mathfrak{p} divides the discriminant of L/K . This proves that only finitely many primes of K *ramify* in L . The following relation

$$\sum_{i=1}^g e_i f_i = [L : K] \quad (1.2)$$

tells us there is a finite number of possibilities for the e_i and f_i . It is sometimes called the *fundamental identity* for its role in many proofs of the results we discuss.

1.1.1 The Galois case

If L/K is Galois then the situation is simplified, because if we let $G = \text{Gal}(L/K)$ then G acts on the set of prime ideals of \mathcal{O}_L because $\sigma\mathcal{O}_L = \mathcal{O}_L$ for $\sigma \in G$. Moreover, if we fix \mathfrak{p} and choose \mathfrak{P} above \mathfrak{p} the primes \mathfrak{P}_i in the factorization of $\mathfrak{p}\mathcal{O}_L$ all lie in the G -orbit of \mathfrak{P} , so G acts transitively on the \mathfrak{P}_i . From this fact one can prove that $e = e_i$ and $f = f_i$ for all i , so

$$efg = [L : K]$$

The inertial and ramification degrees are multiplicative: $e(M/K) = e(M/L) \cdot e(L/K)$ and $f(M/K) = f(M/L)f(L/K)$ for an extension M/L .

Some subgroups of G are studied to derive further properties of the decomposition of \mathfrak{p} . The *decomposition group* $G_{\mathfrak{P}} = G(\mathfrak{P}|\mathfrak{p})$ is the stabilizer of \mathfrak{P} (G acts on \mathcal{O}_L):

$$G_{\mathfrak{P}} = \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\}$$

The *inertia group* $I_{\mathfrak{P}} = I(\mathfrak{P}|\mathfrak{p})$ is

$$I_{\mathfrak{P}} = \{\sigma \in G : \sigma x \equiv x \pmod{\mathfrak{P}} \text{ for all } x \in L\}$$

It follows that $I_{\mathfrak{P}} \subset G_{\mathfrak{P}}$, and each $\sigma \in G_{\mathfrak{P}}$ naturally induces an automorphism $\mathcal{Q}(\sigma) = \bar{\sigma} \in \bar{G} = \text{Gal}(\mathbb{F}_{\mathfrak{P}}^L/\mathbb{F}_{\mathfrak{p}}^K)$ making the following diagram² commute:

$$\begin{array}{ccc} \mathcal{O}_L & \xrightarrow{\sigma} & \mathcal{O}_L \\ \downarrow \pi_{\mathfrak{P}} & & \downarrow \pi_{\mathfrak{P}} \\ \mathbb{F}_{\mathfrak{P}}^L & \xrightarrow{\bar{\sigma}} & \mathbb{F}_{\mathfrak{P}}^L \end{array}$$

²Here $\pi_{\mathfrak{P}}$ is the natural quotient by \mathfrak{P} map

The map $\mathcal{Q} : G_{\mathfrak{P}} \rightarrow \bar{G}$ is a group homomorphism, and $\ker \mathcal{Q} = I_{\mathfrak{P}}$ because $\mathcal{Q}(\sigma) = 1$ if and only if for any x one has $\bar{\sigma}\pi_{\mathfrak{P}}x = \pi_{\mathfrak{P}}x = \pi_{\mathfrak{P}}\sigma x$, and this is to say $\sigma \in I_{\mathfrak{P}}$. The fixed subfields of L by the decomposition and inertia groups are called the *decomposition field* $Z_{\mathfrak{P}}$ and the *inertia field* $T_{\mathfrak{P}}$. Therefore $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ is a normal extension because $\ker \mathcal{Q} = I_{\mathfrak{P}} \triangleleft G_{\mathfrak{P}}$ is a normal subgroup. It can be shown that \mathcal{Q} is surjective, so we have an exact sequence

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \longrightarrow \bar{G} \longrightarrow 1$$

The reason of introducing the decomposition and inertia fields will become clear now in the following diagram

$$\frac{\text{ramification index}}{\text{inertial degree}} \quad \mathfrak{p} \xrightarrow{\frac{1}{1}} \mathfrak{P}_Z \xrightarrow{\frac{1}{f}} \mathfrak{P}_T \xrightarrow{\frac{e}{1}} \mathfrak{P}$$

Let \mathfrak{P} be a prime of L above \mathfrak{p} and consider the factorization of \mathfrak{p} in the tower of extensions $K \subset Z_{\mathfrak{P}} \subset T_{\mathfrak{P}} \subset L$. Then \mathfrak{p} is inert in the inertia field, and splits completely in the decomposition field and finally can ramify in L .

In the case L/K is an *abelian extension*, i.e. that G is abelian then the decomposition and inertia groups $G_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ only depend on \mathfrak{p} and not \mathfrak{P} , because in general

$$\begin{cases} G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1} \\ I_{\sigma\mathfrak{P}} = \sigma I_{\mathfrak{P}} \sigma^{-1} \end{cases}$$

and all the subgroups of G are normal.

1.2 The Artin symbol

We recall that \bar{G} is the Galois group of a finite field, so it is cyclic and generated by a power of the *Frobenius automorphism* φ which maps $\bar{x} \mapsto \bar{x}^p$, namely by $\bar{\phi} = \varphi^{N\mathfrak{p}}$ where $N\mathfrak{p} = (\mathcal{O}_K : \mathfrak{p})$ is the *numerical norm* of \mathfrak{p} and $(p) = \mathfrak{p} \cap \mathbb{Z}$. Now consider a prime \mathfrak{p} of K that is *unramified* in L ($e = 1$). It can be shown that $|I_{\mathfrak{P}}| = e$, so in this case the inertia group $I_{\mathfrak{P}}$ is trivial and \mathcal{Q} induces an isomorphism

$$G_{\mathfrak{P}} \cong \bar{G} = \text{Gal}(\mathbb{F}_{\mathfrak{P}}^L / \mathbb{F}_{\mathfrak{p}}^K) = \langle \bar{\phi} \rangle$$

Taking the preimage $\phi = \mathcal{Q}^{-1}(\bar{\phi})$ of $\bar{\phi}$ by \mathcal{Q} gives the generator of $G_{\mathfrak{P}}$. If we recall the definition of \mathcal{Q} , we see that ϕ verifies

$$\phi(x) \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad (1.3)$$

because in \bar{G} we had $\bar{\phi}(\bar{x}) = \bar{x}^{N\mathfrak{p}}$. Note ϕ is the only element in $G_{\mathfrak{P}}$ verifying this condition. In this case, the *Artin symbol* is

$$\left(\frac{L/K}{\mathfrak{P}} \right) := \phi$$

The notation remarks that ϕ depends on L, K and \mathfrak{P} . Note that $|G_{\mathfrak{P}}| = ef$ follows if we recall G acts transitively on the set of primes \mathfrak{P} above \mathfrak{p} ; the number of factors in the factorization (1.1) is $g = (G : G_{\mathfrak{P}})$, and $|G| = efg = [L : K]$. Hence the order of $(\frac{L/K}{\mathfrak{P}})$ is the inertial degree $|\tilde{G}| = (G_{\mathfrak{P}} : I_{\mathfrak{P}}) = ef/e = f = f(\mathfrak{P}/\mathfrak{p})$.

From the uniqueness of an element verifying (1.3) it follows that for any $\sigma \in G$

$$\left(\frac{L/K}{\sigma\mathfrak{P}}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} \quad (1.4)$$

i.e. the Artin symbol of the conjugate by σ of a prime \mathfrak{P} is the conjugate of the Artin symbol by σ .

If L/K is abelian then conjugation by σ is the identity map in G , so $(\frac{L/K}{\mathfrak{P}})$ does not really depend on what prime \mathfrak{P} above \mathfrak{p} we choose. In this case, given a prime \mathfrak{p} of K we define

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \left(\frac{L/K}{\mathfrak{P}}\right) \quad (1.5)$$

where the right hand side is the Artin symbol and \mathfrak{P} is some prime in L above \mathfrak{p} . From our discussion above it follows that is well-defined.

When L/K is not abelian, by taking all the elements in the conjugacy class of $(L/K, \mathfrak{P})$ we define similarly

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \left\{ \left(\frac{L/K}{\mathfrak{P}}\right) \text{ with } \mathfrak{P} \text{ above } \mathfrak{p} \right\} \quad (1.6)$$

Remark 1.1. The Artin symbol also characterizes those unramified primes splitting completely; if \mathfrak{p} is unramified and $(L/K, \mathfrak{p}) = 1$ then \mathfrak{p} splits completely, since the hypotheses imply $e = f = 1$ and $efg = g = [L : K]$.

1.3 Artin reciprocity law

We were able to define the Artin symbol for \mathfrak{p} unramified in L , because \mathcal{Q} was an isomorphism. If one wants to define it for all prime ideals, then one can consider the case of an abelian *unramified extension* L/K ; that all primes in K are unramified in L . Briefly, the commutativity of G lets one define the Artin symbol for a prime \mathfrak{p} of K as in (1.5) and the condition that L/K is unramified is to define it for all primes.

Let $\mathcal{I}(K)$ be the group of fractional ideals of K . One can define the Artin symbol for any fractional ideal

$$\begin{aligned} \left(\frac{L/K}{\cdot}\right) : \mathcal{I}(K) &\longrightarrow \text{Gal}(L/K) \\ \mathfrak{a} = \prod_i \mathfrak{p}_i^{r_i} &\longmapsto \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i} \end{aligned}$$

Note that this expression above makes sense because $\text{Gal}(L/K)$ is abelian, hence we can take the product of the $(\mathfrak{p}_i, L/K)$ in any order. The *Hilbert class field* of K is the maximal abelian unramified extension of K . In the case of $K = \mathbb{Q}$ the Hilbert class field is \mathbb{Q} itself, because every extension of \mathbb{Q} is ramified.

Theorem 1.2 (Artin reciprocity law for the Hilbert class field). *Let L be the Hilbert class field of K . Then the map $\left(\frac{L/K}{\cdot}\right)$ described above is surjective and the kernel is $\mathcal{P}(K)$.*

Hence, to find all the abelian unramified extensions of K one has only to find $\text{Gal}(L/K)$ because of the Galois correspondence i.e. it follows that the Artin symbol induces an isomorphism $\text{cl}(K) \cong \text{Gal}(L/K)$, and by Galois theory we obtain

Corollary 1.3. *There is a one-to-one correspondence between subgroups of $\text{cl}(K)$ and abelian unramified extensions of K .*³

In the case of K being quadratic imaginary, by using some results on elliptic curves the Galois group is completely determined. This is the goal of section 2.

Theorem 1.2 is a particular case of the following result, for which one does not need the extension L/K to be unramified:

Theorem 1.4 (Artin reciprocity). *Let L/K be a finite abelian extension of number fields. Then there exists an integral ideal \mathfrak{c} of K divisible by and only by all primes of K ramifying in L for which the Artin map*

$$\begin{aligned} \left(\frac{L/K}{\cdot}\right) : \mathcal{I}_{\mathfrak{c}}(K) &\longrightarrow \text{Gal}(L/K) \\ \mathfrak{a} = \prod_i \mathfrak{p}_i^{r_i} &\longmapsto \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i} \end{aligned}$$

*is a well-defined morphism from $\mathcal{I}_{\mathfrak{c}}(K)$ = the set of fractional ideals coprime with \mathfrak{c} to the Galois group $\text{Gal}(L/K)$ and so that the kernel of $(\cdot, L/K)$ contains $\mathcal{P}_{\mathfrak{c}}(K)$ = the set of principal ideals (α) with $\alpha \equiv 1 \pmod{\mathfrak{c}}$.*⁴

One can consider the nonempty set of integral ideals \mathfrak{c} of K verifying theorem 1.4. It follows that there must exist a maximal element $\mathfrak{c}_{L/K}$ in this set (because \mathcal{O}_K is a Noetherian ring), and it is called the *conductor* of L/K .

1.4 Completions

We will need some terminology and facts concerning completions of number fields, and we discuss them below.

An *absolute value* on a field K is a map $|\cdot| : K \rightarrow \mathbb{R}$ that verifies the following:

- $|x| \geq 0$ for any $x \in K$, and $|x| = 0$ if and only if $x = 0$.
- $|xy| = |x||y|$
- There exists $C > 0$ such that $|x + y| \leq C \max\{|x|, |y|\}$

³In particular, if \mathcal{O}_K is a principal ideal domain (e.g. $K = \mathbb{Q}(i)$) it has no nontrivial abelian unramified extensions.

⁴Here we must restrict the Artin map to $\mathcal{I}_{\mathfrak{c}}(K) \subset \mathcal{I}(K)$ to avoid the possible ramifying primes of L/K

An absolute value is *trivial* if $|x| = 1$ for $x \neq 0$, and two absolute values are *equivalent* if there exists $a \in \mathbb{R}$ with $|x|_1 = |x|_2^a$: one is a positive power of the other. A *valuation* is an absolute value that satisfies the triangle inequality

$$|x + y| \leq |x| + |y|$$

It is a *nonarchimedean valuation* if $|x + y| \leq \max\{|x|, |y|\}$, or an *archimedean valuation* otherwise. Moreover, if the characteristic of K is $\neq 0$ the only valuations on K are nonarchimedean.

If $K \subset \mathbb{C}$ is a number field one can provide K a natural nontrivial archimedean valuation given by

$$|x|_\iota := |\iota(x)|_{\mathbb{C}}$$

where $|\cdot|_{\mathbb{C}}$ is the usual absolute value in \mathbb{C} and $\iota : K \rightarrow \mathbb{C}$ is an embedding.

We can also construct nonarchimedean valuations on a number field. For $x \in K - \{0\}$ the fractional ideal (x) admits the following factorization

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(x)}$$

for some $\nu_{\mathfrak{p}}(x) \in \mathbb{Z}$. $\nu_{\mathfrak{p}}(x)$ is an *exponential valuation* on K , because the following properties

- $\nu_{\mathfrak{p}}(x) \in \mathbb{Z}$ for any $x \in K - \{0\}$
- $\nu_{\mathfrak{p}}(xy) = \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(y)$
- $\nu_{\mathfrak{p}}(x + y) \geq \min\{\nu_{\mathfrak{p}}(x), \nu_{\mathfrak{p}}(y)\}$

make the map $|x|_{\mathfrak{p}} := c^{\nu_{\mathfrak{p}}(x)}$ a nonarchimedean valuation on K for any $c \in (0, 1)$, if we define $\nu_{\mathfrak{p}}(0) = \infty$ formally. It is called the *\mathfrak{p} -adic valuation* on K .

A *place* is an equivalence class of valuations, and it is a *(non)archimedean prime* if the valuations in the equivalence class are (non)archimedean. A field together with a valuation is *complete* if Cauchy sequences are convergent. A *completion* of K is an extension L/K that is complete with respect to a valuation ν' that extends ν and for which every element in L is a limit of elements in K .

In the same way \mathbb{R} is obtained from \mathbb{Q} by considering Cauchy sequences with respect to the usual absolute value, one can obtain completions of a number field with respect to any of its places:

Theorem 1.5. *Let K be a number field and ν a place of K . Let C be the set of Cauchy sequences in K with respect to ν . Then C has a natural ring structure and the quotient $\hat{K} = C/I$ is a completion of K . Moreover, any two completions of K are isomorphic up to isomorphisms preserving ν .*

We denote by K_{ν} the completion of K with respect to ν . Then one can form a discrete valuation ring (DVR) by considering the set

$$R = \{x \in K_{\nu} : \nu(x) \leq 1\}$$

Its maximal ideal is $\mathfrak{m} = \{x \in K_\nu : \nu(x) < 1\}$.

For instance, the p -adic numbers \mathbb{Q}_p is the completion of \mathbb{Q} with respect the p -adic norm.

2 Complex multiplication

In the last section we explained what was the Artin map and Artin reciprocity law, which were obtained by patching together local data in unramified primes. In this section, we will expose that in the case that K is a quadratic imaginary field there is a geometric interpretation of the Artin map in terms of lattices: the fact that the j -invariant of an elliptic curve with CM by \mathcal{O}_K is algebraic lets one define a Galois action on the set of \mathbb{Q} -isomorphism classes of elliptic curves, which turns out to be the same action of the ideal class group on lattices with endomorphism ring \mathcal{O}_K (if the Galois group is that of the Hilbert class field of K).

In other words, complex multiplication will enable us to do class field theory for quadratic imaginary fields.

2.1 Lattices

To describe the endomorphism ring of an elliptic curve over \mathbb{C} we introduce lattices, a class of geometric groups whose set of homomorphisms is easily found. In other words, we first study lattices and its endomorphisms and then relate them to elliptic curves over \mathbb{C} .

A *lattice* is a discrete abelian group $\Lambda \subset \mathbb{C}$ of the form $\Lambda = \langle w_1, w_2 \rangle_{\mathbb{Z}}$ where $w_1, w_2 \in \mathbb{C}$ are \mathbb{R} -linearly independent with $\Im(w_2 w_1^{-1}) > 0$ ⁵. Denote by Lat the set of lattices $\Lambda \subset \mathbb{C}$. The set of *homomorphisms between two lattices* is

$$\text{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha \Lambda_1 \subset \Lambda_2\}$$

and if $\Lambda_1 = \Lambda_2 = \Lambda$ we set $\text{Hom}(\Lambda, \Lambda) = \text{End}(\Lambda)$. Two lattices are *homothetic* if there is an isomorphism between them, i.e. if $\alpha \Lambda_1 = \Lambda_2$ for some $\alpha \in \mathbb{C}$.⁶ Homothety induces an equivalence relation \sim on Lat . Given an homothety class $[\Lambda] \in \text{Lat}_{\sim}$ with $\Lambda = \langle w_1, w_2 \rangle$ we can choose a representative $\Lambda_{\tau} = \langle 1, \tau \rangle_{\mathbb{Z}}$ where $\tau = w_2 w_1^{-1}$ verifies $\tau \in \mathfrak{H}$. However, it does not follow that $\Lambda_{\tau} \sim \Lambda_{\tau'}$ if and only if $\tau = \tau'$. To find a unique representative and for simplicity, from now on we work with lattices of the form Λ_{τ} . Recall that two points $\tau, \tau' \in \mathfrak{H}$ are *equivalent* if $\tau = \gamma \tau'$ for some $\gamma \in \text{SL}_2(\mathbb{Z})$. We denote this by $\tau \sim \tau'$.

From an homothety $\alpha \Lambda_{\tau} = \Lambda_{\tau'}$ we obtain $\alpha \cdot 1 = a + b\tau'$ and $\alpha \cdot \tau = c + d\tau'$ for some integers $a, b, c, d \in \mathbb{Z}$. By arguing similarly with $\Lambda_{\tau} = \alpha^{-1} \Lambda_{\tau'}$ it follows that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ and τ, τ' lie in the same $\text{SL}_2(\mathbb{Z})$ -orbit of \mathfrak{H} . Conversely, for every $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ and $\tau' \in \mathfrak{H}$ the lattice Λ_{τ} with $\tau = (c + d\tau')(a + b\tau')^{-1}$ verifies $\alpha \Lambda_{\tau} = \Lambda_{\tau'}$ where $\alpha = a + b\tau'$. In other words, $\Lambda_{\tau} \sim \Lambda_{\tau'}$ if and only if $\tau \sim \tau'$ and so there is a natural bijection

$$\text{Lat}_{\sim} \leftrightarrow \mathcal{F}$$

between the set of homothety classes of lattices and the fundamental domain \mathcal{F} for the action of $\text{SL}_2(\mathbb{Z})$ in \mathfrak{H} .

⁵In other words, we are choosing an orientation.

⁶Geometrically, that Λ_2 can be obtained by rotating and zooming Λ_1 .

2.1.1 Orders

The endomorphism ring of lattice is a quadratic imaginary order. We introduce them here to know beforehand some of its properties.

Let K be a quadratic imaginary field. An *order* \mathcal{O} of K is a subring of K containing 1 and a \mathbb{Q} -basis of K which is a finitely generated \mathbb{Z} -module. Then every element of \mathcal{O} must be integral over \mathbb{Z} so $\mathcal{O} \subset \mathcal{O}_K = \langle 1, w_K \rangle_{\mathbb{Z}}$ where $w_K = \frac{d_K + \sqrt{d_K}}{2}$ and d_K is the discriminant of K . Therefore \mathcal{O} is a free \mathbb{Z} -module of rank 2 because it contains a \mathbb{Q} -basis of K and its rank is bounded by the rank of \mathcal{O}_K .

The index $f = (\mathcal{O}_K : \mathcal{O})$ is now finite. It is the *conductor* of \mathcal{O} . Then \mathcal{O} can be written as $\mathcal{O} = \langle 1, fw_K \rangle_{\mathbb{Z}}$, and the *discriminant* D of \mathcal{O} is

$$D = \begin{vmatrix} 2 & fd_K \\ fd_K & f^2 \frac{d_K^2 + d_K}{2} \end{vmatrix} = f^2 d_K$$

An order is completely determined by its discriminant:

Theorem 2.1. *For quadratic imaginary fields, there is only one order of discriminant D .*

2.1.2 The endomorphisms of a lattice

Recall that $\text{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$. Note that $\text{End}(\Lambda)$ depends only on the homothety class $[\Lambda] \in \text{Lat}_{\sim}$. Then $\mathcal{O} = \text{End}(\Lambda)$ is a commutative ring and contains \mathbb{Z} . To describe it more precisely, let $\alpha \in \mathcal{O} - \mathbb{Z}$. We obtain $\alpha \cdot 1 = a + b\tau$ and $\alpha \cdot \tau = c + d\tau$ for some integers $a, b, c, d \in \mathbb{Z}$. There are two differences between this situation and the above; now we cannot deduce that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$. On the other hand, by rewriting these equations into a linear system we deduce that α verifies $\alpha^2 - (a+d)\alpha + (ad-bc) = 0$. But $\alpha \notin \mathbb{Z}$ and $\alpha = a + b\tau$ implies that $\mathbb{Q}(\tau)$ is a quadratic extension of \mathbb{Q} . Then \mathcal{O} is an *order* of the quadratic imaginary field $\mathbb{Q}(\tau)$.

2.2 Tori

To relate lattices with elliptic curves we need another intermediate step.

A *complex torus* for a lattice $\Lambda \subset \mathbb{C}$ is the Riemann surface \mathbb{C}/Λ , together with structure of abelian group induced by \mathbb{C} . Denote by Tor the set of tori \mathbb{C}/Λ . The set of homomorphisms *between two complex tori* $T_j = \mathbb{C}/\Lambda_j$ is

$$\text{Hom}(T_1, T_2) = \{\phi : T_1 \rightarrow T_2 \text{ holomorphic morphism of abelian groups}\}$$

Two tori are *equivalent* if they are isomorphic. The morphisms between tori are easily described:

Proposition 2.2. *If $\phi : T_1 \rightarrow T_2$ is an holomorphic morphism then $\phi(z) = \phi_\alpha(z)$ where $\phi_\alpha(z) = \alpha z$ for some $\alpha \in \text{Hom}(\Lambda_1, \Lambda_2)$. Conversely, every $\alpha \in \text{Hom}(\Lambda_1, \Lambda_2)$ induces $\phi_\alpha \in \text{Hom}(T_1, T_2)$ so there is a one-to-one correspondence*

$$\text{Hom}(\Lambda_1, \Lambda) \leftrightarrow \text{Hom}(T_1, T_2)$$

This establishes an equivalence of categories between Lat and Tor .

In particular, there is a bijection $\text{Tor}_\sim \leftrightarrow \text{Lat}_\sim$.

2.3 Elliptic curves over \mathbb{C}

An *elliptic curve* over \mathbb{C} is a nonsingular planar cubic curve $E \subset \mathbb{P}^2(\mathbb{C})$. Denote by $\text{Ell}_\mathbb{C}$ the set of elliptic curves over \mathbb{C} . An *isogeny* $\phi : E_1 \rightarrow E_2$ of elliptic curves defined over a field k is a surjective morphism of curves that induces a group homomorphism $E_1(\bar{k}) \rightarrow E_2(\bar{k})$. The set of isogenies between two elliptic curves is $\text{Hom}(E_1, E_2)$. Two elliptic curves E_1, E_2 are *isomorphic over k* if there exist mutually inverse bijective isogenies between E_1 and E_2 . From now on $k = \mathbb{C}$.

Given a lattice Λ , let E_Λ be the following curve

$$E_\Lambda : Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$$

where $g_2 = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$.⁷ Then E_Λ is an elliptic curve. Conversely, for every elliptic curve E/\mathbb{C} there exists Λ unique up to homothety with $E \simeq E_\Lambda$. To show this, we introduce the *j-invariant*. It is defined by

$$j(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}$$

Because it is a quotient of two modular forms of weight 12 it is $\text{SL}_2(\mathbb{Z})$ -invariant. It can be shown that $j : \mathcal{F} \rightarrow \mathbb{C}$ is injective and surjective. In fact,

Theorem 2.3. *The j-invariant induces an isomorphism between $X(1)$ and $\hat{\mathbb{C}}$.*

Here $X(1)$ can be thought as \mathcal{F} together with a point at infinity (section 3.1). Moreover, two elliptic curves are isomorphic over \mathbb{C} if and only if their *j*-invariants are the same. Thus, there is a one-to-one correspondence between Lat_\sim and $(\text{Ell}_\mathbb{C})_\sim$:

$$\begin{array}{ccc} \text{Lat}_\sim & \longleftrightarrow & (\text{Ell}_\mathbb{C})_\sim \\ \Lambda & \longmapsto & E_\Lambda \end{array}$$

It turns out that elliptic curves over \mathbb{C} are tori:

Theorem 2.4. *The following map*

$$\begin{array}{ccc} \Phi : & \mathbb{C}/\Lambda & \longrightarrow E_\Lambda \\ & z + \Lambda & \longmapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1) \\ & 0 + \Lambda & \longmapsto (0 : 1 : 0) \end{array}$$

is an holomorphic isomorphism of Riemann surfaces, where \wp_Λ is the Weierstrass \wp function associated to Λ .

⁷Here $G_k(\Lambda)$ or $G_k(\tau)$ is the *Eisenstein series of weight k*

Moreover, \wp and \wp' generate all the functions on a complex torus; the field of the *doubly periodic functions* with respect to Λ is $\mathbb{C}(\wp, \wp')$ where \wp denotes the Weierstrass function with respect to Λ .

Theorem 2.5. *Let \wp_1 and \wp_2 denote the Weierstrass functions associated to Λ_1 and Λ_2 . Then the following are equivalent: $\phi_\alpha \in \text{End}(T_1, T_2)$; $\wp_2(\alpha z) \in \mathbb{C}(\wp_1, \wp_1')$; there is an unique $\alpha \in \mathbb{C}$ making the following diagram commute*

$$\begin{array}{ccc} T_1 & \xrightarrow{\phi_\alpha} & T_2 \\ \downarrow \Phi_1 & & \downarrow \Phi_2 \\ E_1 & \xrightarrow{\phi} & E_2 \end{array}$$

where $\phi = \Phi \circ \phi_\alpha \circ \Phi^{-1}$. Moreover, there is an isomorphism of abelian groups between $\text{Hom}(E_1, E_2)$ and $\text{Hom}(T_1, T_2)$.

The isomorphism of rings exists because if we are given an isogeny $\phi : E_1 \rightarrow E_2$ then $\Phi_2^{-1} \circ \phi \circ \Phi_1(z) = f(z)$ is an holomorphic morphism between complex tori, so $f = \phi_\alpha$ for some $\alpha \in \mathbb{C}$, but then $\alpha\Lambda_1 \subset \Lambda_2$ so $\alpha \in \text{End}(\Lambda_1, \Lambda_2)$. Conversely, given $\alpha \in \text{End}(\Lambda_1, \Lambda_2)$ the map $\phi = \Phi_2 \circ \phi_\alpha \circ \Phi_1^{-1}$ is an isogeny $\phi : E_1 \rightarrow E_2$.

Therefore, we have established Lat, Tor and $\text{Ell}_{\mathbb{C}}$ are **equivalent categories**. We particularize theorem 2.5 for $\Lambda_1 = \Lambda_2 = \Lambda$ to obtain the following:

Corollary 2.6. *Suppose $\text{End}(E) \supsetneq \mathbb{Z}$. Then $\text{End}(E)$ is naturally isomorphic to an order \mathcal{O} of a quadratic imaginary field $K \subset \mathbb{C}$*

$$\begin{array}{ccc} \Psi : \text{End}(E) & \xrightarrow{\cong} & \mathcal{O} \subset \mathbb{C} \\ \phi & \longmapsto & \alpha = \Psi(\phi) \end{array}$$

where $\alpha \in \mathbb{C}$ makes the following diagram commute

$$\begin{array}{ccc} T & \xrightarrow{\phi_\alpha} & T \\ \downarrow \Phi & & \downarrow \Phi \\ E & \xrightarrow{\phi} & E \end{array}$$

Here $T = \mathbb{C}/\Lambda$ and $E_\Lambda \simeq E$.

Remark 2.7. The *dual isogeny* for a degree N isogeny $E \rightarrow E'$ is another isogeny $E' \rightarrow E$ such that the composition is the multiplication-by- N map, and exists whenever the isogeny is not constant. For the case $E = E'$, it is particularly easy to find. Given $\alpha \in \mathcal{O}$, the dual isogeny is just $\Phi(\bar{\alpha})$ where $\bar{\alpha}$ denotes the conjugate of α .⁸

This motivates the following definition:

⁸Note that $\bar{\alpha} \in \mathcal{O} \subset \mathcal{O}_K$ because $\text{Tr}(\alpha) = \alpha + \bar{\alpha} \in \mathbb{Z}$.

Definition 2.8. An elliptic curve E/\mathbb{C} has *complex multiplication* by the quadratic imaginary order \mathcal{O} if $E \simeq E_\Lambda$ and $\text{End}(\Lambda) = \mathcal{O}$. We denote the set of elliptic curves with CM by \mathcal{O} by

$$\text{Ell}_{\mathbb{C}}(\mathcal{O}) = \{[E] \in \text{Ell}_{\mathbb{C}} \text{ with CM by } \mathcal{O}\}$$

We define $[\alpha] = \Psi^{-1}(\alpha)$. The *invariant differential* for an elliptic curve is $w = \frac{dx}{y}$. It is invariant under translations in the elliptic curve, hence its name. For instance, the pullback by Φ of w is cdz for some constant c , which is certainly translation invariant. In this case, the pair $(E, [\cdot])$ is *normalized*. The chosen embedding has an additional property:

Corollary 2.9. For any invariant differential $\omega \in \Omega_E$,

$$[\alpha]^*\omega = \alpha\omega$$

where $[\alpha]^*$ denotes the pullback of differential forms by $[\alpha]$.

Example 2.10. Consider the lattice $\Lambda = \Lambda_i$. Then $\mathcal{O} = \text{End}(\Lambda_i)$ clearly contains the Gaussian integers $\mathbb{Z}[i]$, so $\mathcal{O} = \mathbb{Z}[i]$ because \mathcal{O}_K is the maximal order of $K = \mathbb{Q}(i)$. Therefore any elliptic curve \mathbb{C} -isomorphic to E_Λ has complex multiplication by $\mathbb{Z}[i]$. An expression for the isomorphism $[i] : E_\Lambda \rightarrow E_\Lambda$ is easily found because $(X, Y) = (\wp(z), \wp'(z))$ and

$$[i](X, Y) = (\wp(iz), \wp'(iz)) = (-\wp(z), i\wp'(z)) = (-X, iY)$$

because of the properties of the Weierstrass \wp function.

2.4 Binary quadratic forms

Complex multiplication also arises from an algebraic classification problem, namely classifying the set forms of given discriminant. A *form* is a *binary quadratic form*, i.e. an homogeneous polynomial in two variables,

$$f(X, Y) = (a, b, c) = aX^2 + bXY + cY^2$$

satisfying the following conditions: f is *integral*, *primitive* and positive definite. That is, a, b, c are coprime integers verifying $b^2 - 4ac < 0$ and $a > 0$. These latter conditions follow from Sylvester's criterion of positive definiteness, because one can rewrite f as.

$$f(X, Y) = v^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} v$$

with $v = (X, Y)$. The *discriminant* of a form f is $D = b^2 - 4ac$. The set of forms of discriminant D is denoted by $F(D)$. From now on D is a fixed negative integer.

It follows from its definition that the discriminant is invariant under invertible transformations in \mathbb{Z}^2 , hence by the special linear group $\text{SL}_2(\mathbb{Z})$. Moreover, $\text{SL}_2(\mathbb{Z})$ acts on

$F(D)$; for $\gamma = \begin{pmatrix} u & v \\ s & t \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ let $\gamma(X, Y) = (uX + vY, sX + tY)$ and define the action by

$$f^\gamma(X, Y) = f(\gamma(X, Y))$$

Then $f^\gamma \in F(D)$ remains a form. Two forms f, g are *equivalent* if they lie in the same $\mathrm{SL}_2(\mathbb{Z})$ -orbit of $F(D)$. We denote this by $f \sim g$. The set of orbits is the *form class group* of discriminant D denoted by $\mathrm{cl}(D)$, although it is not obvious from its definition that $\mathrm{cl}(D)$ is a finite group. The group operation is the composition of equivalence classes of quadratic forms found by Gauss. There is also an isomorphism $\mathrm{cl}(D) \cong \mathrm{cl}(\mathcal{O}_K)$ when $K = \mathbb{Q}(\sqrt{D})$ has discriminant D .

2.4.1 The form class group is finite

The *principal root* $\tau(f)$ of a form f is the unique solution of the equation $f(\tau, 1) = 0$ lying in \mathfrak{H}^9 , namely $\tau = \frac{-b + \sqrt{D}}{2a}$. By considering principal roots we will be able to choose an unique representative for each orbit in $\mathrm{cl}(D)$. A *reduced* form verifies $-a < b \leq a \leq c$ or $0 \leq b \leq a = c$. Then f is reduced if and only if $\tau(f) \in \mathcal{F}$ where

$$\mathcal{F} = \{z \in \mathbb{C} : |z| \geq 1 \text{ and } -1/2 \leq \Re z \leq 0\} \cup \{z \in \mathbb{C} : |z| > 1 \text{ and } 0 < \Re z \leq 1/2\}$$

Recall that $\mathrm{SL}_2(\mathbb{Z})$ also acts in \mathfrak{H} . Then $\gamma^{-1}\tau$ is the principal root of f^γ . It follows easily that $f \sim g$ if and only if $\tau(f) \sim \tau(g)$.¹⁰ Therefore, every form is equivalent to an unique reduced form because the $\mathrm{SL}_2(\mathbb{Z})$ -translates of \mathcal{F} form a disjoint cover of \mathfrak{H} ; given f compute $\tau(f)$ and find the only $\tau \in \mathcal{F}$ with $\tau \sim \tau(f)$.

Finally, to show that $\mathrm{cl}(D)$ is finite we observe that

$$\min_{\tau \in \mathcal{F}} \Im(\tau) = \frac{\sqrt{3}}{2}$$

.Hence $\Im \tau(f) = \frac{\sqrt{|D|}}{2a} \geq \frac{\sqrt{3}}{2}$ implies $1 \leq a \leq \sqrt{|D|/3}$, so there are only finitely many possibilities for a , and $b \in (-a, a]$ for a fixed a . Therefore

$$h(D) = |\mathrm{cl}(D)| = \text{the number of reduced forms in } F(D) \leq 2 \left(\frac{\sqrt{|D|/3}}{2} \right) \leq |D|/3$$

and finding the reduced forms in $F(D)$ gives an effective procedure to find $h(D)$.

2.4.2 Lattices, proper ideals and forms

Let \mathcal{O} be an order of $K = \mathbb{Q}(\sqrt{D})$. We want to define an ideal class group $\mathrm{cl}(\mathcal{O})$ for \mathcal{O} as we did for number fields to show that $\mathrm{cl}(D) \simeq \mathrm{cl}(\mathcal{O})$. In fact, we only have to show the number of equivalence class of ideals is $|\mathrm{cl}(D)|$ because the product in $\mathrm{cl}(D)$ will be the induced by that of $\mathrm{cl}(\mathcal{O})$. For this to be true, we will have to consider only some of the ideals, the *proper* ideals.

⁹Recall that D is negative.

¹⁰It is also clear that if $f = (a, b, c)$ is reduced then $aX^2 + bX + c$ is the minimal polynomial of $\tau(f)$.

A *fractional \mathcal{O} -ideal* \mathfrak{b} is a finitely generated \mathcal{O} -submodule of K . It is *invertible* if $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ for some \mathfrak{a} , and *proper* if $\mathcal{O}(\mathfrak{b}) = \mathcal{O}$. It turns out a fractional ideal is proper if and only if it is invertible. Then the set of proper ideals $I(\mathcal{O})$ forms a group, so we can form the ideal class group $\text{cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ where $P(\mathcal{O}) \subset I(\mathcal{O})$ is the subgroup of principal ideals.

Now let $f = (a, b, c) \in F(D)$ be a form. The *associated lattice* is $\Lambda_f = a\langle 1, \tau(f) \rangle_{\mathbb{Z}}$. Then $f \sim g$ if and only if $\Lambda_f \sim \Lambda_g$. In other words, $[f] \mapsto [\Lambda_f]$ defines an injection $\Lambda_{[\cdot]} : \text{cl}(D) \hookrightarrow \text{Lat}_{\sim}$. Moreover, these lattices are proper \mathcal{O} -ideals. To show this, let the *order of a lattice* be its set of endomorphisms $\mathcal{O}(\Lambda) = \text{End}(\Lambda)$. Then

Lemma 2.11. $\mathcal{O} \circ \Lambda(f) = \mathcal{O}(\Lambda_f) = \langle 1, a\tau \rangle_{\mathbb{Z}}$, which is the order of discriminant D of $K = \mathbb{Q}(\sqrt{D})$.

Proof. Note that $\mathcal{O}(\Lambda_f) = \mathcal{O}(\Lambda_{\tau})$. One inclusion follows easily by noting $(a\tau)^2 = -b(a\tau) - ac$. For the other, let $\alpha \in \mathcal{O}(\Lambda_f)$. Then $\alpha \cdot 1 = \alpha = u + v\tau$ for some $u, v \in \mathbb{Z}$ so $\alpha \cdot \tau = (u - \frac{bv}{a})\tau - \frac{vc}{a}$ but a, b, c are coprime so $a|v$. \square

In particular, the injection $\Lambda_{[\cdot]} : \text{cl}(D) \rightarrow \text{Lat}_{\sim}(\mathcal{O})$ restricts to lattices with $\text{End}(\Lambda) = \mathcal{O}$. Thus $|\text{cl}(D)| \leq |\text{cl}(\mathcal{O})|$. It only remains to show that every proper \mathcal{O} -ideal is a lattice of a form in $F(D)$.

2.5 $\text{cl}(\mathcal{O})$ acts on $\text{Ell}_{\mathbb{C}}(\mathcal{O})$

With the results above, one can now find all the elliptic curves over \mathbb{C} with CM. Let \mathcal{O} is a quadratic imaginary order. Then the following map

$$\begin{aligned} \text{cl}(\mathcal{O}) &\longleftrightarrow \text{Ell}_{\mathbb{C}}(\mathcal{O}) \\ [\mathfrak{a}] &\longmapsto E_{\mathfrak{a}} \end{aligned}$$

is a bijection. It is well-defined, since every proper \mathcal{O} -ideal \mathfrak{a} is a lattice with $\text{End}(\mathfrak{a}) = \mathcal{O}$, and so for every $E \in [E_{\mathfrak{a}}]$ one has $\text{End}(E) = \text{End}(\mathfrak{a}) = \mathcal{O}$ since $E \simeq E_{\mathfrak{a}}$. Every lattice Λ with $\text{End}(\Lambda) = \mathcal{O}$ is homothetic to a proper \mathcal{O} -ideal, so surjectivity follows. And if $[E_{\mathfrak{a}}] = [E_{\mathfrak{b}}]$ for two fractional proper \mathcal{O} -ideals $\mathfrak{a}, \mathfrak{b}$ then $j(E_{\mathfrak{a}}) = j(E_{\mathfrak{b}})$ so \mathfrak{a} and \mathfrak{b} must be \mathbb{C} -homothetic, so $[\mathfrak{a}] = [\mathfrak{b}]$ in $\text{cl}(\mathcal{O})$.¹¹ Let us define

$$\text{Lat}_{\sim}(\mathcal{O}) = \{[\Lambda] \in \text{Lat}_{\sim} \text{ with } \text{End}(\Lambda) = \mathcal{O}\}$$

and

$$\mathcal{F}(\mathcal{O}) = \{\tau(f) \text{ with } f = (a, b, c) \in F(D)\}$$

Then the correspondence of section 2.3 restricts to $\text{Ell}_{\mathbb{C}}(\mathcal{O}) \leftrightarrow \text{Lat}_{\sim}(\mathcal{O})$. From the discussion in section 2.4 and the bijection $\text{Lat}_{\sim} \leftrightarrow \mathcal{F}$ of section 2.1 it follows that we have a correspondence between finite sets $\text{Lat}_{\sim}(\mathcal{O}) \leftrightarrow \mathcal{F}(\mathcal{O})$. Thus

$$|\text{cl}(\mathcal{O})| = |\text{cl}(D)| = h(D) = |\text{Ell}_{\mathbb{C}}(\mathcal{O})| = |\mathcal{F}(\mathcal{O})|$$

Now let us define the following action

¹¹In this case, \mathbb{C} -homothety implies \mathcal{O} -homothety.

$$\begin{aligned} \mathrm{cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathbb{C}}(\mathcal{O}) &\longrightarrow \mathrm{Ell}_{\mathbb{C}}(\mathcal{O}) \\ [\mathfrak{a}], E_{\mathfrak{b}} &\longmapsto \mathfrak{a}E_{\mathfrak{b}} = E_{\mathfrak{a}^{-1}\mathfrak{b}} \end{aligned}$$

It is indeed a well-defined action. The crucial fact here is that it is a *free* action: if $[E_{\mathfrak{a}^{-1}\mathfrak{b}}] = [E_{\mathfrak{b}}]$ then \mathfrak{a} is principal, since $\mathfrak{a}^{-1}\mathfrak{b}$ and \mathfrak{b} must be homothetic and \mathfrak{b} is invertible because it is proper. In general, if we have a free group action $G \curvearrowright X$ with $|G| = |X|$ finite then it is *transitive*, i.e. the orbit of any element is X . Hence, our action above is transitive.

Example 2.12. For instance, there is only one isomorphism class of elliptic curves with CM by $\mathcal{O} = \mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{-2}]$ because they are both principal ideal domains, and there are two isomorphism classes when $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$. These are simple examples because they are all maximal orders.

2.5.1 The action in terms of isogenies

The action $\mathrm{cl}(\mathcal{O}) \curvearrowright \mathrm{Ell}_{\mathbb{C}}(\mathcal{O})$ can be interpreted in terms of isogenies.

Let $\phi : E_1 \rightarrow E_2$ be an isogeny with $E_i = E_{\Lambda_i}$ and denote by $T_i = \mathbb{C}/\Lambda_i$. Then by theorem 2.5 there exists $\alpha \in \mathrm{Hom}(\Lambda_1, \Lambda_2)$ with $\alpha\Lambda_1 \subset \Lambda_2$ and $\phi = \Phi_2\phi_\alpha\Phi_1^{-1}$. Denote by $\Lambda'_1 = \alpha\Lambda_1$ and $T'_1 = \mathbb{C}/\Lambda'_1$. The lattices Λ_1 and Λ'_1 are then \mathbb{C} -homothetic, so $\varphi' : T_1 \xrightarrow{z \mapsto \alpha z} T'_1$ is an isomorphism and the natural inclusion $\varphi'' : T'_1 \xrightarrow{z \mapsto z} T_2$ has kernel $\ker \varphi'' \simeq \Lambda'_1/\Lambda_2$. Moreover, $\phi_\alpha = \varphi''\varphi'$. In other words, every isogeny is induced by an inclusion of tori up to \mathbb{C} -isomorphism.¹²

If E_1/\mathbb{C} has CM by \mathcal{O} then Λ_1 is homothetic to a proper \mathcal{O} -ideal \mathfrak{b} , and if \mathfrak{a} is a proper \mathcal{O} -ideal then so is $\mathfrak{a}^{-1}\mathfrak{b}$. The inclusion of lattices $\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{b}$ induces an isogeny $\phi_{\mathfrak{a}} : E_{\mathfrak{b}} \rightarrow E_{\mathfrak{a}^{-1}\mathfrak{b}}$. Therefore, all elliptic curves with CM by \mathcal{O} are isogeneous, because the action is transitive. The kernel of $\phi_{\mathfrak{a}} : E \rightarrow \mathfrak{a}E$ can be shown to be

$$E[\mathfrak{a}] = \{P \in E : \alpha P = 0 \text{ for all } \alpha \in \mathfrak{a}\}$$

2.6 The Hilbert class polynomial

Let \mathcal{O} be a imaginary quadratic order of discriminant D . The *Hilbert class polynomial* is

$$H_D(X) = \prod_{[E] \in \mathrm{Ell}_{\mathbb{C}}(\mathcal{O})} (X - j(E))$$

By using the properties of the modular polynomial Φ_N for N prime in section 3.5.4 we will show that $H_D(X) \in \mathbb{Z}[X]$. We only have to take for granted theorem 3.12 and the following theorem

Theorem 2.13 (Dirichlet, Weber). *There are infinitely many prime ideals \mathfrak{p} of prime norm $(\mathcal{O} : \mathfrak{p})$ in every class of $\mathrm{cl}(\mathcal{O})$.*

¹²Because in general, although $E_i \simeq E_{\Lambda_i}$, $E_i \neq E_{\Lambda_i}$.

We proceed.

Theorem 2.14. *One has $H_D(X) \in \mathbb{Z}[X]$. Thus, the j -invariant of an elliptic curve E with CM is an algebraic integer, and E can be defined over $\overline{\mathbb{Q}}$.*

Proof. Let $E \in \text{Ell}_{\mathbb{C}}(\mathcal{O})$ and $\mathfrak{p} = \alpha\mathcal{O}$ a principal ideal of norm p . Then $[\mathfrak{p}]$ acts trivially on $\text{Ell}_{\mathbb{C}}(\mathcal{O})$ and there is an isomorphism $\varphi : \mathfrak{p}E \xrightarrow{\sim} E$. If \mathfrak{b} is a lattice with $E_{\mathfrak{b}} \simeq E$ then the inclusion of lattices $\mathfrak{b} \subset \mathfrak{p}^{-1}\mathfrak{b}$ induces an isogeny $\phi : E \rightarrow \mathfrak{p}E$ with $\ker \phi \simeq \mathfrak{p}^{-1}\mathfrak{b}/\mathfrak{b}$, but for principal ideals $(\mathfrak{p}^{-1}\mathfrak{b} : \mathfrak{b}) = (\mathfrak{b} : \mathfrak{p}\mathfrak{b}) = (\mathcal{O} : \mathfrak{p}) = p$, thus ϕ is cyclic. Hence $\varphi \circ \phi$ is a degree p isogeny of E onto itself, and so by theorem 3.14 one has $\Phi_p(j(E), j(E)) = 0$. Thus $j(E)$ is an algebraic integer because $\Phi_p(X, X)$ is a monic polynomial by theorem 3.15, and E can be defined over $\overline{\mathbb{Q}}$.

Let $\text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O})$ be the set of equivalence classes of elliptic curves defined over $\overline{\mathbb{Q}}$ modulo $\overline{\mathbb{Q}}$ -isomorphism. Then there is a bijection between $\text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O})$ and $\text{Ell}_{\mathbb{C}}(\mathcal{O})$ ¹³. The absolute Galois group $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O})$ as follows: for every $\sigma \in G$ and $[E] \in \text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O})$ with $E : y^2 = 4x^3 - Ax - B$ we define $E^{\sigma} : y^2 = 4x^3 - A^{\sigma}x - B^{\sigma}$. Given an isogeny $\phi : E \rightarrow E$ defined over $\overline{\mathbb{Q}}$, ϕ^{σ} is obtained by applying σ to the coefficients in an expression for ϕ , so $\text{End}(E) \simeq \text{End}(E^{\sigma})$.

The coefficients are symmetric functions on the j -invariants for $[E] \in \text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O})$, thus invariant under the action of G so $H_D(X) \in \mathbb{Q}$. But E was arbitrary so $H_D(X) | \Phi_p(X, X)$ in $\mathbb{Q}[X]$, because $\Phi_p(X, X) \in \mathbb{Q}[X]$ by theorem 3.12. Finally, Φ_p is monic by theorem 3.15, so by Gauss lemma it follows that $H_D(X) \in \mathbb{Z}[X]$. \square

2.7 The Galois action

Let $\mathcal{O} \subset K$ be an order of discriminant D and K a quadratic imaginary field. In the proof of theorem 2.14 we considered the action of the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Note that many elements do not fix K . To simplify the picture, we take an smaller group $G = \text{Gal}(L/K)$ where L is the splitting field of $H_D(X)$. For each $\sigma \in G$ the curve E^{σ} has CM by \mathcal{O} . The action of the class group in section 2.5 is free and transitive so $E^{\sigma} \simeq \mathfrak{a}E$ for some unique $\mathfrak{a} \in \text{cl}(\mathcal{O})$. Moreover, the Galois action and the class group action are nicely related

Lemma 2.15. *For any $E \in \text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O})$, $\sigma \in G$ and $\mathfrak{b} \in \text{cl}(\mathcal{O})$ one has $(\mathfrak{b}E)^{\sigma} = \mathfrak{b}^{\sigma}E^{\sigma}$.*

Taking this for granted, it follows that \mathfrak{a} depends only on σ : for any $E' \in \text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O})$, $E' \simeq \mathfrak{b}E$ for some $\mathfrak{b} \in \text{cl}(\mathcal{O})$ by transitivity. Thus $E'^{\sigma} \simeq (\mathfrak{b}E)^{\sigma} = \mathfrak{b}^{\sigma}E^{\sigma} = \mathfrak{b}E^{\sigma} \simeq \mathfrak{b}\mathfrak{a}E = \mathfrak{a}\mathfrak{b}E \simeq \mathfrak{a}E'$. Here $\mathfrak{b}^{\sigma} = \mathfrak{b}$ because σ fixes K and $\mathfrak{b} \subset \mathcal{O} \subset K$. Therefore we have a well-defined injective¹⁴ map

¹³If two elliptic curves are $\overline{\mathbb{Q}}$ -isomorphic they are \mathbb{C} -isomorphic. Conversely, if E, E' are \mathbb{C} -isomorphic with CM by \mathcal{O} then both can be defined over $\overline{\mathbb{Q}}$ because their j -invariant is the same and belongs to $\overline{\mathbb{Q}}$. It can be shown that then they are $\overline{\mathbb{Q}}$ -isomorphic.

¹⁴Given $E \in \text{Ell}_{\overline{\mathbb{Q}}}(\mathcal{O})$, the only element in G fixing $j(E)$ is the identity.

$$\begin{aligned}\Psi : \text{Gal}(L/K) &\hookrightarrow \text{cl}(\mathcal{O}) \\ \sigma &\longmapsto \Psi(\sigma) = \mathfrak{a}\end{aligned}$$

where $E^\sigma = \mathfrak{a}E$. It is a group homomorphism since for any E

$$\Psi(\sigma\tau)E = E^{\sigma\tau} = (E^\sigma)^\tau = (\Psi(\sigma)E)^\tau = \Psi(\tau)\Psi(\sigma)E = \Psi(\sigma)\Psi(\tau)E$$

The injectivity of Ψ implies that $\text{Gal}(L/K)$ is abelian, and $[L : K] \leq h(D)$. In fact, Ψ surjects.

The splitting field L is known as the *ring class field* of \mathcal{O} . In the case where the order $\mathcal{O} = \mathcal{O}_K$ is maximal L is the *Hilbert class field*, which is also the maximal unramified abelian extension of K .

2.8 The First Main theorem of Complex Multiplication

The goal of this section is to prove that Ψ is an isomorphism. The previous results together with the Artin map of section 1.2 help in the proof of this result:

Theorem 2.16. *Let \mathcal{O} be a quadratic imaginary order of discriminant D and L the splitting field of $H_D(X)$ over $K = \mathbb{Q}(\sqrt{D})$. Then there is an isomorphism*

$$\begin{aligned}\Psi : \text{Gal}(L/K) &\xrightarrow{\sim} \text{cl}(\mathcal{O}) \\ \sigma &\longmapsto \Psi(\sigma) = \mathfrak{a}\end{aligned}$$

where $E^\sigma = \mathfrak{a}E$.

Proof. Take $[\mathfrak{a}] \in \text{cl}(\mathcal{O})$ and let \mathfrak{p} be a prime of K satisfying the following conditions

- (a) $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}$ is a proper \mathcal{O} -ideal of prime norm with $[\mathfrak{q}] = [\mathfrak{a}]$
- (b) p and \mathfrak{p} are unramified in K and L respectively
- (c) For every $[E] \in \text{Ell}_L(\mathcal{O})$ there exists an elliptic curve E/L with good reduction modulo \mathfrak{P} for any prime \mathfrak{P} of L above \mathfrak{p}
- (d) The elements in $\{j(E)\}_{[E] \in \text{Ell}_L(\mathcal{O})}$ are distinct¹⁵ modulo \mathfrak{P} for $\mathfrak{P}|\mathfrak{p}$

There are infinitely many \mathfrak{p} for which these conditions hold, because theorem 2.13 assures the existence of infinitely many \mathfrak{q} verifying condition a and because we can lift the prime \mathfrak{q} to a prime $\mathfrak{p} = \mathfrak{q}\mathcal{O}_K$ of K provided that \mathfrak{q} does not contain (f) , where f is the conductor of \mathcal{O} defined in section 2.1.1.

For condition b recall that in a finite extension only finitely many primes ramify¹⁶. For c take a representative E of $[E]$ i.e. choose a Weierstrass model and avoid primes \mathfrak{P} of L dividing the discriminant of the curve¹⁷, and for condition d avoid primes \mathfrak{P} of

¹⁵Condition d lets us detect whether two curves are isomorphic or not by checking if they are isomorphic modulo \mathfrak{P} .

¹⁶Namely, those dividing the discriminant of the extension defined in section 1.

¹⁷Because those are the primes of *bad reduction*.

L appearing in the factorizations in \mathcal{O}_L of the elements in $\{j(E) - j(E')\}_{[E] \neq [E']}$ where $[E], [E'] \in \text{Ell}_L(\mathcal{O})$.

Fix \mathfrak{P} above \mathfrak{p} and E/L with good reduction modulo \mathfrak{P} . Let $\overline{E}/\mathbb{F}_{\mathfrak{P}}$ be the reduction of E modulo \mathfrak{P} , obtained by reducing the coefficients in L of the equation of E modulo \mathfrak{P} . So if E is given by $E : Y^2 = X^3 + AX + B$ with $A, B \in \mathcal{O}_L$ then $\overline{E} : Y^2 = X^3 + \overline{A}X + \overline{B}$ and $\Delta(\overline{E}) \neq 0$.

Now \mathfrak{p} is unramified so we may form the Artin symbol $\sigma = (\mathfrak{p}, L/K)$ as in section 1.2, and $(\mathcal{O}_K : \mathfrak{p}) = (\mathcal{O} : \mathfrak{q}) = p$. Recall that σ verifies $\sigma(x) \equiv x^p \pmod{\mathfrak{P}}$, i.e. $\mathcal{Q}(\sigma) = \overline{\sigma}$ is the Frobenius element. Then σ induces an isogeny $\pi : \overline{E} \rightarrow \overline{E}^{\overline{\sigma}}$ by applying $\overline{\sigma}$ coordinatewise $\pi(x, y) = (x^p, y^p)$ from \overline{E} to $\overline{E}^{\overline{\sigma}} : Y^2 = X^3 + \overline{A}^p X + \overline{B}^p$.

Recall from section 2.5.1 that \mathfrak{q} induces a degree p isogeny $\phi_{\mathfrak{q}} : E \rightarrow \mathfrak{q}E$. Note that $\mathfrak{q}E$ has good reduction modulo \mathfrak{P} by condition c. Then by reducing $\phi_{\mathfrak{q}}$ modulo \mathfrak{P} we obtain $\phi : \overline{E} \rightarrow \overline{\mathfrak{q}E}$. It can be shown that ϕ has again degree p . The composition of ϕ with its dual isogeny¹⁸ $\hat{\phi}$ is the multiplication-by- p map m_p , which is *purely inseparable*¹⁹ in characteristic p . Then either ϕ or $\hat{\phi}$ is inseparable, because separability is transitive for extensions, so we may suppose this is the case for ϕ . It turns out that every inseparable isogeny factors as a composition of an n -th power of π and a separable map φ' , for some $n \geq 0$, i.e.

$$\varphi = \varphi' \circ \pi^n$$

But here $\varphi = \phi$ and $\deg \varphi = \deg \varphi' \deg \pi^n = p = d \cdot p^n$ with $p \nmid d$ so $d = 1$ and $n = 1$. Thus $\varphi' : \overline{E}^{\overline{\sigma}} \xrightarrow{\sim} \overline{\mathfrak{q}E}$ is an isomorphism i.e. $j(E^{\sigma}) = j(\overline{E}^{\overline{\sigma}}) = j(\overline{\mathfrak{q}E}) = j(\mathfrak{q}E)$ and condition d implies $[\mathfrak{q}E] = [E^{\sigma}]$. Therefore Ψ surjects. \square

2.8.1 Relating $\text{cl}(\mathcal{O})$ with $\text{cl}(\mathcal{O}_K)$

From now on, we shall denote the field L in the proof of theorem 2.16 by K_f or the *ring class field of conductor f* . Note that the result above is an special case of a weakening of theorem 1.4 i.e. the conductor in this case is principal $\mathfrak{c} = (n)$ and it is generated by the conductor of \mathcal{O} , hence its name. From theorem 1.4 we deduce that the primes of K ramifying in $L = K_n$ are precisely those dividing the conductor n .

Section 4.5 will require an accurate description of some Galois groups involving the ring class fields, and this reduces to relate $\text{cl}(D)$ with $\text{cl}(\mathcal{O}_K)$. For this, we will now relate the proper \mathcal{O} -ideals with the ideals of \mathcal{O}_K , we introduce another family of ideals, and discuss some results on them that we will not prove (see [1] prop. 7.19-7.24). We suppose throughout this section that $\mathcal{O}_K^{\times} = \{\pm 1\}$.

A nonzero \mathcal{O} -ideal \mathfrak{a} is *prime to f* if $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$. This equivalent to the norm $(\mathcal{O} : \mathfrak{a})$ being relatively prime to f , since the injective²⁰ map $\mathcal{O}/\mathfrak{a} \rightarrow \mathcal{O}/\mathfrak{a}$ where $x \mapsto xf$ surjects

¹⁸See remark 2.7

¹⁹A nonconstant morphism $\varphi : C \rightarrow C'$ defined over a field K between curves over K has the property \mathcal{P} if so does the field extension $K(C')/\varphi^*K(C)$ where $\varphi^* : K(C') \rightarrow K(C)$ is defined by $f \mapsto f \circ \varphi$. \mathcal{P} can be separability, Galois, etc.

²⁰The map $\mathcal{O} \rightarrow \mathcal{O}$ where $x \mapsto xf$ injects.

precisely when \mathfrak{a} is prime to f i.e. when f is coprime to the cardinal $(\mathcal{O} : \mathfrak{a})$ of the finite abelian group \mathcal{O}/\mathfrak{a} .

Every \mathcal{O} -ideal prime to f is proper since $f\mathcal{O}_K \subset \mathcal{O}$ and if $\alpha \in \text{End}(\mathfrak{a})$ then $\alpha\mathcal{O} = \alpha(\mathfrak{a} + f\mathcal{O}) \subset \mathfrak{a} + f\mathcal{O}_K \subset \mathfrak{a} + \mathcal{O} \subset \mathcal{O}$ as wanted. The \mathcal{O} -ideals prime to f generate a subgroup $I(\mathcal{O}, f) \subset I(\mathcal{O})$ since the ideal norm is multiplicative. They also suffice to form the ideal class group $\text{cl}(\mathcal{O})$

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq \text{cl}(\mathcal{O})$$

Moreover, there is an isomorphism²¹

$$\begin{array}{ccc} \eta : I(\mathcal{O}, f) & \longrightarrow & I(\mathcal{O}_K, f) \\ \mathfrak{a} \cap \mathcal{O} & \longleftarrow & \mathfrak{a} \\ \mathfrak{b} & \longmapsto & \mathfrak{b}\mathcal{O}_K \end{array} \quad (2.1)$$

2.8.2 Some Galois groups of ring class fields

Taking these results for granted, it follows that if $P = \eta(P(\mathcal{O}, f))$ we have a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & I(\mathcal{O}_K, f) \cap P(\mathcal{O}_K)/P & \longrightarrow & I(\mathcal{O}_K, f)/P & \longrightarrow & I(\mathcal{O}_K)/P(\mathcal{O}_K) \\ & & & & \downarrow \simeq & & \downarrow \simeq \\ & & & & \text{cl}(\mathcal{O}) & \xrightarrow{\pi} & \text{cl}(\mathcal{O}_K) \end{array}$$

Since the induced map $\pi : \text{cl}(\mathcal{O}) \rightarrow \text{cl}(\mathcal{O}_K)$ surjects it follows that

$$\ker \pi \simeq I(\mathcal{O}_K, f) \cap P(\mathcal{O}_K)/P$$

We also have the following exact sequence

$$1 \longrightarrow (\mathbb{Z}/f\mathbb{Z})^\times \longrightarrow (\mathcal{O}_K/f\mathcal{O}_K)^\times \longrightarrow \ker \pi \longrightarrow 1$$

and if we let $f = \ell$ be a prime ℓ which is inert in K , then the residue field for $\mathfrak{P} = \ell\mathcal{O}_K$ above ℓ is $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\ell\mathcal{O}_K$ and the inertial degree is $[\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_\ell] = 2$. Thus

$$\ker \pi \simeq (\mathcal{O}_K/f\mathcal{O}_K)^\times / (\mathbb{Z}/f\mathbb{Z})^\times = \mathbb{F}_{\ell\mathcal{O}_K}^\times / \mathbb{F}_\ell^\times$$

Since theorem 2.16 implies $\text{Gal}(K_1/K) \simeq \text{cl}(\mathcal{O}_K)$ and $\text{Gal}(K_f/K) \simeq \text{cl}(\mathcal{O})$, by the naturality of these isomorphisms we have that the following diagram commutes

$$\begin{array}{ccccccc} 1 & \longrightarrow & \text{Gal}(K_f/K_1) & \longrightarrow & \text{Gal}(K_f/K) & \longrightarrow & \text{Gal}(K_1/K) \longrightarrow 1 \\ & & \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq \\ 1 & \longrightarrow & \ker \pi & \longrightarrow & \text{cl}(\mathcal{O}) & \longrightarrow & \text{cl}(\mathcal{O}_K) \longrightarrow 1 \end{array}$$

In particular, $\text{Gal}(K_\ell/K_1) \simeq \ker \pi$ is cyclic with

$$|\text{Gal}(K_\ell/K_1)| = |\ker \pi| = |\mathbb{F}_{\ell^2}^\times / \mathbb{F}_\ell^\times| = (\ell^2 - 1)/(\ell - 1) = \ell + 1$$

elements.

²¹It also implies the unique factorization for ideals in $I(\mathcal{O}, f)$, since \mathcal{O}_K is Dedekind.

3 Modular curves

In this section we define the modular curve in two ways, as a quotient of the upper half-plane modulo a certain subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and as an algebraic curve. The first approach provides a formula its genus in function of the subgroup by applying results on Riemann surfaces. The second approach shows that the modular curve classifies somehow the isogenies between elliptic curves. This requires studying the field of functions that one can define on the curve.

3.1 The modular curve

The *upper half plane* is $\mathfrak{H} = \{z \in \mathbb{C} : \Im z > 0\}$. The *special linear group* over \mathbb{Z} is

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}$$

and the following map defines an action of $\mathrm{SL}_2(\mathbb{Z})$ on \mathfrak{H} .

$$\begin{aligned} \mathfrak{H} \times \mathrm{SL}_2(\mathbb{Z}) &\longrightarrow \mathfrak{H} \\ (z, \gamma) &\longmapsto \gamma(z) := \frac{az+b}{cz+d} \end{aligned}$$

In particular, note that for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the formula

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

shows that the action is well-defined. However, this action is not faithful. This leads one to consider the *modular group* which identifies elements in $\mathrm{SL}_2(\mathbb{Z})$ according to the action above. This is $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ where $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Each element of the modular group represents a linear fractional transformation, and these can be extended to be the automorphisms of the Riemann sphere. In projective coordinates,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(u : v) = (au + bv : cu + dv)$$

It can be shown that the modular group is generated by $\tau \mapsto \tau + 1$ and $\tau \mapsto \tau^{-1}$.

The *principal congruence subgroup* of level $N \geq 1$ is the following subgroup of $\mathrm{SL}_2(\mathbb{Z})$

$$\Gamma(N) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if there exists $N \geq 1$ with $\Gamma \supset \Gamma(N)$. It can be shown that the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite, hence $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < \infty$ holds too. Given a congruence subgroup Γ , the *modular curve* of Γ is the set of orbits for the action of Γ on \mathfrak{H} , i.e. $Y(\Gamma) = \Gamma \backslash \mathfrak{H}$ together with the quotient topology induced by the map

$$\begin{aligned} \pi : \mathfrak{H} &\longrightarrow Y(\Gamma) \\ s &\longmapsto \Gamma s \end{aligned}$$

if we endow \mathfrak{H} with the Euclidean topology. Here π is an open map because given an open subset $U \subset \mathfrak{H}$ we have

$$\pi^{-1}(\pi(U)) = \bigcup_{\gamma \in \Gamma} \gamma U = \Gamma U$$

which is an open set because the elements $\gamma \in \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ are homeomorphisms. It follows that $Y(\Gamma)$ is connected because π is continuous by construction and \mathfrak{H} is connected.

Example 3.1. One important example is $Y(1) = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}$ because it can be shown that every point in $Y(1)$ represents a \mathbb{C} -isomorphism class of elliptic curves. Moreover, it turns out that if we let \mathcal{F} be

$$\mathcal{F} = \{z \in \mathbb{C} : |z| \geq 1 \text{ and } -1/2 \leq \Re z \leq 0\} \cup \{z \in \mathbb{C} : |z| > 1 \text{ and } 0 < \Re z \leq 1/2\}$$

then $Y(1) = \mathcal{F} / \sim$ where \sim here means identifying $z + 1/2 \equiv z - 1/2$ when $\Re z = 0$ and $z \equiv -z^{-1}$ when $|z| = 1$.²²

3.2 Elliptic points

Moreover, $Y(\Gamma)$ is a Riemann surface. To prove this one has to give local charts in every point of $Y(\Gamma)$. Given $\tau \in \mathfrak{H}$ define the isotropy subgroup of τ to be the elements in Γ that fix τ

$$\Gamma_\tau = \{\gamma \in \Gamma : \gamma(\tau) = \tau\}$$

Then $\tau \in \mathfrak{H}$ is an *elliptic point* for Γ if $\{\pm I\}\Gamma_\tau/\{\pm I\}$ is nontrivial. In other words, if the isotropy subgroup is nontrivial when we identify each element of Γ_τ with a linear fractional transformation. The cardinal $h_\tau^\Gamma = |\{\pm I\}\Gamma_\tau/\{\pm I\}|$ is called the *period of τ* and hence τ is elliptic if $h_\tau^\Gamma > 1$. Moreover, the period depends only on $\Gamma\tau$ because for $\gamma \in \Gamma$

$$\Gamma_{\gamma\tau} = (\gamma\Gamma\gamma^{-1})_{\gamma\tau} = \gamma\Gamma_\tau\gamma^{-1} \simeq \Gamma_\tau$$

Thus the period is defined for points in $Y(\Gamma)$. In fact, if $\Gamma \triangleleft \mathrm{SL}_2(\mathbb{Z})$ is normal subgroup the above is valid for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and the period is the same for all points in the orbit of τ when $\mathrm{SL}_2(\mathbb{Z})$ acts on \mathfrak{H} . It remains to find the elliptic points, and it is sufficient to find them when $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ because Γ_τ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})_\tau$.

Theorem 3.2. *The elliptic points for $\mathrm{SL}_2(\mathbb{Z})$ are the elements in $\mathrm{SL}_2(\mathbb{Z}) \cdot i$ or $\mathrm{SL}_2(\mathbb{Z}) \cdot \zeta$ (the orbit of i and ζ respectively), where $\zeta^3 = 1, \zeta \neq 1$. Moreover, the isotropy subgroup is finite cyclic of order ≤ 3 .*

There are congruence subgroups Γ for which there are no elliptic points, for instance $\Gamma = \Gamma_0(N)$ with $p|N$ for some prime $p \equiv -1 \pmod{12}$ and

$$\Gamma_0(N) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{n}\}$$

²² \mathcal{F} is called a *fundamental domain* for $Y(1)$ because there exists a boundary identification \sim with $Y(1) = \mathcal{F} / \sim$. In particular, the upper-half plane is tiled by the $\mathrm{SL}_2(\mathbb{Z})$ -translates of \mathcal{F} , $\mathfrak{H} = \mathrm{SL}_2(\mathbb{Z}) \cdot \mathcal{F}$.

It can be shown that for every point $\Gamma\tau \in Y(\Gamma)$ there exists a sufficiently small neighborhood U of τ containing at most one elliptic point (when τ is elliptic) such that the following map is a chart

$$\begin{aligned} \varphi : \pi(U) &\longrightarrow V \\ \Gamma u &\longmapsto \delta_\tau(u)^{h_\tau} \end{aligned}$$

where $\delta_\tau(u) = \frac{u-\tau}{u-\bar{\tau}}$ ^{23 24}. These charts define a complex atlas on $Y(\Gamma)$.

3.3 Cusps and $X(\Gamma)$

Let $\mathfrak{H}^* = \mathfrak{H} \cup \{\infty\}$. Then $\mathrm{SL}_2(\mathbb{Z})$ acts on \mathfrak{H}^* and the orbit of ∞ is $\mathbb{Q} \cup \{\infty\}$ because if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $c \neq 0$ then $\gamma(\infty) = a/c$ is a rational number.

We define $X(\Gamma)$ as the set of orbits of the action of Γ on \mathfrak{H}^*

$$X(\Gamma) = \Gamma \backslash \mathfrak{H}^*$$

The *cusps* of Γ are the equivalence classes of $\mathbb{Q} \cup \{\infty\}$ under Γ . If we endow \mathfrak{H}^* with a convenient topology we will be able to include $Y(\Gamma)$ in $X(\Gamma)$ with $X(\Gamma)$ being a compact space, and this fact will allow us to compute the genus after applying some tools for compact Riemann surfaces.

We define the open sets on \mathfrak{H}^* to be the open sets in \mathfrak{H} together with the sets $\gamma(N_m \cup \{\infty\})$ where γ runs over $\mathrm{SL}_2(\mathbb{Z})$ and

$$N_m = \{z \in \mathbb{C} : \Im z > m\}$$

which are the neighborhoods of ∞ . The boundary of these sets $\gamma(N_m \cup \{\infty\})$ are either a line or a circle that is tangent to the real axis, because $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is a fractional linear transformation. Now $X(\Gamma)$ is $Y(\Gamma)$ together with the cusps of Γ

$$X(\Gamma) = \Gamma \backslash \mathfrak{H}^* = Y(\Gamma) \cup \Gamma \cdot (\mathbb{Q} \cup \{\infty\})$$

and endowed with the quotient topology given by $\pi^* : \mathfrak{H}^* \rightarrow X(\Gamma)$. This is adding only finitely many points (the cusps), because the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is finite and

$$\mathrm{SL}_2(\mathbb{Z}) \cdot (\mathbb{Q} \cup \{\infty\}) = \mathbb{Q} \cup \{\infty\} = \left(\bigcup_i \Gamma \gamma_i \right) \cdot (\mathbb{Q} \cup \{\infty\})$$

In this process we have not lost any of the topological properties of $Y(\Gamma)$,

Theorem 3.3. [2] $X(\Gamma)$ is connected, Hausdorff and compact.

²³The map centers the neighborhood by sending $\tau \mapsto 0$ and $\bar{\tau} \mapsto \infty$.

²⁴This suggests that π sends the neighborhood of an elliptic point τ in to a neighborhood of $\pi(\tau)$ in which every point but τ has h_τ preimages.

The compactness of $X(\Gamma)$ follows from the compactness of $\mathcal{F}^* = \mathcal{F} \cup \{\infty\}$ ²⁵ and the finiteness of the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$, because if $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_i \Gamma \gamma_i$ then

$$X(\Gamma) = \Gamma \cdot \mathfrak{H}^* = \Gamma \cdot (\mathrm{SL}_2(\mathbb{Z}) \cdot \mathcal{F}^*) = \bigcup_i \Gamma \gamma_i \mathcal{F}^*$$

and so $X(\Gamma)$ is compact for being a finite union of compacts.

To prove that $X(\Gamma)$ is still a (compact) Riemann surface, one has to give charts at the cusps. Recall that π has h_τ^Γ preimages in a neighborhood of an elliptic point. It turns out that π has infinitely many preimages in a neighborhood of a cusp²⁶. $\mathrm{SL}_2(\mathbb{Z})_\infty$ is generated by $\tau \mapsto \tau + 1$, because if $\gamma(\infty) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(\infty) = \infty$ then $c = 0$ and $ad - bc = 1$ implies that $a = d = \pm 1$ and thus $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\pm b}$ is a translation. In other words, the period is not defined at a cusp. The *width* of a cusp $s \in \mathbb{Q} \cup \{\infty\}$ is defined as

$$h_{s,\Gamma} = |\mathrm{SL}_2(\mathbb{Z})_\infty / (\delta\{\pm I\}\Gamma\delta^{-1})_\infty|$$

where $\delta(s) = \infty$. Then $h_{s,\Gamma}$ is counting the number of $\mathrm{SL}_2(\mathbb{Z})_\infty$ -translates of \mathcal{F}^* which are distinct under Γ -isotropy. At the cusps $\Gamma s \in X(\Gamma)$ the charts are

$$\begin{aligned} \varphi : \pi(U) &\longrightarrow V \\ \Gamma u &\longmapsto \exp(2\pi i \delta_s(u)/h_{s,\Gamma}) \end{aligned}$$

where $\delta_s(s) = \infty$. This transforms \mathcal{F}^* into a $2\pi/h_{s,\Gamma}$ sector of the unit disk, sending $s \mapsto 0$. In short,

Theorem 3.4. *The topology and the charts treated above define a complex atlas for $X(\Gamma)$. Thus $X(\Gamma)$ is a compact Riemann surface.*

3.4 The genus of $X(\Gamma)$

A compact Riemann surface X is in particular a compact topological surface and every such space is homeomorphic to a g -holed torus, where g is the *genus* of X . One can recover the genus g_X of $X = X(\Gamma)$ for Γ a congruence subgroup by counting the cusps and the elliptic points of $X(\Gamma)$, by using some identities that apply to general compact Riemann surfaces.

If $f : X \rightarrow Y$ is a nonconstant holomorphic map between compact connected Riemann surfaces, it surjects because $\mathrm{im} f$ is both open (by the open mapping theorem for holomorphic functions) and closed ($\mathrm{im} f$ is compact in a Hausdorff space, thus closed). The *degree* d is defined as follows. For any $y \in Y$ let

$$d = \sum_{x \in f^{-1}(y)} e_x$$

²⁵Any open cover of \mathcal{F}^* must contain a neighborhood of ∞ of the form N_m . Thus a finite open subcover is N_m together with a finite open subcover of $\mathcal{F}^* - N_m$, which is compact in the Euclidean topology.

²⁶This does not enter in contradiction with the theory of Riemann surfaces, because \mathfrak{H}^* is not compact.

where e_x is the *ramification degree* of f at x defined by the local expression of f given by local charts centered at x . That is

$$\varphi' \circ f \circ \varphi^{-1}(z) = z^{e_x} g(z)$$

for some g holomorphic with $g(0) \neq 0, \infty$. The degree is well-defined by the definition of e_x . Given a nonconstant holomorphic map f , the *Riemann-Hurwitz formula* relates the degree, the ramification degrees and the genus of X and Y

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X} (e_x - 1) \quad (3.1)$$

The map we are going to apply (3.1) is the natural projection

$$\begin{aligned} \Pi : X(\Gamma) &\longrightarrow X(1) \\ \Gamma\tau &\longmapsto \mathrm{SL}_2(\mathbb{Z})\tau \end{aligned}$$

which is an holomorphic map. The ramification index at an elliptic point is

$$|\{\pm I\}\mathrm{SL}_2(\mathbb{Z})_\tau : \{\pm I\}\Gamma_\tau|$$

because a local chart φ in $X(\Gamma)$ sends $\pi(\tau') \mapsto u = \delta_\tau(\tau')^{h_\tau^\Gamma}$, and the local expression of Π sends $u \mapsto \psi \circ \Pi \circ \varphi^{-1}(u) = \delta_\tau(\tau')^{h_\tau^{\mathrm{SL}_2(\mathbb{Z})}}$ and thus

$$\psi \circ \Pi \circ \varphi^{-1}(u) = u^{h_\tau^{\mathrm{SL}_2(\mathbb{Z})}/h_\tau^\Gamma}$$

as wanted. By a similar argument the ramification index at a cusp is

$$|\{\pm I\}\mathrm{SL}_2(\mathbb{Z})_s : \{\pm I\}\Gamma_s|$$

and clearly the ramification index is 1 at everywhere else. Denote by ϵ_h the number of elliptic points τ in $X(\Gamma)$ with $|\Gamma_\tau| = h$ where $h \in \{2, 3\}$, and ϵ_∞ the number of cusps in $X(\Gamma)$. Then by the well-definedness of the degree one has ²⁷

$$\sum_{x \in X(\Gamma)} (e_x - 1) = (d - \epsilon_\infty) + \frac{1}{2}(d - \epsilon_2) + \frac{2}{3}(d - \epsilon_3)$$

Then by (3.1) the genus of $X(\Gamma)$ is

$$g_X = 1 + \frac{d}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}$$

because $X(1)$ has genus 0. This follows from the fact that the j -invariant

$$j : X(1) \rightarrow \hat{\mathbb{C}}$$

²⁷Note that Π sends cusps to cusps and elliptic points to elliptic points, although some elliptic points in $X(1)$ may not come from elliptic points in $X(\Gamma)$.

is an holomorphic isomorphism of compact Riemann surfaces.

We apply the formula above to $X(1)$, although we already know its genus.

$$g = 1 + \frac{1}{12} - \frac{1}{4} - \frac{1}{3} - \frac{1}{2} = 0$$

because $\Pi = \text{id}_{X(1)}$ has degree 1 and $X(1)$ has only one cusp by the transivity of $\text{SL}_2(\mathbb{Z})$ on $\mathbb{Q} \cup \infty$ and two elliptic points, one of period 2 and another of period 3 (namely, i and ζ_3) because these are the only elliptic points in the fundamental domain \mathcal{F} for $X(1)$ by theorem 3.2.

3.5 Modular curves as algebraic curves

There is a general result on Riemann surfaces:

Theorem 3.5. *Every compact connected Riemann surface can be represented as an algebraic curve over \mathbb{C} .* ²⁸

Modular curves are Riemann surfaces, so they must also be represented as algebraic curves over \mathbb{C} . They are in fact curves over \mathbb{Q} :

Theorem 3.6. *There exists an algebraic curve X defined over \mathbb{Q} such that the following is an isomorphism of Riemann surfaces*

$$X(\mathbb{C}) \simeq X_0(N)$$

where $X_0(N) = X(\Gamma_0(N))$ is defined as in 3.3.

There are at least two ways to show this. The first method shows that the field of functions of $X_0(N)$ is $\mathbb{C}(j, j_N)$ where $j_N = j(N\tau)$, and we devote sections 3.5.2, 3.5.3 and 3.5.4 to this approach.

The second approach uses that a moduli space has model over a number field, which in this case can be shown to be \mathbb{Q} . All that is left to do is that $X_0(N)$ is a moduli space (section 3.6).

The first approach is however not easily generalizable to other contexts.

3.5.1 Algebraic curves

To begin we must define what is an algebraic curve. Let k be a field of characteristic 0 and \bar{k} its algebraic closure. Let $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ a set of m polynomials and let I be the following ideal $I = \langle f_1, \dots, f_m \rangle$. Let C be the following set

$$C = \{x \in \bar{k}^n : f(x) = 0 \text{ for all } f \in I\}$$

²⁸Here an algebraic curve over \mathbb{C} is loosely speaking a set given by $\varphi(x, y) = 0$ where $\varphi \in \mathbb{C}[x, y]$ is a bivariate polynomial. We will define them more precisely in section 3.5.1.

The *coordinate ring* of C over \bar{k} is $\bar{k}[C] = \bar{k}[X_1, \dots, X_n]/I$ and the *function field* of C over \bar{k} is the quotient field $\bar{k}(C)$ of $\bar{k}[C]$ when I is a prime ideal in $\bar{k}[X_1, \dots, X_n]$, because to form a quotient field from a ring requires the ring to be an integral domain. The quotient field is the set of rational functions on the coordinates of a point in C when we ignore elements in I . This makes sense because C is the vanishing set of I .

C is an *affine algebraic curve* over k if $\bar{k}(C)$ has transcendence degree 1 over \bar{k} and $\bar{k}(C)/\bar{k}(t)$ is a finite algebraic extension, where t is a transcendence base.

C is *nonsingular* if the matrix $(D_j f_i(P))_{i,j}$ has rank $n - 1$ for any $P \in C$. For nonsingular curves, one can prove that m_P/m_P^2 is a one dimensional vector space over \bar{k} where $m_P = \{f \in \bar{k}[C] : f(P) = 0\}$ by showing that m_P/m_P^2 is isomorphic to the tangent space to C at P , which is the kernel of $(D_j f_i(P))_{i,j}$ and this latter has dimension 1 because C is nonsingular. Moreover,

$$\bar{k}[C]_P = \{f/g \in \bar{k}(C) : g(P) \neq 0\}$$

is a local ring with maximal ideal

$$M_P = \{f/g \in \bar{k}[C]_P : f(P) = 0\}$$

and by using Nakayama's lemma (which can be used because $\bar{k}[C]_P$ is local and Noetherian and $M_P = m_P \cdot \bar{k}[C]_P$ implies that M_P is finitely generated) one can show that M_P is a principal ideal, generated by some t . This element t is called an *uniformizer at P* and it induces a valuation in $\bar{k}[C]$ and by extension on $\bar{k}(C)$

$$\begin{aligned} \nu_P : \quad k(C) &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ f = t^e u &\longmapsto e \end{aligned}$$

Here $\nu_P(0) = \infty$ by definition. From now on C is a nonsingular affine algebraic curve over k .

Affine curves arise from *projective* curves when one chooses an affine chart in the projective space \mathbb{P}^r . Instead, to define a projective curve the polynomials f_i must be homogeneous in order to make $f_i(p) = 0$ a well-defined expression for $p \in \mathbb{P}^r$. Similarly, a nonsingular projective curve is such that every nonempty affine curve associated to every affine chart is nonsingular.

To define morphisms between curves we include them in an ambient space, which is the projective space \mathbb{P}^r . A *morphism* of curves $h : C \rightarrow C'$ is the map

$$h(P) = (t^{-\nu} h_0(P) : \dots : t^{-\nu} h_r(P))$$

(where $\nu = \min_i \nu_P(h_i)$) associated to an element $h = (h_0 : \dots, h_r) \in \mathbb{P}^r(\bar{k}(C))$ so that $h(C) \subset C'$.

Such a map is an *isomorphism* if there exists another morphism of curves h^{-1} with $h \circ h^{-1}$ and $h^{-1} \circ h$ being the identity maps on C' and C , respectively. This induces an equivalence relation. A stricter criterion is to be *isomorphic over k* , when h and h^{-1} are defined over k . A morphism h is *defined over k* if $h_i \in k(C) =$ the field of fractions of

$k[X_j]_j/I_k$ where $I_k = I \cap k[X_j]_j$. Here $k(C)$ can be thought as a subfield of $\bar{k}(C)$ because $I_k \subset I$ ²⁹

A *function field* K over k is a field with $K \cap \bar{k} = k$ and a finite extension of $k(t)$ with t transcendental over k . We introduce another equivalence relation: two function fields K and K' are *conjugate over k* if there exists $\varphi : K \rightarrow K'$ that fixes k pointwise.

The following result from algebraic geometry gives a crucial correspondence:

Theorem 3.7. *There is a bijection between the set isomorphism over k classes of nonsingular projective curves over k and the set of conjugate over k classes of function fields over k , where the class of a curve C is mapped to the class of $k(C)$. Conversely, a function field K is mapped to some desingularization of the curve defined by $F(t, u) = 0$ where $F(x, y)$ is obtained by clearing denominators from f , the minimal polynomial of u over $k(t)$ where $K = k(t, u)$.*

Proof. If two curves C, C' are isomorphic $C \xrightarrow{\sim} C'$ over k then so are their function fields; consider the *pullback* $\varphi^* : k(C') \rightarrow k(C)$ where $\varphi^*(g) = g \circ \varphi$. It is an isomorphism since $(\varphi^{-1})^* = (\varphi^*)^{-1}$, and it also fixes k so $k(C)$ and $k(C')$ are conjugate over k . Thus the map is well-defined. It is also injective, but we will not show this.

To show it surjects take a function field K and suppose that $K/k(t)$ is separable. Then by the primitive element theorem we may write $K = k(u, t)$. Let $f(Y) = \text{minpoly}(u, k(t), Y)$ and define $F(X, Y)$ by clearing denominators from f . If F is not irreducible over \bar{k} then it factors $F = F_1 F_2$ for some $F_i \in \bar{k}[X, Y]$.

The coefficients of F_1, F_2 lie in a finite extension $k(\eta)$. Note that $g(Z) = \text{minpoly}(\eta, k, Z)$ is also irreducible in $k(t)[Z]$, otherwise by unique factorization the coefficients of a factorization of g lie in $k(t) \cap \bar{k} = k$. Now put $L = k(t, \eta)$ so that $[K : k(t)] = \deg(f)$ and $[L : k(t)] = \deg(g)$. Let $M = KL = k(u, t, \eta)$. By hypothesis F factors over $k(\eta)$ so $[M : L] < \deg(f)$ and

$$[M : k(t)] = [M : L][L : k(t)] < \deg(f) \deg(g)$$

Thus $[M : k(t)] = [M : K][K : k(t)]$ implies $[M : K] < \deg(g)$ so g factors $g = g_1 g_2$ for $g_i \in K[Z]$. But g factors also in \bar{k} and $g_i \in (K \cap \bar{k})[Z] = k[Z]$, a contradiction.

Thus F is irreducible over \bar{k} and $C : F = 0$ defines a plane curve. If it is nonsingular we are done, otherwise we *desingularize* it. This process gives another curve which is nonsingular and birationally equivalent to C . Note that the function field remains the same, since any birational equivalence induces an automorphism of the function field. \square

3.5.2 Automorphic forms

If $\gamma \in \text{SL}_2(\mathbb{Z})$ then we define the *weight- k operator* $[\cdot]_k$ as follows

$$f[\gamma]_k(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau))$$

²⁹For instance, if $k = \mathbb{Q}$ the projective curves $C : X^2 + Y^2 = 2Z^2$ and $C' : X^2 + Y^2 = 3Z^2$ are isomorphic when $C, C' \subset \mathbb{P}^2(\mathbb{Q})$, but not isomorphic over \mathbb{Q} : working modulo 4 or over the Gaussian integers one can easily show that C' has no \mathbb{Q} -points in $\mathbb{P}^2(\mathbb{Q})$ while C does (for instance $(1 : 1 : 1) \in C$) and if they were isomorphic over \mathbb{Q} , \mathbb{Q} -points would be mapped to \mathbb{Q} -points.

where $j(\gamma, \tau) = c\tau + d$. A function f is *weight- k invariant with respect to $\Gamma \subset SL_2(\mathbb{Z})$* if $f[\gamma]_k = f$ for any $\gamma \in \Gamma$.

Let Γ be a congruence subgroup. An *automorphic form of weight k with respect to Γ* is a meromorphic weight- k invariant function $f : \mathfrak{H} \rightarrow \hat{\mathbb{C}}$ such that $f[\alpha]_k$ is meromorphic at ∞ for any $\alpha \in SL_2(\mathbb{Z})$ (that is, is meromorphic at the cusps of Γ).

A *modular form of weight k with respect to Γ* is an automorphic form of weight k with respect to $SL_2(\mathbb{Z})$ that is holomorphic, an stronger condition than meromorphic. We denote the set of automorphic forms of weight k with respect to Γ by $\mathcal{A}_k(\Gamma)$. We also define $\mathbb{C}(\Gamma) = \mathcal{A}_0(\Gamma)$.

For instance the j -invariant $j : X(1) \rightarrow \hat{\mathbb{C}}$ is an automorphic form of weight 0 with respect to $SL_2(\mathbb{Z})$, so $\mathbb{C}(j) \subset \mathcal{A}_0(\Gamma(1))$. In fact

Theorem 3.8. *One has $\mathbb{C}(\Gamma(1)) = \mathbb{C}(j)$*

Proof. Let $f : X(1) \rightarrow \hat{\mathbb{C}}$ be an automorphic form for $SL_2(\mathbb{Z})$. Then $f \circ j^{-1} : \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ is an holomorphic map on the Riemann sphere $\hat{\mathbb{C}}$. But every holomorphic map $\hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ is a rational function, so $f \circ j^{-1}(z) = r(z)$ for some $r \in \mathbb{C}(z)$. Therefore $f \in \mathbb{C}(j(z))$ as wanted.

It follows also that if f is holomorphic on $Y(1)$ then it is a polynomial on j , because j is exhaustive and any factor in the denominator of r would create a pole. \square

3.5.3 The modular polynomial

In other words, the function field of the Riemann sphere is just the rational functions $\mathbb{C}(t)$, and the isomorphism $j : X(1) \rightarrow \hat{\mathbb{C}}$ gives $\mathbb{C}(X(1)) = \mathbb{C}(j)$. We will now find $\mathbb{C}(\Gamma_0(N))$, but first a general theorem for $\mathbb{C}(\Gamma)$:

Theorem 3.9. *Let Γ be a congruence subgroup. Then $\mathbb{C}(\Gamma)$ is a finite extension of $\mathbb{C}(\Gamma(1))$, and its degree is at most $[\Gamma(1) : \Gamma]$.*

Proof. Choose n right coset representaties γ_i such that $\Gamma(1) = \bigsqcup_i \Gamma\gamma_i$ with $\gamma_1 = \text{id}$. Let $f \in \mathbb{C}(\Gamma)$. Then the set $\{f_i\}_i$ where $f_i(\tau) = f(\gamma_i(\tau))$ is left invariant by $\tau \mapsto \gamma\tau$ for any $\gamma \in \Gamma(1)$, because f is Γ -invariant and $\gamma_i\gamma = \gamma_{i,j}\gamma_j$ for some j and $\gamma_{i,j} \in \Gamma$. Thus any symmetric function on the f_i is $\Gamma(1)$ -invariant, i.e. is in $\mathbb{C}(j)$. Note that $f = f_1$. Then

$$P(Y) = \prod_i (Y - f_i)$$

is a polynomial $P \in \mathbb{C}(j)[Y]$ with $P(f) = 0$ of degree n , and f was arbitrary.³⁰ \square

Theorem 3.10. *One has $\mathbb{C}(\Gamma_0(N)) = \mathbb{C}(j, j_N(t))$ where $j_N(\tau) = j(N\tau)$.*

Proof. j_N is meromorphic because j is meromorphic, but we still have to show that j_N is $\Gamma_0(N)$ invariant. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Here is crucial that $N|c$. Then

$$j_N(\gamma\tau) = j(N\gamma\tau) = j\left(\frac{Na\tau + bN}{c\tau + d}\right) = j\left(\frac{a(N\tau) + bN}{\frac{c}{N}(N\tau) + d}\right)$$

³⁰The degree of any element is bounded by n and the extension is separable.

$$= j(\gamma'(N\tau)) = j(N\tau) = j_N(\tau)$$

because $\gamma' = \begin{pmatrix} a & bN \\ c/N & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, as wanted.

Again choose $n = [\Gamma(1) : \Gamma_0(N)]$ right coset representatives such that $\Gamma(1) = \bigsqcup_i \Gamma_0(N)\gamma_i$. Let $P \in \mathbb{C}(j)[Y]$ be the minimal polynomial of j_N over $\mathbb{C}(j)$. Then $f(\tau) = P(j(\tau), j_N(\tau))$ is the zero function, and for all i

$$f(\gamma_i\tau) = 0 = P(j(\gamma_i\tau), j_N(\gamma_i\tau)) = P(j(\tau), j_N(\gamma_i\tau))$$

$j_N(\gamma_i\tau)$ is also a root of P . Suppose that $j_N(\gamma_k\tau) = j_N(\gamma_l\tau)$ for some τ . Then $\alpha(N\gamma_k\tau), \beta(N\gamma_l\tau) \in \mathcal{F}$ for some $\alpha, \beta \in \mathrm{SL}_2(\mathbb{Z})$ and by the injectivity of j one has $\alpha(N\gamma_k\tau') = \beta(N\gamma_l\tau')$ for all τ' in a neighborhood of τ . If $\alpha^{-1}\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then

$$\gamma_k\gamma_l^{-1} = \begin{pmatrix} 1/N & 0 \\ 0 & 1 \end{pmatrix} \alpha^{-1}\beta \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b/N \\ cN & d \end{pmatrix} \in \Gamma_0(N)$$

so $k = l$, and $[\mathbb{C}(j, j_N) : \mathbb{C}(j)] = n$ has degree n . \square

The *modular polynomial* Φ_N is the minimal polynomial of j_N over $\mathbb{C}(j)$. By the above it has degree $n = [\Gamma(1) : \Gamma_0(N)]$ and it can be written as

$$\Phi_N(Y) = \prod_i (Y - j_N(\gamma_i\tau)) = \sum_i \phi_{N,i}(j) Y^i$$

for some rational functions $\phi_{N,i}(j) \in \mathbb{C}(j)$ in j .

Remark 3.11. Each $\phi_{N,i}$ is a symmetric polynomial in $j_N(\gamma_i\tau)$, hence holomorphic in \mathfrak{H} and $\Gamma(1)$ -invariant, so it must be a polynomial in j by theorem 3.8. Thus we may write $\Phi_N(X, Y)$ as the polynomial obtained by replacing $j \mapsto X$ in $\Phi_N(Y) \in \mathbb{C}(j)[Y]$.

3.5.4 Properties of the modular polynomial

Throughout this section N is a prime number. Although the results remain to be true for elliptic curves over any field with characteristic not dividing N we expose only the cases for N prime, because the proofs for the general case are more involved but with the same ideas, i.e. writing down a set of coset representatives explicitly. In other words, we claim that

$$\left\{ \gamma_k = ST^k = \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} \right\}_{0 \leq k < N}$$

is a set of right coset representatives of $\Gamma(1)/\Gamma_0(N)$, i.e. $\Gamma(1) = \bigsqcup_{0 \leq k < N} \Gamma_0(N)\gamma_k$.

By theorem 3.7, $X_0(N)$ is a desingularization of the plane curve $\Phi_N(x, y) = 0$. First we show Φ_N has integer coefficients. This is relevant, for it lets one consider the reduction of the modular curve modulo a prime.

Theorem 3.12. *One has $\phi_{N,i}(X) \in \mathbb{Z}[X]$. Thus $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$.*

Proof. Consider the following expression for $\Phi_N(Y)$

$$\Phi_N(Y) = \left(Y - j_N(\tau)\right) \prod_{k=0}^{N-1} \left(Y - j_N(\gamma_k \tau)\right)$$

Note that $\phi_{N,i} \in \mathbb{C}[j]$ by remark 3.11. The q -expansion of the j -invariant has integer coefficients, i.e. $j(\tau) = q^{-1} + 744 + \sum_{n \geq 1} a_n q^n$ with $a_n \in \mathbb{Z}$, because $j(\tau) = 1728g_2(\tau)^3(g_2(\tau)^3 - 27g_3(\tau)^2)^{-1}$ and Eisenstein series have integral q -expansions. Thus if we let $\zeta_N = e^{\frac{2\pi i \tau}{N}}$ one has

$$j_N(\gamma_k \tau) = j\left(\frac{\tau + k}{N}\right) = \sum_{n \geq -1} a_n q^{n/N} \zeta_N^{kn}$$

because $e^{2\pi i \frac{\tau+k}{N}} = q^{1/N} \zeta_N^k$. Hence $j_N(\gamma_k \tau) \in \mathbb{Q}(\zeta_N)[[q^{1/N}]]$ i.e. it is a $q^{1/N}$ -series with coefficients in $\mathbb{Q}(\zeta_N)$. The Galois group $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ acts naturally on $\mathbb{Q}(\zeta_N)[[q^{1/N}]]$ coefficientwise. In particular, the set $S = \{j_N(\gamma_k \tau)\}$ is the union of two orbits because $j_N(t)$ is fixed, so $\phi_{N,i} \in \mathbb{Q}[[q^{1/N}]]$ for it is a symmetric function on S hence invariant by the action. Moreover, since $\phi_{N,i} \in \mathbb{C}[j]$ is a polynomial on j all of its q -powers must be integral i.e. $\phi_{N,i} \in \mathbb{Q}[[q]]$. On the other hand, as the coefficients $a_n \zeta_N^{kn}$ of $j_N(\gamma_k \tau)$ are algebraic integers so are the coefficients of $\phi_{N,i}$. Thus $\phi_{N,i} \in (\mathbb{Q} \cap \overline{\mathbb{Z}})[[q]] = \mathbb{Z}[[q]]$ since \mathbb{Z} is integrally closed. Lemma 3.13 then implies $\phi_{N,i} \in \mathbb{Z}[j]$ is a polynomial with integer coefficients. \square

Lemma 3.13 (Hasse q -expansion principle). *Let $f \in \mathbb{C}(\Gamma(1))$ be holomorphic in \mathfrak{H} with $f \in A[[q]]$ i.e. the coefficients in its q -expansion lie in A for some \mathbb{Z} -module $A \subset \mathbb{C}$. Then $f \in A[j]$ is a polynomial in j with coefficients in A .*

Proof. Theorem 3.8 implies $f \in \mathbb{C}[j]$ i.e. $f = P(j)$ for some $P \in \mathbb{C}[X]$ so our goal is to show $P \in A[X]$. We proceed by induction on $d = \deg P$. The case $d = 0$ is clear, since f is constant. Suppose $d > 0$. Since $j(\tau) = q^{-1} + O(1)$ one has $f(\tau) = a_{-d} q^{-d} + O(q^{-d+1})$. Let $Q(X) = P(X) - a_{-d} X^d$ and $g(\tau) = Q(j(\tau))$. Then $g \in A[[q]]$ and $\deg Q < d$ so by induction hypothesis $Q \in A[X]$ and thus $P \in A[X]$. \square

The second result says that the modular curve parametrizes somehow the isogenies of degree³¹ N . This point of view is used in section 4 to construct Heegner points, which by the following theorem can also be seen to correspond to diagrams $\phi : E \rightarrow E'$ where E, E' are two elliptic curves and ϕ is a *cyclic* isogeny. A more precise statement is

Theorem 3.14. *A point $(j, j') \in \mathbb{C}^2$ is in $X_0(N) : \Phi_N(x, y) = 0$ if and only if there exist elliptic curves E, E' over \mathbb{C} with j -invariants j and j' and a cyclic isogeny $E \rightarrow E'$ of degree N .*

³¹Here the degree is the cardinal of the kernel, because \mathbb{C} is separable.

An isogeny is *cyclic* if it has cyclic kernel. Our isogenies here will have degree N with N prime, hence cyclic.

Proof. With this result, we write down $\Phi_N(j, Y)$

$$\Phi_N(j(\tau), Y) = (Y - j_N(\tau)) \prod_{0 \leq k < N} (Y - j_N(\gamma_k \tau)) = (Y - j(N\tau)) \prod_{0 \leq k < N} (Y - j\left(\frac{\tau + k}{N}\right)) \quad (3.2)$$

By the surjectivity of j we may put $j' = j(\tau')$. Thus $\Phi_N(j, j') = 0$ if and only if $\tau' \sim N\tau$ or $\tau' \sim \frac{\tau+k}{N}$, or equivalently if $\Lambda_{\tau'} \sim \Lambda_{N\tau}$ or $\Lambda_{\tau'} \sim \langle N, \tau + k \rangle$ as homothety of lattices. Note that these are sublattices of Λ_τ of index N . Conversely, a sublattice of Λ_τ of index N must be one of these: let $\Lambda' \subset \Lambda$ with $[\Lambda : \Lambda'] = N$ and d the smallest positive integer in Λ' . Then $\Lambda' = \langle d, a\tau + k \rangle$ with $ad = N$ and $0 \leq k < N$. But N is prime so either $(a, d) = (1, N)$ or $(a, d) = (N, 1)$, as wanted.

The natural inclusion $\Lambda' \subset \Lambda$ with $[\Lambda : \Lambda'] = N$ induces a cyclic isogeny $E_{\Lambda'} \rightarrow E_\Lambda$. Conversely, every degree N isogeny is induced by an inclusion of lattices $\Lambda' \subset \Lambda$ with $[\Lambda : \Lambda'] = N$. It is then cyclic because the kernel is isomorphic to Λ/Λ' . \square

The existence of the dual isogeny implies that $\Phi_N(j, j') = 0$ if and only if $\Phi_N(j', j) = 0$. Moreover,

Theorem 3.15. *One has $\Phi_N(X, Y) = \Phi_N(Y, X)$. Moreover, $\Phi_N(X, X)$ has leading term $-X^{2N}$ i.e. is monic.*

Proof. Recall that $j_N(\gamma_0 \tau) = j\left(\frac{\tau}{N}\right)$ is a root of $\Phi_N(j(\tau), Y)$. We also had $\Phi_N(j(\tau), j(N\tau)) = 0$ for all τ . Hence $j\left(\frac{\tau}{N}\right)$ is also a root of $\Phi_N(Y, j(\tau))$. $\Phi_N(j, Y)$ is irreducible in $\mathbb{C}(j)[Y]$ so it divides $\Phi_N(Y, j)$. Now for any fixed lattice $\Lambda \subset \mathbb{C}$ the equations $\Phi(j(\Lambda), Y) = 0$ and $\Phi_N(Y, j(\Lambda)) = 0$ have the same number of roots in \mathbb{C} . Hence $\Phi_N(j, Y) \cdot f = \Phi_N(Y, j)$ for some $f \in \mathbb{C}(j)$. Now $\mathbb{C}(j)/\mathbb{C}$ is transcendental so $\Phi_N(j, j) \neq 0$ and $f(j) = 1$, as wanted.

The j -invariant has the following q -expansion $j(\tau) = \frac{1}{q} + O(1)$, while $f(\tau) = \Phi_N(j(\tau), j(\tau))$ verifies

$$f(\tau) = \left(j(\tau) - j(N\tau)\right) \prod_{0 \leq k < N} \left(j(\tau) - j\left(\frac{\tau + k}{N}\right)\right) = -\frac{1}{q^{2N}} + \dots$$

because $j(\tau) - j(N\tau) = q^{-1} - q^{-N} + \dots$ and $j(\tau) - j\left(\frac{\tau+k}{N}\right) = q^{-1} - \zeta_N^{-k} q^{1/N} + \dots$ where ζ_N is an N -th primitive root of unity. \square

3.6 Modular curves as moduli spaces

The result of this section is equivalent to theorem 3.14; that modular curve parametrize somehow elliptic curves together with some additional data. There is a definition of moduli space in terms of categories given by Mumford in the 1960s. Because of this, a moduli space is unique up to unique isomorphism.

An *enhanced elliptic curve* for $\Gamma_0(N)$ is a pair (E, C) where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N (a N -cyclic group). Two enhanced elliptic curves (E, C) and (E', C') are equivalent if there exists an isomorphism $E \xrightarrow{\sim} E'$ sending C to C' . The set of equivalence classes of enhanced elliptic curves is denoted by $S_0(N)$.

$$S_0(N) = \{[(E, C)] : E \text{ elliptic curve and } C \subset E \text{ an } N\text{-cyclic subgroup}\}$$

Then $Y_0(N)$ (defined in section 3.1) is a moduli space with the following bijection

$$\begin{aligned} Y_0(N) &\longrightarrow S_0(N) \\ \Gamma_0(N)\tau &\longmapsto [(E_\tau, C_\tau)] \end{aligned}$$

Here $E_\tau = \mathbb{C}/\Lambda_\tau$ is a complex torus where $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$ and

$$C_\tau = \langle 1/N + \Lambda_\tau \rangle$$

is the N -cyclic subgroup of E_τ generated by $Q_\tau = 1/N + \Lambda_\tau$.

In other words,

Proposition 3.16. *Every enhanced elliptic curve is equivalent to $[(E_\tau, C_\tau)]$ for some $\tau \in \mathfrak{H}$, and the map above is a well-defined bijection.*

Proof. Let (E, C) is an enhanced elliptic curve. We may suppose $E \xrightarrow{\sim} \mathbb{C}/\Lambda_{\tau'}$ for some $\tau' \in \mathfrak{H}$, so that $C \xrightarrow{\sim} \langle Q \rangle$ for $Q = (c\tau' + d)/N$, but $\gcd(c, d, N) = 1$ so $ad - bc - kN = 1$ for some $a, b, k \in \mathbb{Z}$. Therefore $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and we can suppose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ because the natural map $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ surjects and Q depends only on the classes of c and d modulo N . Let $\tau = \gamma\tau'$ and $m = c\tau' + d$ so that $m\tau = a\tau' + b$ and $m\Lambda_\tau = \Lambda_{\tau'}$. Then $\mathbb{C}/\Lambda_\tau \xrightarrow{z \mapsto mz} \mathbb{C}/\Lambda_{\tau'}$ is an isogeny sending $Q_\tau \mapsto Q$ so $(E_\tau, Q_\tau) \sim (E, C)$ as wanted.

If $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$ then $\tau = \gamma\tau'$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}$. Let $m = c\tau' + d$ so that $m\tau = a\tau' + b$ and $mQ_\tau = (c\tau' + d)/N + \Lambda_{\tau'}$ and $m\Lambda_\tau = \Lambda_{\tau'}$ as before. But $(c, d) \equiv (0, *) \pmod{N}$ so $mQ_\tau = d/N + \Lambda_{\tau'}$ with $\bar{d} \in (\mathbb{Z}/N\mathbb{Z})^\times$. This implies that $\mathbb{C}/\Lambda_\tau \xrightarrow{z \mapsto mz} \mathbb{C}/\Lambda_{\tau'}$ is an isogeny sending $\langle Q_\tau \rangle \mapsto \langle d/N + \Lambda_{\tau'} \rangle = \langle Q_{\tau'} \rangle$.

Finally, suppose that $[(\mathbb{C}/\Lambda_\tau, \langle Q_\tau \rangle)] = [(\mathbb{C}/\Lambda_{\tau'}, \langle Q_{\tau'} \rangle)]$. Then $\mathbb{C}/\Lambda_\tau \xrightarrow{z \mapsto mz} \mathbb{C}/\Lambda_{\tau'}$ is an isogeny for some $m \in \mathbb{C}$ and $\begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Let $m = c\tau' + d$. Then $mC_\tau = C_{\tau'}$ implies $c \equiv 0 \pmod{N}$ hence $\bar{d} \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $\gamma \in \Gamma_0(N)$. This shows $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. \square

4 Heegner points on $X_0(N)$

The last two sections are an ad hoc approach to class field theory for quadratic imaginary extensions, since we relied on the correspondence between elliptic curves and torii, and the fact that the endomorphism ring of an elliptic curve is an order in a quadratic imaginary field. We also constructed the ring class fields K_f analytically through the j -invariant.

Moreover, the *First main theorem of CM* (theorem 2.16) is just a weakening of *Artin reciprocity law* (theorem 1.4) and while we proved theorem 2.16 using properties of elliptic curves, theorem 1.4 usually requires Tate cohomology, which we will not discuss here.

In this section, by using the *Modularity theorem* we will show that with this approach one can produce algebraic points on elliptic curves over \mathbb{Q} , the *Heegner points*.

4.1 The modularity theorem

The following is a very powerful result

Theorem 4.1 (Modularity theorem). *Let E/\mathbb{Q} be an elliptic curve. Then there exists³² N and a surjective morphism over \mathbb{Q} of curves over \mathbb{Q}*

$$\varphi : X_0(N)_{\text{alg}} \longrightarrow E$$

Here $X_0(N)_{\text{alg}}$ is the set of algebraic points of $X_0(N) : \Phi_N(x, y) = 0$. The morphism φ is called a modular parametrization of E .

In other words, every elliptic curve defined over \mathbb{Q} can be parametrized by some modular curve. In general, an elliptic curve over a number field K is *modular* if the parametrization φ is defined over K . Although it was thought to be inaccessible, a special case of theorem 4.1 proven by Taylor and Wiles in 1994 was crucial to prove *Fermat's last theorem*. The full proof was completed in 2001 by Breuil *et al.*

The application of theorem 4.1 that we are interested in is to produce points of infinite order on an elliptic curve, known as *Heegner points*. With these points one can prove some special cases of the *Birch and Swinnerton-Dyer conjecture*.

4.2 The L -function

Given an elliptic curve E over \mathbb{Q} and a number field F , the rank of the abelian group $E(F)$ is known to be finite:

Theorem 4.2 (Mordell-Weil). *If E and F are as above then one has*

$$E(F) \simeq \mathbb{Z}^r \oplus T$$

where T is a finite abelian group and r is the rank of $E(F)$.

³²The minimal N for which theorem 4.1 holds is now known to be the *conductor* of E .

The torsion subgroup $T = E(K)_{\text{tors}}$ can be effectively found using Nagell-Lutz theorem. However, there is no known algorithm for computing the rank r . To be true, the BSD conjecture would solve this problem by giving an effective procedure to determine r . To state this conjecture we introduce the L -function, although discussing more of its properties are out of the scope of this thesis.

Given E/\mathbb{Q} an elliptic curve of conductor N we let

$$L(E, s) = \prod_{p|N} (1 - a_p p^{-s}) \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

Here the a_p depend³³ on how does E reduce modulo p . Note that for primes $p|N$ of bad reduction the factor in $L(E, s)$ is different to that of a generic prime. The L -function can also be defined over other number fields than \mathbb{Q} .

One can consider the behavior of $L(E, s)$ at $s = 1$, since it turns out $L(E, s)$ can be extended to a meromorphic function in \mathbb{C} , although this fact was unknown when Birch and Swinnerton-Dyer posed their conjecture:

Conjecture 4.3 (Birch and Swinnerton-Dyer). *Let E/K be an elliptic curve of rank r . Then $L_{E/K}(s)$ has order r at $s = 1$.*

There is also an stronger version of BSD additionally involving the coefficient

$$\lim_{s \rightarrow 1} L_{E/K}(s)(s - 1)^{-r}$$

with additional arithmetical data of E/K , for instance the cardinal of the *Tate-Shafarevich group* $\text{III}(E/K)$ that we will define in section 4.4.1.

4.2.1 Reduction over local fields

Here L is an arbitrary local field, for instance the p -adic numbers \mathbb{Q}_p . To reduce an elliptic curve E over \mathbb{Q} in L is to consider the equation defining E as an equation over L . In order to do this, one first has to find a *good* equation for E that can be reduced over L . In section 2.3 we claimed that every elliptic curve over \mathbb{C} admits a Weierstrass equation of the form

$$E_{\Lambda} Y^2 = 4X^3 - g_2 X - g_3$$

This claim becomes false in general if instead E is over an arbitrary field K . However, by Riemann-Roch theorem every elliptic curve can be put as follows

$$Y^2 Z + a_1 X Y Z + a_3 Y Z^2 = X^3 + a_2 X^2 Z + a_4 X Z^2 + a_6 Z^3$$

³³If $p \nmid N$ then $a_p = p+1 - \#E(\mathbb{F}_p)$. Otherwise $a_p = 0, -1$ or 1 when E has additive, split multiplicative or nonsplit multiplicative reduction modulo p .

4.3 Heegner points

Let E be an elliptic curve over \mathbb{Q} without CM, and fix a modular parametrization $\varphi : X_0(N) \rightarrow E$. Note that φ exists by theorem 4.1. Let $K = \mathbb{Q}(\sqrt{D})$ an imaginary quadratic field of discriminant D with³⁴ $D \neq -3, -4$ and such that every prime $p|N$ splits completely in \mathcal{O}_K . This condition on N is known as *Heegner's hypothesis*.

Then there exists \mathfrak{N} with $N\mathcal{O}_K = \mathfrak{N}\bar{\mathfrak{N}}$.³⁵ Let \mathcal{O} be an order of K with conductor f , and let $\mathfrak{M} = \mathcal{O} \cap \mathfrak{N}$. Recall that we can write $\mathcal{O}_K = \langle 1, w_K \rangle$ and $\mathcal{O} = \langle 1, w \rangle$, where w_K is as in section 2.1.1 and $w = fw_K$. Then \mathfrak{M} is proper \mathcal{O} -ideal³⁶ The lattice inclusion $\mathcal{O} \subset \mathfrak{M}^{-1}$ induces a degree N cyclic isogeny $\phi : E_{\mathcal{O}} \rightarrow E_{\mathfrak{M}^{-1}}$. By theorem 3.14 the point $x_f = (j(\mathcal{O}), j(\mathfrak{M}^{-1}))$ belongs to the modular curve $X_0(N)$. We write x_f to remark that x_f depends only on the conductor f . Moreover, both \mathfrak{M}^{-1} and \mathcal{O} have CM by \mathcal{O} because they are proper fractional \mathcal{O} -ideals, so by theorem 2.14 the coordinates of x_f are algebraic integers, i.e. $x_f \in \bar{\mathbb{Q}}$. In fact, $x_f \in L$ where $L = K_f$ is the splitting field of the Hilbert class polynomial $H_D(X)$ of section 2.6.

The constructed point $x_f \in X_0(N)$ is called a *Heegner point*. The modular parametrization φ is defined over \mathbb{Q} and x_f has coordinates in K_f , so if we let $y_f = \varphi(x_f)$ then y_f is defined over K_f and $y_f \in E$, i.e. $y_f \in E(K_f)$. Then if we take the trace of y_f we obtain

$$y_{f,K} = \text{Tr}_{K_f/K}(y_f) \quad (4.1)$$

But y_f is $\text{Gal}(K_f/K)$ -invariant if we consider the natural action of $\text{Gal}(K_f/K)$ on $E(K_f)$, so it is defined over K , i.e. $y_f \in E(K)$.

4.4 Group cohomology

We introduce some key concepts and define cohomology in simple terms, via cochains. For a group G , the *group ring* of G is the ring

$$\mathbb{Z}[G] = \bigoplus_{g \in G} \mathbb{Z}g$$

with the natural sum and the product defined by $(\sum_g a_g g)(\sum_h b_h h) = (\sum_{g,h} a_g b_h gh)$. Then an abelian group A is a G -module if it is a $\mathbb{Z}[G]$ -module.

The *group of i -cochains of G with coefficients in A* is the abelian group $\mathcal{C}^i(G, A) = \{f : G^i \rightarrow A\}$, and the *i -th differential* is the map $d^i : \mathcal{C}^i(G, A) \rightarrow \mathcal{C}^{i+1}(G, A)$ defined by

$$d^i(f)(g_0, \dots, g_i) = g_0 f(g_1, \dots, g_i) + \sum_{j=1}^i (-1)^j f(g_0, \dots, g_{j-1} g_j, \dots, g_i) + (-1)^{i+1} f(g_0, \dots, g_{i-1})$$

The set of *i -cocycles* is $\mathcal{Z}^i(G, A) = \ker d^i$, and the set of *i -coboundaries* is $\mathcal{B}^i(G, A) = \text{im } d^{i-1}$.³⁷ Moreover, the sequence abelian groups

³⁴Then $\mathcal{O}_K^\times = \{\pm 1\}$.

³⁵That is, if $N = \prod_i p_i^{e_i}$ then $p_i \mathcal{O}_K = \mathfrak{p}_i \bar{\mathfrak{p}}_i$ and $N\mathcal{O}_K = \mathfrak{N}\bar{\mathfrak{N}}$ where $\mathfrak{N} = \prod_i \mathfrak{p}_i^{e_i}$. By the Chinese Remainder theorem, $\mathcal{O}_K/\mathfrak{N} \simeq \prod_i \mathcal{O}_K/\mathfrak{p}_i^{e_i} \simeq \prod_i \mathbb{Z}/p_i^{e_i} \mathbb{Z} \simeq \mathbb{Z}/N\mathbb{Z}$.

³⁶Because $\mathfrak{M} = \mathfrak{N} \cap \mathcal{O}$ is proper by the isomorphism in (2.1).

³⁷Here by definition $\mathcal{B}^0(G, A) = 0$.

$$0 \longrightarrow \mathcal{C}^0(G, A) \xrightarrow{d^0} \mathcal{C}^1(G, A) \xrightarrow{d^1} \dots$$

forms a *cochain complex*, i.e. $d^{i+1} \circ d_i = 0$. That is, every coboundary is a cocycle³⁸ so one can define the *i-th cohomology group* by $H^i(G, A) = \mathcal{Z}^i(G, A)/\mathcal{B}^i(G, A)$.

Every morphism of G -modules $f : A \rightarrow B$ induces a natural morphism of groups $f^i : \mathcal{C}^i(G, A) \rightarrow \mathcal{C}^i(G, B)$ that is compatible with the differentials, i.e. $d_B^i f^i = f^{i+1} d_A^i$. Then the natural map $f_i^\bullet : H^i(G, A) \rightarrow H^i(G, B)$ induced by f^i is well-defined because of this compatibility. The following result is crucial for our purposes

Proposition 4.4. *The short exact sequence*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

*induces the long exact sequence*³⁹

$$0 \longrightarrow H^0(G, A) \xrightarrow{f_0^\bullet} H^0(G, B) \xrightarrow{g_0^\bullet} H^0(G, C) \xrightarrow{\delta_0} H^1(G, A) \xrightarrow{f_1^\bullet} H^1(G, B) \xrightarrow{g_1^\bullet} H^1(G, C) \xrightarrow{\delta_1} \dots$$

4.4.1 The Selmer and Tate-Shafarevich groups

Galois cohomology is the study of group cohomology when G is a Galois group, which may be infinite. Because of this we need to modify our definition of cohomology; the groups $\mathcal{C}^i(G, A)$ are not convenient for our purposes when G is infinite. This issue can be solved by introducing a topology. Here we endow G with the Krull topology and G becomes a profinite group, and endow A with the discrete topology. Recall that a profinite group is the inverse limit of an inverse system of finite groups,

$$G = \varprojlim_{i \in I} G_i$$

We will not treat in detail this theory, but in the case of Galois groups the G_i ranges over the finite Galois extensions of K . Then the action map $G \times A \rightarrow A$ can be shown to be continuous, and if we take $\mathcal{C}_{\text{cts}}^i(G, A) = \{f : G^i \rightarrow A \text{ continuous}\}$ instead of $\mathcal{C}^i(G, A)$ all the standard results remain to be true, in particular proposition 4.4.

Now fix an elliptic curve E over K and a prime number p , and consider the following exact sequence⁴⁰

$$0 \longrightarrow E_p \xrightarrow{\iota} E \xrightarrow{p} E \longrightarrow 0 \tag{4.2}$$

We set $H^i(K, A) = H^i(\text{Gal}(\bar{K}/K), A)$. By proposition 4.4 one has

$$0 \longrightarrow E(K)_p \xrightarrow{\iota_0} E(K) \xrightarrow{p_0} E(K) \xrightarrow{\delta_0} H^1(K, E_p) \xrightarrow{\iota_1} H^1(K, E) \xrightarrow{p_1} H^1(K, E) \xrightarrow{\delta_1} \dots$$

because in general $H^0(G, A) \simeq A^G$ is the group of G -invariants of A . By exactness we obtain

³⁸Note that $H^i = 0$ only when the converse is true.

³⁹The *connecting* morphisms δ_i are given by the Snake lemma and are *natural*.

⁴⁰Here p is the multiplication-by- p map, $E_p = \ker p$ is the *p-torsion* of E and ι the natural inclusion.

$$0 \rightarrow \operatorname{coker} p_0^\bullet = E(K)/pE(K) \xrightarrow{\bar{\delta}_0} H^1(K, E_p) \xrightarrow{\iota_1} \ker p_1^\bullet = H^1(K, E)_p \rightarrow 0$$

For any prime v of K , the restriction map embeds the Galois group $\operatorname{Gal}(\bar{K}_v/K_v) \hookrightarrow \operatorname{Gal}(\bar{K}/K)$ into the absolute Galois group⁴¹, so that the induced maps in the cohomology make the diagram commute

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\bar{\delta}_0} & H^1(K, E_p) & \xrightarrow{\iota_1} & H^1(K, E)_p \longrightarrow 0 \\ & & \downarrow & & \downarrow & \searrow \alpha = \rho \circ \iota_1 & \downarrow \rho \\ 0 & \longrightarrow & \prod_v E(K_v)/pE(K_v) & \longrightarrow & \prod_v H^1(K_v, E_p) & \longrightarrow & \prod_v H^1(K_v, E)_p \longrightarrow 0 \end{array}$$

Then the p -Selmer group is $\operatorname{Sel}_p(E/K) = \ker \alpha$, and the Tate-Shafarevich group $\operatorname{III}(E/K)$ is the kernel of the product of the restriction maps $\hat{\rho}$ ⁴², i.e.

$$\hat{\rho} = \prod_v \left(\operatorname{Res} : H^1(K, E) \rightarrow H^1(K_v, E) \right)$$

That is, the kernel of ρ is the p -torsion of $\operatorname{III}(E/K)$. The following expression for $\bar{\delta}_0$ can be obtained by diagram chasing

$$\begin{array}{ccccc} \bar{\delta}_0 : & E(K)/pE(K) & \longrightarrow & H^1(K, E_p) & \\ & P & \longmapsto & \bar{\delta}_0(P) : \operatorname{Gal}(\bar{K}/K) & \longrightarrow E_p \\ & & & \sigma & \longmapsto \sigma\left(\frac{1}{p}P\right) - \frac{1}{p}P \end{array}$$

This is shown by recalling how the connecting morphism of the Snake lemma was constructed. Given an exact sequence

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

let $\mathcal{Q}^k(G, M) = \mathcal{C}^k(G, A)/\mathcal{B}^k(G, A)$ and consider the following diagram of exact rows and columns

$$\begin{array}{ccccccc} & 0 & & 0 & & 0 & \\ & \downarrow & & \downarrow & & \downarrow & \\ H^0(G, A) & \xrightarrow{\bar{f}_0} & H^0(G, B) & \xrightarrow{\bar{g}_0} & H^0(G, C) & & \\ & \downarrow \iota_A & & \downarrow \iota_B & & \downarrow \iota_C & \\ \mathcal{Q}^0(G, A) & \xrightarrow{\bar{f}_0} & \mathcal{Q}^0(G, B) & \xrightarrow{\bar{g}_0} & \mathcal{Q}^0(G, C) & \longrightarrow & 0 \\ & \downarrow \bar{d}_A^0 & & \downarrow \bar{d}_B^0 & & \downarrow \bar{d}_C^0 & \\ 0 \longrightarrow & \mathcal{Z}^1(G, A) & \xrightarrow{\bar{f}_1} & \mathcal{Z}^1(G, B) & \xrightarrow{\bar{g}_1} & \mathcal{Z}^1(G, C) & \\ & \downarrow \pi_A & & \downarrow \pi_B & & \downarrow \pi_C & \\ H^1(G, A) & \xrightarrow{\bar{f}_1} & H^1(G, B) & \xrightarrow{\bar{g}_1} & H^1(G, C) & & \\ & \downarrow & & \downarrow & & \downarrow & \\ & 0 & & 0 & & 0 & \end{array}$$

⁴¹Here K_v is the completion of K at v .

⁴² $\operatorname{III}(E/\mathbb{Q})$ is hard to compute in general, but it is conjectured to be finite.

By the commutativity of the diagram and the exactness of the second and third rows, for any $c \in H^0(G, C)$ there is $b \in \mathcal{Q}^0(G, B)$ with $\overline{g_0}b = \iota_C c$ and there is $a \in \mathcal{Z}^1(G, A)$ with $\overline{f_1}a = \overline{d_B^0}b$. We⁴³ define $\delta_0(c) = \pi_A(a)$. In our case (eq 4.2) this is to say that $p \cdot b = c$ and $a = \sigma b - b$ by the definition of d_B^0 .

Moreover, the Selmer and Tate-Shafarevich groups fit in the exact sequence

$$0 \longrightarrow E(K)/pE(K) \xrightarrow{\bar{\delta}_0} \text{Sel}_p(E/K) \xrightarrow{\iota'} \text{III}(E/K)_p \longrightarrow 0$$

where $\iota' = \iota_1|_{\text{Sel}_p(E/K)}$.

4.5 Kolyvagin's theorem

Kolyvagin's theorem relates the Tate-Shafarevich group with the group $E(K)$

Theorem 4.5 (Kolyvagin). *Let E/\mathbb{Q} be an elliptic curve, construct K and $y_{f,K}$ for $f = 1$ as in section 4.3. If $y_{1,K}$ has infinite order in $E(K)$ then $E(K)$ has rank 1 and $\text{III}(E/K)$ is finite.*

To relate Kolyvagin's result with the BSD conjecture one makes use of the following theorem, proven by Gross and Zagier showed in 1986:

Theorem 4.6 (Gross and Zagier). *Let E and K be as above. Then $y_{1,K}$ has infinite order⁴⁴ if and only if the analytic rank of E/K is 1.*

In other words, under the current hypotheses on E and K the analytic and algebraic rank over K agree.

Since the proof of theorem 4.5 is quite involved, we will discuss instead the following weakening proven by Gross to highlight the main ideas:

Theorem 4.7.

From now on E will be an elliptic curve over \mathbb{Q} of conductor N . Here the conductor is a number divisible precisely by those rational primes p for which E has *bad reduction*, i.e. the reduction modulo p is singular, although the precise definition of the conductor is not essential in what follows.

4.5.1 Galois action on torsion points

If E/\mathbb{Q} is an elliptic curve, the Galois group $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally on $E(\overline{\mathbb{Q}})$ coordinatewise and this action is compatible with the group law⁴⁵ of E , i.e. $\sigma(P + Q) = \sigma(P) + \sigma(Q)$ for any $\sigma \in G_{\mathbb{Q}}$. In particular, a point is in the p -torsion $P \in E_p$ if and

⁴³Proving the Snake lemma is showing that this is a well-defined morphism.

⁴⁴Here $f = 1$, so $\mathcal{O} = \mathcal{O}_K$ is maximal.

⁴⁵Because it can be expressed in terms of \mathbb{Q} -rational functions.

only if so does $\sigma(P)$. Here $E_p = E(\overline{\mathbb{Q}})_p$ and the inclusion $E(\overline{\mathbb{Q}})_p \subset E(\mathbb{C})$ and theorem 2.5 imply⁴⁶ that $|E_p| = p^2$, because there are precisely p^2 p -torsion points in a lattice $\Lambda \subset \mathbb{C}$.

Let $\mathbb{Q}(E_p)$ be the field obtained by adjoining the x and y coordinates of points of E_p and let $G(p) = \text{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})$. Note that the action $G(p)$ on E_p is faithful. Then E_p has a natural structure of \mathbb{F}_p -vector space and so there exists a representation $\rho_p : G(p) \hookrightarrow \text{GL}_2(\mathbb{F}_p)$, not surjective in general. However, if E has no CM then by a corollary of Serre's Uniformity theorem ρ is surjective, i.e. $G(p) \simeq \text{GL}_2(\mathbb{F}_p)$. We will take p sufficiently large so that this is the case.

We let $L = K(E_p)$ be the field obtained by adjoining the x and y coordinates of points in E_p to K . Note that the extension L/K is Galois. Then

Proposition 4.8. *The extension L/K is unramified outside the primes that divide pN .*

Proof. Let S be the set of primes of K not dividing pN . Take $\mathfrak{p} \in S$ and \mathfrak{P} a prime of L dividing \mathfrak{p} . Then it is clear that E has good reduction over $\mathcal{O}_{K_{\mathfrak{p}}}$. The fundamental identity for number fields of section 1.1 can be applied also to local fields⁴⁷, and it reads⁴⁸

$$ef = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$$

Therefore L/K is unramified for $\mathfrak{p} \in S$ if so does $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ for $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{p} \in S$ or equivalently, if $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = f = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}]$. Now the reduction map $E_p \hookrightarrow \tilde{E}(\mathbb{F}_{\mathfrak{P}})$ injects, and the inertia group

$$I_{\mathfrak{P}}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \{\sigma \in \text{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) : \sigma x \equiv x \pmod{\mathfrak{P}} \text{ for all } x \in L_{\mathfrak{P}}\}$$

is trivial since it fixes pointwise $L_{\mathfrak{P}}$ because both $\mathbb{F}_{\mathfrak{P}} \simeq L_{\mathfrak{P}}/\mathfrak{P}$ and $\tilde{E}(\mathbb{F}_{\mathfrak{P}})$ are fixed. Thus $e = |I(L_{\mathfrak{P}}/K_{\mathfrak{p}})| = 1$ as wanted. \square

In other words, a rational prime ℓ is unramified in L precisely when it is unramified in K .

4.5.2 The Heegner points form an Euler system

Let us recall the current hypotheses - and impose some more - on the objects:

- E/\mathbb{Q} has no CM and has conductor N and every prime $q|N$ splits completely in \mathcal{O}_K (*Heegner hypothesis*).
- The conductor f of \mathcal{O} is squarefree and the rational prime ℓ considered throughout this section divides f and is coprime with NDp so ℓ is either inert or split in K . We can additionally assume that ℓ is inert, since by Chebotarev density theorem for quadratic extensions there is a positive density of inert primes.

⁴⁶The same is true in nonzero characteristic for all but finitely many primes p .

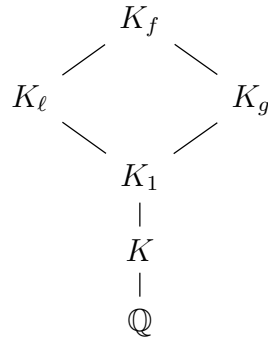
⁴⁷Recall that $L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$ are the completions of L and K by the places $|\cdot|_{\mathfrak{P}}, |\cdot|_{\mathfrak{p}}$.

⁴⁸Note that in local fields $g = 1$, because there is only one prime ideal.

- The prime p we fixed to consider the short exact sequence in equation 4.2 is sufficiently large so that ρ_p surjects.
- p does not divide $y_{1,K}$ (equation 4.1) in $E(K)/E(K)_{\text{tors}}$ i.e. there exists no point $Q \in E(K)$ with $p \cdot Q - y_{1,K} \in E(K)_{\text{tors}}$; since $E(K)/E(K)_{\text{tors}}$ is a finitely generated free \mathbb{Z} -module one can rewrite the equation $pQ = y_{1,K} = (c_1, \dots, c_r)$ in terms of matrices and take $p \nmid c_i$ for all i with $c_i \neq 0$.

All of these conditions leave the objects in their most generic cases.

Put $f = \ell g$ and consider the tower of extensions



- $\text{Tr}_\ell y_n = a_\ell y_m$
- Let $\mathfrak{z}_K = \ell \mathcal{O}_K$. Then \mathfrak{z}_K is prime and principal in K and with norm coprime with g . Thus $(K_g/K, \mathfrak{z}_K) = 1$ since it is unramified and principal (theorem 1.4) so by remark 1.1 the prime \mathfrak{z}_K splits completely in K_g .
The primes \mathfrak{p}_{K_g} of K_g dividing \mathfrak{z}_{K_g} are totally ramified in K_f i.e.

$$\mathfrak{p}_{K_g} \mathcal{O}_{K_f} = \mathfrak{p}_{K_f}^{\ell+1}$$

since $[K_f : K_g] = \ell + 1$ and ℓ ramifies in K_f so

$$\mathbb{F}_{\mathfrak{p}_{K_f}} = \mathbb{F}_{\mathfrak{p}_{K_g}} = \mathbb{F}_{\mathfrak{z}_K} = \mathbb{F}_{\ell^2}$$

Let $x_g, x_f \in X_0(N)$ be as in section 4.3 $\text{Tr}_\ell(x$

4.5.3 Constructing cohomology classes in $H^1(K, E_p)$

The congruences

$$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$$

follow from the fact that ℓ is inert in K .

Let $G_{K_1} = \text{Gal}(K_f/K_1)$. Recall that for a prime ℓ with $\ell g = f$ the subgroup $G_{K_g} = \text{Gal}(K_f/K_g) \subset G_{K_1}$ is a cyclic of order $\ell + 1$. Now we define some elements in the group ring $\mathbb{Z}[G]$.

The *augmentation ideal* of the group ring $\mathbb{Z}[G_\ell]$ is the kernel of the *augmentation map*

$$\begin{aligned}\epsilon : \mathbb{Z}[G_\ell] &\longmapsto \mathbb{Z} \\ \sum_{\sigma \in G_\ell} n_\sigma \sigma &\longmapsto \sum_\sigma n_\sigma\end{aligned}$$

Note that the kernel $\ker \epsilon$ is the \mathbb{Z} -submodule generated by elements of the form $\sigma - \sigma'$ for $\sigma, \sigma' \in G_\ell$. Now fix a generator $\sigma_\ell \in G_\ell$ and write

$$\sigma - \sigma' = \sigma_\ell^t - \sigma_\ell^s = \sum_{i=0}^{t-s-1} \sigma_\ell^{t-i} - \sigma_\ell^{t-i-1} = (\sigma_\ell - \text{id})\sigma''$$

for any σ, σ' and some σ'' . It follows that $\ker \epsilon = \mathbb{Z}[G_\ell] \cdot (\sigma_\ell - \text{id})$ is principal. Let $\text{Tr}_\ell = \sum_{\sigma \in G_\ell} \sigma \in \mathbb{Z}[G_\ell]$ and let S_ℓ be a solution of the following equation in $\mathbb{Z}[G_\ell]$

$$(\sigma_\ell - \text{id}) \cdot S_\ell = (\ell + 1)\text{id} - \text{Tr}_\ell \quad (4.3)$$

Write $\tau_j = \text{id} + \sigma_\ell + \sigma_\ell^2 + \cdots + \sigma_\ell^{j-1}$ and note that $(\sigma_\ell - \text{id}) \cdot \tau_j = \sigma_\ell^j - \text{id}$. It follows that

$$(\sigma_\ell - \text{id}) \sum_{j=1}^{\ell+1} \tau_j = \sum_{j=1}^{\ell+1} \sigma_\ell^j - (\ell + 1) = \text{Tr}_\ell - (\ell + 1)\text{id}$$

thus $S_\ell = -\sum_{j=1}^{\ell+1} \tau_j$ is a solution of equation 4.3. Note that the class of S_ℓ in $\mathbb{Z}[G_\ell]/\mathbb{Z} \cdot \text{Tr}_\ell$ is well-defined since $(\sigma_\ell - \text{id}) \cdot \text{Tr}_\ell = 0$. Let

$$S_f = \prod_{\ell|f} S_\ell$$

Note that S_f is well-defined since the S_ℓ commute. Recall the construction of y_f in section 4. Then the class of the point $S_f y_f \in E(K_f)$ in $E(K_f)/pE(K_f)$ is invariant by G , since for $\ell \mid f$ one has

$$(\sigma_\ell - \text{id})S_f y_f = (\sigma_\ell - \text{id})S_\ell S_g y_f = \left((\ell + 1)\text{id} - \text{Tr}_\ell\right) S_g y_f \equiv (0 - \text{Tr}_\ell) S_g y_f \pmod{pE(K_f)}$$

and it suffices to check invariance for σ_ℓ and $\ell + 1 \equiv 0 \pmod{p}$. But $\text{Tr}_\ell S_g = S_g \text{Tr}_\ell$ so

$$(\sigma_\ell - \text{id})S_f y_f \equiv -S_g \text{Tr}_\ell y_f \pmod{pE(K_f)}$$

But $a_\ell \equiv 0 \pmod{p}$ and

$$\text{Tr}_\ell y_f = a_\ell y_g \in pE(K_g) \subset pE(K_f)$$

It follows that the class $[S_f y_f] \in E(K_f)/pE(K_f)$ is well-defined. Moreover, the point $P_f = \sum_{\sigma \in G_K/G_{K_1}} \sigma S_f y_f$ has a class $[P_f] \in E(K_f)/pE(K_f)$ invariant under the action of $G_K = \text{Gal}(K_f/K)$. E has no p -torsion rational over K_f . There is an isomorphism

$$H^1(K, E_p) \xrightarrow{\sim} H^1(K_f, E_p)^{G_K}$$

The *inflation restriction sequence*

Alphabetical index

- G -module, 38
- $\mathrm{SL}_2(\mathbb{Z})$ equivalence, 11
- abelian extension, 6
- affine curve, 29
- algebraic integer, 4
- Artin symbol, 6
- augmentation map, 43
- automorphic form, 31
- bad reduction, 20, 41
- binary quadratic form, 15
- BSD conjecture, 36
- class number, 4
- cochain, 38
- cohomology, 39
- complex multiplication, 15
- complex torus, 12
- conductor of an elliptic curve, 36, 41
- conductor of an extension, 8
- conductor of an order, 12
- congruence subgroup, 23
- conjugate function fields over a field, 30
- coordinate ring of a curve, 29
- curves isomorphic over a field, 29
- cuspidal, 25
- decomposition group, 5
- Dedekind domain, 4
- degree of an holomorphic map, 26
- differential, 38
- Dirichlet's unit theorem, 4
- discriminant of an order, 12
- elliptic curve, 13
- elliptic point, 24
- enhanced elliptic curve, 35
- Fermat's last theorem, 36
- fractional ideal, 4
- free action, 18
- Frobenius automorphism, 6
- function field, 30
- function field of a curve, 29
- fundamental domain, 24
- fundamental identity, 5
- genus, 26
- group ring, 38
- Heegner point, 36, 38
- Heegner's hypothesis, 38, 42
- Hilbert class field, 7, 20
- Hilbert class polynomial, 18
- homothety of lattices, 11
- ideal class group, 4
- ideals prime to the conductor, 21
- inertia group, 5
- inertial degree, 4
- isogeny, 13
- isomorphism of curves, 29
- lattice, 11
- modular curve, 23
- modular elliptic curve, 36
- modular form, 31
- modular group, 23
- modular parametrization, 36
- morphism defined over a field, 29
- morphism of curves, 29
- nonsingular curve, 29
- norm, 4
- number field, 4
- numerical norm of an ideal, 6
- order, 12
- period of a point, 24
- place of a number field, 9
- principal congruence subgroup, 23
- proper ideal, 16
- purely inseparable morphism, 21

quadratic form, [15](#)
 ramification degree, [27](#)
 ramification index, [4](#)
 ramified prime, [5](#)
 Riemann-Hurwitz formula, [27](#)
 ring class field, [20](#), [21](#)
 Selmer group, [40](#)
 special linear group, [23](#)
 Tate-Shafarevich group, [37](#), [40](#)
 trace, [4](#)
 transitive action, [18](#)
 uniformizer at a point, [29](#)
 unramified extension, [7](#)
 upper half plane, [23](#)
 width of a cusp, [26](#)

References

- [1] COX, D. *Primes of the form $x^2 + ny^2$* . Wiley, 1997.
- [2] DIAMOND, F., AND SHURMAN, J. *A First Course in Modular Forms*. Springer (Graduate Texts in Mathematics), 2005.
- [3] MARCUS, D. *Number fields*. Springer, 1977.
- [4] NEUKIRCH, J. *Algebraic Number Theory*. Springer, 1999.