# Some more or less explicit class field theory



1 AUTHOR:

Dennis Eriksson
University of Gothenburg
8 PUBLICATIONS 20 CITATIONS

SEE PROFILE

# Some more or less explicit class field theory

Dennis Eriksson

May 25, 2004

**Abstract**

A little survey of explicit class field theory, both local and global. In particular, for imaginary quadratic fields we give the theory of complex multiplication for elliptic curves, and we also construct the Lubin-Tate group. Torsion points in various groups will turn out to generate particular ramified extensions of our fields. This makes the reciprocity laws of class field theory explicit.

## Contents

**1 Outline and Prerequisites** **2**
1.1 Conductors and Ray Class Fields . . . . . 2
1.2 Summary of Results . . . . . 3

**2 Explicit Local Class Field Theory** **4**
2.1 The Lubin-Tate Group . . . . . 4
2.2 Construction of Totally Ramified Extensions . . . . . 7
2.3 Local Kronecker-Weber . . . . . 8

**3 Class Field Theory for $\mathbb{Q}$** **11**
3.1 Kronecker-Weber . . . . . 11

**4 Complex Multiplication of Elliptic Curves** **12**
4.1 General Theory . . . . . 12
4.2 The Associated $\ell$-adic Galois Representation . . . . . 14
4.3 Integrality of the j-Invariant . . . . . 15
4.4 Construction of Class Fields for Imaginary Quadratic Fields 16
4.5 Examples . . . . . 20

# 1 Outline and Prerequisites

## 1.1 Conductors and Ray Class Fields

$K$ is a number field.
$\mathcal{O}_K$ is the maximal order of $F$.

The following material was partially taken from [6] and [1].

**Definition 1.** *Let $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$ be the formal product of the following two objects:*

$$\mathfrak{M}_0 = \mathfrak{a} = \prod_i \mathfrak{P}_i^{e_i}$$

*and*

$$\mathfrak{M}_\infty = \prod \infty_i.$$

*The first one is an ideal, factored into prime components, so that $e_i = 0$ for all but finitely many primes. The second one is a formal sum of a number of infinite primes. We call $\mathfrak{M}$ a divisor.*

**Definition 2.** *Let $I$ denote the group of fractional ideals of $K$, and $P$ the group of principal ideals. Let $I_\mathfrak{M} = I_{\mathfrak{M}_\circ}$ be the subgroup of fractional ideals relatively prime to $\mathfrak{M}_0$. Furthermore, let $P_\mathfrak{M}$ be the subgroup of $P$ such that $(\alpha) \in P_\mathfrak{M}$ if $\alpha \equiv 1 (\mathrm{mod}\, \mathfrak{M}_0)$ and $\alpha|_{\infty_i} > 0$ for $\infty_i | \mathfrak{M}_\infty$.*

To a finite abelian extension $L/K$ we can associate a divisor $\mathfrak{c}_L$, called the "conductor", with the property that it is divisible by exactly the ramified primes (finite and infinite) and if $\mathfrak{c}_L | \mathfrak{M}$, another divisor, then there is a surjective homomorphism

$$I_\mathfrak{M} \to \mathrm{Gal}(L/K)$$

sending a prime ideal $\mathfrak{p}$ to $\sigma_\mathfrak{p}$, the $\mathfrak{p}$ Frobenius element of $L/K$, and extending by linearity. The kernel is furthermore exactly $H = P_\mathfrak{M} N_{L/K} I_\mathfrak{M}(L)$, where $N_{L/K}$ is the obvious norm map on ideals from $L$ to $K$. The converse on $H$ is also true, i.e. given a subgroup $P_\mathfrak{M} \subseteq H \subseteq I_\mathfrak{M}$, there is an extension $L/K$ with conductor dividing $\mathfrak{M}$ such that $H = P_\mathfrak{M} N_{L/K} I_\mathfrak{M}(L)$ and an isomorphism, using the same map as above,

$$I_\mathfrak{M}/H \simeq \mathrm{Gal}(L/K).$$

This is essentially functorial, i.e. if you have two groups $H_1 \subseteq H_2$, then we have associated fields $L_1 \supseteq L_2$ and vice versa. In particular, now choose $H = P_\mathfrak{M}$.

The associated field $K_\mathfrak{M}$ is called the ray class field, and it has the property that if $K \subseteq L$ has conductor $\mathfrak{c} = \mathfrak{c}_L$ dividing $\mathfrak{M}$, then $L \subseteq K_\mathfrak{M}$, and furthermore, it is characterized by the fact that a prime ideal $\mathfrak{p}$ splits completely, if and only if it is principal over $K$, $\mathfrak{p} = (\alpha)$, $\alpha \equiv 1 (\mathrm{mod}\, \mathfrak{M}_0)$ and $\alpha|_{\infty_i} > 0$, for all $\infty_i | M_\infty$. Its Galois group is naturally isomorphic to $I_\mathfrak{M}/P_\mathfrak{M}$.

In particular, take $\mathfrak{M} = (1)$, then the associated field $H$ is called the Hilbert class field, and is by construction the maximal abelian unramified extension of $K$, characterized by the fact that $\mathfrak{p}$ of $K$ splits completely if and only if it is principal, and not ramified at any infinite primes. Furthermore, the above isomorphism allows us to identify $\mathrm{Gal}(H/K)$ with

$I/P$, the class group.

The following will be needed at one point: For a finite abelian group $G$, let $\widehat{G} = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ be the Piontryiagin dual of $G$. $G$ is non-canonically isomorphic to $\widehat{G}$, and canonically isomorphic to $\widehat{G}$ by the map $g \mapsto [\chi \mapsto \chi(g)]$, and we will often use the latter identification implicitly.

We have a natural non-degenerate pairing,

$$G \times \widehat{G} \to \mathbb{C}^\times$$

$$(g, \chi) \mapsto \chi(g).$$

This sets up a duality between subgroups $H$ of $G$ and subgroups $H'$ of $\widehat{G}$, by $H \mapsto H^\perp = \{\chi \in \widehat{G} | \chi(h) = 1, h \in H\}$.

## 1.2 Summary of Results

Our main objective will be to determine the ray class fields of various fields of arithmetic interest, local fields and global fields. The most famous result in this direction is the Kronecker-Weber theorem, which asserts that the maximal abelian extension of $\mathbb{Q}$ is obtained by adjoining the $n$-th roots of unity. Geometrically, one adds all the torsion points of the circle. We will have similar results when considering imaginary quadratic fields, and local fields. Here the circle is replaced by an elliptic curve and a formal group respectively.

One can take two different viewpoints in this game. On the one hand, it has been observed that ramified extensions are obtained by adjoining torsion as just mentioned. We show that one can pick out an invariant differential on some complex group-variety and obtain functions whose values at certain torsion points give abelian extensions. The other course of action one can take is to follow up what happens in the chapter on the Kronecker-Weber theorem. There we use the local Kronecker-Weber theorem to deduce a result in the global case. In principle, if one is able to solve the "local Kronecker-Weber"-problem, which amounts to finding the maximal abelian totally ramified extension of the completion of the global field at a prime, and generate the Hilbert class field, then one should be able to find all abelian extensions of any global field.

This study is divided into three parts:

- Local fields: Here we show that the maximal unramified extension of a local field with finite residue field of characteristic $p$ is generated by $n$-th roots of unity, $n$ being prime to $p$. We also construct the Lubin-Tate groups, whose torsion points will generate the maximal totally ramified abelian extension. We round off with a proof of a local Kronecker-Weber theorem for $\mathbb{Q}_p$.
- The global field $\mathbb{Q}$: Here we prove the famous Kronecker-Weber theorem.
- Imaginary quadratic fields, $K$: To every imaginary quadratic field we can associate an elliptic curve with a big endomorphism algebra. This leads us into the theory of complex multiplication, which in the end gives rise to the following two results: the $j$-invariant of the associated elliptic curve generates the Hilbert class field of $K$, and torsion points of the same elliptic curve will generate ramified extensions.

# 2 Explicit Local Class Field Theory

| | |
|---|---|
| $K$ | is a local field. |
| $\mathcal{O}_K$ | is the valuation ring of $K$. |
| $\mathfrak{m} = (\pi)$ | is the maximal ideal of $\mathcal{O}_K$. |
| $\overline{K}$ | is the residue field, $\mathcal{O}_K/(\pi)$. |

We wish to construct the maximal abelian extension of a local field, i.e. the fraction field of a complete local ring with finite residue field. We will distinguish between totally ramified extensions and unramified extensions, and treating each case separately and using the decomposition $K^{ab} = K^{nr}K_\pi$ of $K^{ab}$ into an unramified part and a totally ramified part, we will arrive at our conclusion.

The case of unramified extensions is easily sketched. Indeed, finite unramified extensions $L$ of $K$ corresponds bijectively to finite extensions $\overline{L}$ of $\overline{K}$, as is shown in [3]. If we have a finite extension $\overline{L}$ of $\overline{K}$, lift elements of $\overline{L}$ to $\mathcal{O}_L$, and denote such a set of representatives by $S_{\overline{L}}$. Any element $x$ of $L$ can then be written as

$$x = \sum_{n=-n_0}^{\infty} s_n \pi^n, s_n \in S_{\overline{L}}.$$

Hence, using this notation we have

$$K^{nr} = \bigcup_{\overline{L}/\overline{K} \text{ finite}} L$$

and the completion of $K^{nr}$ is given by

$$\widehat{K^{nr}} = \left\{ \sum_{n=-n_0}^{\infty} s_n \pi^n, s_n \in S = \bigcup S_{\overline{L}} \right\}$$

Notice that this is an analogue of the Hilbert class field in the local case, in the sense that it is the maximal unramified abelian extension.

As was just noted, an unramified extension $L/K$ of degree $n$, corresponds to an extension of residue fields $\overline{L}/\overline{K}$. We obtained unramified extensions by lifting elements of $\overline{L}$ to $L$. Because $\overline{L}$ is generated by roots of unity and of degree $n$ over $\overline{K}$, it contains a primitive $n$-th root of unity. Let $\zeta$ be a multiplicative representative of a primitive root $n$-th root of unity with $p$ not divining $n$. This is also a primitive $n$-root of unity, and must thus generate $L$ as an $K$-algebra. One obtains the result by passage to a limit and the observation that the algebraic closure of $\overline{K}$ is obtained by adjoining all $n$-th roots of unity with $n$ being prime to $p$. We have just shown:

**Theorem 1.** *The maximal unramified extension of a local field $K$ with finite residue field is obtained by adjoining $n$-th roots of unity, with $n$ being prime to the characteristic of the residue field.*

## 2.1 The Lubin-Tate Group

| | |
|---|---|
| $K$ | is a local field. |
| $\mathcal{O}_K$ | is the subring of $K$ consisting of elements of positive evaluation. |
| $\pi$ | is a unformizer of the maximal ideal of $\mathcal{O}_K$. |
| $q$ | is the cardinality of the residue field $\mathcal{O}_K/(\pi)$. |

In this section we will construct a group structure on the maximal ideal on the algebraic closure of a local field, such that the torsion on this corresponds to ramified extensions of the same.

First we need a small detour to the land of abelian formal groups. We say that a polynomial $F \in \mathcal{O}_K[[X,Y]]$ is an (abelian) formal group (with respect to $\mathcal{O}_K$) , if

- $F$ is without constant term, i.e. $F(X,Y) = \sum a_{n,m}X^nY^m$ and $a_{0,0} = 0$.
- $F$ is "associative", i.e. $F(F(X,Y),Z) = F(X,F(Y,Z))$.
- We have an "identity", $F(X,0) = X$ and $F(0,Y) = Y$.
- It is abelian, $F(X,Y) = F(Y,X)$.

One can include in this definition the existence of an "inverse", a formal power-series $i$ in one variable such that $F(X,i(X)) = 0$. However, this can easily be constructed, as in [2].

There are two basic examples of a formal group.

- The formal additive group, $\widehat{\mathbb{G}}_a$, where

$$F(X,Y) = X + Y$$

.

- The formal multiplicative group, $\widehat{\mathbb{G}}_m$, where

$$F(X,Y) = (1+X)(1+Y) - 1$$

.

If we let $X$ and $Y$ be elements of $\mathfrak{m} = (\pi)$. Then $\widehat{\mathbb{G}}_a$ is just the usual additive group on $\mathfrak{m}$, and $\widehat{\mathbb{G}}_m$ reflect the multiplicative group-structure that can be put upon $\mathfrak{m}$, by sending $x \in \mathfrak{m}$ to $1 + x \in 1 + \mathfrak{m}$ and use the multiplicative group structure on this.

Denote by $O_n(X)$ the power-series in the variable/multivariable $X$ whose monomials all have degrees at least $n$. Now, let $L_\pi$ be the set of formal power-series in $\mathcal{O}_K$ such that they verify the following properties:

- $f(X) = \pi X + O_2(X)$
- $f(X) = X^q + \pi g(X)$ where $g \in \mathcal{O}_K[[X]]$.

Thus, $L_\pi$ is a set of "Eisenstein" power-series. We will need the following lemma to associate a sane formal group to elements of $L_\pi$, a lemma which Oesterlé, [2], calls "une lemme technique":

**Lemma 2.** *Let $f, g \in L_\pi$ and $a_1, \ldots, a_m \in \mathcal{O}_K$. Then there exists a unique formal power-series $\Phi$ such that*

- *$\Phi$ is without constant term and $\Phi(X_1, \ldots, X_m) = a_1X_1 + \ldots + a_mX_m + O_2(X_i)$.*
- *$f(\Phi(X_1, \ldots, X_m)) = \Phi(g(X_1), \ldots, g(X_m))$.*

*Proof.* If $\Phi_1 = \sum_{i=1}^{m} a_i X_i$, one checks that, using multi-index notation $X = (X_1, \ldots, X_m)$ that

$$f(\Phi_1(X)) = \Phi_1(g(X)) + O_2(X).$$

Now, if we have a polynomial $\Phi_n$ of degree $n$ such that

$$f(\Phi_n(X)) = \Phi_n(g(X)) + O_n(X)$$

we wish to construct a better approximation $\Phi_{n+1}$ up to $O_{n+1}(X)$-terms. It is not difficult to show that we necessarily have

$$\Phi_{n+1} = \Phi_n + [\pi(1 - \pi^n)]^{-1} S(X)$$

where $S(X)$ is the homogenous degree $n+1$-part of $\Phi_n(g(X)) - f(\Phi_n(X))$. One needs an argument to show that the latter part of this is actually a polynomial with coefficients in $\mathcal{O}_K$, and for this we refer to [2]. Uniqueness follows from the fact that all every $\Phi_i$ is uniquely determined by $\Phi_{i-1}$, and that $\Phi_1$ is the first best approximation. □

In particular, we can take $a_1 = a_2 = 1$ and $f = g$, in which case one gets a power-series in two variables $F$, such that

$$f(F(X, Y)) = F(f(X), f(Y)).$$

We wish to show that this is a formal group, in which case one can interpret the above formula as $f$ being a homomorphism of formal groups. All the properties to be shown are either obvious or follow from the uniqueness-property in the above lemma. To give a taste of how the proofs go, we show associativity. So, let $G_1(X, Y, Z) = F(F(X, Y), Z)$ and $G_2(X, Y, Z) = F(X, F(Y, Z))$. Both $G_1$ and $G_2$ are of the form $X + Y + Z + O_2(X, Y, Z)$, because $F$ is. It is thus of the form prescribed in the lemma. It is also obvious that $f$ commutes with both $G_1$ and $G_2$ in the above sense, and our uniqueness-property tells us that $G_1 = G_2$. We have thus showed the first half of:

**Theorem 3.** *Let $f \in L_\pi$, then there exists a unique formal group $F = F_f$ such that $f(F(X, Y)) = F(f(X), f(Y))$. Also, every element $a \in \mathcal{O}_K$ defines (uniquely) an endomorphism $[a] = [a](X)$ of $F_f$, such that*

- $[a](X) = aX + O_2(X)$.
- $[a](f(X)) = f([a](X))$.

*These furthermore satisfy that*

- $[a + b] = [a] + [b]$.
- $[ab] = [a] \circ [b]$
- $[\pi] = f$.

*Proof.* It remains to prove the existence of $[a]$. However, the existence and uniqueness follows from our technical lemma. That it is an endomorphism of our formal group $F$ means just that $[a](F(X, Y)) = F([a](X), [a](Y))$. However, $f$ commutes with both sides, and both sides have leading term $aX + aY$, so uniqueness says they are the same. The remaining properties are shown in the same way. □

**Definition 3.** *The formal group $F_f$ is called the Lubin-Tate group (associated to $f$).*

One shows, again using the technical lemma, that two Lubin-Tate groups $F_f$ and $F_g$ are isomorphic, i.e. there exists a formal power-series $u(X) = X + O_2(X)$, which means that $u$ is invertible, and such that $u \circ F_f = F_g \circ u$. One just finds a such a $u$ verifying $u \circ f = g \circ u$ and $u = X + O_2(X)$ and it will verify the the other written property.

## 2.2 Construction of Totally Ramified Extensions

We now wish to associate a group, in the usual sense, to $F_f$, on which $\mathcal{O}_K$ acts. The torsion of this group will happen to generate all totally ramified abelian extensions. The proof of this fact will essentially lead us to a construction of local class field theory in its entirety.

Let $K_S$ be the separable closure of $K$, and $\mathfrak{m}_S$ its maximal ideal. Fixing an $f \in L_\pi$, $\mathfrak{m}_L$ will be, for each separable extension $L/K$, an abelian group, with group law $x \oplus x' := F_f(x, x')$, $\ominus x = i(x)$. Because $x$ and $x'$ are in $\mathfrak{m}_L$ and $F \in \mathcal{O}_K[[X, Y]]$, $x \oplus x'$ actually defines a converging sum. Also, because the coefficients of $F$ are in $\mathcal{O}_K$, $G_S := \mathrm{Gal}(K_S/K)$ acts on $\mathfrak{m}_L$, and it is formal that it is a $\mathcal{O}_K$-module by $a.x := [a](x)$. Finally, we now construct the candidates for generating ramified extensions of $K$, namely one defines

$$T_{f,\pi}(\pi^n) = \{x \in \mathfrak{m}_S, \pi^n.x = 0\},$$

the $\pi^n$-torsion of $\mathfrak{m}_S$ and

$$T_{f,\pi} = \bigcup_{n=1}^{\infty} T_{f,\pi}(\pi^n).$$

**Theorem 4.** *Let $T_{f,\pi}$ be as above, then*

**a** *$T_{f,\pi}$ is isomorphic to $K/\mathcal{O}_K$ as an $\mathcal{O}_K$-module.*

**b** *the field $K(T_{f,\pi}(\pi^n))$ is a separable algebraic extension of $K$ and is a totally ramified abelian extension of $K$ of degree $q^{n-1}(q-1)$.*

**c** *For every $\sigma \in \mathrm{Gal}(K(T_{f,\pi}(\pi^n))/K)$, there is an $a(\sigma) \in \mathcal{O}_K^\times$ defined modulo $1 + \pi^n\mathcal{O}_K$ such that for any $x \in K(T_{f,\pi}(\pi^n))$, one has*

$$\sigma(x) = a(\sigma)x$$

*and the map $\sigma \mapsto a(\sigma)$ is an isomorphism $\mathrm{Gal}(K(T_{f,\pi}(\pi^n))/K) \to \mathcal{O}_K^\times/(1 + \pi^n\mathcal{O}_K)$. Furthermore, this doesn't depend on the choice of $f$.*

*Proof.* We have already seen that we have an isomorphism $u : F_f \to F_g$ for two different $f, g \in L_\pi$, and one checks without trouble that $u \circ [a]_f \circ u^{-1} = [a]_g$, for $a \in \mathcal{O}_K$, and thus $u$ defines an isomorphism $\mathfrak{m}_{S,f} \to \mathfrak{m}_{S,g}$ of $\mathcal{O}_K$-modules. Hence $u(T_{f,\pi}(\pi^n)) = T_{g,\pi}(\pi^n)$, and because $u$ also commutes with the action of the Galois group $G_S$, we see that $K(T_{f,\pi}(\pi^n))$ and $K(T_{g,\pi}(\pi^n))$ are both fixed by the same elements of $G_S$, hence the same.

We can thus in particular take $f = \pi x + x^q$. One then sees, noting that $\pi$ acts as $f$, that the torsion group $T_{f,\pi}(\pi)$ consists of the zeros of $x^q + \pi x$,

and that all those zeros are in this group, because the polynomial is separable. Fixing a zero $x_0 \neq 0$ of $f$ gives a map $\mathcal{O}_K \to T_{f,\pi}(\pi), a \mapsto a.x_0$, with kernel exactly $\mathfrak{m}_K$. Because the residue field has exactly $q$ elements, as does the number of roots of $x^q + \pi x$, it is surjective. Because the polynomial $X^q + \pi X - x$ is separable, one can find a $y$ such that $\pi.y = x$, and this shows that $T_{f,\pi}$ is $\pi$-divisible. A simple algebraic lemma then shows that we have an $\mathcal{O}_K$-module isomorphism $K/\mathcal{O}_K \to T_{f,\pi}$, namely one takes representatives from $A$ so that they surject to $A/\mathfrak{m} \simeq T_{f,\pi}(\pi)$. In particular, taking 1 mapped to $x_1$, one can find an $x_2$ s.th. $\pi x_2 = x_1$, and so on. Then one maps $\pi^{-n} \in K/\mathcal{O}_K$ to $x_n$, extends linearly and shows this gives an isomorphism.

Since, by the above, $T_{f,\pi}(\pi^n) = \mathcal{O}_K/\pi^n\mathcal{O}_K$, and is thus generated, as an $\mathcal{O}_K$-module, by a single element $x$, so $K(x) = K(T_{f,\pi}(\pi^n))$. Hence, for any $\sigma \in \mathrm{Gal}(K(x)/K)$, one has $\sigma(x) = a.x$ for some $a \in \mathcal{O}_K$, and one sees that $\sigma$ defines an element in $\mathcal{O}_K^\times/(1+\pi^n\mathcal{O}_K)$, and that this association is an injective homomorphism. To show that it is surjective, suppose that, as above, that $x$ is a generator of the $\pi^n$-torsion. Then, writing $f^{(k)} = f \circ f \circ \ldots \circ f$ ($k$ times), one has $f^{(n)}(x) = 0$, but $f^{(n-1)}(x) \neq 0$, and one calculates

$$0 = \frac{f^{(n)}(x)}{f^{(n-1)}(x)} = \left(f^{(n-1)}(x)\right)^{q-1} + \pi.$$

But $\left(f^{(n-1)}(X)\right)^{q-1} = X^{q^{n-1}(q-1)} \bmod \pi$, so $x$ is the zero of an Eisenstein polynomial, and $K(x)$ is a totally ramified extension of degree $q^{n-1}(q-1)$. Because $\pi^n$-torsion is stable under $G_S$, $K(T_{f,\pi}(\pi^n))$ is Galois. $\mathcal{O}_K^\times/(1+\pi^n\mathcal{O}_K)$ and $\mathrm{Gal}(K(x)/K)$ both have the same cardinality, and the constructed correspondence was injective, hence an isomorphism. This also shows the extension is abelian, and all three assertions of the theorem have been proved. □

Some natural questions that can be asked at this point are: Are the above extensions dependent on the choice of uniformizer $\pi$, do they generate all abelian totally ramified extensions? As one may suspect, the answer to these questions is indeed yes.

## 2.3 Local Kronecker-Weber

Let the field obtained by adding all torsion be denoted by $K_\pi$. Because all finite subextensions are finite and totally ramified, this is linearly disjoint with $K^{nr}$.

Hence, to show that two different uniformizers $\pi$ and $\pi'$ give rise to the same $K_\pi$ and $K_{\pi'}$, it will be sufficient to show that $K^{nr}K_\pi = K^{nr}K_{\pi'}$. This is however not too hairy, and we will be content with giving the following lemma without proof, but it can be found in [2]:

**Lemma 5.** *Suppose that $f \in L_\pi, g \in L_\omega$. Then there exists a formal power-series $\Phi \in \mathcal{O}_{K^{nr}}[[X]]$ such that*

$$[\omega]_g \circ \Phi = \Phi^F \circ [\pi]_f$$

*and*

$$\Phi(x) = \varepsilon x + O_2(x)$$

*where $F$ is the Frobenius element $F : K^{nr} \to K^{nr}$ prolonged to $\hat{K}^{nr}$ and $\varepsilon$ is a unit in $\hat{K}^{nr}$ such that $\varepsilon\omega = F(\varepsilon)\pi$. This can also be written, regarding $\Phi$ as a homomorphism of formal groups,*

$$\begin{array}{ccc} F_{f,\pi} & \xrightarrow{\Phi} & F_{g,\omega} \\ \downarrow{\scriptstyle [\pi]_f} & & \downarrow{\scriptstyle [\omega]_g} \\ F_{f,\pi} & \xrightarrow{\Phi^F} & F_{g,\omega}. \end{array}$$

So, now take two polynomials $f$ and $g$ as in the lemma, together with the map $\Phi$. $\Phi$ is in fact an isomorphism of formal groups over $\widehat{K^{nr}}$, which is not so difficult to show, using the techniques from the earlier chapter, but with $\widehat{K^{nr}}$ instead of $\mathcal{O}_K$. For details, see [2]. Because of this, the induced groups $\mathfrak{m}_{\widehat{K^{nr}}}$ associated to $f$ and $g$ respectively, are isomorphic over $\widehat{K^{nr}}$, and thus their torsion groups as well, and so $\widehat{K^{nr}K_\pi} = \widehat{K^{nr}K_\omega}$. Taking completions once more one obtains $\widehat{K^{nr}K_\pi} = \widehat{K^{nr}K_\omega}$. Let $L$ be the largest separable algebraic extension of $K$ that is contained in $\widehat{K^{nr}K_\pi}$. $L$ is Galois and contains $K^{nr}K_\pi$. Take any $\sigma \in \mathrm{Gal}(L/K^{nr}K_\pi)$. $\sigma$ is continuous with respect to$\mathfrak{m}_{\widehat{K^{nr}}}$ the valuation of $L$, and prolongs by continuity to $\widehat{K^{nr}K_\pi}$, and because $\sigma$ is the identity on $K^{nr}K_\pi$, it is the identity on this, and $L = K^{nr}K_\pi = K^{nr}K_\omega$. Lastly, if we have two uniformizers $\omega$ and $\pi$, they differ by an invertible element $\pi$. The above lemma gives us that $\Phi^F \circ [\pi]_f = [\omega]_g \circ \Phi = \Phi \circ [\omega]_f = \Phi \circ [u]_f \circ [\pi]_f$, and dividing with $[\pi]_f$ gives that $\Phi^F = \Phi \circ [u]_f$.

**Theorem 6 (Local Class Field Theory).** *Keeping the notation above, $K^{nr}K_\pi = K^{ab}$ and the reciprocity homomorphism*

$$K^{\hat{\times}} \to \mathrm{Gal}(K^{ab}/K)$$

*is an isomorphism of topological groups, where $K^{\hat{\times}} = \mathcal{O}_K^\times \oplus \pi^{\hat{\mathbb{Z}}}$ and $\hat{\mathbb{Z}}$ is the completion of $\mathbb{Z}$ with respect to the ideal topology.*

As a remark, we mention how above map associates to an element $\alpha \in K^{\hat{\times}}$ an reciprocity element $(\alpha, K^{ab}/K)$. We briefly recall how this homomorphism is constructed:
Let $L/K$ be a finite abelian Galois extension, $G = \mathrm{Gal}(L/K)$. Consider the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ of $G$-modules (with trivial action), and the induced morphism $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$. Now, $H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, which is just the character group of $G$. This furnishes a map $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \times K^\times = H^1(G, \mathbb{Q}/\mathbb{Z}) \times H^0(G, L^\times) \to H^2(G, \mathbb{Z}) \times H^0(G, L^\times) \to H^2(G, L^\times) \simeq \mathrm{Br}(L/K) \hookrightarrow \mathrm{Br}(K)$. Local class field theory computes $\mathrm{Br}(K)$ to be equal to $\mathbb{Q}/\mathbb{Z}$, so we get a pairing

$$\langle , \rangle : \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \times K^\times \to \mathbb{Q}/\mathbb{Z}.$$

One checks that $\langle , \rangle$ is bimultiplicative. Because $L/K$ is abelian, one has a perfect pairing between $G$ and its dual, $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, and the above map amounts to evaluating $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ at some $(\alpha, L/K) \in G$, i.e.

$$\langle \chi, \alpha \rangle = \chi((\alpha, L/K)).$$

The reciprocity map associates to $\alpha \in K^{\hat{x}}$ the automorphism $(\alpha, K^{ab}/K)$ determined as above.

The same argument goes through with any finite Galois extension, but with replacing $G$ with $G^{ab}$ at appropriate places.

*Proof.* (of the theorem of local class field theory) We will suppose some facts from local class field theory for this proof. For example, we will use that the map is continuous. Thus, because $K^{\hat{\times}}$ is compact, so is its image. Also, for any finite extension $L$ of $K$, one has $\mathrm{Gal}(L/K) \simeq K^\times/NL^\times$ by the Tate local duality theorem, so the image is also dense. Now, since $K^{nr}$ and $K^\pi$ are linearly disjoint, one has the series of maps

$$K^{\hat{\times}} \to \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(K^{nr}K_\pi/K) \to \mathrm{Gal}(K^{nr}/K) \times \mathrm{Gal}(K_\pi/K)$$

and all of these are either obviously surjective, or by the aboveare easily seen to be so. $\mathcal{O}_K^\times$ is sent to $\mathrm{Gal}(K_\pi/K)$ and $\pi^{\hat{\mathbb{Z}}}$ is sent to $\mathrm{Gal}(K^{nr}/K)$. To prove the theorem it will suffice to show that the above composition of maps is injective. To see this we have to write down the action of $(\alpha, K^{ab}/K)$ on $K^{nr}$ and $K_\pi$ explicitly. It is well-known that this acts as $F^v(\alpha)$, where $F$ is the Frobenius map and $v$ the usual valuation. The case of the action on $K_\pi$ takes a little more analysis. Remember we have a commutative diagram

$$\begin{array}{ccc} K(T(\pi^n))^\times & \longrightarrow & \mathrm{Gal}(K^{ab}/K(T(\pi^n)) \\ \downarrow{\scriptstyle Norm} & & \downarrow{\scriptstyle Res} \\ K^\times & \longrightarrow & \mathrm{Gal}(K^{ab}/K) \end{array}.$$

$K(T(\pi^n))$ is generated by some torsion point $x$, i.e. a root of a Eisenstein polynomial of degree $q^{n-1}(q-1)$ and constant term $\pi$, so $\pi$ is a norm in this extension. Hence $(\pi, K^{ab}/K)$ fixes $K(T(\pi^n))$ and thus $K_\pi$. If $u$ is in $\mathcal{O}_K^\times$, this gives two different primes $\pi$ and $\omega = \pi u$. We wish to show that $\sigma = (\omega, K^{ab}/K)$ acts as $[u^{-1}]_f$ on $K_\pi$. Now, let $\lambda \in T_\lambda$. Then, because $(\omega, K^{ab}/K)$ acts as the identity on $T_\omega$ and thus $\Phi(T_\pi) = T_\omega$, one has

$$\sigma(\Phi(\lambda)) = \Phi(\lambda)$$

and so

$$\sigma(\Phi(\lambda)) = \Phi^F(\sigma(\lambda)) = \Phi([u]_f\sigma(\lambda)) = \Phi(\lambda)$$

by the remarks preceding this theorem. Because $\Phi$ is invertible, the result follows. Finally, the result just shown demonstrates that the above maps are injective, and the theorem is proven. □

We note an important and immediate corollary

**Theorem 7 (Local Kronecker-Weber).** *Every abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension $\mathbb{Q}_p(\sqrt[n]{1})$.*

*Proof.* Next, we take our local field to be $K = \mathbb{Q}_p$, and $\pi = p$, $f = px + x^p$. Then a small calculation shows that the formal group associated to $f$ is isomorphic to nothing else than $\widehat{\mathbb{G}}_m$, or rather, if

$$F(X, Y) = (1 + X)(1 + Y) - 1,$$

then $f \circ F(X, Y) = F(f(X), f(Y)$. Hence, when taking $\mathfrak{m}$-points, one obtains an isomorphism with torsion in the two respective groups. Thus $1+T_\pi$ is the torsion of the formal multiplicative group $\widehat{\mathbb{G}}_m$, and its torsion is given by $\{1 + x, (1 + x)^{p^n} = 1\}$. Hence, $(\mathbb{Q}_p)_\pi = \bigcup_{n=1}^\infty Q_p(\sqrt[p^n]{1})$, and we already know the structure of the unramified extensions. □

# 3 Class Field Theory for $\mathbb{Q}$

Consider the affine group scheme $\mathbb{G}_m = \operatorname{Spec}\mathbb{Z}[T, T^{-1}]$, and its set of complex points, $\mathbb{C}^\times$. As a complex analytic group, this has up to a scalar multiple one single holomorphic translation-invariant holomorphic 1-form, namely $dz/z$. Normalizing it so that

$$\omega = (2\pi i)^{-1}\frac{dz}{z}$$

we obtain a map

$$\Phi : \mathbb{C}^\times \to \mathbb{C}/H_1(\mathbb{C}^\times, \mathbb{Z}) \simeq \mathbb{C}/\mathbb{Z}$$

by

$$\Phi(P) = \int_1^P \omega.$$

Here $H_1(\mathbb{C}^\times, \mathbb{Z}) \simeq \mathbb{Z}$ denotes the singular homology with coefficients in $\mathbb{Z}$, and one embeds it into $\mathbb{C}$ by taking a cycle $\gamma$ to the complex number $\int_\gamma \omega$.. This map is just the logarithm map, $\Phi(P) = (2\pi i)^{-1}\log P$, and its inverse is $z \mapsto e^{2\pi i z}$. This shows we have a complex analytic isomorphism of Lie groups $\mathbb{C}^\times$ and $\mathbb{C}/\mathbb{Z}$. This might seem trivial, but in the next chapter about complex multiplication of elliptic curves the same procedure is carried out, and there as here, the value of the inverse map $\Phi^{-1}$ under torsion points will be related in a very explicit way to ramified abelian extensions of our ground field. Also, notice that the torsion points under the map $\Phi^{-1}$ would have been the same regardless of normalization.

## 3.1 Kronecker-Weber

**Theorem 8 (Kronecker-Weber Theorem).** *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

*Proof. First proof*: Let $\mu_N = \{\zeta \in \mathbb{C}, \zeta^N = 1\}$ be the group of $n$-th roots of unity and $\mathbb{Q}(\mu_N)/\mathbb{Q}$ be the $N$-th cyclotomic field. It is well known that this is an abelian extension of $\mathbb{Q}$ ramified exactly at primes dividing $N$, with Galois group $(\mathbb{Z}/N\mathbb{Z})^\times$. For a prime $\mathfrak{P}$ of $\mathbb{Q}(\mu_N)$ lying above a prime $p \nmid N$ of $\mathbb{Q}$, we can consider the Frobenius element $\sigma_\mathfrak{P}$. Fixing a primitive $N$-th root of unity, this is determined by the action

$$\zeta^{\sigma_\mathfrak{P}} \equiv \zeta^p (\operatorname{mod} \mathfrak{P}).$$

Because $p \nmid N$, the equation $x^N - 1$ is separable in characteristic $p$, and one concludes that

$$\zeta^{\sigma_\mathfrak{P}} = \zeta^p.$$

Furthermore, this immediately implies that $\sigma_\mathfrak{P} = 1$ is equivalent to that $p \equiv 1 (\operatorname{mod} N)$. The Frobenius element is independent of the prime $\mathfrak{P}$ above $p$ chosen, and hence the decomposition group of $\mathfrak{P}$ is trivial, and that $p$ splits completely is equivalent to that $p \equiv 1 (\operatorname{mod} N)$. We obviously also have ramification at infinity (a real prime becomes complex), and by class field theory, this is the ray class field of $\mathbb{Q}$ modulo $N\infty$. Hence, if we choose any number field $L$ of conductor $\mathfrak{c} = N$, $L$ is contained in $\mathbb{Q}(\mu_N)$.

*Second proof*: We build the second proof on the fact that Kronecker-Weber is true for $\mathbb{Q}_p$, the $p$-adic integers. So, let $L/\mathbb{Q}$ be abelian. If $p$ ramifies, consider the completion $L_\mathfrak{P}$ of $L$ at any prime lying above

$p$. This is an abelian extension of $\mathbb{Q}_p$, and hence contained in $\mathbb{Q}_p(\mu_{n_p})$, for some minimally chosen integer $n_p$. Let $p^{e_p}$ be the highest power of $p$ dividing $n_p$, and construct the number $n = \prod p^{e_p}$, and form the field $L' = L(\mu_n)$. Our goal is to show that $L' = \mathbb{Q}(\mu_n)$. Let $I_p$ be the inertia group of a prime $p$ in $L'$. This can be computed locally, so

$$I_p \simeq \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^{e_p}})/\mathbb{Q}_p)$$

which has order $\phi(p^{e_p})$. Taking products of these inertia groups, denoting it by $I$, we get,

$$|I| \leq \prod |I_p| = \phi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}].$$

The fixed field of $I$ is just $\mathbb{Q}$, because $\mathbb{Q}$ has no nontrivial unramified extensions. But then

$$[L' : \mathbb{Q}] = [L' : L'^I] = |I| \leq [\mathbb{Q}(\mu_n) : \mathbb{Q}]$$

and

$$\mathbb{Q}(\mu_n) \subseteq L(\mu_n) = L'$$

gives that in fact $\mathbb{Q}(\mu_n) = L'$. □

# 4 Complex Multiplication of Elliptic Curves

## 4.1 General Theory

| | |
|---|---|
| $K$ | is an imaginary quadratic extension of $\mathbb{Q}$. |
| $\mathcal{O}$ | is an order of $K$. |
| $\mathcal{O}_K$ | is the maximal order of $K$. |

Let $E/\mathbb{C}$ be an elliptic curve with invariant differential $dx/y$. Consider the inverse of the map

$$F : E(\mathbb{C}) \to \mathbb{C}/H_1(E(\mathbb{C}), \mathbb{Z})$$

given by

$$F(P) = \int_0^P dx/y (\mathrm{mod}\, H_1(E(\mathbb{C}), \mathbb{Z})).$$

It is the well known isomorphism (of compact complex Lie groups) $\mathbb{C}/\Lambda \simeq E(\mathbb{C}) \subseteq \mathbb{CP}^2$ given by $z \mapsto (\wp(z), \wp'(z), 1)$ if $z \neq 0$ and $0 \mapsto (0 : 1 : 0)$. Here $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ and

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus 0} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

is the Weierstrass $\wp$-function, which satisfies the equation

$$(\wp'(z))^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Furthermore, $g_2$ and $g_3$ are scalar multiples of the Eisenstein series $G_4$ and $G_6$.

The main object of study in this section will be the endomorphism algebra of $E$. This is defined to be the set of all morphisms $E \to E$ taking $O$, the neutral element of $E$, to itself. Every such morphism is in fact a homomorphism of groups, and the ring of endomorphisms will be denoted $\mathrm{End}(E)$. Using the analytic isomorphism to the torus $\mathbb{C}/\Lambda$, we see that the elements of the endomorphism ring are in 1-1-correspondence with all the complex numbers $\alpha$ such that $\alpha\Lambda \subseteq \Lambda$.

**Proposition 9.** *The endomorphism ring of $E$ is either $\mathbb{Z}$ or an order of an imaginary quadratic field, $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, for some positive integer $f$.*

*Proof.* Let $\Lambda = \langle 1, \tau \rangle$ and take any $\alpha$ such that $\alpha\Lambda \subseteq \Lambda$, then $\alpha = a + b\tau, \alpha\tau = c + d\tau$. Hence, if $\alpha$ is not an integer we can eliminate it from the equation to arrive at

$$b\tau^2 - (a - d)\tau - c = 0.$$

One concludes that $b\tau$ is an algebraic integer, and thus $\alpha$ is in $\mathcal{O}_K$, $K = \mathbb{Q}(\tau)$. We also get that $K = \mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$, and finally $\mathrm{End}(E)$ is an order of the same, which we denote by $\mathcal{O}$. That orders of $K$ are of this form is well known and not difficult to show. □

Furthermore, the lattice $\Lambda$ is a proper ideal of $\mathcal{O}$, by which we mean that $\{\alpha \in \mathbb{C} | \alpha\Lambda \subseteq \Lambda\} = \mathcal{O}$. This is the same as requiring that $\Lambda$ is a projective $\mathcal{O}$-module of rank 1: more precisely, $\Lambda \otimes \mathrm{Hom}(\Lambda, \mathcal{O}) \simeq \mathcal{O}$ and $\Lambda$ has rank 1.

Conversely, given a order $\mathcal{O}$ with fraction field $K$, any proper ideal determines a lattice with an endomorphism ring equal to $\mathcal{O}$. Furthermore, any lattice for $E$ is determined uniquely up to homothethy, so we further restrict ourselves to fractional ideals of $K$ modulo homothethy, if we want a fixed endomorphism ring. But this is precisely the ideal class group.[1]

**Proposition 10.** *For an order of an imaginary quadratic field $\mathcal{O}$, there is a bijection*

*Elliptic curves with complex multiplication by $\mathcal{O}$/Isomorhpism $\leftrightarrow$ $Cl(\mathcal{O})$.*

We also have an action of the class group on $E = E_{\mathfrak{a}}$, given by $\mathfrak{p} * E_{\mathfrak{a}} = E_{\mathfrak{a}\mathfrak{p}^{-1}}$. This is quite an analytic action, because it uses the analytic realization of an elliptic curve as a torus.
If $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, $E^\sigma$, obtained by transforming the coefficients of the polynomial(s) defining the curve, has endomorphism ring naturally isomorphic to the one of $E$. Because there are only finitely many classes of elliptic curves with a given complex multiplication (finiteness of the class group), we see that there are only finitely many values of $j(\tau)^\sigma = j(E)^\sigma = j(E^\sigma)$ as $\sigma$ goes through the automorphisms of the above Galois group. One concludes that $j(\tau)$ is algebraic, and there is a model for $E$ over a number field $\mathbb{Q}(j(\tau))$. Not only is $j(\tau)$ algebraic, it is indeed an algebraic integer, which we will see below.

**Remark 11.** *If $[\mathbb{Q}(\tau) : \mathbb{Q}] \geq 3$, $j(\tau)$ is transcendental, see [5].*

If $E$ has complex multiplication by $\mathcal{O}$, and $u \in \mathcal{O}$, we denote the action of $u$ on $E$ by $[u]$. Unless otherwise stated, we now restrict ourselves to the case $\mathcal{O} = \mathcal{O}_K$, the maximal order.

[1] in fact, for non-maximal orders $O_f$, we let $Cl(O_f) = Pic(O_f)$ denote the isomorphism classes of projective $O_f$-modules of rank 1. This is naturally isomorphic to the group of proper fractional ideals modulo proper principal ideals. For $f = 1$, $O$ is Dedekind and every ideal is proper and this coincides with the usual notion of fractional ideals modulo principal ideals. Lastly, the condition $\{\alpha \in \mathbb{C}, \alpha\Lambda \subseteq \Lambda\} = O_f$ means exactly that $\Lambda$ is proper, which is equivalent to being projective of rank 1.

## 4.2 The Associated $\ell$-adic Galois Representation

For imaginary quadratic fields $K$, we can associate another group variety with complex multiplication by $\mathcal{O}_K$. This exists, just take any elliptic curve with the lattice being any element of the class group. Let $L$ be a field of $E$. In particular, we can pick $L = K(j(E))$.

Now, we wish to show that adjoining torsion points to the $L$ yields abelian extensions of the same. First of all, it is clear that if an endomorphism $\alpha$ commutes with the action of $G_L = \mathrm{Gal}(\bar{L}/L)$, the finiteness of $\ker \alpha$ implies the algebraicity of these points too. To see that these are abelian, we study the Galois representation associated to $E$. We briefly recall what it is. Fix a prime number $\ell$. First of all, the $\ell$-adic Tate module of $E$ is defined by the inverse limit

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

were $E[m]$ denotes the set of all points $P$ in $E$ such that $mP = O$, i.e. the $m$-torsion. The absolute Galois group $G_L$ acts on each $E[\ell^n]$, and its action commutes with multiplication by $\ell$. Hence we have a action by $G_L$ on the Tate module. $G_L$ acting continuously on each discrete (finite) group $E[\ell^n]$ and $G_L$ profinite implies that the action on $T_\ell(E)$ is continuous. The associated representation

$$\rho_\ell : \mathrm{Gal}(\bar{L}/L) \to \mathrm{Aut}(T_\ell(E)) = GL_2(\mathbb{Q}_\ell)$$

is of the utmost interest. If the elliptic curve is arbitrary, we cannot say much about this. However, if it has complex multiplication we can say more. The theorem is

**Theorem 12.** *Suppose $E/L$ has complex multiplication by $\mathcal{O}_K$, and that $K$ is contained in $L$. Then the representation $\rho_\ell$ is abelian, i.e. it factors through the abelianization of $G_L$.*

*Proof.* Letting $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ denote the $m$-torsion points of $E(\mathbb{C})$, $L = K(j(E))$ and $L_m = L(E[m])$. We wish to show that $\mathrm{Gal}(L_m/L)$ is abelian. For this we study our representation

$$\rho_{\ell,m} : \mathrm{Gal}(L_m/L) \to \mathrm{Aut}(E[m]),$$

and our proposition follows if we can show that this injects into the abelian part of $\mathrm{Aut}(E[m])$. For arbitrary elliptic curves, this only gives us an injection of $\mathrm{Gal}(L_m/L)$ into $GL_2(\mathbb{Z}/m\mathbb{Z})$, which is almost never abelian. However, given complex multiplication we obtain more. Because of the assumptions, endomorphisms of $E$ commute with the action of $\mathrm{Gal}(L_m/L)$. This implies that $\mathrm{Gal}(L_m/L)$ determines $\mathcal{O}_K/(m\mathcal{O}_K)$-automorphisms of $E[m]$. However, the following argument shows that $E[m]$ is a free $\mathcal{O}_K/(m\mathcal{O}_K)$-module of rank 1: Fix a lattice $\Lambda$ for $E$, obtained by the parameterization via the Weierstrass $\wp$-function. For any integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$, $E[\mathfrak{a}] := \{P \in E(\mathbb{C}), \forall \gamma \in \mathfrak{a}, [\gamma]P = O\}$ is isomorphic, as an $\mathcal{O}_K/\mathfrak{a}$-module, to $\mathfrak{a}^{-1}\Lambda/\Lambda$. Also, because of the isomorphism $A/I \otimes B/J \simeq A \otimes B/(I \otimes B + A \otimes J)$ the Chinese remainder theorem gives, if $\mathfrak{a} = \prod \mathfrak{p}^{e_i}$, that

$$E[\mathfrak{a}] \simeq \prod \mathfrak{a}^{-1}\Lambda/\mathfrak{p}^{e_i}\mathfrak{a}^{-1}\Lambda$$

as an $\mathcal{O}_K/\mathfrak{a}$-module. We have already seen that $\Lambda$ can be considered as a fractional ideal, so we show the following fact: Let $\mathfrak{b}$ be any fractional

ideal of $\mathcal{O}_K$, $\mathfrak{p}$ a prime ideal and $e$ any integer. Then $\mathfrak{b}/\mathfrak{p}^e\mathfrak{b}$ is a free $\mathcal{O}_K/\mathfrak{p}^e$-module of rank 1. However, $\mathfrak{b}$ is a flat $\mathcal{O}_K$-module of rank 1 so when localizing at $\mathfrak{p}$ it becomes free, i.e. $\mathfrak{b} \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}} \simeq \mathcal{O}_{K,\mathfrak{p}}$. However, $\mathcal{O}_{K,\mathfrak{p}}/(\mathfrak{p}^e\mathcal{O}_{K,\mathfrak{p}}) \simeq \mathcal{O}_K/(\mathfrak{p}^e\mathcal{O}_K)$, and then one sees the above fact. This shows that $E[\mathfrak{a}]$ is free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1. Hence the $\mathcal{O}_K/(m\mathcal{O}_K)$-automorphisms of $E[\mathfrak{a}]$ amount to being $(\mathcal{O}_K/(m\mathcal{O}_K))^\times$, and one sees that $\rho$ maps into something abelian. □

Notice that the above proof shows that

## 4.3 Integrality of the j-Invariant

| | |
|---|---|
| $K$ | is a local field contained in $\mathbb{C}$, with finite residue field. |
| $\mathcal{O}_K$ | is the valuation ring of $K$. |
| $\mathfrak{m}$ | is the maximal ideal of $\mathcal{O}_K$. |
| $G_K$ | is the absolute Galois groups, $\mathrm{Gal}(\overline{K}/K)$, where $\overline{K}$ is the algebraic closure of $K$. |
| $k$ | $= \mathcal{O}_K/\mathfrak{m}$, of characteristic $p > 0$. |

We say that a $G_K$-module is unramified if the action of the inertia subgroup $I$ of $G_K$ is trivial. The terminology makes sense, because triviality of the inertia group in algebraic number theory is the same thing as saying that something is unramified. This notion is intimately connected with the notion of good reduction, as the following criterion of Néron-Ogg-Shafarevich shows.

**Theorem 13 (Criterion of Néron-Ogg-Shafarevich).** *Let $E/K$ an elliptic curve. The following are equivalent:*

- *$E$ has good reduction over $K$.*
- *$E[m]$ is unramified at the prime of $\mathcal{O}_K$ ,for all or infinitely many integers $m \geq 1$ relatively prime to char $k$.*
- *The Tate module $T_\ell(E)$ is unramified for some or all primes with $\ell \neq char(k)$.*

For a proof, see [4], p. 184.

**Theorem 14 (Serre-Tate).** *Let $E/K$ be an elliptic curve with complex multiplication. Then $E$ has potential good reduction, that is, there exists a finite extension $K'$ of $K$ such that $E \times_K K'/K'$ has good reduction over $K'$.*

*Proof.* We wish to show that there is a finite extension of $K$ such that the inertia group acts trivially on the Tate module, so that we can apply the above criterion. Because the Galois representation has an abelian action on this module, the action of the inertia group $I$ factors through $I^{ab}$. Local class field theory then gives us an isomorphism

$$I^{ab} \simeq U = \mathcal{O}_K^*.$$

Of the latter we furthermore have the decomposition

$$1 \to U_1 \to U \to k^* \to 1$$

with $U_1 = \{x \in U, x = 1(\mathrm{mod}\,\mathfrak{m})\}$. The first one is a pro-$\mathfrak{p}$-group, the latter is finite. In the same manner we have, fixing a $\mathbb{Z}_\ell$-basis of $T_\ell(E)$, a decomposition of $\mathrm{Aut}(T_\ell(E)) = GL_2(\mathbb{Z}_\ell)$ by

$$1 \to GL_2(\mathbb{Z}_\ell)_1 \to GL_2(\mathbb{Z}_\ell) \to GL_2(\mathbb{Z}/\ell) \to 1.$$

Again, the first group above is a pro-$\ell$-group, and the latter is finite. Hence the Galois representation factors through $I \to I^{ab} \to U \to \mathrm{Aut}(T_\ell(E))$. A pro-$\ell$-group cannot have a nontrivial homomorphism to a pro-$p$-group if $p \neq \ell$ (consider the Piontriyagin dual of two such groups, this consists of $p$ respectively $\ell$-torsion), so choosing $\ell$ such an, we see that the $\mathrm{Im}(U_1 \to U \to \mathrm{Aut}(T_\ell(E))$ and $\mathrm{Im}(GL_2(\mathbb{Z}_\ell)_1 \to \mathrm{Aut}(T_\ell(E))$ have nonempty intersection, and so the first image gives an injection $\mathrm{Im}(U_1 \to \mathrm{Aut}(T_\ell(E)) \hookrightarrow GL_2(\mathbb{Z}_\ell/\ell)$. Hence, since $k^*$ is finite, so is also the image of $U$ in $\mathrm{Aut}(T_\ell(E))$. Hence the image of $I$ in $\mathrm{Aut}(T_\ell(E))$ is finite. We cannot quite apply the lemma of Néron-Ogg-Shafarevich yet, we need the action to be trivial. On the other hand, the kernel of the map is of finite index in $I$. The fixed field of $I$ is just $K^{nr}$, and the fixed field of the kernel is a finite extension $K''$ of $K^{nr}$. There is thus a finite extension $K'/K$ such that $K'' = K'K^{nr}$. $K'$ has inertia group equal to the kernel, and this acts, by assumption, trivially on $\mathrm{Aut}(T_\ell(E))$. Application of Néron-Ogg-Shafarevich gives that $E$ has good reduction over $K'$. □

The fact that $j(E)$ has potential good reduction indicates that $j(E) \in \mathcal{O}_K$. Indeed, there is a finite extension $K'/K$ such that $E$ has good reduction in $K'$. But that means that $\Delta' \in \mathcal{O}_{K'}^*$, and hence $j(E) \in K \cap \mathcal{O}_{K'} = \mathcal{O}_K$.

**Corollary 15.** *If $K$ is a number field, $E/K$ an elliptic curve with complex multiplication, then $E$ has potential good reduction everywhere and $j(E)$ is an algebraic integer.*

*Proof.* Obviously if $E/K$ has CM, so does the completion at any prime $\mathfrak{p}$, and so $E$ has potential good reduction everywhere. Furthermore, following the discussion above $j(E)$ is an algebraic integer locally everywhere, and hence globally. □

## 4.4 Construction of Class Fields for Imaginary Quadratic Fields

| | |
|---|---|
| $K$ | is an imaginary quadratic extension of $\mathbb{Q}$. |
| $\mathcal{O}$ | is an order of $K$. |
| $\mathcal{O}_K$ | is the maximal order of $K$. |
| $h_K$ | is the class number of $K$. |
| $E$ | is an elliptic curve with complex multiplication by $\mathcal{O}_K$. |
| $\langle , \rangle_E$ | is the Weil pairing for $E$. |

We begin by showing that $K(j(E))$ is the Hilbert class field $H$ of $K$. In what follows, we take a model of $E$ over $K(j(E))$. If $j \neq 0, 1728$, then the elliptic curve

$$E : y^2 + xy = x^3 + \frac{36}{j - 1728}x + \frac{1}{j - 1728}$$

has $j$-invariant $j(E) = j$. For the other cases, one can take either the curve $y^2 + y = x^3$ or $y^2 = x^3 + x$. They have $j$-invariants 0 and 1728, respectively.

**Proposition 16.** *Suppose that $\mathfrak{P}$ is a prime where $E$ has good reduction. If $\sigma_{\mathfrak{p}}$ is the Frobenius element, $\mathfrak{p}$ the prime of $K$ which $\mathfrak{P}$ is lying above, then*

$$j(\mathfrak{p} * E) \equiv j(E)^{N\mathfrak{p}} (\mathrm{mod}\, \mathfrak{P}).$$

Before giving a proof, we give some immediate corollaries

**Corollary 17.** *If $E$ has good reduction at a prime $\mathfrak{P}$ of $K(j(E))$ lying above a "nice" prime $\mathfrak{p}$ of $K$ (to be specified below), and $\sigma_{\mathfrak{p}}$ is the associated Frobenius element, then*

$$j(\mathfrak{p} * E) = j(E)^{\sigma_{\mathfrak{p}}}.$$

*Proof.* Denote by $\{E_i\}$ a set of representatives of elliptic curves with complex multiplication by $\mathcal{O}_K$, with models over the fields $K(j(E_i))$. For any $i$, by the Cebotarev density theorem, we can find an unramified prime $\mathfrak{p}$, excluding a finite set of primes, such that $E_i \simeq \mathfrak{p} * E$. For this we know that

$$j(E_i) \equiv j(\mathfrak{p} * E) \equiv j(E)^{\sigma_{\mathfrak{p}}} (\mathrm{mod}\, \mathfrak{P})$$

and choosing $\mathfrak{p}$ such that it doesn't divide any of the $N(j(E_i) - j(E_j))$, one concludes that $j(\mathfrak{p} * E) = j(E)^{\sigma_{\mathfrak{p}}}$. Notice that we only exclude finitely many primes during our "sieve", so that we can use the Cebotarev density theorem later. □

**Corollary 18 (Kronecker's Jugendtraum).** *Let $\{E_i\}$ be the $h_K$ elliptic curves with complex multiplication by $\mathcal{O}_K$. Then*
*(i) for any of these $E = E_i$, $H = K(j(E))$ is the Hilbert class field of $K$.*
*(ii) all the $j(E_i)$ are conjugate over* $\mathrm{Gal}(H/K)$.
*(iii) $h_K = [K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}]$*

*Proof.* We know that the conjugates of $j(E)$ may be found among the $j(E_i)$. However, we know that we can find a prime $\mathfrak{p}$ such that $\mathfrak{p} * E \simeq E_i$, and it can be chosen to be "nice", and hence $j(\mathfrak{p} * E) = j(E)^{\sigma_{\mathfrak{p}}} = j(E_i)$. One concludes that all the $j(E_i)$ are conjugate to $j(E)$ and $K(j(E))/K$ is Galois.

Suppose that for $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K(j(E))/K)$ is the Frobenius element of a "nice" prime in the above sense, and $j(E)^{\sigma_{\mathfrak{p}}} = j(\mathfrak{p} * E) = j(E)$ so that $\mathfrak{p}$ splits completely in $K(j(E))$. Then $\mathfrak{p} * E \simeq E$, and $\mathfrak{p}$ is principal. Conversely, $\sigma_{\mathfrak{p}}$ fixes $j(E)$ if $\mathfrak{p}$ is principal, in which case $\mathfrak{p}$ splits completely in $K(j(E))$.[2] Adding the fact that $K$ is totally complex, so there is no infinite ramification, and this property for a set of primes of density 1, which the set of degree 1 primes minus a finite set of primes is, we have a property which characterizes the Hilbert class field, and we conclude $H = K(j(E))$.

Further, this immediately gives that $j(E)$ has degree $h_K$ over $K$. The third point follows from the fact that $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$ combined with $[K : \mathbb{Q}] = 2$ and $h_K = [K(j(E)) : K]$.

□

[2] A short argument is the following: If $\sigma_{\mathfrak{p}}$ fixes $j(E)$, then it is the identity on $K(j(E))$ and indeed the decomposition group of any prime ideal $\mathfrak{P}$ of $K(j(E))$ lying above $\mathfrak{p}$ is trivial. But the decomposition group of $\mathfrak{P}$ has order equal to $f_{\mathfrak{P}} e_{\mathfrak{P}}$, inertial degree times ramification index, and these are thus always 1. Hence $\mathfrak{p}$ splits completely.

*Proof.* (of Proposition 16) We prove the proposition for primes of degree 1. Take a prime $\mathfrak{p}$ such that $N\mathfrak{p} = p$, and choose an ideal $\mathfrak{a}$ prime to $\mathfrak{p}$ such that $\mathfrak{a}\mathfrak{p}$ is principal, say $\mathfrak{a}\mathfrak{p} = (\alpha)$. We then have isogenies

$$E \to \mathfrak{p} * E \to \mathfrak{a}\mathfrak{p} * E \simeq E,$$

composing to multiplication by $\alpha$. This is defined over $K(j(E))$, and hence also makes sense modulo a prime $\mathfrak{P}$ lying above $\mathfrak{p}$. It it inseparable modulo $\mathfrak{P}$, since $\alpha$ is in $\mathfrak{p}$, so it acts as multiplication by 0 on the tangent space at the origin $\mathfrak{P}$, and by translations it acts by multiplication by 0 at the tangent space of every point. Every point such that $\alpha$ acts by multiplication by 0 is a ramification point, and if $\alpha$ was separable it would only have finitely many ramified points. The degree of the map $\mathfrak{p} * E \to \mathfrak{a}\mathfrak{p} * E$ is $N\mathfrak{a}$ which was chosen prime to $p$, hence it is separable modulo $\mathfrak{P}$. Hence the map $E \to \mathfrak{p} * E$ is inseparable modulo $\mathfrak{P}$. We wish to show that it is of degree $N\mathfrak{p} = p$, so it is Frobenius composed with an isomorphism. In that case

$$j(E)^p = j(\mathfrak{p} * E) (\mathrm{mod}\, \mathfrak{P}).$$

Hence we are reduced to showing that reduction modulo a prime ideal $\mathfrak{P}$ preserves degrees. This is an easy application of the Weil-pairing, noticing that it is compatible with reduction $\mathfrak{P}$. More precisely, we have

$$\widetilde{\langle x, y \rangle}_E = \langle \widetilde{x}, \widetilde{y} \rangle_{\widetilde{E}}.$$

Hence, for an endomorphism $\phi$ of $E$ and we compute, for $x, y \in T_\ell(E)$,

$$\begin{aligned} \langle \widetilde{x}, \widetilde{y} \rangle_{\widetilde{E}}^{\deg \phi} &= \widetilde{\langle x, y \rangle}_E^{\deg \phi} \\ &= \widetilde{\langle \phi x, \phi y \rangle}_E \\ &= \langle \widetilde{\phi} \widetilde{x}, \widetilde{\phi} \widetilde{y} \rangle_{\widetilde{E}} \\ &= \langle \widetilde{x}, \widetilde{y} \rangle_{\widetilde{E}}^{\deg \widetilde{\phi}}. \end{aligned}$$

From the fact that $T_\ell(E) \simeq T_\ell(\widetilde{E})$ for $\ell \neq p$, it is true for all $x, y \in T_\ell(\widetilde{E})$ too. From the non-degeneracy of the Weil pairing, we get $\deg \phi = \deg \widetilde{\phi}$. This proves the proposition. □

Now, we are lead to the construction of the ramified extensions, and we will even accomplish a description of the ray class fields. Because an imaginary quadratic field doesn't have any real primes, we don't have any problems with ramification at infinity, so we can restrict all of our attention to ramification of the finite primes. It is tempting to add the torsion points, i.e. $x$ and $y$ of $P = (x, y)$ for all torsion points $P$. However, this will unfortunately not always even yield abelian extensions. One problem which we will face is that if we add some point $x$, we wish to say that it is "invariant" under automorphisms so that if $x$ and $x'$ come from the same point $P$ and $P'$, then $x$ and $x'$ are indeed the same. This amounts to killing all the automorphisms of our elliptic curve, and if the curve is given in the form $y^2 = x^3 + Ax + B$ this can most of the time be accomplished by

$$h : (x, y) \mapsto x.$$

In the cases $j(E) = 0, 1728$, the automorphism group is larger, and one has to take another $h$.

**Definition 4.** *The Weber function $h$ of an elliptic curve of the form $y^2 = x^3 + Ax + B$ is the map $h : E \to E/\operatorname{Aut}(E) \simeq \mathbb{P}^1$ given as follows:*

- *$AB \neq 0$, then $h(x, y) = x$.*
- *$B = 0$, so that $\operatorname{Aut}(E) \simeq \mathbb{Z}/4\mathbb{Z}$, then $h(x, y) = x^2$.*
- *$A = 0$, so that $\operatorname{Aut}(E) \simeq \mathbb{Z}/6\mathbb{Z}$, then $h(x, y) = x^3$.*

In particular, any automorphism of $E$ corresponds to an element $u \in \mathcal{O}_K^\times$, and for any $T \in E$, one has $h([u]T) = h(T)$. For a proof of that the Weber function is independent of model and that it defines a morphism over the Hilbert class field of $K$, see [5], p. 155.

Now, we will need the following lemma from [5], p.133, which is really at the core of the result:

**Lemma 19.** *Let $K$ be a quadratic imaginary field, $H$ the Hilbert class field of $K$, and $E/H$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$. For all but finitely many degree 1 prime ideals $\mathfrak{p}$ of $K$ that satisfy $\sigma_\mathfrak{p}|_H = 1$, there is a unique prime $\pi = \pi_\mathfrak{p} \in \mathcal{O}_K$ such that*

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{X \mapsto X^p} & \widetilde{E} \end{array}$$

*where $\widetilde{E}$ is the reduction of $E$ modulo $\mathfrak{p}$.*

Finally, letting $\mathfrak{c}$ be an integral ideal of $\mathcal{O}_K$, and $E[\mathfrak{c}] = \{T \in E | \forall \gamma \in \mathfrak{c}, [\gamma](T) = O\}$. We refer to this as the $\mathfrak{c}$-torsion of $E$. We are now ready to give a demonstration of the main theorem of this section:

**Theorem 20.** *Let $L_\mathfrak{c} = K(j(E), h(E[c]))$, then $L_\mathfrak{c}$ is the ray class field of $K$ modulo $\mathfrak{c}$. In particular, one obtains the maximal abelian extension as*

$$K^{ab} = K(j(E), h(E_{tors})).$$

*Proof.* For clarity, we write the Frobenius element of $L/K$ with respect to a prime $\mathfrak{p}$ as $(\sigma_\mathfrak{p}, L/K)$. We need to prove that $\mathfrak{p} \in P(\mathfrak{c})$ exactly when the induced Frobenius element $(\mathfrak{p}, L_\mathfrak{c}/K) = 1$.

First, assume the latter. Then automatically $(\mathfrak{p}, H/K) = 1$, and taking one prime of degree 1, excluding only finitely many, one gets a prime $\pi$ such that $\mathfrak{p} = \pi\mathcal{O}_K$, according to the lemma, and the given diagram commutes. In particular, a short calculation shows that for a $\mathfrak{c}$-torsion point $T$, one has $\widetilde{h}([\widetilde{\pi}]\widetilde{T}) = \widetilde{h}(\widetilde{T})$. But the reduction morphism $\widetilde{h}$ maps to $\widetilde{E}/\widetilde{\operatorname{Aut} E}$, since it can be interpreted as the map $\widetilde{E} \to \widetilde{E/\operatorname{Aut} E} \simeq \widetilde{E}/\widetilde{\operatorname{Aut} E}$. Hence there is an $\xi \in \operatorname{Aut} E$ that reduces mod $\mathfrak{p}$ to give $[\widetilde{\pi - \xi}]\widetilde{T} = O$. However, excluding the finite number of primes that divide the order of $E[\mathfrak{c}]$, we have a injective map from the $\mathfrak{c}$-torsion to the $\mathfrak{c}$-torsion mod $\mathfrak{P}$, and so this equality can be lifted to say

$$[\pi - \xi]T = O.$$

We know that $E[\mathfrak{c}]$ is a free $\mathcal{O}_K/\mathfrak{c}$-module of rank one, so it is generated by a single element $T$. Choosing this $T$ above, we find a $\xi \in \mathcal{O}_K^\times$ such

that $[\pi - \xi]$ kills $E[\mathfrak{c}]$. But then $\pi \equiv \xi \bmod \mathfrak{c}$, and $\pi\xi^{-1} \equiv 1 \bmod \mathfrak{c}$. Hence, one finds that $\mathfrak{p} = \pi\mathcal{O}_K = \pi\xi^{-1}\mathcal{O}_K$, and thus $\mathfrak{p} \in P(\mathfrak{c})$.

Conversely, one finds, excluding finitely many primes, for any $\mathfrak{p} \in P(\mathfrak{c})$ there is a $\pi$ such that the usual diagram commutes and $\mathfrak{p} = \pi\mathcal{O}_K$. Then $\pi = \xi\mu$ for some $\mu \in \mathcal{O}_K^\times$, and $\xi = 1 \bmod \mathfrak{c}$. For $(\mathfrak{p}, L_\mathfrak{c}/K)$ to be the identity it will suffice to check that it fixes the torsion, because it fixes the Hilbert class field since it is principal. So, take any $T \in E[\mathfrak{c}]$. Then using the definition of the Frobenius element, one finds that $(\mathfrak{p}, L_\mathfrak{c}/K)\widetilde{T} = \widetilde{[\pi]T}$. Excluding finitely many primes as above, we have the injectivity on the reduction of the torsion, and one concludes that $(\mathfrak{p}, L_\mathfrak{c}/K)T = [\pi]T$. Now, an obvious computation gives that $(\mathfrak{p}, L_\mathfrak{c}/K)h(T) = h(T)$, so this Frobenius is the identity, and the proposition has been proved. □

## 4.5 Examples

In this chapter we have sketched a proof of the fact that if $E$ has complex multiplication, then among other things, that $K(j(E))$ is the Hilbert class field of $K$, and that $j(E)$ is algebraic of degree equal to the class number of $K$. In particular, an elliptic curve with complex multiplication is defined over $\mathbb{Q}$ if and only if $j(E)$ is an integer, and there is only one isomorphism class, due to the bijection of isomorphism classes with the right endomorphism ring and the class group.

**Lemma 21.** *Let $\alpha \in End(E)$, then the degree of $\alpha$ is just $|\alpha|^2$.*

In particular, we see that if an endomorphism is an isomorphism it is equal to multiplication by $\pm 1, \pm\sqrt{-1}$ or $(1 \pm \sqrt{-3})/2$. Let us look at the case of an elliptic curve having complex multiplication by $\mathbb{Z}[i]$.
Since multiplication by $i$ is an automorphism, we have $i\Lambda = \Lambda$. Looking at the Eisenstein-series $G_6$ we get

$$\begin{aligned} G_6(i) &= \sum_{w \in \Lambda \setminus 0} w^{-6} \\ &= \sum_{wi \in i\Lambda \setminus 0} (iw)^{-6} \\ &= -G_6(i). \end{aligned}$$

From this we conclude that $g_3 = 140G_6 = 0$. Hence any elliptic curve with complex multiplication by $\mathbb{Z}[i]$ has to be (after a linear transformation)

$$y^2 = x^3 + x.$$

More precisely, multiplication by $i$ is given by the morphism $[i](x, y) = (-x, iy)$. Incidently, this shows that every isomorphism class of elliptic curves with complex multiplication by $\mathbb{Z}[i]$ is isomorphic to the above one, and hence the class number of $\mathbb{Z}[i]$ has to be 1. Alternatively, we see that its $j$-invariant is an integer. The same kind of argument but using $G_4$ shows that elliptic curves with complex multiplication by $Z[\rho]$, with $\rho = \exp(2\pi i/3)$ are isomorphic to

$$y^2 = x^3 + 1$$

and $[\rho](x, y) = (\rho x, y)$. Hence this field also has class number 1.

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

| $D$ | $j(\mathcal{O}_K)$ |
|---|---|
| 1 | $2^6 3^3$ |
| 2 | $2^6 5^3$ |
| 3 | 0 |
| 7 | $-3^3 5^3$ |
| 11 | $-2^{15}$ |
| 19 | $-2^{15} 3^3$ |
| 43 | $-2^{18} 3^3 5^3$ |
| 67 | $-2^{15} 3^3 5^3 11^3$ |
| 163 | $-2^{18} 3^3 5^3 23^3 29^3$ |

We also have the following list of actual elliptic curves over $\mathbb{Q}$ with the above endomorphism rings, in minimal Weierstrass equation.

| | |
|---|---|
| $\mathbb{Z}[\sqrt{-1}]$ | $y^2 = x^3 + x$ |
| $\mathbb{Z}[\sqrt{-2}]$ | $y^2 = x^3 + 4x + 2$ |
| $\mathbb{Z}[(1+\sqrt{-3})/2]$ | $y^2 + y = x^3$ |
| $\mathbb{Z}[(1+\sqrt{-7})/2]$ | $y^2 + xy = x^3 - x^2 - 2x - 1$ |
| $\mathbb{Z}[(1+\sqrt{-11})/2]$ | $y^2 + y = x^3 - x^2 - 7x + 10$ |
| $\mathbb{Z}[(1+\sqrt{-19})/2]$ | $y^2 + y = x^3 - 38x + 90$ |
| $\mathbb{Z}[(1+\sqrt{-43})/2]$ | $y^2 + y = x^3 - 860x + 9707$ |
| $\mathbb{Z}[(1+\sqrt{-67})/2]$ | $y^2 + y = x^3 - 7370x + 243528$ |
| $\mathbb{Z}[(1+\sqrt{-163})/2]$ | $y^2 + y = x^3 - 2174420x + 1234136692$ |

Now, set $\rho = \exp(2\pi i/3) = (1+\sqrt{-3})/2$, and consider $Z[\rho]$. We know from above that the elliptic curve $E : y^2 = x^3 + 1$ has CM with $\mathbb{Z}[\rho]$, and we wish to calculate some of its torsion points. So, let $P = (x, y)$ be any point on $E$ with $[\alpha]P = O$, $\alpha \in \mathrm{End}(E)$.

$\alpha = 2$ It is easy to check that $E[2] = \{O, (1,0), (\rho, 0), (\rho^2, 0)\}$.

$\alpha = 3$ The duplication formula ([4], p. 59) gives, since $2P = -P$, that

$$x^4 - 8x = x(4x^3 + 4) \Leftrightarrow x^4 + 4x = 0.$$

$$\text{Hence } E[3] = \{O, (0, \pm 1), (\sqrt[3]{4}, \pm\sqrt{5}), (\rho\sqrt[3]{4}, \pm\sqrt{5}), (\rho^2\sqrt[3]{4}, \pm\sqrt{5})\}.$$

The above tables are from a course on elliptic curves by Per Salberger at Göteborg university, spring 2001. They can also be found at the back of [5].

# References


[1] Cassels and Fröhlich, et al *Algebraic Number Theory* Academic Press (1967)

[2] Joseph Oesterlé, *Corps de Classes, Theorie Locale et Globale* lecturenotes from a course at Université Pierre et Marie Curie 1985-1986.

[3] J-P. Serre, *Corps Locaux* Hermann, 1963

[4] J.H. Silverman *The Arithmetic of Elliptic Curves* Springer GTM (1986)

[5] J.H. Silverman *Advanced Topics in the Arithmetic of Elliptic Curves*

[6] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Springer Verlag (1982) Springer GTM (1994)