Complex Multiplication of Elliptic Curves and Class Field Theory

Author. Jas Singh

Abstract

We present in this report an account of the theory of complex multiplication of elliptic curves and its relation to the class field theory of imaginary quadratic number fields. By analyzing the relationship between the arithmetic of these fields and their associated elliptic curves, we attain a complete description of their maximal abelian extensions.

Sections $0-2$ of the report will consist of the necessary prerequisite knowledge, namely Galois theory, class field theory, and the complex theory of elliptic curves. The remainder will consist of an explanation of the basic theory of complex multiplication of elliptic curves and how it relates to the class field theory of the associated imaginary quadratics. Our primary reference for complex multiplication and its impact in class field theory is [Silverman, Ch. II]. Most of the proofs will be omitted, and they can be found there.

Acknowledgment. I'd like to thank my friend Ken Willyard for his very helpful feedback.

0 Galois theory

We present here an introduction to the necessary Galois theory for the remainder of the report. Many texts exist covering this subject. We point the reader, for instance, to [Lang] – a general reference book for the fundamentals of algebra. A wonderful little book dedicated to Galois theory itself is [Artin]. We will also need some infinite Galois theory, which is typically covered in algebraic number theory texts. For instance, one can see [Neukirch], [Lang – ANT], or [CF].

Definition 0.1. A number field is a field K which contains the rational numbers $\mathbb{Q}$ in such a way that K is finite dimensional over $\mathbb{Q}$. We denote by $[K:\mathbb{Q}]$ the dimension of K as a $\mathbb{Q}$ vector space. This is often called the degree of the extension.

Definition 0.2. An imaginary quadratic number field is a number field of degree 2 over $\mathbb{Q}$ which has no maps into the field of real numbers $\mathbb{R}$. Equivalently, it is a field of the form $\mathbb{Q}(\sqrt{-d})$ for d a positive squarefree integer.

Elements of number fields are referred to as algebraic numbers. It is a fundamental question in algebraic number theory to understand and classify the algebraic numbers. A key tool along these lines is Galois theory, which allows us to study field extensions in terms of their group of automorphisms.

Definition 0.3. Let K/F be a finite field extension, meaning that F is a subfield of K and $[K:F]$ is finite. The automorphism group of K/F is

$$\mathrm{Aut}(K/F) = \{\sigma : K \longrightarrow K \mid \sigma \text{ is a field isomorphism with } \sigma|_F = \mathrm{id}_F\}$$

For a subgroup H of $\mathrm{Aut}(K/F)$, we let the fixed field of H be

$$K^H = \{a \in K \mid h(a) = a \text{ for all } h \in H\}$$

If $K^{\mathrm{Aut}(K/F)} = F$, we say that the extension K/F is Galois. It is then customary to refer to $\mathrm{Aut}(K/F)$ as the Galois group $G(K/F)$.

A laboriously proven but incredible fact is the Galois correspondence between the subgroup lattice of the Galois group of K/F and the lattice of intermediate field extensions in K/F.

Theorem 0.1 (The Galois correspondence)**.** *Let K/F be a finite Galois extension. Then for any intermediate field $K/E/F$ we have that K/E is a (finite) Galois extension. Notice also that $G(K/E)$ is then a subgroup of $G(K/F)$.*

There is an order reversing bijection

$$\begin{aligned} \{\textit{intermediate fields in } K/F\} &\longleftrightarrow \{\textit{subgroups of } G(K/F)\} \\ E &\longmapsto G(K/E) \\ K^H &\longleftarrow\!\shortmid H \end{aligned}$$

Furthermore, an intermediate field extension $K/E/F$ has that E/F is Galois if and only if $G(K/E)$ is a normal subgroup of $G(K/F)$. If so, there is a surjective restriction map

$$\begin{aligned} G(K/F) &\longrightarrow G(E/F) \\ \sigma &\longmapsto \sigma|_E \end{aligned}$$

with kernel equal to $G(K/E)$.

Finally, we record some relationships between the index of subgroups and the degree of extensions.

$$\begin{aligned} |H| &= [K : K^H] \\ [G(K/F) : H] &= [K^H : F] \end{aligned}$$

The Galois correspondence allows us to translate the problem of understanding number fields to understanding certain groups and how they act. We would now like to extend this idea to infinite extensions, specifically the algebraic closure $\overline{\mathbb{Q}}/\mathbb{Q}$. However, naïvely replacing all the extensions above with infinite ones does not quite work. For instance, it can be the case in an infinite Galois extension that there is a greater cardinality of subgroups than of intermediate fields.

Infinite Galois theory becomes topological in nature. For instance, consider the fixed point condition $K^H = \{a \in K \mid h(a) = a \text{ for all } h \in H\}$. This is a closed condition in H (although we have not yet given ourselves a topology), which is vacuous if the groups are finite, but potentially meaningful if they are infinite.

Definition 0.4. Let K/F be a possibly infinite extension of fields. We say that K/F is Galois if it is algebraic and if $K^{\mathrm{Aut}(K/F)} = F$. We again will write $G(K/F) = \mathrm{Aut}(K/F)$.

In this case, we can determine that K is the union of all of the finite intermediate extensions $K/E/F$ with E/F Galois. As such, we have natural restriction maps $G(K/F) \longrightarrow G(E/F)$ for all such E. We then assemble all these restriction maps together into a product.

Theorem 0.2. *The map*

$$G(K/F) \longrightarrow \prod_{\substack{K/E/F \\ E/F \textit{ finite Galois}}} G(E/F)$$

is an injection of groups. Furthermore, we give each finite group $G(E/F)$ the discrete topology and then endow the codomain with the product topology. Then the image of this map is closed. Via this, we define a topology on $G(K/F)$.

Remark. Those familiar with category theory will recognize that $G(K/F)$ is an inverse limit over

the finite intermediate Galois extensions E of $G(E/F)$. As such, we are taking this inverse limit in the category of topological groups.

Notice by the way that for K/F finite Galois, the Galois group is discrete. This topology has a number of other properties we cannot explore in depth right now.

Theorem 0.3 (The infinite Galois correspondence)**.** *Let K/F be a Galois extension. There is an order reversing bijection*

$$\begin{aligned} \{\textit{intermediate fields in } K/F\} &\longleftrightarrow \{\textit{closed subgroups of } G(K/F)\} \\ E &\longmapsto G(K/E) \\ K^H &\longleftarrow\!\shortmid H \end{aligned}$$

Furthermore, if H is closed and finite index then $[K^H : F] = [G(K/F) : H]$

The fundamental application of this result in algebraic number theory is for the extension $\overline{K}/K$ of a number field K, which is always Galois. Then the finite extensions of K are in correspondence with the finite index closed subgroups of $G(\overline{K}/K)$ In particular, number fields correspond to closed finite index subgroups of $G(\overline{\mathbb{Q}}/\mathbb{Q})$, which is called the absolute Galois group of $\mathbb{Q}$. This reduces the question of understanding number fields to understanding the structure of this topological group. This is easier said than done, so in the course of this report we will focus instead on abelian extensions.

Definition 0.5. A Galois extension K/F is called abelian if $G(K/F)$ is an abelian group. The union of all intermediate abelian extensions in $\overline{K}/K$ is denoted K^{ab}.

By the Galois correspondence, we have that $G(K^{ab}/K)$ is the abelianization of the absolute Galois group $G(\overline{K}/K)$.

Remark. A careful reader might wonder if the commutator subgroup is closed. In general, this need not be the case. The abelianization is happening in the category of profinite groups, not just groups. Concretely, when abelianizing, we are quotienting by the closure of the commutator subgroup.

The abelian extensions of a number field K therefore correspond to closed subgroups of $G(K^{ab}/K)$. Unlike studying all extensions, studying abelian extensions of a number field is tractable and known classically via class field theory.

1 Class field theory

To state the main theorems of class field theory we will use in this report, we must first introduce some essential notions from algebraic number theory. These can be found more in depth in most algebraic number theory references, such as [Lang – ANT], [Neukirch], [CF]. These texts will each cover class field theory as well. Our primary reference [Silverman] provides a description of the results and definitions needed for class field theory of imaginary quadratic number fields in chapter II §3. Each of these references for class field theory cover the more modern and technical idèlic approach, whereas we only use the ideal theoretic approach. A fleshed out introduction to the ideal theoretic approach to class field theory can be found in [Janusz].

Definition 1.1. Let K be a number field. The ring of integers in K is

$$\mathcal{O}_K = \{a \in K \mid a \text{ is the root of an integer polynomial with leading coefficient } 1\}$$

We'll collect here a few fundamental properties of the ring of integers.

Proposition 1.1. *(i) $\mathcal{O}_K$ is a ring which contains $\mathbb{Z}$ as a subring.*

(ii) $\mathcal{O}_K$ is, as an underlying additive group, free of rank $[K:\mathbb{Q}]$.

(iii) Every nonzero ideal of $\mathcal{O}_K$ factors uniquely into a product of nonzero prime ideals of $\mathcal{O}_K$.

(iv) $\mathcal{O}_K$ is an integral domain with quotient field K.

(v) The nonzero primes $\mathfrak{p}$ of $\mathcal{O}_K$ are maximal, and the quotients $\mathcal{O}_K/\mathfrak{p}$ are finite.

The third part of this proposition is an approximation to the unique factorization property of the integers – that is, the fundamental theorem of arithmetic. The ring of integers of a number field needn't satisfy unique factorization on the level of elements, but it will satisfy it on the level of ideals. As a result, we adopt arithmetic sounding language when discussing ideals. For instance, we will say a prime $\mathfrak{p}$ divides an ideal I if it appears in the factorization of I.

We can measure the failure of element – wise unique factorization by a group called the class group of K.

Definition 1.2. A fractional ideal of K is a finitely generated $\mathcal{O}_K$ submodule of K. In particular, the ideals of $\mathcal{O}_K$ are fractional ideals. We call these integral ideals, as they are contained in the ring of integers. A fractional ideal is called principal if it is generated as an $\mathcal{O}_K$ module by some $a \in K$. This is denoted (a).

The unique factorization property of nonzero ideals ensures that the set of nonzero fractional ideals of K is an abelian group under ideal multiplication, and is in fact a free abelian group generated by the nonzero primes of $\mathcal{O}_K$. The nonzero principal ideals are a subgroup of this.

Definition 1.3. The class group $Cl(\mathcal{O}_K)$ is the quotient of the group of nonzero fractional ideals by the subgroup of nonzero principal ideals.

The class group measures how far away the ring $\mathcal{O}_K$ is from having unique factorization on its elements. That is, $Cl(\mathcal{O}_K)$ is trivial if and only if $\mathcal{O}_K$ is a unique factorization domain. Amazingly, we have the following:

Proposition 1.2. *The class group $Cl(\mathcal{O}_K)$ is finite. Its order is called the class number and is denoted h_K.*

We now use the unique factorization of ideals to discuss ramification of primes.

Definition 1.4. Let L/K be an extension of number fields. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L$ is a nonzero ideal of $\mathcal{O}_L$ and therefore admits a factorization $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$. The number e_i is referred to as the ramification index of $\mathfrak{P}_i/\mathfrak{p}$. We say that $\mathfrak{p}$ is unramified in L if all the e_i are 1. Furthermore, L/K is said to be unramified if every nonzero prime of $\mathcal{O}_K$ is unramified in L.

Proposition 1.3. *Only finitely many primes in K are ramified in L.*

From now on, we will insist that K be an imaginary quadratic. Class field theory extends far beyond this narrow scope, but for the sake of brevity we will focus our attention here. Experts, for instance, will notice that this affords us the ability to completely neglect a conversation about infinite places.

Proposition 1.4. *Let L/K be a finite abelian extension with K an imaginary quadratic. Let $\mathfrak{p}$ be an unramified prime of K and let $\mathfrak{P}$ be some prime appearing in the factorization of $\mathfrak{p}\mathcal{O}_L$. Then $\mathcal{O}_L/\mathfrak{P}$ is a finite Galois extension of the finite field $\mathcal{O}_K/\mathfrak{p}$. There is an isomorphism*

$$\{\sigma \in G(L/K) \mid \sigma[\mathfrak{P}] = \mathfrak{P}\} \longrightarrow G(\mathcal{O}_L/\mathfrak{P}/\mathcal{O}_K/\mathfrak{p})$$

given by reduction mod $\mathfrak{P}$.

The Galois group of the extension of finite fields is generated by the Frobenius element $x \mapsto x^{|\mathcal{O}_K/\mathfrak{p}|}$. As L/K is abelian and unramified at $\mathfrak{p}$, there is a unique lift $\phi(\mathfrak{p}) \in G(L/K)$ which reduces to the Frobenius element on the quotient by $\mathfrak{P}$. We also refer to $\phi(\mathfrak{p})$ as the Frobenius element.

Recalling that the nonzero primes form free generators for the group of nonzero fractional ideals, we are led to believe that we can extend ϕ from the proposition to a group homomorphism. This is almost correct, but we have to omit the primes that ramify.

Definition 1.5. For a nonzero integral ideal I of $\mathcal{O}_K$ we let $\Psi(I)$ be the subgroup of the group of nonzero fractional ideals consisting of those which are coprime to I. That is, those which contain no primes appearing in the factorization of I. This is a free abelian group on the primes not dividing I.

Then we have a group homomorphism $\Psi(I) \longrightarrow G(L/K)$ sending $\mathfrak{p} \mapsto \phi(\mathfrak{p})$ for any ideal I divisible by all the primes ramified in L. We refer to this as the Artin map and denote it as $(\cdot, L/K)$.

Definition 1.6. For a nonzero integral ideal I of $\mathcal{O}_K$. Let $P(I) = \{(a) \mid a \in K^* \text{ and } a \equiv 1 \pmod{I}\}$. This is a subgroup of $\Psi(I)$.

Theorem 1.1 (Artin reciprocity)**.** *Let L/K be finite abelian. There is an nonzero integral ideal I of $\mathcal{O}_K$ so that $P(I)$ is contained in the kernel of the Artin map. Furthermore, I is divisible precisely by the primes ramifying in L. There is in fact a maximal such integral ideal I, which we write as $I_{L/K}$ and call the conductor of L/K.*

Definition 1.7. Let I be a nonzero integral ideal of $\mathcal{O}_K$ for K an imaginary quadratic. A ray class field for K modulo I is a finite abelian extension K_I/K so that for any abelian extension L/K with $I \subseteq I_{L/K}$ we have $L \subseteq K_I$.

Theorem 1.2 (Some statements of class field theory)**.** *Let K be an imaginary quadratic number field and L/K be finite abelian.*

(i) The Artin map $(\cdot, L/K) : \Psi(I_{L/K}) \longrightarrow G(L/K)$ is onto with kernel containing $P(I_{L/K})$.

(ii) A ray class field of modulus I exists for all nonzero integral ideals I of $\mathcal{O}_K$. Furthermore, the ray class field is unique.

If we take the particular case of $I = (1)$ the unit ideal, the corresponding ray class field is called the Hilbert class field. We denote this by H/K. We'll also record some properties of the Hilbert class field.

Corollary 1.2.1. *The Hilbert class field H/K is the maximal extension of K which is abelian and unramified. We have an isomorphism $(\cdot, H/K) : Cl(\mathcal{O}_K) \longrightarrow G(H/K)$.*

2 Complex elliptic curves

Our main reference for the theory of elliptic curves in general is [AEC]. In this text, elliptic curves are covered over general base fields. We are interested primarily in elliptic curves over $\mathbb{C}$, though we will later need the theory of elliptic curves over $\overline{\mathbb{Q}}$. For the complex analytic theory, especially with respect to lattices, a nice reference is [Serre, Ch. VII].

Elliptic curves form a basic object in algebraic geometry and algebraic number theory. For those familiar with algebraic geometry, the following is a good intrinsic definition.

Definition 2.1. A (complex) elliptic curve is a nonsingular curve of genus 1 over $\mathbb{C}$ with a designated base point O.

More explicitly, elliptic curves are known to have Weierstrass equations, which affords us the following more concrete (if less intrinsic) definition.

Definition 2.2. An elliptic curve is a curve in $\mathbb{CP}^2$ given by an equation of the form $y^2z = x^3 + axz^2 + bz^3$ for some $a, b \in \mathbb{C}$ so that $\Delta = -16(4a^3 + 27b^2) \neq 0$.

The value Δ is called the discriminant of the curve, and its nonvanishing ensures smoothness. Notice that in the affine open neighborhood $\{z \neq 0\}$ this equation becomes $y^2 = x^3 + ax + b$. Furthermore, this curve intersects the line at infinity, i.e. the curve $\{z = 0\}$ in $\mathbb{CP}^2$, at exactly one point, which we take as our base point $O = [0 : 1 : 0]$.

With whatever definition we take, an elliptic curve has a group structure on it by setting the designated based point O as the identity element and insisting that the sum of three colinear points (counting multiplicity) is O.

Definition 2.3. A map between elliptic curves is a holomorphic group homomorphism, which we call an isogeny.

The above definitions work equally well for any algebraically closed field of characteristic not equal to 2 or 3. But when the ground field is $\mathbb{C}$, we are afforded the use of complex analysis. This will lead us to a powerful classification of complex elliptic curves.

Definition 2.4. A lattice Λ in $\mathbb{C}$ is a free abelian group generated by some basis for $\mathbb{C}$ as an $\mathbb{R}$ vector space.

Definition 2.5. Given a lattice Λ we define the following

(i) The Weierstrass $\wp$ function with respect to Λ is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$$

This is a meromorphic function which descends to the quotient $\mathbb{C}/\Lambda$.

(ii) We let

$$G_k(\Lambda) = \sum_{\lambda \in \Lambda - \{0\}} \lambda^{-k}$$

for k a natural number. This is called the Eisenstein series of weight k. Note that the series is 0 if we were to take k odd by symmetry about $\lambda \mapsto -\lambda$.

(iii) $g_2 = 60G_4$

(iv) $g_3 = 140G_6$

Proposition 2.1. *Let Λ be a lattice. There is a map $\mathbb{C}/\Lambda \longrightarrow \mathbb{CP}^2$ given in the affine open coordinate patch $\{z \neq 0\}$ as $t \mapsto (\wp(t), \wp'(t))$. This extends to $\mathbb{CP}^2$ by sending the poles to $[0:1:0]$. In turn, this map becomes an isomorphism onto the curve defined by $y^2z = 4x^3 - g_2xz^2 - g_3z^3$. This is an isomorphism of groups and of Riemann surfaces. We denote this elliptic curve by E_Λ. Furthermore, all elliptic curves arise in this fashion.*

This proposition is the beginning of a classification of complex elliptic curves. We would like to consider the issue of uniqueness as well. For one, we are only interested in elliptic curves up to isomorphism. As elliptic curves all arise from lattices, we are led to consider a condition on lattices which classifies isomorphism. Indeed, we have the following.

Proposition 2.2. *E_Λ and $E_{\Lambda'}$ are isomorphic if and only if $\Lambda = c\Lambda'$ for some nonzero constant $c \in \mathbb{C}^*$.*

Definition 2.6. We refer to lattices Λ and Λ' so that $\Lambda = c\Lambda'$ as homothetic.

We therefore have the equivalence

$$\{\text{lattices}\}/\text{homothety} \cong \{\text{elliptic curves}\}/\text{isomorphism}$$

We can go further by classifying the collection of lattices themselves. Notice that a lattice is specified by a $GL_2(\mathbb{Z})$ orbit of an $\mathbb{R}$ basis of $\mathbb{C}$. If we insist that our bases are positively oriented, we can focus on $SL_2(\mathbb{Z})$ orbits of positively oriented $\mathbb{R}$ bases of $\mathbb{C}$. Furthermore, any positively oriented $\mathbb{R}$ basis of $\mathbb{C}$ can be dilated to be of the form $(1, \omega)$ for some ω in the upper half plane $\mathbb{H}$. Carrying forward this reasoning eventually leads us to the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \omega = \frac{az+b}{cz+d}$$

and the equivalence

$$\begin{aligned} SL_2(\mathbb{Z})\backslash\mathbb{H} &\xrightarrow{\sim} \{\text{lattices}\}/\text{homothety} \\ \omega &\longmapsto \mathbb{Z} + \omega\mathbb{Z} \end{aligned}$$

This has the impressive feature of endowing the set of elliptic curves up to isomorphism with a holomorphic structure via the bijection to $SL_2(\mathbb{Z})\backslash\mathbb{H}$. To analyze what precisely this structure is, we use the j invariant.

Definition 2.7. Let Λ be a lattice. The discriminant is given as

$$\Delta = g_2^3 - 27g_3^2$$

and the j invariant is

$$j = \frac{1728g_2^3}{\Delta}$$

It is the case that $\Delta(\Lambda)$ is never zero. Furthermore, j deserves the name "invariant" due to the following.

Proposition 2.3. *j : {lattices}/homothety $\longrightarrow \mathbb{C}$ is a bijection. Furthermore, when composed with the bijection to $SL_2(\mathbb{Z})\backslash\mathbb{H}$, we get a biholomorphism $SL_2(\mathbb{Z})\backslash\mathbb{H} \longrightarrow \mathbb{C}$.*

We have therefore determined that the collection of elliptic curves up to isomorphism goes under a variety of names, and in fact has the structure of a Riemann surface. One of these names is very familiar – $\mathbb{C}$ itself. To summarize, we have the following result.

Theorem 2.1 (Classification of complex elliptic curves)**.** *We have equivalances*

$$\{\text{elliptic curves}\}/\text{isomorphism} \cong \{\text{lattices}\}/\text{homothety} \cong SL_2(\mathbb{Z})\backslash\mathbb{H} \cong \mathbb{C}$$

with the various maps as described above.

Note that we provided the fewest number of maps necessary to understand these equivalences. There are other maps between these sets which are notable. For instance, we can go from an elliptic curve to a lattice using a homology group (see [AEC, VI.§5.6]). These connections are not necessary, so we won't discuss them any further.

We will use j informally as defined on any of the first three spaces via the given bijections between them. For instance, we will refer to j of a lattice, an element of $\mathbb{H}$, and of an elliptic curve. By the way, the j invariant exists over any algebraically closed field of characteristic not 2 or 3 and still uniquely parameterizes elliptic curves up to isomorphism over said base field. So as powerful as this classification by j is, it is not the unique feature of complex elliptic curves. It's really the two sets in between, i.e. lattices and $SL_2(\mathbb{Z})\backslash\mathbb{H}$, that are unique to the complex analytic theory.

3 Introduction to complex multiplication

Here we begin the exploration of complex multiplication. We appeal mostly to our primary reference [Silverman], where one can find the omitted proofs. One can also refer to [Cox].

3.1 Definition

To begin our investigation of complex multiplication, we have to understand the endomorphism ring of an elliptic curve.

Proposition 3.1. *Let Λ be a lattice. The endomorphism ring of E_Λ, i.e. the ring of isogenies E_Λ to itself, is described via the following isomorphism:*

$$\begin{aligned} \{a \in \mathbb{C} \mid a\Lambda \subseteq \Lambda\} &\xrightarrow{\sim} \mathrm{End}(E_\Lambda) \\ a &\longrightarrow ([x] \mapsto [ax]) \end{aligned}$$

We see here that the complex analytic description of elliptic curves as complex torii $\mathbb{C}/\Lambda$ has afforded us a unique understanding of their structure. Indeed, the proof of this result bases itself fundamentally on the covering map $\mathbb{C} \longrightarrow \mathbb{C}/\Lambda$. It will continue to be fruitful to understand elliptic curves in terms of a defining lattice. For instance, the above proposition shows in particular that $\mathrm{End}(E)$ is isomorphic to a subring of $\mathbb{C}$, and is hence an integral domain. We take this further with the following key result.

Proposition 3.2. *If $E = E_\Lambda$ for $\Lambda = \mathbb{Z} + \omega\mathbb{Z}$ then $K = \mathbb{Q}(\omega)$ is an imaginary quadratic number field and $\mathrm{End}(E)$ is isomorphic to a subring of the ring of integers $\mathcal{O}_K$.*

Definition 3.1. Let E be an elliptic curve so that $\mathrm{End}(E)$ is isomorphic to a subring $R \subseteq \mathcal{O}_K$ for an imaginary quadratic number field K. Suppose that $\mathrm{End}(E)$ properly contains $\mathbb{Z}$. We say then that E has complex multiplication by R.

Typically, the only endomorphisms of an elliptic curve will be given by multiplication by some integer. In the case of complex multiplication, there are additional complex numbers we can multiply our elliptic curve by. In turn, there are additional symmetries of the curve, or equivalently, additional symmetries of the lattice. A more technical way to phrase this is that elliptic curves with complex multiplication by R become R modules rather than mere abelian groups.

Examples. (i) Consider the lattice $\Lambda = \mathbb{Z} + i\mathbb{Z}$. Notice that $i\Lambda = \Lambda$. It follows then that $i \in \mathrm{End}(E_\Lambda)$. We know the ring of integers of $\mathbb{Q}(i)$ to be $\mathbb{Z}[i]$, so $\mathrm{End}(E_\Lambda) = \mathbb{Z}[i]$. Thus, E_Λ has complex multiplication by $\mathbb{Z}[i]$. This ring is called the Gaussian integers.

(ii) Consider the lattice $\Lambda = \mathbb{Z} + \zeta\mathbb{Z}$ for $\zeta = e^{\pi i/3}$. One may compute $\zeta\Lambda = \Lambda$. As in the case of the Gaussian integers, we may conclude $\mathrm{End}(E_\Lambda) = \mathbb{Z}[\zeta]$. This is called the ring of Eisenstein integers.

A common feature in both of these examples is that the lattices themselves were rings. Indeed, $\mathbb{Z} + i\mathbb{Z} = \mathbb{Z}[i]$ and $\mathbb{Z} + \zeta\mathbb{Z} = \mathbb{Z}[\zeta]$. This will inform our attempt to understand these special highly symmetric elliptic curves.

Recall the classification of elliptic curves

$$\{\text{elliptic curves}\}/\text{isomorphism} \cong \{\text{lattices}\}/\text{homothety} \cong SL_2(\mathbb{Z})\backslash\mathbb{H} \cong \mathbb{C}$$

A natural way to further understand these correspondences is to determine how certain special classes of objects behave under them. For instance, there are special lattices which arise from rings, as in the above examples. Furthermore, within $\mathbb{C}$ there are the algebraic numbers, and even the algebraic integers. And of course, within the class of elliptic curves, there are those which admit complex multiplication. We will come to explore the relationship between these various special classes of objects under these correspondences.

3.2 First principles

We first fix some notation. The set of all elliptic curves up to isomorphism with complex multiplication by R is denoted $\mathrm{Ell}(R)$.

Now we will perform a large generalization of the previous two examples. Take an imaginary quadratic number field K and a nonzero fractional ideal I in the ring of integers $\mathcal{O}_K$. Then I is a lattice in $\mathbb{C}$ and hence defines an elliptic curve $E_I = \mathbb{C}/I$. E_I has complex multiplication by $\mathcal{O}_K$. Indeed,

$$\begin{aligned}\mathrm{End}(E_I) &= \{a \in \mathbb{C} \mid aI \subseteq I\} \\ &= \{a \in K \mid aI \subseteq I\} \\ &= \mathcal{O}_K\end{aligned}$$

In this way, we have found a myriad of examples of elliptic curves with complex multiplication by $\mathcal{O}_K$. We can go further. Fractional ideals have additional structure on them – they form a group

under ideal multiplication. Our next step is to understand how this group structure on the ideal side affects the elliptic curve side.

Lemma 3.1. *Let E_Λ be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Also let I be a nonzero fractional ideal of $\mathcal{O}_K$. Then $I\Lambda$ is a lattice and $E_{I\Lambda}$ has complex multiplication by $\mathcal{O}_K$. We thus define a group action from the group of fractional ideals of $\mathcal{O}_K$ on $\mathrm{Ell}(\mathcal{O}_K)$ via $IE_\Lambda = E_{I^{-1}\Lambda}$. This is a transitive action.*

Remark. That we twist this action by I^{-1} is solely to make the connection with class field theory cleaner. It has no deep importance beyond this nicety.

In fact, as we are interested in elliptic curves up to isomorphism, we are free to replace lattices by homothetic replacements. For instance, we can scale our lattices by elements of K^* without affecting this group action. Thus, the action descends to the quotient and yields an action of $Cl(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$.

Theorem 3.2. *There is an action of the ideal class group $Cl(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$ via $[I]E_\Lambda = E_{I^{-1}\Lambda}$. This action is free and transitive.*

In effect, we have determined all the elliptic curves with complex multiplication by $\mathcal{O}_K$, modulo our understanding of the class group of K. This is by no means a trivial obstruction. But a coarser invariant than the class group is the class number $h_K = |Cl(\mathcal{O}_K)|$. This yields a coarser result about elliptic curves – a count.

Corollary 3.2.1. *There are exactly h_K isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}_K$.*

We have found already quite a remarkable result. Casting aside even the specificity of what the class number is, this means that $\mathrm{Ell}(\mathcal{O}_K)$ is a finite set. This was not at all obvious a priori.

We turn now to another player in the classification of elliptic curves: $\mathbb{C}$ and the j invariant. What does the j invariant of an elliptic curve with complex multiplication look like? The finiteness just proven will show that it is actually an algebraic number.

Definition 3.2. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ and E an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$. Then we denote by E^σ the elliptic curve given by $y^2 = x^3 + \sigma(a)x + \sigma(b)$.

We see readily that $\mathrm{End}(E) \cong \mathrm{End}(E^\sigma)$, so this leads to an action of $\mathrm{Aut}(\mathbb{C})$ on the finite set $|\mathrm{Ell}(\mathcal{O}_K)|$.

Corollary 3.2.2. *$j(E)$ is an algebraic number for $E \in \mathrm{Ell}(\mathcal{O}_K)$. In fact, $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$.*

Proof. The j invariant of an elliptic curve is a rational function of the coefficients of a Weierstrass equation for said curve. As such, $j(E^\sigma) = \sigma(j(E))$. There are only h_K many elements in $\mathrm{Ell}(\mathcal{O}_K)$, so $\sigma(j(E))$ ranges over h_K many values as σ ranges in $\mathrm{Aut}(\mathbb{C})$. This shows that $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$. □

Corollary 3.2.3. *If K has class number 1, i.e. if $\mathcal{O}_K$ has unique factorization, then $j(E)$ is a rational number for any elliptic curve E with complex multiplication by K.*

For instance, $j(i)$ and $j(e^{\pi i/3})$ are rational numbers. One can actually compute these values explicitly as 1728 and 0 respectively. Notably, these are integers. And in fact, a stronger fact than what we just described is true. The j invariant of an elliptic curve with complex multiplication by $\mathcal{O}_K$ is an algebraic integer. One can see [Silverman, II.§6] for multiple proofs of integrality.

4 Applications of complex multiplication to class field theory

We have now shown an intimate connection between the ideal class group of an imaginary quadratic number field K and the set of elliptic curves with complex multiplication by $\mathcal{O}_K$, as well as their j invariants. By class field theory, we therefore expect these elliptic curves to tell us something about the Hilbert class field of K. Indeed, it will turn out to be the case that $K(j(E))$ is exactly the Hilbert class field of K. We will furthermore be able to understand the entire extension K^{ab}/K using the torsion of some $E \in \text{Ell}(\mathcal{O}_K)$.

4.1 The Hilbert class field of an imaginary quadratic

To make such a connection, we will first need to explain the Galois action on $\text{Ell}(\mathcal{O}_K)$. When discussing algebraicity of the j invariant of an elliptic curve with complex multiplication by $\mathcal{O}_K$, we used the action of $\text{Aut}(\mathbb{C})$. This is a group even more unwieldy than the absolute Galois group $G(\overline{\mathbb{Q}}/\mathbb{Q})$. We'd like to have this group act on $\text{Ell}(\mathcal{O}_K)$ instead. This is a reasonable request, as the j invariants therein were proven to be algebraic. So there is a Galois action (meaning an action of the absolute Galois group) on the j invariants of the elements of $\text{Ell}(\mathcal{O}_K)$. We can use this to pull back a Galois action on $\text{Ell}(\mathcal{O}_K)$, but this is a hacky approach. Our goal now is to describe a more intrinsic Galois action on these elliptic curves.

The problem is that our elliptic curves are insofar defined over $\mathbb{C}$, so there is no current way to define an action of the absolute Galois group. However, if $E \in \text{Ell}(\mathcal{O}_K)$ then $j(E)$ is algebraic over $\mathbb{Q}$. If $j \neq 0, 1728$ then consider the curve

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

which has j invariant equal to $j(E)$, and is hence isomorphic to E. For $j(E) = 1728$ we have the equation $y^2 = x^3 + x$, and for $j(E) = 0$ we have $y^2 + y = x^3$. We can therefore represent all elements of $\text{Ell}(\mathcal{O}_K)$ by elliptic curves defined over $\overline{\mathbb{Q}}$.

Elements of $\text{Ell}(\mathcal{O}_K)$ are isomorphism classes of elliptic curves. By taking representatives defined over $\overline{\mathbb{Q}}$, we'd like to replace "isomorphism classes" with "$\overline{\mathbb{Q}}$ isomorphism classes". This reduction too is possible, as the classification of elliptic curves by their j invariant holds over any algebraically closed field of characteristic not 2 or 3.

In summary, we can replace $\text{Ell}(\mathcal{O}_K)$ with the set of $\overline{\mathbb{Q}}$ isomorphism classes of elliptic curves E defined over $\overline{\mathbb{Q}}$ so that $\text{End}(E) \cong \mathcal{O}_K$. In doing so, we define a Galois action on $\text{Ell}(\mathcal{O}_K)$ as follows. Take an elliptic curve E with Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \overline{\mathbb{Q}}$. For $\sigma \in G(\overline{\mathbb{Q}}/\mathbb{Q})$, we let E^σ be defined by $y^2 = x^3 + \sigma(a)x + \sigma(b)$.

As such, we have a Galois action on $\text{Ell}(\mathcal{O}_K)$. Understanding this action will afford us understanding of the extensions of K via Galois theory. For instance, we compare the Galois action with the action of the ideal class group $Cl(\mathcal{O}_K)$ on $\text{Ell}(\mathcal{O}_K)$.

Proposition 4.1. *There is a group homomorphism $F : G(\overline{K}/K) \longrightarrow Cl(\mathcal{O}_K)$ so that $E^\sigma = F(\sigma)E$ for any $E \in \text{Ell}(\mathcal{O}_K)$.*

Proof. We have described a Galois action on $\text{Ell}(\mathcal{O}_K)$. Let $\sigma \in G(\overline{K}/K)$. As the action of $Cl(\mathcal{O}_K)$ on $(\mathcal{O}_K)$ is free and transitive, E and E^σ are off by a unique ideal class. That is, there is some unique $F(\sigma) \in Cl(\mathcal{O}_K)$ so that $E^\sigma = F(\sigma)E$. Verifying that F is a group homomorphism is routine, and can be found in [Silverman, II.§2.4]. □

By analyzing this function F, we will connect elliptic curves with complex multiplication by $\mathcal{O}_K$ with the Hilbert class field of K. First off, to connect it to the j invariant of some $E \in \mathrm{Ell}(\mathcal{O}_K)$, let's compute its kernel.

Lemma 4.1. $\ker(F) = G(\overline{K}/K(j(E)))$.

Proof. Suppose $F(\sigma) = 1$. As the action of $Cl(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$ is free, this is the same as saying that $F(\sigma)E = E$ for any particular $E \in \mathrm{Ell}(\mathcal{O}_K)$. By definition of F, we have $F(\sigma)E = E^\sigma$. Equality in $\mathrm{Ell}(\mathcal{O}_K)$ is a question of isomorphism of elliptic curves, which is controlled by the j invariant. So this is equivalent to saying $j(E^\sigma) = j(E)$. And $j(E^\sigma) = \sigma(j(E))$. Thus, we have shown

$$\ker(F) = \{\sigma \in G(\overline{K}/K) \mid \sigma(j(E)) = j(E)\}$$

which is precisely $G(\overline{K}/K(j(E)))$. □

It follows from this lemma that F is in fact continuous when $Cl(\mathcal{O}_K)$ is given the discrete topology, as $G(\overline{K}/K(j(E)))$ is closed in $G(\overline{K}/K)$.

Now, to make our connection with class field theory, consider another important map with the same domain and codomain. That is, the composition:

$$F' : G(\overline{K}/K) \longrightarrow G(H/K) \xrightarrow{\sim} Cl(\mathcal{O}_K)$$

Here H is the Hilbert class field of K, the first map is restriction, and the second map is the inverse of the Artin map $(\cdot, H/K)$. We seek to show that $K(j(E)) = H$. In fact, we will show that F and F' are actually the very same map. The latter result is more powerful, as it implies $\ker(F) = \ker(F')$ whence $H = K(j(E))$ by infinite Galois theory. So not only is F is independent of the choice of elliptic curve E, the class field theoretically defined F' can be interpreted and understood using elliptic curves.

Remark. If we defined the action of $Cl(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$ without the inverse, it'd rear its ugly head here so that F and F' would be off by the inversion map $[I] \mapsto [I]^{-1}$.

Theorem 4.2. *Let $L = K(j(E))$ and H/K be the Hilbert class field. Then $L = H$ and $F = F'$.*

The proof of this result is too long and technical to include, so we will present a summary of the method.

Proof sketch. First, the map F is computed on a certain class of primes $\mathfrak{p}$ in $\mathcal{O}_K$. Specifically, on those $\mathfrak{p}$ which lie above a prime $p \in \mathbb{Z}$ which splits into two distinct prime factors $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$. This class is known by the Chebotarev density theorem to consist of half the primes of K.

The computation is to first view F as a map $G(K^{ab}/K) \longrightarrow Cl(\mathcal{O}_K)$, which is possible by continuity of F and commutativity of the ideal class group. Consider then a Frobenius element $\phi(\mathfrak{p})$ for such a prime $\mathfrak{p}$. Note that these elements do exist in an infinite extension, but by ramification they are only well defined modulo a subgroup of $G(K^{ab}/K)$ called the inertia subgroup of $\mathfrak{p}$. In any case, this abuse of notation will not be problematic to us.

One shows that $F(\phi(\mathfrak{p})) = [\mathfrak{p}]$, meaning the class of $\mathfrak{p}$ in the class group $Cl(\mathcal{O}_K)$. This is precisely how F' acts on the Frobenius elements too.

Using this result for primes, we can furthermore show upon factoring F through $G(L/K)$ that $F((I, L/K)) = [I]$ for any $I \in \Psi(I_{L/K})$.

From this, $F(((a), L/K)) = 1$ for all principal ideals $(a) \in \Psi(I_{L/K})$. Because $\ker(F) = G(\overline{K}/L)$, the factorization of F through $G(L/K)$ is injective. Thus, $((a), L/K) = \mathrm{id}$ within $G(L/K)$ for all such principal ideals (a). By definition, this means that the conductor $I_{L/K}$ is the unit ideal.

It follows then by class field theory that L is contained in the Hilbert class field H. Furthermore, the above will also show that $G(L/K)$ is carried isomorphically onto $Cl(\mathcal{O}_K)$ via F. We also know that $G(H/K) \cong Cl(\mathcal{O}_K)$. As such, by counting, we conclude equality $L = H$.

We've therefore also shown that F can be factored as $G(K^{ab}/K) \longrightarrow G(L/K) \longrightarrow Cl(\mathcal{O}_K)$. This is exactly how F' was defined. □

We have therefore found an explicit description of the Hilbert class field of an imaginary quadratic number field, as well as a description of the inverse to the Artin map, using the theory of complex multiplication of elliptic curves.

4.2 Torsion and the ray class fields

Before we proceed with analyzing the remainder of the maximal abelian extension K^{ab} of an imaginary quadratic number field, let's briefly recall the theory from $\mathbb{Q}$.

Theorem 4.3 (The Kronecker – Weber theorem)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in a cycloctomic extension $\mathbb{Q}(\zeta_n)$ for some primitive n^{th} root of unity n.*

Proof sketch. One can show that the ray class group of modulus $n\infty$ is exactly $\mathbb{Q}(\zeta_n)$. The result follows from class field theory. □

We can phrase this by saying that the maximal abelian extension of $\mathbb{Q}$ comes from adjoining all roots of unity. The roots of unity are parameterized by special values of the exponential function $e^{2\pi ix}$, namely those x in $\mathbb{Q}/\mathbb{Z}$. Furthermore, the roots of unity can be thought of as the torsion points of the unit group $\mathbb{C}^*$. Algebraic geometers refer to $\mathbb{C}^*$ as $\mathbb{G}_m(\mathbb{C})$ – the $\mathbb{C}$ points of the multiplicative group scheme $\mathbb{G}_m$. So the maximal abelian extension of $\mathbb{Q}$ arises from adjoining torsion points of $\mathbb{G}_m(\mathbb{C})$, which are parameterized by special values of a transcendental function exp.

The same story will hold for understanding K^{ab} where K is an imaginary quadratic number field. The group $\mathbb{G}_m$ is replaced by the E, and the exponential function is replaced by what we will soon call a Weber function. A notable difference here is that the Kronecker – Weber theorem didn't mention the Hilbert class field of $\mathbb{Q}$ at all. That's because the Hilbert class field of $\mathbb{Q}$ is just $\mathbb{Q}$ itself. Indeed, $\mathbb{Z}$ has unique factorization by the fundamental theorem of arithmetic so the class number of $\mathbb{Q}$ is 1.

Our understanding of K^{ab} is summarized in the following theorem.

Theorem 4.4. *Let K be an imaginary quadratic number field and $E \in \mathrm{Ell}(\mathcal{O}_K)$. The maximal abelian extension K^{ab} is described as*

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

for a Weber function $h : E \longrightarrow \mathbb{P}^1$, meaning a finite map invariant under the action of $\mathrm{Aut}(E)$ which is defined over the Hilbert class field.

In fact, for a nonzero integral ideal I of $\mathcal{O}_K$, we have that the ray class field of modulus I is given by

$$K_I = K(j(E), h[E[I]])$$

where $E[I]$ is the elements of E which are annihilated by I.

The proof of this result is more technical than can be presented here, as it heavily uses properties of reducing an elliptic curve to a finite field. The key is to understand the action of the Frobenius elements to prove that the ray class fields are as we describe. We will not explain much more, but a definition of a Weber function h is in order.

Definition 4.1. One definition of a Weber function $h : E \longrightarrow \mathbb{P}^1$ is to take a Weierstrass equation $y^2 = x^3 + ax + b$ where a, b are in $K(j(E))$. As discussed above, $K(j(E)) = H$ the Hilbert class field. We then define

$$h(x,y) = \begin{cases} x^3 & j = 0 \\ x^2 & j = 1728 \\ x & \text{otherwise} \end{cases}$$

So in almost all cases, h is simply the x coordinate on E.

A more analytic definition, which follows the same cases, is as follows:.

Let $f : \mathbb{C}/\Lambda \xrightarrow{\sim} E$ be given by $(\wp, \wp')$.

$$h \circ f = \begin{cases} \frac{g_3}{\Delta}\wp^3 & j = 0 \\ \frac{g_2^2}{\Delta}\wp^2 & j = 1728 \\ \frac{g_2 g_3}{\Delta}\wp & \text{otherwise} \end{cases}$$

We therefore have a complete description of the maximal abelian extension of an imaginary quadratic number field K using complex multiplication of elliptic curves.

5 Conclusion

Class field theory provides us with a description of the maximal abelian extension of a number field. In the specific cases of $\mathbb{Q}$ and imaginary quadratic number fields, a much more explicit description can be given. Over $\mathbb{Q}$, the abelian extensions are controlled by adjoining torsion points of $\mathbb{G}_m(\mathbb{C}) = \mathbb{C}^*$, i.e. roots of unity. These are parameterized by an analytic function exp. For imaginary quadratics, we have discussed that a wholly analogous story arises. The abelian extensions of an imaginary quadratic number field are controlled by the j invariant, which is an analytic function, and torsion points of an elliptic curve E with complex multiplication. Said torsion points are parameterized by an analytic function called a Weber function. A similar story is known to occur in local class field theory, where the maximal abelian extension of a local field is given in terms of the torsion points of a formal group law. See, for instance, [CF, VI.§3] for this case.

The similarity in all of these class field theories led number theorists to wonder if the same sort of scenario holds for all number fields. Are abelian extensions of a number field always determined by special values of some analytic function? Do they always arise in terms of torsion points of some group scheme like $\mathbb{G}_m$ or $\mathbb{C}$? This is Hilbert's 12^{th} problem. It is also referred to as Kronecker's *Jugendtraum* – a German word translating to "boyhood dream". A more detailed historical account of complex multiplication and the *Jugendtraum* can be found in [Vladut].

Additionally, complex multiplication has seen a vast generalization to abelian varieties, an essential object of algebraic geometry. One can see [ST] for an account of complex multiplication in this generality and its impact in number theory.

References

[ST] Goro Shimura and Yutaka Taniyama. *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*. The Mathemcatical Society of Japan, 1961.

[Serre] Jean-Pierre Serre. *A Course in Arithmetic*. Vol. 7. Graduate Texts in Mathematics. New York, NY: Springer New York, 1973. ISBN: 9780387900414 9781468498844. DOI: 10.1007/978-1-4684-9884-4. URL: http://link.springer.com/10.1007/978-1-4684-9884-4.

[AEC] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Vol. 106. Graduate Texts in Mathematics. New York, NY: Springer New York, 1986. ISBN: 9781475719222 9781475719208. DOI: 10.1007/978-1-4757-1920-8. URL: http://link.springer.com/10.1007/978-1-4757-1920-8.

[Cox] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. eng. Pbk. ed. Pure and applied mathematics (John Wiley & Sons : Unnumbered). New York: Wiley, 1989. ISBN: 9780471190790.

[Vladut] S. G. Vlăduț. *Kronecker's Jugendtraum and modular functions*. eng. Studies in the development of modern mathematics v. 2. New York: Gordon and Breach Science Pub, 1991. ISBN: 9782881247545.

[Lang – ANT] Serge Lang. *Algebraic Number Theory*. Vol. 110. Graduate Texts in Mathematics. New York, NY: Springer New York, 1994. ISBN: 9781461269229 9781461208532. DOI: 10.1007/978-1-4612-0853-2. URL: http://link.springer.com/10.1007/978-1-4612-0853-2.

[Silverman] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Vol. 151. Graduate Texts in Mathematics. New York, NY: Springer New York, 1994. ISBN: 9780387943282 9781461208518. DOI: 10.1007/978-1-4612-0851-8. URL: http://link.springer.com/10.1007/978-1-4612-0851-8.

[Janusz] Gerald J. Janusz. *Algebraic number fields*. 2nd ed. Graduate studies in mathematics v. 7. Providence, R.I: American Mathematical Society, 1996. ISBN: 9780821804292.

[Artin] Emil Artin and Arthur N. Milgram. *Galois theory*. Mineola, N.Y: Dover Publications, 1998. ISBN: 9780486623429.

[Neukirch] Jürgen Neukirch. *Algebraic number theory*. eng. Grundlehren der mathematischen Wissenschaften 322. Berlin ; New York: Springer, 1999. ISBN: 9783540653998.

[Lang] Serge Lang. *Algebra*. Ed. by S. Axler, F. W. Gehring, and K. A. Ribet. Vol. 211. Graduate Texts in Mathematics. New York, NY: Springer New York, 2002. ISBN: 9781461265511 9781461300410. DOI: 10.1007/978-1-4613-0041-0. URL: http://link.springer.com/10.1007/978-1-4613-0041-0.

[CF] J. W. S. Cassels and A. Fröhlich, eds. *Algebraic number theory: proceedings of an instructional conference organized by the London Mathematical Society (a NATO advanced study institute) with the support of the International Mathematical Union*. 2nd ed. OCLC: ocn573377924. London: London Mathematical Society, 2010. ISBN: 9780950273426.