Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Computational class field theory

HENRI COHEN AND PETER STEVENHAGEN

ABSTRACT. Class field theory furnishes an intrinsic description of the abelian extensions of a number field which is in many cases not of an immediate algorithmic nature. We outline the algorithms available for the explicit computation of such extensions.

CONTENTS

1. Introduction

Class field theory is a twentieth century theory describing the set of finite *abelian* extensions L of certain base fields K of arithmetic type. It provides a canonical description of the Galois groups $\mathrm{Gal}(L/K)$ in terms of objects defined 'inside K', and gives rise to an explicit determination of the maximal abelian quotient G_K^{ab} of the absolute Galois group G_K of K. In the classical examples, K is either a *global field*, that is, a number field or a function field in one variable over a finite field, or a *local field* obtained by completing a global field at one of its primes. In this paper, which takes an algorithmic approach, we restrict to the fundamental case in which the base field K is a number field. By doing so, we avoid the complications arising for p-extensions in characteristic $p > 0$.

Class field theory describes G_K^{ab} for a number field K in a way that can be seen as a first step towards a complete description of the full group $G_K \subset G_{\mathbb{Q}}$. At the moment, such a description is still far away, and it is not even clear what kind of description one might hope to achieve. Grothendieck's anabelian Galois theory and his theory of *dessins d'enfant* [Schneps 1994] constitute one direction of progress, and the largely conjectural *Langlands program* [Bump et al. 2003] provides an other approach. Despite all efforts and partial results [Völklein 1996], a concrete question such as the *inverse problem of Galois theory* — which asks whether, for a number field K, all finite groups G occur as the Galois group of some finite extension L/K — remains unanswered for all K.

A standard method for gaining insight into the structure of G_K, and for realizing certain types of Galois groups over K as quotients of G_K, consists of studying the action of G_K on 'arithmetical objects' related to K, such as the division points in $\overline{\mathbb{Q}}$ of various algebraic groups defined over K. A good example is the *Galois representation* arising from the group $E[m](\overline{\mathbb{Q}})$ of m-torsion points of an elliptic curve E that is defined over K. The action of G_K on $E[m](\overline{\mathbb{Q}})$ factors via a finite quotient $T_m \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ of G_K, and much is known [Serre 1989] about the groups T_m. Elliptic curves with *complex multiplication* by an order in an imaginary quadratic field K give rise to *abelian* extensions of K and yield a particularly explicit instance of class field theory.

For the much simpler example of the multiplicative group $\mathbf{G}_m$, the division points of $\mathbf{G}_m(\overline{\mathbb{Q}})$ are the *roots of unity* in $\overline{\mathbb{Q}}$. The extensions of K they generate are the *cyclotomic extensions* of K. Because the Galois group of the extension $K \subset K(\zeta_m)$ obtained by adjoining a primitive m-th root of unity ζ_m to K naturally embeds into $(\mathbb{Z}/m\mathbb{Z})^*$, all cyclotomic extensions are abelian. For $K = \mathbb{Q}$, Kronecker discovered in 1853 that *all* abelian extensions are accounted for in this way.

THEOREM 1.1 (KRONECKER–WEBER). *Every finite abelian extension $\mathbb{Q} \subset L$ is contained in some cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_m)$.*

Over number fields $K \neq \mathbb{Q}$, there are more abelian extensions than just cyclotomic ones, and the analogue of Theorem 1.1 is what class field theory provides: every abelian extension $K \subset L$ is contained in some *ray class field extension* $K \subset H_{\mathfrak{m}}$. Unfortunately, the theory does not provide a 'natural' system of generators for the fields $H_{\mathfrak{m}}$ that plays the role of the roots of unity in Theorem 1.1. Finding such a system for all K is one of the Hilbert problems from 1900 that is still open. Notwithstanding this problem, class field theory is in principle constructive, and, once one finds in some way a possible generator of $H_{\mathfrak{m}}$ over K, it is not difficult to verify that it does generate $H_{\mathfrak{m}}$. The information we have on $H_{\mathfrak{m}}$ is essentially an intrinsic description, in terms of the splitting and ramification of the primes in the extension $K \subset H_{\mathfrak{m}}$, of the Galois group

$\mathrm{Gal}(H_{\mathfrak{m}}/K)$ as a *ray class group* $\mathrm{Cl}_{\mathfrak{m}}$. This group replaces the group $(\mathbb{Z}/m\mathbb{Z})^*$ that occurs implicitly in Theorem 1.1 as the underlying Galois group:

$$(\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}), \quad (a \bmod m) \longmapsto (\sigma_a : \zeta_m \mapsto \zeta_m^a). \tag{1-2}$$

We can in principle find generators for any specific class field by combining our knowledge of its ramification data with a classical method to generate arbitrary solvable field extensions, namely, the adjunction of *radicals*. More formally, we call an extension L of an arbitrary field K a *radical extension* if L is contained in the splitting field over K of a finite collection of polynomials of the form $X^n - a$, with $n \in \mathbb{Z}_{\geq 1}$ not divisible by $\mathrm{char}(K)$ and $a \in K$. If the collection of polynomials can be chosen so that K contains a primitive n-th root of unity for each polynomial $X^n - a$ in the collection, then the radical extension $K \subset L$ is said to be a *Kummer extension*. Galois theory tells us that every Kummer extension is abelian and, conversely, that an abelian extension $K \subset L$ of exponent n is Kummer if K contains a primitive n-th root of unity. Here the *exponent* of an abelian extension $K \subset L$ is the smallest positive integer n that annihilates $\mathrm{Gal}(L/K)$. Thus, for every finite abelian extension $K \subset L$ of a number field K, there exists a cyclotomic extension $K \subset K(\zeta)$ such that the 'base-changed' extension $K(\zeta) \subset L(\zeta)$ is Kummer.

In Section 5, we compute the class fields of K as subfields of Kummer extensions of $K(\zeta)$ for suitable cyclotomic extensions $K(\zeta)$ of K. The practical problem of the method is that the auxiliary fields $K(\zeta)$ may be much larger than the base field K, and this limits its use to not-too-large examples.

If K is imaginary quadratic, elliptic curves with complex multiplication solve the Hilbert problem for K, and this yields methods that are much faster than the Kummer extension constructions for general K. We describe these complex multiplication methods in some detail in our Sections 6 to 8. We do not discuss their extension to abelian varieties with complex multiplication [Shimura 1998]; nor do we discuss the analytic generation of class fields of totally real number fields K using *Stark units* [Cohen 2000, Chapter 6].

2. Class field theory

Class field theory generalizes Theorem 1.1 by focusing on the Galois group $(\mathbb{Z}/m\mathbb{Z})^*$ of the cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_m)$ rather than on the specific generator ζ_m. The extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_m)$ is unramified at all primes $p \nmid m$, and the splitting behavior of such p only depends on the residue class $(p \bmod m) \in (\mathbb{Z}/m\mathbb{Z})^*$. More precisely, the residue class degree $f_p = [\mathbf{F}_p(\zeta_m) : \mathbf{F}_p]$ of the primes over $p \nmid m$ equals the order of the *Frobenius automorphism* $(\sigma_p : \zeta_m \mapsto \zeta_m^p) \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, and this is the order of $(p \bmod m) \in (\mathbb{Z}/m\mathbb{Z})^*$ under the standard identification (1-2).

Now let $K \subset L$ be *any* abelian extension of number fields. Then for each prime $\mathfrak{p}$ of K that is unramified in L, by [Stevenhagen 2008, Section 15] there is a unique element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$ that induces the Frobenius automorphism $x \mapsto x^{\#k_\mathfrak{p}}$ on the residue class field extensions $k_\mathfrak{p} \subset k_\mathfrak{q}$ for the primes $\mathfrak{q}$ in L extending $\mathfrak{p}$. The order of this *Frobenius automorphism* $\mathrm{Frob}_\mathfrak{p}$ of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$ equals the residue class degree $[k_\mathfrak{q} : k_\mathfrak{p}]$, and the subgroup $\langle \mathrm{Frob}_\mathfrak{p} \rangle \subset \mathrm{Gal}(L/K)$ is the decomposition group of $\mathfrak{p}$.

We define the *Artin map* for L/K as the homomorphism

$$\psi_{L/K} : I_K(\Delta_{L/K}) \longrightarrow \mathrm{Gal}(L/K), \quad \mathfrak{p} \longmapsto \mathrm{Frob}_\mathfrak{p} \tag{2-1}$$

on the group $I_K(\Delta_{L/K})$ of fractional $\mathbb{Z}_K$-ideals generated by the primes $\mathfrak{p}$ of K that do not divide the discriminant $\Delta_{L/K}$ of the extension $K \subset L$. Such primes $\mathfrak{p}$ are known to be unramified in L by [Stevenhagen 2008, Theorem 8.5]. For an ideal $\mathfrak{a} \in I_K(\Delta_{L/K})$, we call $\psi_{L/K}(\mathfrak{a})$ the *Artin symbol* of $\mathfrak{a}$ in $\mathrm{Gal}(L/K)$.

For $K = \mathbb{Q}$, we can rephrase Theorem 1.1 as follows.

THEOREM 2.2 (KRONECKER–WEBER). *If $\mathbb{Q} \subset L$ is an abelian extension, there exists an integer $m \in \mathbb{Z}_{>0}$ such that the kernel of the Artin map $\psi_{L/\mathbb{Q}}$ contains all $\mathbb{Z}$-ideals $x\mathbb{Z}$ with $x > 0$ and $x \equiv 1 \bmod m$.*

The equivalence of Theorems 1.1 and 2.2 follows from the analytic fact that an extension of number fields is trivial if all primes outside a density zero subset split completely in it. Thus, if all primes $p \equiv 1 \bmod m$ split completely in $\mathbb{Q} \subset L$, then all primes of degree one are split in $\mathbb{Q}(\zeta_m) \subset L(\zeta_m)$ and L is contained in the cyclotomic field $\mathbb{Q}(\zeta_m)$.

The positivity condition on x in Theorem 2.2 can be omitted if the primes $p \equiv -1 \bmod m$ also split completely in L, that is, if L is totally real and contained in the maximal real subfield $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ of $\mathbb{Q}(\zeta_m)$. The allowed values of m in Theorem 2.2 are the multiples of some minimal positive integer, the *conductor* of $\mathbb{Q} \subset L$. It is the smallest integer m for which $\mathbb{Q}(\zeta_m)$ contains L. The prime divisors of the conductor are exactly the primes that ramify in L, and p^2 divides the conductor if and only if p is *wildly* ramified in L.

For a quadratic field L of discriminant d, the conductor equals $|d|$, and Theorem 2.2 says that the Legendre symbol $\left(\frac{d}{x}\right)$ only depends on x modulo $|d|$. This is Euler's version of the quadratic reciprocity law. The main statement of class field theory is the analogue of Theorem 2.2 over arbitrary number fields K.

THEOREM 2.3 (ARTIN'S RECIPROCITY LAW). *If $K \subset L$ is an abelian extension, there exists a nonzero ideal $\mathfrak{m}_0 \subset \mathbb{Z}_K$ such that the kernel of the Artin map $\psi_{L/K}$ in* (2-1) *contains all principal $\mathbb{Z}_K$-ideals $x\mathbb{Z}_K$ with x totally positive and $x \equiv 1 \bmod \mathfrak{m}_0$.*

This innocuous-looking statement is highly nontrivial. It shows there is a powerful global connection relating the splitting behavior in L of *different* primes of K. Just as Theorem 2.2 implies the quadratic reciprocity law, Artin's reciprocity law implies the general *power reciprocity laws* from algebraic number theory; see [Artin and Tate 1990, Chapter 12, §4; Cassels and Fröhlich 1967, p. 353].

It is customary to treat the positivity conditions at the real primes of K and the congruence modulo $\mathfrak{m}_0$ in Theorem 2.3 on equal footing. To this end, one formally defines a *modulus* $\mathfrak{m}$ of K to be a nonzero $\mathbb{Z}_K$-ideal $\mathfrak{m}_0$ times a subset $\mathfrak{m}_\infty$ of the real primes of K. For a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, we write

$$x \equiv 1 \bmod^* \mathfrak{m}$$

if x satisfies $\operatorname{ord}_\mathfrak{p}(x-1) \geq \operatorname{ord}_\mathfrak{p}(\mathfrak{m}_0)$ at the primes $\mathfrak{p}$ dividing the *finite part* $\mathfrak{m}_0$ and if x is positive at the real primes in the *infinite part* $\mathfrak{m}_\infty$ of $\mathfrak{m}$.

In the language of moduli, Theorem 2.3 asserts that there exists a modulus $\mathfrak{m}$ such that the kernel $\ker \psi_{L/K}$ of the Artin map contains the *ray group* $R_\mathfrak{m}$ of principal $\mathbb{Z}_K$-ideals $x\mathbb{Z}_K$ generated by elements $x \equiv 1 \bmod^* \mathfrak{m}$. As in the case of Theorem 2.2, the set of these *admissible* moduli for $K \subset L$ consists of the multiples $\mathfrak{m}$ of some minimal modulus $\mathfrak{f}_{L/K}$, the *conductor* of $K \subset L$. The primes occurring in $\mathfrak{f}_{L/K}$ are the primes of K, both finite and infinite, that ramify in L. An infinite prime of K is said to ramify in L if it is real but has complex extensions to L. As for $K = \mathbb{Q}$, a finite prime $\mathfrak{p}$ occurs with higher multiplicity in the conductor if and only if it is wildly ramified in L.

If $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ is an admissible modulus for $K \subset L$ and $I_\mathfrak{m}$ denotes the group of fractional $\mathbb{Z}_K$-ideals generated by the primes $\mathfrak{p}$ coprime to $\mathfrak{m}_0$, then the Artin map induces a homomorphism

$$\psi_{L/K} : \mathrm{Cl}_\mathfrak{m} = I_\mathfrak{m}/R_\mathfrak{m} \longrightarrow \mathrm{Gal}(L/K), \quad [\mathfrak{p}] \longmapsto \mathrm{Frob}_\mathfrak{p} \tag{2-4}$$

on the *ray class group* $\mathrm{Cl}_\mathfrak{m} = I_\mathfrak{m}/R_\mathfrak{m}$ modulo $\mathfrak{m}$. Our earlier remark on the triviality of extensions in which almost all primes split completely implies that it is *surjective*. By the Chebotarev density theorem [Stevenhagen and Lenstra 1996], even more is true: the Frobenius automorphisms $\mathrm{Frob}_\mathfrak{p}$ for $\mathfrak{p} \in I_\mathfrak{m}$ are *equidistributed* over the Galois group $\mathrm{Gal}(L/K)$. In particular, a modulus $\mathfrak{m}$ is admissible for an abelian extension $K \subset L$ if and only if (almost) all primes $\mathfrak{p} \in R_\mathfrak{m}$ of K split completely in L.

Since the order of the Frobenius automorphism $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$ equals the residue class degree $f_\mathfrak{p}$ of the primes $\mathfrak{q}$ in L lying over $\mathfrak{p}$, the norm $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{p}}$ of every prime ideal $\mathfrak{q}$ in $\mathbb{Z}_L$ coprime to $\mathfrak{m}$ is contained in the kernel of the Artin map. A nontrivial index calculation shows that the norms of the $\mathbb{Z}_L$-ideals coprime to $\mathfrak{m}$ actually generate the kernel in (2-4). In other words, the *ideal group* $A_\mathfrak{m} \subset I_\mathfrak{m}$ that corresponds to L, in the sense that we have $\ker \psi_{L/K} =$

$A_{\mathfrak{m}}/R_{\mathfrak{m}}$, is equal to

$$A_{\mathfrak{m}} = N_{L/K}(I_{\mathfrak{m}\mathbb{Z}_L}) \cdot R_{\mathfrak{m}}. \tag{2-5}$$

The *existence theorem* from class field theory states that for every modulus $\mathfrak{m}$ of K, there exists an extension $K \subset L = H_{\mathfrak{m}}$ for which the map $\psi_{L/K}$ in (2-4) is an isomorphism. Inside some fixed algebraic closure $\overline{K}$ of K, the extension $H_{\mathfrak{m}}$ is uniquely determined as the maximal abelian extension L of K in which all primes in the ray group $R_{\mathfrak{m}}$ split completely. It is the *ray class field* $H_{\mathfrak{m}}$ modulo $\mathfrak{m}$ mentioned in the introduction, for which the analogue of Theorem 1.1 holds over K. If $K \subset L$ is abelian, we have $L \subset H_{\mathfrak{m}}$ whenever $\mathfrak{m}$ is an admissible modulus for L. For $L = H_{\mathfrak{m}}$, we have $A_{\mathfrak{m}} = R_{\mathfrak{m}}$ in (2-5) and an Artin isomorphism $\mathrm{Cl}_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{m}}/K)$.

EXAMPLE 2.6.1. It will not come as a surprise that for $K = \mathbb{Q}$, the ray class field modulo $(m) \cdot \infty$ is the cyclotomic field $\mathbb{Q}(\zeta_m)$, and the ray class group $\mathrm{Cl}_{(m)\cdot\infty}$ is the familiar group $(\mathbb{Z}/m\mathbb{Z})^*$ acting on the m-th roots of unity. Leaving out the real prime ∞ of $\mathbb{Q}$, we find the ray class field modulo (m) to be the maximal real subfield $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ of $\mathbb{Q}(\zeta_m)$. This is the maximal subfield in which the real prime ∞ is unramified.

EXAMPLE 2.6.2. The ray class field of conductor $\mathfrak{m} = (1)$ is the *Hilbert class field* $H = H_1$ of K. It is the largest abelian extension of K that is unramified at all primes of K, both finite and infinite. Since I_1 and R_1 are the groups of all fractional and all principal fractional $\mathbb{Z}_K$-ideals, respectively, the Galois group $\mathrm{Gal}(H/K)$ is isomorphic to the ordinary class group Cl_K of K, and the primes of K that split completely in H are precisely the *principal* prime ideals of K. This peculiar fact makes it possible to derive information about the class group of K from the existence of unramified extensions of K, and conversely.

The ray group $R_{\mathfrak{m}}$ is contained in the subgroup $P_{\mathfrak{m}} \subset I_{\mathfrak{m}}$ of principal ideals in $I_{\mathfrak{m}}$, and the quotient $I_{\mathfrak{m}}/P_{\mathfrak{m}}$ is the class group Cl_K of K for all $\mathfrak{m}$. Thus, the ray class group $\mathrm{Cl}_{\mathfrak{m}} = I_{\mathfrak{m}}/R_{\mathfrak{m}}$ is an extension of Cl_K by a finite abelian group $P_{\mathfrak{m}}/R_{\mathfrak{m}}$ that generalizes the groups $(\mathbb{Z}/m\mathbb{Z})^*$ from (1-2). More precisely, we have a natural exact sequence

$$\mathbb{Z}_K^* \longrightarrow (\mathbb{Z}_K/\mathfrak{m})^* \longrightarrow \mathrm{Cl}_{\mathfrak{m}} \longrightarrow \mathrm{Cl}_K \longrightarrow 0 \tag{2-7}$$

in which the residue class of $x \in \mathbb{Z}_K$ coprime to $\mathfrak{m}_0$ in the finite group

$$(\mathbb{Z}_K/\mathfrak{m})^* = (\mathbb{Z}_K/\mathfrak{m}_0)^* \times \textstyle\prod_{\mathfrak{p}|\mathfrak{m}_\infty} \langle -1 \rangle$$

consists of its ordinary residue class modulo $\mathfrak{m}_0$ and the signs of its images under the real primes $\mathfrak{p}|\mathfrak{m}_\infty$. This group naturally maps onto $P_{\mathfrak{m}}/R_{\mathfrak{m}} \subset \mathrm{Cl}_{\mathfrak{m}}$, with a kernel reflecting the fact that generators of principal $\mathbb{Z}_K$-ideals are only unique up to multiplication by units in $\mathbb{Z}_K$.

Interpreting both class groups in (2-7) as Galois groups, we see that all ray class fields contain the Hilbert class field $H = H_1$ from Example 2.6.2, and that we have an Artin isomorphism

$$(\mathbb{Z}_K/\mathfrak{m})^*/\mathrm{im}[\mathbb{Z}_K^*] \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{m}}/H) \tag{2-8}$$

for their Galois groups over H. By Example 2.6.1, this is a generalization of the isomorphism (1-2).

In class field theoretic terms, we may specify an abelian extension $K \subset L$ by giving an admissible modulus $\mathfrak{m}$ for the extension together with the corresponding ideal group

$$A_{\mathfrak{m}} = \ker[I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)] \tag{2-9}$$

arising as the kernel of the Artin map (2-4). In this way, we obtain a *canonical bijection* between abelian extensions of K inside $\overline{K}$ and ideal groups $R_{\mathfrak{m}} \subset A_{\mathfrak{m}} \subset I_{\mathfrak{m}}$ of K, provided that one allows for the fact that the 'same' ideal group $A_{\mathfrak{m}}$ can be defined modulo different multiples $\mathfrak{m}$ of its *conductor*, that is, the conductor of the corresponding extension. More precisely, we call the ideal groups $A_{\mathfrak{m}_1}$ and $A_{\mathfrak{m}_2}$ *equivalent* if they satisfy $A_{\mathfrak{m}_1} \cap I_{\mathfrak{m}} = A_{\mathfrak{m}_2} \cap I_{\mathfrak{m}}$ for some common multiple $\mathfrak{m}$ of $\mathfrak{m}_1$ and $\mathfrak{m}_2$.

Both from a theoretical and an algorithmic point of view, (2-5) provides an immediate description of the ideal group corresponding to L as the *norm group* $A_{\mathfrak{m}} = N_{L/K}(I_{\mathfrak{m}\mathbb{Z}_L}) \cdot R_{\mathfrak{m}}$ as soon as we are able to find an admissible modulus $\mathfrak{m}$ for L. In the reverse direction, finding the *class field* L corresponding to an ideal group $A_{\mathfrak{m}}$ is much harder. Exhibiting practical algorithms to do so is the principal task of computational class field theory, and the topic of this paper. Already in the case of the Hilbert class field H of K from Example 2.6.2, we know no 'canonical' generator of H, and the problem is nontrivial.

3. Local aspects: ideles

Over $K = \mathbb{Q}$, all abelian Galois groups are described as quotients of the groups $(\mathbb{Z}/m\mathbb{Z})^*$ for some modulus $m \in \mathbb{Z}_{\geq 1}$. One may avoid the ubiquitous choice of moduli that arises when dealing with abelian fields by combining the Artin isomorphisms (1-2) at all 'finite levels' m into a single *profinite* Artin isomorphism

$$\varprojlim_m (\mathbb{Z}/m\mathbb{Z})^* = \widehat{\mathbb{Z}}^* \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}/\mathbb{Q}) \tag{3-1}$$

between the unit group $\widehat{\mathbb{Z}}^*$ of the profinite completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$ and the absolute abelian Galois group of $\mathbb{Q}$. The group $\widehat{\mathbb{Z}}^*$ splits as a product $\prod_p \mathbb{Z}_p^*$ by the Chinese remainder theorem, and $\mathbb{Q}_{\mathrm{ab}}$ is obtained correspondingly as a compositum of the fields $\mathbb{Q}(\zeta_{p^\infty})$ generated by the p-power roots of unity. The

automorphism corresponding to $u = (u_p)_p \in \widehat{\mathbb{Z}}^*$ acts as $\zeta \mapsto \zeta^{u_p}$ on p-power roots of unity. Note that the component group $\mathbb{Z}_p^* \subset \widehat{\mathbb{Z}}^*$ maps to the inertia group at p in any finite quotient $\mathrm{Gal}(L/\mathbb{Q})$ of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}/\mathbb{Q})$.

For arbitrary number fields K, one can take the projective limit in (2-7) over all moduli and describe $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ by an exact sequence

$$1 \longrightarrow \mathbb{Z}_K^* \longrightarrow \widehat{\mathbb{Z}}_K^* \times \textstyle\prod_{\mathfrak{p}\ \mathrm{real}} \langle -1 \rangle \xrightarrow{\psi_K} \mathrm{Gal}(K_{\mathrm{ab}}/K) \longrightarrow \mathrm{Cl}_K \longrightarrow 1, \qquad (3\text{-}2)$$

which treats somewhat asymmetrically the finite primes occurring in $\widehat{\mathbb{Z}}_K^* = \prod_{\mathfrak{p}\ \mathrm{finite}} U_{\mathfrak{p}}$ and the infinite primes. Here ψ_K maps the element -1 at a real prime $\mathfrak{p}$ to the complex conjugation at the extensions of $\mathfrak{p}$. The image of ψ_K is the Galois group $\mathrm{Gal}(K_{\mathrm{ab}}/H)$ over the Hilbert class field H, which is of finite index $h_K = \#\,\mathrm{Cl}_K$ in $\mathrm{Gal}(K_{\mathrm{ab}}/K)$. For an abelian extension L of K containing H, the image of the component group $U_{\mathfrak{p}} \subset \widehat{\mathbb{Z}}_K^*$ in $\mathrm{Gal}(L/H)$ is again the inertia group at $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$. As H is totally unramified over K, the same is true if L does not contain H: the inertia groups for $\mathfrak{p}$ in $\mathrm{Gal}(LH/K)$ and $\mathrm{Gal}(L/K)$ are isomorphic under the restriction map.

A more elegant description of $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ than that provided by the sequence (3-2) is obtained if one treats all primes of K in a uniform way and redefines the Artin map ψ_K — as we will do in (3-7) — using the *idele group*

$$\mathbf{A}_K^* = \textstyle\prod_{\mathfrak{p}}' K_{\mathfrak{p}}^* = \{(x_{\mathfrak{p}})_{\mathfrak{p}} : x_{\mathfrak{p}} \in U_{\mathfrak{p}} \text{ for almost all } \mathfrak{p}\}$$

of K. This group [Stevenhagen 2008, Section 14], consists of those elements in the Cartesian product of the multiplicative groups $K_{\mathfrak{p}}^*$ at *all* completions $K_{\mathfrak{p}}^*$ of K that have their $\mathfrak{p}$-component in the local unit group $U_{\mathfrak{p}}$ for almost all $\mathfrak{p}$. Here $U_{\mathfrak{p}}$ is, as before, the unit group of the valuation ring at $\mathfrak{p}$ if $\mathfrak{p}$ is a finite prime of K; for infinite primes $\mathfrak{p}$, the choice of $U_{\mathfrak{p}}$ is irrelevant as there are only finitely many such $\mathfrak{p}$. We take $U_{\mathfrak{p}} = K_{\mathfrak{p}}^*$, and write U_∞ to denote $\prod_{\mathfrak{p}\ \mathrm{infinite}} K_{\mathfrak{p}}^* = K \otimes_{\mathbb{Q}} \mathbb{R}$. Note that we have $\prod_{\mathfrak{p}\ \mathrm{finite}} U_{\mathfrak{p}}^* = \widehat{\mathbb{Z}}_K^*$.

The topology on $\mathbf{A}_K^*$ is the *restricted* product topology: elements are close if they are $\mathfrak{p}$-adically close at finitely many $\mathfrak{p}$ *and* have a quotient in $U_{\mathfrak{p}}$ for all other $\mathfrak{p}$. With this topology, K^* embeds diagonally into $\mathbf{A}_K^*$ as a discrete subgroup. As the notation suggests, $\mathbf{A}_K^*$ is the unit group of the *adele ring* $\mathbf{A}_K = \prod_{\mathfrak{p}}' K_{\mathfrak{p}}$, the subring of $\prod_{\mathfrak{p}} K_{\mathfrak{p}}$ consisting of elements having integral components for almost all $\mathfrak{p}$.

To any idele $x = (x_{\mathfrak{p}})_{\mathfrak{p}}$, we can associate an ideal $x\mathbb{Z}_K = \prod_{\mathfrak{p}\ \mathrm{finite}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}})}$, and this makes the group I_K of fractional $\mathbb{Z}_K$-ideals into a quotient of $\mathbf{A}_K^*$. For a global element $x \in K^* \subset \mathbf{A}_K^*$, the ideal $x\mathbb{Z}_K$ is the principal $\mathbb{Z}_K$-ideal generated by x, and so we have an exact sequence

$$1 \longrightarrow \mathbb{Z}_K^* \longrightarrow \widehat{\mathbb{Z}}_K^* \times U_\infty \longrightarrow \mathbf{A}_K^*/K^* \longrightarrow \mathrm{Cl}_K \longrightarrow 1 \qquad (3\text{-}3)$$

that describes the *idele class group* $\mathbf{A}_K^*/K^*$ of K in a way reminiscent of (3-2).

To obtain $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ as a quotient of $\mathbf{A}_K^*/K^*$, we show that the ray class groups $\mathrm{Cl}_{\mathfrak{m}}$ defined in the previous section are natural quotients of $\mathbf{A}_K^*/K^*$. To do so, we associate to a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ of K an open subgroup $W_{\mathfrak{m}} \subset \mathbf{A}_K^*$, as follows. Write $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ as a formal product, with $n(\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$ for finite $\mathfrak{p}$, and $n(\mathfrak{p}) \in \{0, 1\}$ to indicate the infinite $\mathfrak{p}$ in $\mathfrak{m}_\infty$. Now put

$$W_{\mathfrak{m}} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n(\mathfrak{p}))}$$

for subgroups $U_{\mathfrak{p}}^{(k)} \subset K_{\mathfrak{p}}^*$ that are defined by

$$U_{\mathfrak{p}}^{(k)} = \begin{cases} U_{\mathfrak{p}} & \text{if } k = 0; \\ 1 + \mathfrak{p}^k & \text{if } \mathfrak{p} \text{ is finite and } k > 0; \\ U_{\mathfrak{p}}^+ \subset U_{\mathfrak{p}} = \mathbb{R}^* & \text{if } \mathfrak{p} \text{ is real and } k = 1. \end{cases}$$

Here we write $U_{\mathfrak{p}}^+$ for real $\mathfrak{p}$ to denote the subgroup of positive elements in $U_{\mathfrak{p}}$. Because $\mathbb{C}^*$ and $\mathbb{R}_{>0}^*$ have no proper open subgroups, one sees from the definition of the restricted product topology on $\mathbf{A}_K^*$ that a subgroup $H \subset \mathbf{A}_K^*$ is open if and only if it contains $W_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$.

LEMMA 3.4. *For every modulus* $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ *of* K, *there is an isomorphism*

$$\mathbf{A}_K^*/K^*W_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Cl}_{\mathfrak{m}}$$

that maps $(x_{\mathfrak{p}})_{\mathfrak{p}}$ *to the class of* $\prod_{\mathfrak{p}\text{ finite}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(yx_{\mathfrak{p}})}$. *Here* $y \in K^*$ *is a global element satisfying* $yx_{\mathfrak{p}} \in U_{\mathfrak{p}}^{n(\mathfrak{p})}$ *for all* $\mathfrak{p}|\mathfrak{m}$.

PROOF. Note first that the global element y required in the definition exists by the approximation theorem. The precise choice of y is irrelevant, since for any two elements y and y' satisfying the requirement, we have $y/y' \equiv 1 \bmod^* \mathfrak{m}$. We obtain a homomorphism $\mathbf{A}_K^* \to \mathrm{Cl}_{\mathfrak{m}}$ that is surjective since it maps a prime element $\pi_{\mathfrak{p}}$ at a finite prime $\mathfrak{p} \nmid \mathfrak{m}$ to the class of $\mathfrak{p}$. Its kernel consists of the ideles that can be multiplied into $W_{\mathfrak{m}}$ by a global element $y \in K^*$. □

If $\mathfrak{m}$ is an admissible modulus for the finite abelian extension $K \subset L$, we can compose the isomorphism in Lemma 3.4 with the Artin map (2-4) for $K \subset L$ to obtain an idelic Artin map

$$\widehat{\psi}_{L/K} : \mathbf{A}_K^*/K^* \longrightarrow \mathrm{Gal}(L/K) \tag{3-5}$$

that no longer refers to the choice of a modulus $\mathfrak{m}$. This map, which exists as a corollary of Theorem 2.3, is a continuous surjection that maps the class of a prime element $\pi_{\mathfrak{p}} \in K_{\mathfrak{p}}^* \subset \mathbf{A}_K^*$ to the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ whenever $\mathfrak{p}$ is finite and unramified in $K \subset L$.

For a finite extension L of K, the adele ring $\mathbf{A}_L$ is obtained from $\mathbf{A}_K$ by a base change $K \subset L$, so we have a norm map $N_{L/K} : \mathbf{A}_L \to \mathbf{A}_K$ that maps $\mathbf{A}_L^*$ to $\mathbf{A}_K^*$ and restricts to the field norm on $L^* \subset \mathbf{A}_L^*$. Since it induces the ideal norm $I_L \to I_K$ on the quotient I_L of $\mathbf{A}_K^*$, one deduces that the kernel of (3-5) equals $(K^* \cdot N_{L/K}[\mathbf{A}_L^*])$ mod K^*, and that we have isomorphisms

$$\mathbf{A}_K^*/K^* N_{L/K}[\mathbf{A}_L^*] \cong I_{\mathfrak{m}}/A_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(L/K), \tag{3-6}$$

with $A_{\mathfrak{m}}$ the ideal group modulo $\mathfrak{m}$ that corresponds to L in the sense of (2-9). Taking the limit in (3-5) over all finite abelian extensions $K \subset L$ inside $\overline{K}$, one obtains the idelic Artin map

$$\psi_K : \mathbf{A}_K^*/K^* \longrightarrow G_K^{\mathrm{ab}} = \mathrm{Gal}(K_{\mathrm{ab}}/K). \tag{3-7}$$

This is a continuous surjection that is uniquely determined by the property that the ψ_K-image of the class of a prime element $\pi_{\mathfrak{p}} \in K_{\mathfrak{p}}^* \subset \mathbf{A}_K^*$ maps to the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ for every finite abelian extension $K \subset L$ in which $\mathfrak{p}$ is unramified. It exhibits all abelian Galois groups over K as a quotient of the idele class group $\mathbf{A}_K^*/K^*$ of K.

The kernel of the Artin map (3-7) is the connected component of the unit element in $\mathbf{A}_K^*/K^*$. In the idelic formulation, the finite abelian extensions of K inside $\overline{K}$ correspond bijectively to the open subgroups of $\mathbf{A}_K^*/K^*$ under the map

$$L \longmapsto \psi_K^{-1}[\mathrm{Gal}(K_{\mathrm{ab}}/L)] = (K^* \cdot N_{L/K}[\mathbf{A}_L^*]) \bmod K^*.$$

In this formulation, computational class field theory amounts to generating, for any given open subgroup of $\mathbf{A}_K^*/K^*$, the abelian extension $K \subset L$ corresponding to it.

EXAMPLE 3.8. Before continuing, let us see what the idelic reformulation of (3-1) comes down to for $K = \mathbb{Q}$. Every idele $x = ((x_p)_p, x_\infty) \in \mathbf{A}_{\mathbb{Q}}^*$ can uniquely be written as the product of the rational number

$$\mathrm{sign}(x_\infty) \prod_p p^{\mathrm{ord}_p(x_p)} \in \mathbb{Q}^*$$

and a 'unit idele' $u_x \in \prod_p \mathbb{Z}_p^* \times \mathbb{R}_{>0} = \widehat{\mathbb{Z}}^* \times \mathbb{R}_{>0}$. In this way, the Artin map (3-7) becomes a continuous surjection

$$\psi_{\mathbb{Q}} : \mathbf{A}_{\mathbb{Q}}^*/\mathbb{Q}^* \cong \widehat{\mathbb{Z}}^* \times \mathbb{R}_{>0} \longrightarrow \mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}/\mathbb{Q}).$$

Its kernel is the connected component $\{1\} \times \mathbb{R}_{>0}$ of the unit element in $\mathbf{A}_{\mathbb{Q}}^*/\mathbb{Q}^*$. Comparison with (3-1) leads to a commutative diagram of isomorphisms

$$\begin{array}{ccc} \widehat{\mathbb{Z}}^* & \xrightarrow{\quad -1 \quad} & \widehat{\mathbb{Z}}^* \\ {\scriptstyle \text{can}}\big\downarrow{\scriptstyle \sim} & & {\scriptstyle (3\text{-}1)}\big\downarrow{\scriptstyle \sim} \\ \mathbf{A}_{\mathbb{Q}}^*/(\mathbb{Q}^* \cdot \mathbb{R}_{>0}) & \xrightarrow{\quad \sim \quad} & \mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}/\mathbb{Q}) \end{array} \tag{3-8}$$

in which the upper horizontal map is *not* the identity. To see this, note that the class of the prime element $\ell \in \mathbb{Q}_\ell^* \subset \mathbf{A}_{\mathbb{Q}}^*$ in $\mathbf{A}_{\mathbb{Q}}^*/(\mathbb{Q}^* \cdot \mathbb{R}_{>0})$ is represented by the idele $x = (x_p)_p \in \widehat{\mathbb{Z}}^*$ having components $x_p = \ell^{-1}$ for $p \neq \ell$ and $x_\ell = 1$. This idele maps to the Frobenius of ℓ, which raises roots of unity of order coprime to ℓ to their ℓ-th power. Since x is in all $W_{\mathfrak{m}}$ for all conductors $\mathfrak{m} = \ell^k$, it fixes ℓ-power roots of unity. Thus, the upper isomorphism -1 is *inversion* on $\widehat{\mathbb{Z}}^*$.

Even though the idelic and the ideal group quotients on the left hand side of the arrow in (3-6) are the 'same' finite group, it is the idelic quotient that neatly encodes information at the *ramifying* primes $\mathfrak{p}|\mathfrak{m}$, which seem 'absent' in the other group. More precisely, we have for all primes $\mathfrak{p}$ an injective map $K_{\mathfrak{p}}^* \to \mathbf{A}_K^*/K^*$ that can be composed with (3-7) to obtain a *local* Artin map $\psi_{K_{\mathfrak{p}}}$: $K_{\mathfrak{p}}^* \to \mathrm{Gal}(L/K)$ at every prime $\mathfrak{p}$ of K. If $\mathfrak{p}$ is finite and unramified in $K \subset L$, we have $U_{\mathfrak{p}} \subset \ker \psi_{K_{\mathfrak{p}}}$ and an induced isomorphism of finite cyclic groups

$$K_{\mathfrak{p}}^*/\langle \pi_{\mathfrak{p}}^{f_{\mathfrak{p}}} \rangle U_{\mathfrak{p}} = K_{\mathfrak{p}}^*/N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}[L_{\mathfrak{q}}^*] \xrightarrow{\sim} \langle \mathrm{Frob}_{\mathfrak{p}} \rangle = \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}),$$

since $\mathrm{Frob}_{\mathfrak{p}}$ generates the decomposition group of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$, which may be identified with the Galois group of the local extension $K_{\mathfrak{p}} \subset L_{\mathfrak{q}}$ at a prime $\mathfrak{q}|\mathfrak{p}$ in L. It is a nontrivial fact that (3-5) induces for *all* primes $\mathfrak{p}$ of K, including the ramifying and the infinite primes, a *local Artin isomorphism*

$$\psi_{L_{\mathfrak{q}}/K_{\mathfrak{p}}} : K_{\mathfrak{p}}^*/N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}[L_{\mathfrak{q}}^*] \xrightarrow{\sim} \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}). \tag{3-10}$$

In view of our observation after (3-2), it maps $U_{\mathfrak{p}}/N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}[U_{\mathfrak{q}}]$ for finite $\mathfrak{p}$ isomorphically onto the inertia group of $\mathfrak{p}$.

We can use (3-10) to *locally* compute the exponent $n(\mathfrak{p})$ to which $\mathfrak{p}$ occurs in the conductor of $K \subset L$: it is the smallest nonnegative integer k for which we have $U_{\mathfrak{p}}^{(k)} \subset N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}[L_{\mathfrak{q}}^*]$. For unramified primes $\mathfrak{p}$ we obtain $n(\mathfrak{p}) = 0$, as the local norm is then surjective on the unit groups. For tamely ramified primes we have $n(\mathfrak{p}) = 1$, and for wildly ramified primes $\mathfrak{p}$, the exponent $n(\mathfrak{p})$ may be found by a local computation. In many cases it is sufficient to use an upper bound coming from the fact that every d-th power in $K_{\mathfrak{p}}^*$ is a norm from $L_{\mathfrak{q}}$, with d the degree of $K_{\mathfrak{p}} \subset L_{\mathfrak{q}}$ (or even $K \subset L$). Using Hensel's Lemma [Buhler and Wagon 2008], one then finds

$$n(\mathfrak{p}) \leq e(\mathfrak{p}/p)\Big(\frac{1}{p-1} + \mathrm{ord}_p(e_{\mathfrak{p}})\Big) + 1, \tag{3-11}$$

where $e(\mathfrak{p}/p)$ is the absolute ramification index of $\mathfrak{p}$ over the underlying rational prime p and $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ in $K \subset L$. Note that $e_{\mathfrak{p}}$ is independent of the choice of an extension prime as $K \subset L$ is Galois.

4. Computing class fields: preparations

Our fundamental problem is the computation of the class field L that corresponds to a given ideal group $A_{\mathfrak{m}}$ of K in the sense of (2-5). One may 'give' $A_{\mathfrak{m}}$ by specifying $\mathfrak{m}$ and a list of ideals for which the classes in the ray class group $\mathrm{Cl}_{\mathfrak{m}}$ generate $A_{\mathfrak{m}}$. The first step in computing L is the computation of the group $I_{\mathfrak{m}}/A_{\mathfrak{m}}$ that will give us control of the Artin isomorphism $I_{\mathfrak{m}}/A_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(L/K)$. Because linear algebra over $\mathbb{Z}$ provides us with good algorithms [Cohen 2000, Section 4.1] to deal with finite or even finitely generated abelian groups, this step essentially reduces to computing the finite group $\mathrm{Cl}_{\mathfrak{m}}$ of which $I_{\mathfrak{m}}/A_{\mathfrak{m}}$ is quotient.

For the computation of the ray class group $\mathrm{Cl}_{\mathfrak{m}}$ modulo $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$, one computes, in line with [Schoof 2008], the three other groups in the exact sequence (2-7) in which it occurs, and the maps between them. The class group Cl_K and the unit group $\mathbb{Z}_K^*$ in (2-7) can be computed using the algorithm described in [Stevenhagen 2008, Section 12], which factors *smooth* elements of $\mathbb{Z}_K$ over a *factor base*. As this takes exponential time as a function of the base field K, it can only be done for moderately sized K. For the group $(\mathbb{Z}_K/\mathfrak{m}_0)^*$, one uses the Chinese remainder theorem to decompose it into a product of local multiplicative groups the form $(\mathbb{Z}_K/\mathfrak{p}^k)^*$. Here we need to assume that we are able to factor $\mathfrak{m}_0$, but this is a safe assumption as we are unlikely to deal with extensions for which we cannot even factor the conductor. The group $(\mathbb{Z}_K/\mathfrak{p}^k)^*$ is a product of the cyclic group $k_{\mathfrak{p}}^* = (\mathbb{Z}_K/\mathfrak{p})^*$ and the subgroup $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$, the structure of which can be found inductively using the standard isomorphisms $(1+\mathfrak{p}^a)/(1+\mathfrak{p}^{a+1}) \cong k_{\mathfrak{p}}$ and, more efficiently,

$$(1+\mathfrak{p}^a)/(1+\mathfrak{p}^{2a}) \xrightarrow{\sim} \mathfrak{p}^a/\mathfrak{p}^{2a}$$

between multiplicative and additive quotients. In many cases, the result can be obtained in one stroke using the $\mathfrak{p}$-adic logarithm [Cohen 2000, Section 4.2.2]. Finding $\mathrm{Cl}_{\mathfrak{m}}$ from the other groups in (2-7) is now a standard application of linear algebra over $\mathbb{Z}$. The quotient $I_{\mathfrak{m}}/A_{\mathfrak{m}}$ gives us an explicit description of the Galois group $\mathrm{Gal}(L/K)$ in terms of Artin symbols of $\mathbb{Z}_K$-ideals.

For the ideal group $A_{\mathfrak{m}}$, we next compute its conductor $\mathfrak{f}$, which may be a proper divisor of $\mathfrak{m}$. This comes down to checking whether we have $A_{\mathfrak{m}} \supset I_{\mathfrak{m}} \cap R_{\mathfrak{n}}$ for some modulus $\mathfrak{n}|\mathfrak{m}$. Even in the case $A_{\mathfrak{m}} = R_{\mathfrak{m}}$, the conductor can be smaller than $\mathfrak{m}$, as the trivial isomorphism $(\mathbb{Z}/6\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/3\mathbb{Z})^*$ of ray class groups over $K = \mathbb{Q}$ shows. The conductor $\mathfrak{f}$ obtained, which is the same as

the conductor $\mathfrak{f}_{L/K}$ of the corresponding extension, is exactly divisible by the primes that ramify in $K \subset L$. In particular, we know the signature of L from the real primes dividing $\mathfrak{f}$. With some extra effort, one can even compute the discriminant $\Delta_{L/K}$ using Hasse's *Führerdiskriminantenproduktformel*

$$\Delta_{L/K} = \prod_{\chi: I_{\mathfrak{m}}/A_{\mathfrak{m}} \to \mathbb{C}^*} \mathfrak{f}(\chi)_0. \tag{4-1}$$

Here χ ranges over the characters of the finite group $I_{\mathfrak{m}}/A_{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$, and $\mathfrak{f}(\chi)_0$ denotes the finite part of the conductor $\mathfrak{f}(\chi)$ of the ideal group A_χ modulo $\mathfrak{m}$ satisfying $A_\chi/A_{\mathfrak{m}} = \ker \chi$. All these quantities can be computed by the standard algorithms for finite abelian groups.

EXAMPLE 4.2. If $K \subset L$ is cyclic of prime degree ℓ, we have a trivial character of conductor (1) and $\ell - 1$ characters of conductor $\mathfrak{f}_{L/K}$, so (4-1) reduces to

$$\Delta_{L/K} = (\mathfrak{f}_{L/K})_0^{\ell-1}.$$

In particular, we see that the discriminant of a quadratic extension $K \subset L$ is not only for $K = \mathbb{Q}$, but generally equal to the finite part of the conductor of the extension.

Having at our disposal the Galois group $\mathrm{Gal}(L/K)$, the discriminant $\Delta_{L/K}$, and the Artin isomorphism $I_{\mathfrak{m}}/A_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(L/K)$ describing the splitting behavior of the primes in $K \subset L$, we proceed with the computation of a generator for L over K, that is, an irreducible polynomial in $K[X]$ with the property that its roots in $\overline{K}$ generate L.

Because the computation of class fields is not an easy computation, it is often desirable to decompose $\mathrm{Gal}(L/K)$ as a product $\prod_i \mathrm{Gal}(L_i/K)$ of Galois groups $\mathrm{Gal}(L_i/K)$ and to realize L as a compositum of extensions L_i that are computed separately. This way one can work with extensions L/K that are cyclic of prime power order, or at least of prime power exponent. The necessary reduction of the global class field theoretic data for L/K to those for each of the L_i is only a short computation involving finite abelian groups.

5. Class fields as Kummer extensions

Let K be *any* field containing a primitive n-th root of unity ζ_n, and let $K \subset L$ be an abelian extension of *exponent* dividing n. In this situation, Kummer theory [Lang 2002, Chapter VIII, § 6–8] tells us that L can be obtained by adjoining to K the n-th roots of certain elements of K. More precisely, let $W_L = K^* \cap L^{*n}$ be the subgroup of K^* of elements that have an n-th root in L. Then we have

$L = K(\sqrt[n]{W_L})$, and there is the canonical *Kummer pairing*

$$\begin{aligned} \mathrm{Gal}(L/K) \times W_L/K^{*n} &\longrightarrow \langle \zeta_n \rangle \\ (\sigma, w) &\longmapsto \langle \sigma, w \rangle = (w^{1/n})^{\sigma-1} = \frac{\sigma(\sqrt[n]{w})}{\sqrt[n]{w}}. \end{aligned} \tag{5-1}$$

By *canonical*, we mean that the natural action of an automorphism $\tau \in \mathrm{Aut}(\overline{K})$ on the pairing for $K \subset L$ yields the Kummer pairing for $\tau K \subset \tau L$, that is,

$$\langle \tau\sigma\tau^{-1}, \tau w \rangle = \langle \sigma, w \rangle^{\tau}. \tag{5-2}$$

The Kummer pairing is *perfect*, that is, it induces an isomorphism

$$W_L/K^{*n} \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{C}^*). \tag{5-3}$$

In the case where $\mathrm{Gal}(L/K)$ is cyclic of order n, this means that $L = K(\sqrt[n]{\alpha})$ and $W_L = K^* \cap L^{*n} = \langle \alpha \rangle \cdot K^{*n}$ for some $\alpha \in K$. If $\sqrt[n]{\beta}$ also generates L over K, then α and β are powers of each other modulo n-th powers.

We will apply Kummer theory to generate the class fields of a number field K. Thus, let L be the class field of K from Section 4 that is to be computed. Suppose that we have computed a 'small' modulus $\mathfrak{f}$ for L that is only divisible by the ramifying primes, such as the conductor $\mathfrak{f}_{L/K}$, and an ideal group $A_{\mathfrak{f}}$ for L by the methods of Section 4. With this information, we control the Galois group of our extension via the Artin isomorphism $I_{\mathfrak{f}}/A_{\mathfrak{f}} \xrightarrow{\sim} \mathrm{Gal}(L/K)$. Let n be the exponent of $\mathrm{Gal}(L/K)$. Then we can directly apply Kummer theory if K contains the required n-th roots of unity; if not, we need to pass to a cyclotomic extension of K first. This leads to a natural case distinction.

<u>*Case 1*</u>: K contains a primitive n-th root of unity ζ_n. Under the restrictive assumption that K contains ζ_n, the class field L is a Kummer extension of K, and generating $L = K(\sqrt[n]{W_L})$ comes down to finding generators for W_L/K^{*n}. We first compute a *finite* group containing W_L/K^{*n}. This reduction is a familiar ingredient from the *proofs* of class field theory [Artin and Tate 1990; Cassels and Fröhlich 1967].

LEMMA 5.4. *Let $K \subset L$ be finite abelian of exponent n, and assume $\zeta_n \in K$. Suppose S is a finite set of primes of K containing the infinite primes such that*

(1) *$K \subset L$ is unramified outside S;*
(2) *$\mathrm{Cl}_K/\mathrm{Cl}_K^n$ is generated by the classes of the finite primes in S.*

Then the image of the group U_S of S-units in K^*/K^{*n} is finite of order $n^{\#S}$, and it contains the group W_L/K^{*n} from (5-1).

The first condition in Lemma 5.4 means that S contains all the primes that divide our small modulus $\mathfrak{f}$. The second condition is automatic if the class number of K is prime to n, and it is implied by the first if the classes of the ramifying primes

generate $\mathrm{Cl}_K/\mathrm{Cl}_K^n$. Any set of elements of Cl_K generating $\mathrm{Cl}_K/\mathrm{Cl}_K^n$ actually generates the full 'n-part' of the class group, that is, the product of the p-Sylow subgroups of Cl_K at the primes $p|n$. In general, there is a lot of freedom in the choice of primes in S outside $\mathfrak{f}$. One tries to have S 'small' in order to minimize the size $n^{\#S}$ of the group $(U_S \cdot K^{*n})/K^{*n}$ containing W_L/K^{*n}.

PROOF OF LEMMA 5.4. By the Dirichlet unit theorem [Stevenhagen 2008, Theorem 10.9], the group U_S of S-units of K is isomorphic to $\mu_K \times \mathbb{Z}^{\#S-1}$. As μ_K contains ζ_n, the image $(U_S \cdot K^{*n})/K^{*n} \cong U_S/U_S^n$ of U_S in K^*/K^{*n} is finite of order $n^{\#S}$.

To show that $(U_S \cdot K^{*n})/K^{*n}$ contains W_L/K^{*n}, pick any $\alpha \in W_L$. Since $K \subset K(\sqrt[n]{\alpha})$ is unramified outside S, we have $(\alpha) = \mathfrak{a}_S\mathfrak{b}^n$ for some product $\mathfrak{a}_S$ of prime ideals in S and $\mathfrak{b}$ coprime to all finite primes in S. As the primes in S generate the n-part of Cl_K, we can write $\mathfrak{b} = \mathfrak{b}_S\mathfrak{c}$ with $\mathfrak{b}_S$ a product of prime ideals in S and $\mathfrak{c}$ an ideal of which the class in Cl_K is of order u coprime to n. Now α^u generates an ideal of the form $(\alpha^u) = \mathfrak{a}'_S(\gamma^n)$ with $\mathfrak{a}'_S$ a product of prime ideals in S and $\gamma \in K^*$. It follows that $\alpha^u\gamma^{-n} \in K^*$ is an S-unit, and so α^u and therefore α is contained in $U_S \cdot K^{*n}$. □

In the situation of Lemma 5.4, we see that $K \subset L$ is a subextension of the Kummer extension $K \subset N = K(\sqrt[n]{U_S})$ of degree $n^{\#S}$. We have to find the subgroup of U_S/U_S^n corresponding to L. This amounts to a computation in linear algebra using the Artin map and the Kummer pairing. For ease of exposition, we assume that the set S we choose to satisfy Lemma 5.4 contains all primes dividing n. This implies that N is the maximal abelian extension of exponent n of K that is unramified outside S.

As we compute L as a subfield of the abelian extension $K \subset N$, we replace the modulus $\mathfrak{f}$ of $K \subset L$ by some multiple $\mathfrak{m}$ that is an admissible modulus for $K \subset N$. Clearly $\mathfrak{m}$ only needs to be divisible by the ramified primes in $K \subset N$, which are all in S. Wild ramification only occurs at primes $\mathfrak{p}$ dividing n, and for these primes we can take $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$ equal to the bound given by (3-11). The ideal group modulo $\mathfrak{m}$ corresponding to N is $I_{\mathfrak{m}}^n \cdot P_{\mathfrak{m}}$ because N is the maximal exponent-n extension of K of conductor $\mathfrak{m}$; hence the Artin map for $K \subset N$ is

$$I_{\mathfrak{m}} \longrightarrow I_{\mathfrak{m}}/(I_{\mathfrak{m}}^n \cdot P_{\mathfrak{m}}) = \mathrm{Cl}_{\mathfrak{m}}/\mathrm{Cl}_{\mathfrak{m}}^n \xrightarrow{\sim} \mathrm{Gal}(N/K). \tag{5-5}$$

The induced map $I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is the Artin map for $K \subset L$, which has the ideal group $A_{\mathfrak{m}}$ corresponding to L as its kernel. Let $\Sigma_L \subset I_{\mathfrak{m}}$ be a finite set of ideals of which the classes generate the $\mathbb{Z}/n\mathbb{Z}$-module $A_{\mathfrak{m}}/(I_{\mathfrak{m}}^n \cdot P_{\mathfrak{m}}) \cong \mathrm{Gal}(N/L)$. We then have to determine the subgroup $V_L \subset U_S$ consisting of those S-units $v \in U_S$ that have the property that $\sqrt[n]{v}$ is left invariant by the Artin symbols of all ideals in Σ_L, since the class field we are after is $L = K(\sqrt[n]{V_L})$.

We are here in a situation to apply linear algebra over $\mathbb{Z}/n\mathbb{Z}$, because the Kummer pairing (5-1) tells us that the action of the Artin symbols $\psi_{N/K}(\mathfrak{a})$ of the ideals $\mathfrak{a} \in I_{\mathfrak{m}}$ on the n-th roots of the S-units is described by the pairing of $\mathbb{Z}/n\mathbb{Z}$-modules given by

$$\begin{aligned} I_{\mathfrak{m}}/I_{\mathfrak{m}}^n \times U_S/U_S^n &\longrightarrow \langle \zeta_n \rangle \\ (\mathfrak{a}, u) &\longmapsto \langle \psi_{N/K}(\mathfrak{a}), u \rangle = (u^{1/n})^{\psi_{N/K}(\mathfrak{a})-1}. \end{aligned} \tag{5-6}$$

Making this computationally explicit amounts to computing the pairing for some choice of basis elements of the three modules involved.

For $\langle \zeta_n \rangle$ we have the obvious $\mathbb{Z}/n\mathbb{Z}$-generator ζ_n, and $I_{\mathfrak{m}}/I_{\mathfrak{m}}^n$ is a free $\mathbb{Z}/n\mathbb{Z}$-module generated by the primes $\mathfrak{p} \notin S$. If K is of moderate degree, the general algorithm [Stevenhagen 2008, Section 12] for computing units and class groups can be used to compute generators for U_S, which then form a $\mathbb{Z}/n\mathbb{Z}$-basis for U_S/U_S^n. In fact, finding $s - 1 = \#S - 1$ independent units in U_S that generate a subgroup of index coprime to n is enough: together with a root of unity generating μ_K, these will generate U_S/U_S^n. This is somewhat easier than finding actual generators for U_S, because maximality modulo n-th powers is not difficult to establish for a subgroup $U \subset U_S$ having the right rank $s = \#S$. Indeed, each reduction modulo a small prime $\mathfrak{p} \notin S$ provides a character $U \subset U_S \to k_{\mathfrak{p}}^*/(k_{\mathfrak{p}}^*)^n \cong \langle \zeta_n \rangle$, the n-th power residue symbol at $\mathfrak{p}$. By finding s independent characters, one shows that the intersection of their kernels equals $U^n = U \cap U_S^n$.

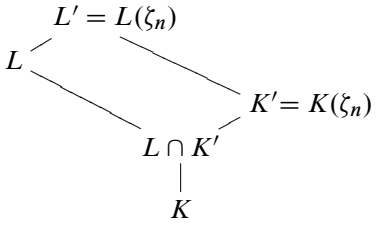
For a prime $\mathfrak{p} \notin S$ and $u \in U_S$, the definitions of the Kummer pairing and the Frobenius automorphism yield

$$\langle \mathrm{Frob}_{\mathfrak{p}}, u \rangle = (u^{1/n})^{\mathrm{Frob}_{\mathfrak{p}}-1} \equiv u^{(N\mathfrak{p}-1)/n} \in k_{\mathfrak{p}}^*,$$

where $N\mathfrak{p} = \#k_{\mathfrak{p}}$ is the absolute norm of $\mathfrak{p}$. Thus $\langle \mathrm{Frob}_{\mathfrak{p}}, u \rangle$ is simply the power of ζ_n that is congruent to $u^{(N\mathfrak{p}-1)/n} \in k_{\mathfrak{p}}^*$. Even when $\mathfrak{p}$ is large, this is not an expensive discrete logarithm problem in $k_{\mathfrak{p}}^*$, since in practice the exponent $n \leq [L : K]$ is small: one can simply check all powers of $\overline{\zeta}_n \in k_{\mathfrak{p}}^*$. Since $\langle \zeta_n \rangle$ reduces injectively modulo primes $\mathfrak{p} \nmid n$, the n-root of unity $\langle \mathrm{Frob}_{\mathfrak{p}}, u \rangle$ can be recovered from its value in $k_{\mathfrak{p}}^*$.

From the values $\langle \mathrm{Frob}_{\mathfrak{p}}, u \rangle$, we compute all symbols $\langle \psi_{N/K}(\mathfrak{a}), u \rangle$ by linearity. It is now a standard computation in linear algebra to find generators for the subgroup $V_L/U_S^n \subset U_S/U_S^n$ that is annihilated by the ideals $\mathfrak{a} \in \Sigma_L$ under the pairing (5-6). This yields explicit generators for the Kummer extension $L = K(\sqrt[n]{V_L})$, and concludes the computation of L in the case where K contains ζ_n, with n the exponent of $\mathrm{Gal}(L/K)$.

Case 2: K does not contain ζ_n. In this case L is not a Kummer extension of K, but $L' = L(\zeta_n)$ is a Kummer extension of $K' = K(\zeta_n)$.



(5-7)

To find generators of L' over K' by the method of Case 1, we need to 'lift' the class field theoretic data from K to K' to describe L' as a class field of K'. Lifting the modulus $\mathfrak{f} = \mathfrak{f}_0\mathfrak{f}_\infty$ for $K \subset L$ is easy: as K' is totally complex, $\mathfrak{f}' = \mathfrak{f}_0\mathbb{Z}_{K'}$ is admissible for $K' \subset L'$. From the definition of the Frobenius automorphism, it is immediate that we have a commutative diagram

$$\begin{array}{ccc} I_{K',\mathfrak{f}'} & \xrightarrow{\text{Artin}} & \mathrm{Gal}(L'/K') \\ \downarrow{\scriptstyle N_{K'/K}} & & \downarrow{\scriptstyle \text{res}} \\ I_{K,\mathfrak{f}} & \xrightarrow{\text{Artin}} & \mathrm{Gal}(L/K) \end{array}$$

As the restriction map on the Galois groups is injective, we see that the inverse norm image $N_{K'/K}^{-1} A_{\mathfrak{f}} \subset I_{K',\mathfrak{f}'}$ is the ideal group of K' corresponding to the extension $K' \subset L'$. Because $N_{K'/K}^{-1} A_{\mathfrak{f}}$ contains $P_{K',\mathfrak{f}'}$, computing this inverse image takes place inside the finite group $\mathrm{Cl}_{K',\mathfrak{f}'}$, a ray class group for K'.

We perform the algorithm from Case 1 for the extension $K' \subset L'$ to find generators of L' over K'. We are then working with (ray) class groups and S-units in K' rather than in K, and S has to satisfy Lemma 5.4 condition (2) for $\mathrm{Cl}_{K'}$. All this is only feasible if K' is of moderate degree, and this seriously restricts the values of n one can handle in practice. Our earlier observation that we may decompose $I_{\mathfrak{f}}/A_{\mathfrak{f}} \cong \mathrm{Gal}(L/K)$ into a product of cyclic groups of prime power order and generate L accordingly as a compositum of cyclic extensions of K is particularly relevant in this context, as it reduces our problem to a number of instances where $K \subset L$ is cyclic of prime power degree. Current implementations [Fieker 2001] deal with prime power values up to 20.

We further assume for simplicity that we are indeed in the case where $K \subset L$ is cyclic of prime power degree n, with $K' = K(\zeta_n) \neq K$. Suppose that, using the algorithm from Case 1, we have computed a Kummer generator $\theta \in L'$ for which we have $L' = K'(\theta) = K(\zeta_n, \theta)$ and $\theta^n = \alpha \in K'$. We then need to 'descend' θ efficiently to a generator η of L over K. If n is prime, one has

$L = K(\eta)$ for the trace

$$\eta = \mathrm{Tr}_{L'/L}(\theta). \tag{5-8}$$

For prime powers this does not work in all cases. One can however replace θ by $\theta + k\zeta_n$ for some small integer $k \in \mathbb{Z}$ to ensure that θ generates L' over K, and then general field theory tells us that the coefficients of the irreducible polynomial

$$f_L^\theta = \prod_{\tau \in \mathrm{Gal}(L'/L)} (X - \tau(\theta)) \in L[X] \tag{5-9}$$

of θ over L generate L over K. As we took $K \subset L$ to be cyclic of prime power degree, one of the coefficients is actually a generator, and in practice the trace works. In all cases, one needs an explicit description of the action of the Galois group $\mathrm{Gal}(L'/L)$ on θ and ζ_n in order to compute the trace (5-8), and possibly other coefficients of f_L^θ in (5-9). Finally, if we have $L = K(\eta)$, we need the action of $\mathrm{Gal}(L/K)$ on η in order to write down the generating polynomial

$$f_K^\eta = \prod_{\sigma \in \mathrm{Gal}(L/K)} (X - \sigma(\eta)) \in K[X]$$

for $K \subset L$ that we are after.

As before, the Artin map gives us complete control over the action of the abelian Galois group $\mathrm{Gal}(L'/K)$ on $L' = K(\zeta_n, \theta)$, provided that we describe the elements of $\mathrm{Gal}(L'/K)$ as Artin symbols. We let $\mathfrak{m}$ be an admissible modulus for $K \subset L'$; the least common multiple of $\mathfrak{f}_{L/K}$ and $n \cdot \prod_{\mathfrak{p}\ \mathrm{real}} \mathfrak{p}$ is an obvious choice for $\mathfrak{m}$. All we need to know is the explicit action of the Frobenius automorphism $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L'/K)$ of a prime $\mathfrak{p} \nmid \mathfrak{m}$ of K on the generators ζ_n and θ of L' over K. Note that $\mathfrak{p}$ does not divide n, and that we may assume that $\alpha = \theta^n$ is a unit at $\mathfrak{p}$.

The cyclotomic action of $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L'/K)$ is given by $\mathrm{Frob}_\mathfrak{p}(\zeta_n) = \zeta_n^{N\mathfrak{p}}$, with $N\mathfrak{p} = \#k_\mathfrak{p}$ the absolute norm of $\mathfrak{p}$. This provides us with the Galois action on K' and yields canonical isomorphisms

$$\mathrm{Gal}(K'/K) \cong \mathrm{im}[N_{K/\mathbb{Q}} : I_\mathfrak{m} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*],$$
$$\mathrm{Gal}(K'/(L \cap K')) \cong \mathrm{im}[N_{K/\mathbb{Q}} : A_\mathfrak{m} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*].$$

In order to understand the action of $\mathrm{Frob}_\mathfrak{p}$ on $\theta = \sqrt[n]{\alpha}$, we first observe that $K \subset L' = K'(\theta)$ can only be abelian if α is in the *cyclotomic* eigenspace of $(K')^*$ modulo n-th powers under the action of $\mathrm{Gal}(K'/K)$. More precisely, applying (5-2) for $K' \subset L'$ with $\tau = \mathrm{Frob}_\mathfrak{p}$, we have $\mathrm{Frob}_\mathfrak{p} \cdot \sigma \cdot \mathrm{Frob}_\mathfrak{p}^{-1} = \sigma$ since $\mathrm{Gal}(L'/K)$ is abelian, and therefore

$$\langle \sigma, \mathrm{Frob}_\mathfrak{p}(\alpha) \rangle = \langle \sigma, \alpha \rangle^{\mathrm{Frob}_\mathfrak{p}} = \langle \sigma, \alpha \rangle^{N\mathfrak{p}} = \langle \sigma, \alpha^{N\mathfrak{p}} \rangle$$

for all $\sigma \in \mathrm{Gal}(L'/K')$. By (5-3), we conclude that

$$\mathrm{Frob}_{\mathfrak{p}}(\alpha) = \alpha^{N\mathfrak{p}} \cdot \gamma_{\mathfrak{p}}^{n} \tag{5-10}$$

for some element $\gamma_{\mathfrak{p}} \in K'$. Knowing how $\mathrm{Frob}_{\mathfrak{p}}$ acts on $\alpha \in K' = K(\zeta_n)$, we can compute $\gamma_{\mathfrak{p}}$ by extracting some n-th root of $\mathrm{Frob}_{\mathfrak{p}}(\alpha)\alpha^{-N\mathfrak{p}}$ in K'. The element $\gamma_{\mathfrak{p}}$ is only determined up to multiplication by n-th roots of unity by (5-10). Because we took α to be a unit at $\mathfrak{p}$, we have $\gamma_{\mathfrak{p}}^{n} \equiv 1 \bmod \mathfrak{p}$ by definition of the Frobenius automorphism, and so there is a unique element $\gamma_{\mathfrak{p}} \equiv 1 \bmod \mathfrak{p}$ satisfying (5-10). With this choice of $\gamma_{\mathfrak{p}}$, we have

$$\mathrm{Frob}_{\mathfrak{p}}(\theta) = \theta^{N\mathfrak{p}} \cdot \gamma_{\mathfrak{p}}$$

because the n-th powers of both quantities are the same by (5-10), and they are congruent modulo $\mathfrak{p}$. This provides us with the explicit Galois action of $\mathrm{Frob}_{\mathfrak{p}}$ on θ for unramified primes $\mathfrak{p}$.

The description of the Galois action on θ and ζ_n in terms of Frobenius symbols is all we need. The Galois group $\mathrm{Gal}(L'/L) \cong \mathrm{Gal}(K'/(L \cap K'))$, which we may identify with the subgroup $N_{K/\mathbb{Q}}(A_{\mathfrak{m}})$ of $(\mathbb{Z}/n\mathbb{Z})^*$, is either cyclic or, if n is a power of 2, generated by 2 elements. Picking one or two primes $\mathfrak{p}$ in $A_{\mathfrak{m}}$ with norms in suitable residue classes modulo n is all it takes to generate $\mathrm{Gal}(L'/L)$ by Frobenius automorphisms, and we can use these elements to descend θ to a generator η for L over K. We also control the Galois action of $\mathrm{Gal}(L/K) = I_{\mathfrak{m}}/A_{\mathfrak{m}}$ on η, and this makes it possible to compute the irreducible polynomial f_K^{η} for the generator η of L over K.

6. Class fields arising from complex multiplication

As we observed in Example 2.6.1, the ray class fields over the rational number field $\mathbb{Q}$ are the cyclotomic fields. For these fields, we have explicit generators over $\mathbb{Q}$ that arise 'naturally' as the values of the analytic function $q : x \mapsto e^{2\pi i x}$ on the unique archimedean completion $\mathbb{R}$ of $\mathbb{Q}$. The function q is periodic modulo the ring of integers $\mathbb{Z} \subset \mathbb{R}$ of $\mathbb{Q}$, and it induces an isomorphism

$$\begin{aligned} \mathbb{R}/\mathbb{Z} &\xrightarrow{\sim} T = \{z \in \mathbb{C} : z\bar{z} = 1\} \subset \mathbb{C} \\ x &\longmapsto q(x) = e^{2\pi i x} \end{aligned} \tag{6-1}$$

between the quotient group $\mathbb{R}/\mathbb{Z}$ and the 'circle group' T of complex numbers of absolute value 1. The Kronecker–Weber theorem 1.1 states that the values of the analytic function q at the points of the *torsion subgroup* $\mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z}$ generate the maximal abelian extension $\mathbb{Q}_{\mathrm{ab}}$ of $\mathbb{Q}$. More precisely, the q-values at the m-torsion subgroup $\frac{1}{m}\mathbb{Z}/\mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$ generate the m-th cyclotomic field $\mathbb{Q}(\zeta_m)$. Under this parametrization of roots of unity by $\mathbb{Q}/\mathbb{Z}$, the Galois action

on the m-torsion values comes from multiplications on $\frac{1}{m}\mathbb{Z}/\mathbb{Z}$ by integers $a \in \mathbb{Z}$ coprime to m, giving rise to the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \mathrm{Aut}(\tfrac{1}{m}\mathbb{Z}/\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})^* \tag{6-2}$$

from (1-2). Taking the projective limit over all m, one obtains the identification of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}/\mathbb{Q})$ with $\mathrm{Aut}(\mathbb{Q}/\mathbb{Z}) = \widehat{\mathbb{Z}}^*$ from (3-1), and we saw in Example 3.8 that the relation with the Artin isomorphism is given by the commutative diagram (3-8). To stress the analogy with the complex multiplication case, we rewrite (3-8) as

$$\begin{array}{ccc} \widehat{\mathbb{Z}}^* & \xrightarrow{\quad -1 \quad} & \widehat{\mathbb{Z}}^* = \mathbf{A}_{\mathbb{Q}}^*/(\mathbb{Q}^* \cdot \mathbb{R}_{>0}) \\ {\scriptstyle \mathrm{can}}\downarrow{\scriptstyle \sim} & & {\scriptstyle \mathrm{Artin}}\downarrow{\scriptstyle \sim} \\ \mathrm{Aut}(\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\ \sim\ } & \mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}/\mathbb{Q}) \end{array} \tag{6-3}$$

where -1 denotes inversion on $\widehat{\mathbb{Z}}^*$.

From now on, we take K to be an imaginary quadratic field. Then K has a single archimedean completion $K \to \mathbb{C}$, and much of what we said for the analytic function q on $\mathbb{R}/\mathbb{Z}$ has an analogue for the quotient group $\mathbb{C}/\mathbb{Z}_K$. In complete analogy, we will define an analytic function $f_K : \mathbb{C}/\mathbb{Z}_K \to \mathbb{P}^1(\mathbb{C})$ in (6-14) with the property that its finite values at the m-torsion subgroup $\frac{1}{m}\mathbb{Z}_K/\mathbb{Z}_K$ of $\mathbb{C}/\mathbb{Z}_K$ generate the ray class field H_m of K of conductor $m\mathbb{Z}_K$. However, to define this *elliptic function* f_K on the complex *elliptic curve* $\mathbb{C}/\mathbb{Z}_K$, we need an algebraic description of $\mathbb{C}/\mathbb{Z}_K$, which exists over an *extension* of K that is usually larger than K itself. The Hilbert class field $H = H_1$ of K from Example 2.6.2 is the smallest extension of K that one can use, and the torsion values of f_K generate class fields over H. This makes the construction of H itself into an important preliminary step that does not occur over $\mathbb{Q}$, as $\mathbb{Q}$ is its own Hilbert class field.

In this section, we give the classical algorithms for constructing the extensions $K \subset H$ and $H \subset H_m$. The next section provides some theoretical background and different views on complex multiplication. Our final Section 8 shows how such views lead to algorithmic improvements.

Complex multiplication starts with the fundamental observation [Silverman 1986, Chapter VI] that for every lattice $\Lambda \subset \mathbb{C}$, the complex torus $\mathbb{C}/\Lambda$ admits a meromorphic function, the Weierstrass $\wp$-function

$$\wp_\Lambda : z \mapsto z^{-2} + \textstyle\sum_{\omega \in \Lambda \setminus \{0\}} [(z-\omega)^{-2} - \omega^{-2}],$$

that has period lattice Λ and is holomorphic except for double poles at the points of Λ. The corresponding Weierstrass map

$$W : \mathbb{C}/\Lambda \longrightarrow E_\Lambda \subset \mathbb{P}^2(\mathbb{C}), \quad z \longmapsto [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1]$$

is a complex analytic isomorphism between the torus $\mathbb{C}/\Lambda$ and the complex elliptic curve $E_\Lambda \subset \mathbb{P}^2(\mathbb{C})$ defined by the affine Weierstrass equation

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

The Weierstrass coefficients

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-4} \quad \text{and} \quad g_3(\Lambda) = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-6} \tag{6-4}$$

of E_Λ are the *Eisenstein series* of weight 4 and 6 for the lattice Λ. The natural addition on $\mathbb{C}/\Lambda$ translates into an algebraic group structure on $E_\Lambda(\mathbb{C})$ sometimes referred to as 'chord and tangent addition'. On the Weierstrass model E_Λ, the point $O = [0 : 1 : 0] = W(0 \bmod \Lambda)$ at infinity is the zero point, and any line in $\mathbb{P}^2(\mathbb{C})$ intersects the curve E_Λ in 3 points, counting multiplicities, that have sum O.

All complex analytic maps $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ fixing the zero point are multiplications $z \mapsto \lambda z$ with $\lambda \in \mathbb{C}$ satisfying $\lambda\Lambda_1 \subset \Lambda_2$. These are clearly group homomorphisms, and in the commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda_1 & \xrightarrow{\lambda} & \mathbb{C}/\Lambda_2 \\ {\scriptstyle w_1}\downarrow{\scriptstyle \sim} & & {\scriptstyle w_1}\downarrow{\scriptstyle \sim} \\ E_{\Lambda_1} & \xrightarrow{\phi_\lambda} & E_{\Lambda_2} \end{array} \tag{6-5}$$

the corresponding maps $\phi_\lambda : E_{\Lambda_1} \longrightarrow E_{\Lambda_2}$ between algebraic curves are known as *isogenies*. For $\lambda \neq 0$, the isogeny ϕ_λ is a finite algebraic map of degree $[\Lambda_2 : \lambda\Lambda_1]$, and E_{Λ_1} and E_{Λ_2} are isomorphic as complex algebraic curves if and only if we have $\lambda\Lambda_1 = \Lambda_2$ for some $\lambda \in \mathbb{C}$. The isogenies $E_\Lambda \to E_\Lambda$ form the *endomorphism ring*

$$\mathrm{End}(E_\Lambda) = \{\lambda \in \mathbb{C} : \lambda\Lambda \subset \Lambda\} \tag{6-6}$$

of the curve E_Λ, which we can view as a discrete subring of $\mathbb{C}$. The λ-value of the analytically defined endomorphism 'multiplication by $\lambda \in \mathbb{C}$' is reflected algebraically as a true multiplication by λ of the *invariant differential* dx/y on E_Λ coming from $dz = d(\wp_\Lambda)/\wp'_\Lambda$. If $\mathrm{End}(E_\Lambda)$ is strictly larger than $\mathbb{Z}$, it is a complex quadratic order $\mathbb{O}$ and E_Λ is said to have *complex multiplication* (CM) by $\mathbb{O}$.

To generate the class fields of our imaginary quadratic field K, we employ an elliptic curve E_Λ having CM by $\mathbb{Z}_K$. Such a curve can be obtained by taking Λ equal to $\mathbb{Z}_K$ or to a fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$, but the Weierstrass coefficients (6-4) for $\Lambda = \mathfrak{a}$ will not in general be algebraic.

In order to find an *algebraic* model for the complex curve E_Λ, we scale Λ to a *homothetic* lattice $\lambda\Lambda$ to obtain a $\mathbb{C}$-isomorphic model

$$E_{\lambda\Lambda} : y^2 = 4x^3 - \lambda^{-4} g_2(\Lambda)x - \lambda^{-6} g_3(\Lambda)$$

under the Weierstrass map. The discriminant $\Delta = g_2^3 - 27g_3^2$ of the Weierstrass polynomial $4x^3 - g_2 x - g_3$ does not vanish, and the lattice function

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$$

is of weight 12: it satisfies $\Delta(\lambda\Lambda) = \lambda^{-12}\Delta(\Lambda)$. Thus, the j-invariant

$$j(\Lambda) = 1728\,\frac{g_2(\Lambda)^3}{\Delta(\Lambda)} = 1728\,\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} \tag{6-7}$$

is of weight zero and is an invariant of the homothety class of Λ or, equivalently, the isomorphism class of the complex elliptic curve $\mathbb{C}/\Lambda$. It generates the minimal field of definition over which $\mathbb{C}/\Lambda$ admits a Weierstrass model.

If E_Λ has CM by $\mathbb{Z}_K$, then Λ is homothetic to some $\mathbb{Z}_K$-ideal $\mathfrak{a}$. It follows that, up to isomorphism, there are only finitely many complex elliptic curves E_Λ having CM by $\mathbb{Z}_K$, one for each ideal class in Cl_K. Because any automorphism of $\mathbb{C}$ maps the algebraic curve E_Λ to an elliptic curve with the same endomorphism ring, we find that the j-invariants of the ideal classes of $\mathbb{Z}_K$ form a set of $h_K = \#\mathrm{Cl}_K$ distinct *algebraic* numbers permuted by the absolute Galois group $G_\mathbb{Q}$ of $\mathbb{Q}$. This allows us to define the *Hilbert class polynomial* of K as

$$\mathrm{Hil}_K(X) = \prod_{[\mathfrak{a}]\in\mathrm{Cl}_K} (X - j(\mathfrak{a})) \in \mathbb{Q}[X]. \tag{6-8}$$

Its importance stems from the following theorem, traditionally referred to as the *first main theorem of complex multiplication.*

THEOREM 6.9. *The Hilbert class field H of K is the splitting field of the polynomial* $\mathrm{Hil}_K(X)$ *over K. This polynomial is irreducible in $K[X]$, and the Galois action of the Artin symbol $\sigma_\mathfrak{c} = \psi_{H/K}(\mathfrak{c})$ of the ideal class $[\mathfrak{c}] \in \mathrm{Cl}_K \cong \mathrm{Gal}(H/K)$ on the roots $j(\mathfrak{a})$ of* $\mathrm{Hil}_K(X)$ *is given by $j(\mathfrak{a})^{\sigma_\mathfrak{c}} = j(\mathfrak{a}\mathfrak{c}^{-1})$.*

To compute $\mathrm{Hil}_K(X)$ from its definition (6-8), one compiles a list of $\mathbb{Z}_K$-ideal classes in the style of Gauss, who did this in terms of binary quadratic forms. Every $\mathbb{Z}_K$-ideal class $[\mathfrak{a}]$ has a representative of the form $\mathbb{Z}\tau + \mathbb{Z}$, with $\tau \in K$ a root of some irreducible polynomial $aX^2 + bX + c \in \mathbb{Z}[X]$ of discriminant $b^2 - 4ac = \Delta_{K/\mathbb{Q}}$. If we take for τ the root in the complex upper half plane $\mathbf{H}$, the *orbit* of τ under the natural action

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}(z) = \frac{\alpha z + \beta}{\gamma z + \delta}$$

of the modular group $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbf{H}$ is uniquely determined by $[\mathfrak{a}] \in \mathrm{Cl}_K$. In this orbit, there is a unique element

$$\tau_{\mathfrak{a}} = \frac{-b+\sqrt{b^2-4ac}}{2a} \in \mathbf{H}$$

that lies in the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbf{H}$ consisting of those $z \in \mathbf{H}$ that satisfy the two inequalities $|\mathrm{Re}(z)| \leq \frac{1}{2}$ and $z\bar{z} \geq 1$ and, in case we have equality in either of them, also $\mathrm{Re}(z) \leq 0$. This yields a description

$$[\mathfrak{a}] = \left[\mathbb{Z} \cdot \frac{-b+\sqrt{b^2-4ac}}{2a} + \mathbb{Z}\right] \qquad \longleftrightarrow \qquad (a,b,c)$$

of the elements of Cl_K as *reduced* integer triples (a,b,c) whose discriminant is $b^2-4ac = \Delta_{K/\mathbb{Q}}$. As we have $\mathrm{Re}(\tau_{\mathfrak{a}}) = -b/2a$ and $\tau_{\mathfrak{a}}\bar{\tau}_{\mathfrak{a}} = c/a$, the reduced integer triples (a,b,c) corresponding to $\tau_{\mathfrak{a}}$ in the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ are those satisfying

$$|b| \leq a \leq c \qquad \text{and} \qquad b^2-4ac = \Delta_{K/\mathbb{Q}},$$

where b is nonnegative if $|b| = a$ or $a = c$. For reduced forms, one sees from the inequality $\Delta_{K/\mathbb{Q}} = b^2-4ac \leq a^2-4a^2 = -3a^2$ that we have bounds $|b| \leq a \leq \sqrt{|\Delta_{K/\mathbb{Q}}|/3}$, so the list is indeed finite and can easily be generated [Cohen 1993, Algorithm 5.3.5]. See [Cox 1989] for the classical interpretation of the triples (a,b,c) as positive definite integral binary quadratic forms $aX^2+bXY+cY^2$ of discriminant $b^2-4ac = \Delta_{K/\mathbb{Q}}$.

If we put $j(\tau) = j(\mathbb{Z}\tau+\mathbb{Z})$, the j-function (6-7) becomes a holomorphic function $j : \mathbf{H} \to \mathbb{C}$ invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. As it is in particular invariant under $\tau \mapsto \tau+1$, it can be expressed in various ways in terms of the variable $q = e^{2\pi i\tau}$ from (6-1). Among them is the well-known *integral* Fourier expansion

$$j(\tau) = j(q) = q^{-1}+744+196884q+\ldots \in q^{-1}+\mathbb{Z}[[q]] \tag{6-10}$$

that explains the normalizing factor 1728 in the definition (6-7) of j. It implies [Lang 1987, Chapter 5, §2] that the roots of $\mathrm{Hil}_K(X)$ in (6-8) are algebraic integers, and so $\mathrm{Hil}_K(X)$ is a polynomial in $\mathbb{Z}[X]$ that can be computed *exactly* from complex approximations of its roots that are sufficiently accurate to yield the right hand side of (6-8) in $\mathbb{C}[X]$ to 'one-digit precision'. For numerical computations of $j(\tau)$, one uses approximate values of the Dedekind η-function

$$\eta(\tau) = q^{1/24}\prod_{n\geq 1}(1-q^n) = q^{1/24}\sum_{n\in\mathbb{Z}}(-1)^n q^{n(3n-1)/2}, \tag{6-11}$$

which has a lacunary Fourier expansion that is better suited for numerical purposes than (6-10). From η-values one computes $\mathfrak{f}_2(\tau) = \sqrt{2}\eta(2\tau)/\eta(\tau)$ and finally $j(\tau)$ as

$$j(\tau) = \frac{(\mathfrak{f}_2^{24}(\tau) + 16)^3}{\mathfrak{f}_2^{24}(\tau)}. \tag{6-12}$$

This finishes the description of the classical algorithm to compute the Hilbert class field H of K.

Having computed the irreducible polynomial $\mathrm{Hil}_K(X)$ of $j_K = j(\mathbb{Z}_K)$, we can write down a Weierstrass model E_K for $\mathbb{C}/\mathbb{Z}_K$ over $H = K(j_K)$ (or even over $\mathbb{Q}(j_K)$) and use it to generate the ray class field extensions $H \subset H_m$. Choosing E_K is easy in the special cases $K = \mathbb{Q}(\zeta_3), \mathbb{Q}(i)$, when one of $g_2 = g_2(\mathbb{Z}_K)$ and $g_3 = g_3(\mathbb{Z}_K)$ vanishes and the other can be scaled to have any nonzero rational value. For $K \neq \mathbb{Q}(\zeta_3), \mathbb{Q}(i)$, the number $\lambda = \sqrt{g_3/g_2} \in \mathbb{C}^*$ is determined up to sign, and since we have

$$c_K = \lambda^{-4} g_2 = \lambda^{-6} g_3 = g_2^3 g_3^{-2} = 27\frac{j_K}{j_K - 1728},$$

the model $y^2 = 4x^3 - c_K x - c_K$ for $\mathbb{C}/\lambda\mathbb{Z}_K$ is defined over $\mathbb{Q}(j_K) \subset H$. A more classical choice is $\lambda^2 = \Delta/(g_2 g_3)$, with g_2, g_3 and Δ associated to $\mathbb{Z}_K$, giving rise to the model

$$E_K : y^2 = w_K(x) = 4x^3 - \frac{c_K}{(c_K - 27)^2}x - \frac{c_K}{(c_K - 27)^3}. \tag{6-13}$$

Any scaled Weierstrass parametrization $W_K : \mathbb{C}/\mathbb{Z}_K \xrightarrow{\sim} E_K$ with E_K defined over H can serve as the imaginary quadratic analogue of the isomorphism $q : \mathbb{R}/\mathbb{Z} \xrightarrow{\sim} T$ in (6-1). For the model E_K in (6-13), the x-coordinate $\wp_{\lambda\mathbb{Z}_K}(\lambda z) = \lambda^{-2}\wp_{\mathbb{Z}_K}(z)$ of $W_K(z)$ is given by the *Weber function*

$$f_K(z) = \frac{g_2(\mathbb{Z}_K)g_3(\mathbb{Z}_K)}{\Delta(\mathbb{Z}_K)}\wp_{\mathbb{Z}_K}(z). \tag{6-14}$$

It has 'weight 0' in the sense that the right side is invariant under simultaneous scaling $(\mathbb{Z}_K, z) \to (\lambda\mathbb{Z}_K, \lambda z)$ by $\lambda \in \mathbb{C}^*$ of the lattice $\mathbb{Z}_K$ and the argument z.

In the special cases $K = \mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_3)$ that have $\mathbb{Z}_K^*$ of order 4 and 6, there are slightly different Weber functions f_K that are not the x-coordinates on a Weierstrass model for $\mathbb{C}/\mathbb{Z}_K$ over H, but an appropriately scaled *square* and *cube* of such x-coordinates, respectively. In all cases, the analogue of the Kronecker–Weber theorem for K is the following *second main theorem of complex multiplication*.

THEOREM 6.15. *The ray class field H_m of conductor $m\mathbb{Z}_K$ of K is generated over the Hilbert class field H of K by the values of the Weber function f_K at the nonzero m-torsion points of $\mathbb{C}/\mathbb{Z}_K$.*

In the non-special cases, the values of f_K at the m-torsion points of $\mathbb{C}/\mathbb{Z}_K$ are the x-coordinates of the nonzero m-torsion points of the elliptic curve E_K in (6-13). For $K = \mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_3)$, one uses squares and cubes of these coordinates. In all cases, generating H_m over H essentially amounts to computing *division polynomials* $T_m \in \mathbb{C}[X]$ that have these x-coordinates as their roots. We will define these polynomials as elements of $H[x]$, because the recursion formulas at the end of this section show that their coefficients are elements of the ring generated over $\mathbb{Z}$ by the coefficients of the Weierstrass model of E_K.

If m is odd, the nonzero m-torsion points come in pairs $\{P, -P\}$ with the same x-coordinate $x_P = x_{-P}$, and we can define a polynomial $T_m(x) \in H[x]$ of degree $(m^2-1)/2$ up to sign by

$$T_m(x)^2 = m^2 \prod_{\substack{P \in E_K[m](\mathbb{C}),\\ P \neq O}} (x - x_P).$$

For even m, we adapt the definition by excluding the 2-torsion points satisfying $P = -P$ from the product, and define $T_m(X) \in H[x]$ of degree $(m^2-4)/2$ by

$$T_m(x)^2 = (m/2)^2 \prod_{\substack{P \in E_K[m](\mathbb{C}),\\ 2P \neq O}} (x - x_P).$$

The 'missing' x-coordinates of the nonzero 2-torsion points are the zeros of the cubic polynomial $w_K \in H[x]$ in (6-13). This is a square in the *function field* of the elliptic curve (6-13), and in many ways the natural object to consider is the 'division polynomial'

$$\psi_m(x, y) = \begin{cases} T_m(x) & \text{if } m \text{ is odd;} \\ 2yT_m(x) & \text{if } m \text{ is even.} \end{cases}$$

This is an element of the function field $\mathbb{C}(x, y)$ living in the quadratic extension $H[x, y]$ of the polynomial ring $H[x]$ defined by $y^2 = w_K(x)$. It is uniquely defined up to the sign choice we have for T_m. Most modern texts take the sign of the highest coefficient of T_m equal to 1. Weber [1908, p. 197] takes it equal to $(-1)^{m-1}$, which amounts to a sign change $y \mapsto -y$ in $\psi_m(x, y)$.

By construction, the function ψ_m has divisor $(1-m^2)[O]+\sum_{P\neq O,\, mP=O}[P]$. The normalizing highest coefficients m and $m/2$ in T_m lead to neat recursive

formulas

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m+1}^3\psi_{m-1},$$
$$\psi_{2m} = (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m+1}^2\psi_{m-2})$$

for ψ_m that are valid for $m > 1$ and $m > 2$. These can be used to compute ψ_m and T_m recursively, using 'repeated doubling' of m. One needs the initial values $T_1 = T_2 = 1$ and

$$T_3 = 3X^4 + 6aX^2 + 12bX - a^2,$$
$$T_4 = 2X^6 + 10aX^4 + 40bX^3 - 10a^2X^2 - 8abX - 16b^2 - 2a^3,$$

where we have written the Weierstrass polynomial in (6-13) as $w_K = 4(x^3 + ax + b)$ to indicate the relation with the nowadays more common affine model $y^2 = x^3 + ax + b$ to which E_K is isomorphic under $(x, y) \mapsto (x, y/2)$.

7. Class fields from modular functions

The algorithms in the previous section are based on the main Theorems 6.9 and 6.15 of complex multiplication, which can be found already in Weber's textbook [1908] and predate the class field theory for general number fields. The oldest proofs of 6.9 and 6.15 are of an analytic nature, and derive arithmetic information from congruence properties of Fourier expansions such as (6-10). Assuming general class field theory, one can shorten these proofs as it suffices, just as after Theorem 2.2, to show that, up to sets of primes of zero density, the 'right' primes split completely in the purported class fields. In particular, it is always possible to restrict attention to the primes of K of residue degree one in such arguments. Deuring [1958] provides analytic proofs of both kinds in his survey monograph.

Later proofs [Lang 1987, Part 2] of Deuring and Shimura combine class field theory with the *reduction* of the endomorphisms in (6-6) modulo primes, which yields endomorphisms of elliptic curves over finite fields. These proofs are firmly rooted in the algebraic theory of elliptic curves [Silverman 1986; Silverman 1994]. Here one takes for E_Λ in (6-6) an elliptic curve E that has CM by $\mathbb{Z}_K$ and is given by a Weierstrass equation over the splitting field H' over K of the Hilbert class polynomial $\mathrm{Hil}_K(X)$ in (6-8). In this case the Weierstrass equation can be considered modulo any prime $\mathfrak{q}$ of H', and for almost all primes, known as the primes *of good reduction*, this yields an elliptic curve $E_\mathfrak{q} = E \bmod \mathfrak{q}$ over the finite field $k_\mathfrak{q} = \mathbb{Z}_{H'}/\mathfrak{q}$. For such $\mathfrak{q}$, the choice of an extension of $\mathfrak{q}$ to $\overline{\mathbb{Q}}$ yields a reduction homomorphism $E_K(\overline{\mathbb{Q}}) \to E_\mathfrak{q}(\bar{k}_\mathfrak{q})$ on points that is *injective* on torsion points of order coprime to $\mathfrak{q}$. The endomorphisms of E are given by rational functions with coefficients in H', and for

primes $\mathfrak{q}$ of H' of good reduction there is a natural reduction homomorphism

$$\mathrm{End}(E) \to \mathrm{End}(E_{\mathfrak{q}})$$

that is injective and preserves degrees. The 'complex multiplication' by an element $\alpha \in \mathrm{End}(E) = \mathbb{Z}_K$ multiplies the invariant differential dx/y on E by α, so it becomes inseparable in $\mathrm{End}(E_{\mathfrak{q}})$ if and only if $\mathfrak{q}$ divides α. The first main theorem of complex multiplication (Theorem 6.9), which states that H' equals the Hilbert class field H of K and provides the Galois action on the roots of $\mathrm{Hil}_K(X)$, can now be derived as follows.

PROOF OF THEOREM 6.9. Let $\mathfrak{p}$ be a prime of degree one of K that is coprime to the discriminant of $\mathrm{Hil}_K(X)$, and let $\alpha \in \mathbb{Z}_K$ be an element of order 1 at $\mathfrak{p}$, say $\alpha\mathfrak{p}^{-1} = \mathfrak{b}$ with $(\mathfrak{b}, \mathfrak{p}) = 1$. Let $\mathfrak{a}$ be a fractional $\mathbb{Z}_K$-ideal. Then the complex multiplication $\alpha : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}$ factors in terms of complex tori as

$$\mathbb{C}/\mathfrak{a} \xrightarrow{\mathrm{can}} \mathbb{C}/\mathfrak{a}\mathfrak{p}^{-1} \xrightarrow[\alpha]{\sim} \mathbb{C}/\mathfrak{a}\mathfrak{b} \xrightarrow{\mathrm{can}} \mathbb{C}/\mathfrak{a}.$$

If E and E' denote Weierstrass models over H' for $\mathbb{C}/\mathfrak{a}$ and $\mathbb{C}/\mathfrak{a}\mathfrak{p}^{-1}$, we obtain isogenies $E \to E' \to E$ of degree $p = N\mathfrak{p}$ and $N\mathfrak{b}$ with composition α. If we assume that E and E' have good reduction above $\mathfrak{p}$, we can reduce the isogeny $E \to E'$ at some prime $\mathfrak{q}|\mathfrak{p}$ to obtain an isogeny $E_{\mathfrak{q}} \to E'_{\mathfrak{q}}$ of degree p. This isogeny is inseparable as α lies in $\mathfrak{q}$, and therefore equal to the Frobenius morphism $E_{\mathfrak{q}} \to E_{\mathfrak{q}}^{(p)}$ followed by an isomorphism $E_{\mathfrak{q}}^{(p)} \xrightarrow{\sim} E'_{\mathfrak{q}}$. The result is an equality $j(E_{\mathfrak{q}}^{(p)}) = j(E'_{\mathfrak{q}})$ of j-invariants that amounts to $j(\mathfrak{a})^p = j(\mathfrak{a}\mathfrak{p}^{-1})$ mod $\mathfrak{q}$, and this implies the Frobenius automorphism $\sigma_{\mathfrak{q}} \in \mathrm{Gal}(H'/K)$ acts as $j(\mathfrak{a})^{\sigma_{\mathfrak{q}}} = j(\mathfrak{a}\mathfrak{p}^{-1})$, independent of the choice of the extension prime $\mathfrak{q}|\mathfrak{p}$. Because the j-function is an invariant for the homothety class of a lattice, we have $j(\mathfrak{a}) = j(\mathfrak{a}\mathfrak{p}^{-1})$ if and only if $\mathfrak{p}$ is principal. It follows that up to finitely many exceptions, the primes $\mathfrak{p}$ of degree one splitting completely in $K \subset H'$ are the principal primes, so H' equals the Hilbert class field H of K, and the splitting primes in $K \subset H$ are *exactly* the principal primes. Moreover, we have $j(\mathfrak{a})^{\sigma_{\mathfrak{c}}} = j(\mathfrak{a}\mathfrak{c}^{-1})$ for the action of the Artin symbol $\sigma_{\mathfrak{c}}$, and Hil_K is irreducible over K as its roots are transitively permuted by $\mathrm{Gal}(H/K) = \mathrm{Cl}_K$. □

In a similar way, one can understand the content of the second main theorem of complex multiplication. If E_K is a Weierstrass model for $\mathbb{C}/\mathbb{Z}_K$ defined over the Hilbert class field H of K, then the torsion points in $E_K(\mathbb{C})$ have algebraic coordinates. As the group law is given by algebraic formulas over H, the absolute Galois group G_H of H acts by group automorphisms on

$$E_K^{\mathrm{tor}}(\mathbb{C}) \cong K/\mathbb{Z}_K.$$

Moreover, the action of G_H commutes with the complex multiplication action of $\mathrm{End}(E_K) \cong \mathbb{Z}_K$, which is given by isogenies defined over H. It follows that

G_H acts by $\mathbb{Z}_K$-module automorphisms on $E_K^{\mathrm{tor}}(\mathbb{C})$. For the cyclic $\mathbb{Z}_K$-module $E_K[m](\mathbb{C}) \cong \frac{1}{m}\mathbb{Z}_K/\mathbb{Z}_K$ of m-torsion points, the resulting Galois representation

$$G_H \longrightarrow \mathrm{Aut}_{\mathbb{Z}_K}(\tfrac{1}{m}\mathbb{Z}_K/\mathbb{Z}_K) \cong (\mathbb{Z}_K/m\mathbb{Z}_K)^*$$

of G_H is therefore *abelian*. It shows that, just as in the cyclotomic case (6-2), the Galois action *over* H on the *m-division field* of E_K, which is the extension of H generated by the m-torsion points of E_K, comes from *multiplications* on $\frac{1}{m}\mathbb{Z}_K/\mathbb{Z}_K$ by integers $\alpha \in \mathbb{Z}_K$ coprime to m. The content of Theorem 6.15 is that, in line with (2-8), we obtain the m-th ray class field of K from this m-division field by taking invariants under the action of $\mathbb{Z}_K^* = \mathrm{Aut}(E_K)$. In the 'generic case' where $\mathbb{Z}_K^* = \{\pm 1\}$ has order 2, adjoining m-torsion points 'up to inversion' amounts to the equality

$$H_m = H\big(\{x_P : P \in E_K[m](\mathbb{C}),\, P \neq O\}\big) \tag{7-1}$$

occurring in Theorem 6.15, since the x-coordinate x_P determines P up to multiplication by ± 1. More generally, a root of unity $\zeta \in \mathbb{Z}_K^*$ acts as an automorphism of E_K by $x_{[\zeta]P} = \zeta^{-2}x_P$, and so in the special cases where K equals $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$ and $\mathbb{Z}_K^*$ has order $2k$ with $k = 2, 3$, one replaces x_P by x_P^k in (7-1). The classical Weber functions replacing (6-14) for $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\zeta_3)$ are $f_K(z) = (g_2^2(\mathbb{Z}_K)/\Delta(\mathbb{Z}_K))\wp_{\mathbb{Z}_K}^2(z)$ and $f_K(z) = (g_3(\mathbb{Z}_K)/\Delta(\mathbb{Z}_K))\wp_{\mathbb{Z}_K}^3(z)$.

PROOF OF THEOREM 6.15. As in the case of Theorem 6.9, we show that the primes of degree one of K that split completely in the extension $K \subset H'_m$ defined by adjoining to H the m-torsion points of E_K 'up to automorphisms' are, up to a zero density subset of primes, the primes in the ray group R_m. Primes $\mathfrak{p}$ of K splitting in H'_m are principal as they split in H. For each $\mathbb{Z}_K$-generator π of $\mathfrak{p}$, which is uniquely determined up to multiplication by $\mathbb{Z}_K^*$, one obtains a complex multiplication by $\pi \in \mathbb{Z}_K \cong \mathrm{End}(E_K)$ that fixes $E_K[m](\mathbb{C})$ 'up to automorphisms' if and only if $\mathfrak{p} \in R_m$.

Let $\mathfrak{p} = \pi\mathbb{Z}_K$ be a prime of degree 1 over p for which E_K has good reduction modulo $\mathfrak{p}$. Then the isogeny $\phi_\pi : E_K \to E_K$, which corresponds to multiplication by π as in (6-5), reduces modulo a prime $\mathfrak{q}|\mathfrak{p}$ of the m-division field of E_K to an endomorphism of degree p. Since π is in $\mathfrak{q}$, this reduction is inseparable, and so it equals the Frobenius endomorphism of $E_{K,\mathfrak{q}}$ up to an automorphism. One shows [Lang 1987, p. 125] that this *local* automorphism of $E_{K,\mathfrak{q}}$ is induced by a global automorphism of E_K, that is, a complex multiplication by a unit in $\mathbb{Z}_K^*$, and concludes that ϕ_π induces a Frobenius automorphism above $\mathfrak{p}$ on H'_m. As the reduction modulo $\mathfrak{q}$ induces an isomorphism $E_K[m] \xrightarrow{\sim} E_{K,\mathfrak{q}}[m]$ on the m-torsion points, this Frobenius automorphism is trivial if and only if we have $\pi \equiv 1 \bmod^* m\mathbb{Z}_K$ for a suitable choice of π. Thus, $\mathfrak{p}$ splits completely in H'_m if and only if $\mathfrak{p}$ is in R_m, and H'_m is the ray class field H_m. □

The argument just given shows that we have a concrete realization of the Artin isomorphism $(\mathbb{Z}_K/m\mathbb{Z}_K)^*/\mathrm{im}[\mathbb{Z}_K^*] \xrightarrow{\sim} \mathrm{Gal}(H_m/H)$ from (2-8) by complex multiplications. Passing to the projective limit, this yields the analogue

$$\widehat{\mathbb{Z}}_K^*/\mathbb{Z}_K^* \xrightarrow{\sim} \mathrm{Gal}(K_{\mathrm{ab}}/H) \subset G_K^{\mathrm{ab}}$$

of (3-1). For the analogue of (6-3), we note first that for imaginary quadratic K, the subgroup U_∞ in (3-3), which equals $\mathbb{C}^*$, maps isomorphically to the connected component of the unit element in $\mathbf{A}_K^*/K^*$. Because it is the kernel of the Artin map ψ_K in (3-7), we obtain a commutative diagram

$$\begin{array}{ccccc} \widehat{\mathbb{Z}}_K^* & \xrightarrow{-1} & \mathbb{Z}_K^*/\mathbb{Z}_K^* & \subset & \mathbf{A}_K^*/(K^*\cdot\mathbb{C}^*) \\ {\scriptstyle\mathrm{can}}\downarrow\sim & & \downarrow\sim & & {\scriptstyle\mathrm{Artin}}\downarrow\sim \\ \mathrm{Aut}_{\mathbb{Z}_K}(K/\mathbb{Z}_K) & \longrightarrow & \mathrm{Gal}(K_{\mathrm{ab}}/H) & \subset & \mathrm{Gal}(K_{\mathrm{ab}}/K) \end{array} \tag{7-2}$$

in which the inversion map -1 arises just as in (3-8). A slight difference with the diagram (6-3) for $\mathbb{Q}$ is that the horizontal arrows now have a small finite kernel coming from the unit group $\mathbb{Z}_K^*$. Moreover, we have only accounted for the automorphisms of K_{ab} over H, not over K. Automorphisms of H_m that are not the identity on H arise as Artin maps $\sigma_{\mathfrak{c}}$ of nonprincipal ideals $\mathfrak{c}$ coprime to m, and the proof of Theorem 6.9 shows that for the isogeny $\phi_{\mathfrak{c}}$ in the commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\mathbb{Z}_K & \xrightarrow{\mathrm{can}} & \mathbb{C}/\mathfrak{c}^{-1} \\ w\downarrow\sim & & w'\downarrow\sim \\ E_K & \xrightarrow{\phi_{\mathfrak{c}}} & E'_K, \end{array} \tag{7-3}$$

we have to compute the restriction $\phi_{\mathfrak{c}} : E_K[m] \to E'_K[m]$ to m-torsion points. To do so in an efficient way, we view the j-values and x-coordinates of torsion points involved as weight zero functions on complex lattices such as $\mathbb{Z}_K$ or $\mathfrak{c}$. As we may scale all lattices as we did for (6-10) to $\mathbb{Z}\tau + \mathbb{Z}$ with $\tau \in \mathbf{H}$, such functions are *modular functions* $\mathbf{H} \to \mathbb{C}$ as defined in [Lang 1987, Chapter 6].

The j-function itself is the primordial modular function: a holomorphic function on $\mathbf{H}$ that is invariant under the full modular group $\mathrm{SL}_2(\mathbb{Z})$. Every meromorphic function on $\mathbf{H}$ that is invariant under $\mathrm{SL}_2(\mathbb{Z})$ and, when viewed as a function of $q = e^{2\pi i\tau}$, meromorphic in $q = 0$, is in fact a rational function of j. The Weber function f_K in (6-14) is a function

$$f_\tau(z) = \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)}\wp_{[\tau,1]}(z)$$

that depends on the lattice $\mathbb{Z}_K = \mathbb{Z}\tau + \mathbb{Z} = [\tau, 1]$, and fixing some *choice* of a generator τ of $\mathbb{Z}_K$ over $\mathbb{Z}$, we can label its m-torsion values used in generating

H_m as

$$F_u(\tau) = f_\tau(u_1\tau + u_2) \quad \text{with } u = (u_1, u_2) \in \tfrac{1}{m}\mathbb{Z}^2/\mathbb{Z}^2 \setminus \{(0,0)\}. \tag{7-4}$$

For $m > 1$, the functions $F_u : \mathbf{H} \to \mathbb{C}$ in (7-4) are known as the *Fricke functions* of level m. These are holomorphic functions on $\mathbf{H}$ that are x-coordinates of m-torsion points on a 'generic elliptic curve' over $\mathbb{Q}(j)$ with j-invariant j. As they are zeroes of division polynomials in $\mathbb{Q}(j)[X]$, they are algebraic over $\mathbb{Q}(j)$ and generate a finite algebraic extension of $\mathbb{Q}(j)$, the m-th modular function field

$$\mathcal{F}_m = \mathbb{Q}(j, \{F_u\}_{u \in (\frac{1}{m}\mathbb{Z}/\mathbb{Z})^2 \setminus \{(0,0)\}}). \tag{7-5}$$

Note above that $\mathcal{F}_1 = \mathbb{Q}(j)$. We may now rephrase the main theorems of complex multiplication in the following way.

THEOREM 7.6. *Let K be an imaginary quadratic field with ring of integers $\mathbb{Z}[\tau]$. Then the m-th ray class field extension $K \subset H_m$ is generated by the finite values $f(\tau)$ of the functions $f \in \mathcal{F}_m$.*

For generic K this is directly clear from Theorems 6.9 and 6.15. In the special cases $K = \mathbb{Q}(i), \mathbb{Q}(\zeta_3)$, the functions $F_u(\tau)$ in (7-4) vanish at the generator τ of $\mathbb{Z}_K$, so an extra argument [Lang 1987, p. 128] involving modified Weber functions in $\mathcal{F}_m$ is needed.

It is not really necessary to take τ in Theorem 7.6 to be a generator of $\mathbb{Z}_K$; it suffices that the elliptic curve $\mathbb{C}/[\tau, 1]$ is an elliptic curve having CM by $\mathbb{Z}_K$.

In computations, it is essential to have the explicit action of $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ on the values $f(\tau)$ from Theorem 7.6 for arbitrary functions f in the modular function field $\mathcal{F} = \cup_{m \geq 1} \mathcal{F}_m$. As class field theory gives us the group $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ in (7-2) as an explicit quotient of the idele class group $\mathbf{A}_K^*/K^*$ under the Artin map (3-7), this means that we need to find the natural action of $x \in \mathbf{A}_K^*$ on the values $f(\tau)$ in Theorem 7.6. We will do so by reinterpreting the action of the Artin symbol $\sigma_x \in \mathrm{Gal}(K_{\mathrm{ab}}/K)$ on the function value of f at τ as the value of some *other* modular function $f^{g_\tau(x)}$ at τ, that is,

$$(f(\tau))^{\sigma_x} = f^{g_\tau(x)}(\tau), \tag{7-7}$$

for some natural homomorphism $g_\tau : \mathbf{A}_K^* \to \mathrm{Aut}(\mathcal{F})$ induced by τ.

To understand the automorphisms of $\mathcal{F}$, we note first that the natural left action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbf{H}$ gives rise to a right action on $\mathcal{F}_m$ that is easily made explicit for the Fricke functions (7-4), using the 'weight 0' property of f_K. For $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$\begin{aligned} F_u(M\tau) = F_u\Big(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\Big) &= \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)}\wp_{[\tau,1]}(u_1(\alpha\tau+\beta) + u_2(\gamma\tau+\delta)) \\ &= F_{uM}(\tau). \end{aligned}$$

As $u = (u_1, u_2)$ is in $\frac{1}{m}\mathbb{Z}^2/\mathbb{Z}^2$, we only need to know M modulo m, so the Fricke functions of level m are invariant under the congruence subgroup

$$\Gamma(m) = \ker[\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})]$$

of $\mathrm{SL}_2(\mathbb{Z})$, and they are permuted by $\mathrm{SL}_2(\mathbb{Z})$. As we have $F_{-u_1,-u_2} = F_{u_1,u_2}$, we obtain a natural right action of $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$ on $\mathcal{F}_m$.

Besides this 'geometric action', there is a cyclotomic action of $(\mathbb{Z}/m\mathbb{Z})^*$ on the functions $f \in \mathcal{F}_m$ via their Fourier expansions, which lie in $\mathbb{Q}(\zeta_m)((q^{1/m}))$ since they involve rational expansions in

$$e^{2\pi i(a_1\tau + a_2)/m} = \zeta_m^{a_2} q^{a_1/m} \quad \text{for } a_1, a_2 \in \mathbb{Z}.$$

On the Fricke function $F_u = F_{(u_1,u_2)}$, the automorphism $\sigma_k : \zeta_m \mapsto \zeta_m^k$ clearly induces $\sigma_k : F_{(u_1,u_2)} \mapsto F_{(u_1,ku_2)}$. Thus, the two actions may be combined to give an action of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$ on $\mathcal{F}_m$, with $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$ acting geometrically and $(\mathbb{Z}/m\mathbb{Z})^*$ acting as the subgroup $\{\pm\left(\begin{smallmatrix}1 & 0\\ 0 & k\end{smallmatrix}\right) : k \in (\mathbb{Z}/m\mathbb{Z})^*\}/\{\pm 1\}$. The invariant functions are $\mathrm{SL}_2(\mathbb{Z})$-invariant with rational q-expansion; so they lie in $\mathbb{Q}(j)$, and we have a natural isomorphism

$$\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\} \xrightarrow{\sim} \mathrm{Gal}(\mathcal{F}_m/\mathbb{Q}(j)), \tag{7-8}$$

or, if we take the union $\mathcal{F} = \bigcup_m \mathcal{F}_m$ on the left hand side and the corresponding projective limit on the right hand side,

$$\mathrm{GL}_2(\widehat{\mathbb{Z}})/\{\pm 1\} \xrightarrow{\sim} \mathrm{Gal}(\mathcal{F}/\mathbb{Q}(j)). \tag{7-9}$$

Note that $\mathcal{F}_m$ contains $\mathbb{Q}(\zeta_m)(j)$ as the invariant field of $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$, and that the action of $\mathrm{GL}_2(\widehat{\mathbb{Z}})/\{\pm 1\}$ on the subextension $\mathbb{Q}(j) \subset \mathbb{Q}_{\mathrm{ab}}(j)$ with group $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^*$ is via the determinant map $\det : \mathrm{GL}_2(\widehat{\mathbb{Z}})/\{\pm 1\} \to \widehat{\mathbb{Z}}^*$.

To discover the explicit form of the homomorphism g_τ in (7-7), let $\mathfrak{p} = \pi\mathbb{Z}_K$ be a principal prime of K. Then the Artin symbol $\sigma_\mathfrak{p}$ is the identity on H, and the proof of Theorem 6.15 shows that its action on the x-coordinates of the m-torsion points of E_K for m not divisible by π can be written as

$$F_u(\tau)^{\sigma_\mathfrak{p}} = F_u(\pi\tau) = F_{uM_\pi}(\tau),$$

where M_π is the matrix in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ that represents the multiplication by π on $\frac{1}{m}\mathbb{Z}_K/\mathbb{Z}_K$ with respect to the basis $\{\tau, 1\}$. In explicit coordinates, this means that if $\tau \in \mathbf{H}$ is a zero of the polynomial $X^2 + BX + C$ of discriminant $B^2 - 4C = \Delta_K$ and $\pi = x_1\tau + x_2$ is the representation of π on the $\mathbb{Z}$-basis $[\tau, 1]$ of $\mathbb{Z}_K$, then we have

$$M_\pi = \begin{pmatrix} -Bx_1 + x_2 & -Cx_1 \\ x_1 & x_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}). \tag{7-10}$$

As the Fricke functions of level m generate $\mathcal{F}_m$, we obtain in view of (7-8) the identity

$$f(\tau)^{\sigma_{\mathfrak{p}}} = f^{M_\pi}(\tau) \quad \text{for } f \in \mathcal{F}_m \text{ and } \pi \nmid m,$$

which is indeed of the form (7-7). We can rewrite this in the style of the diagram (7-2) by observing that the Artin symbol of $\pi \in K_{\mathfrak{p}}^* \subset \mathbf{A}_K^*$ acts as $\sigma_{\mathfrak{p}}$ on torsion points of order m coprime to $\mathfrak{p}$, and trivially on π-power torsion points. Moreover, $(\pi \bmod K^*) \in \mathbf{A}_K/K^*$ is in the class of the idele $x \in \widehat{\mathbb{Z}}_K^*$ having component 1 at $\mathfrak{p}$ and π^{-1} elsewhere. Thus, if we define

$$\begin{aligned} g_\tau : \widehat{\mathbb{Z}}_K^* &\longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}) \\ x &\longmapsto M_x^{-1} \end{aligned} \tag{7-11}$$

by sending $x = x_1\tau + x_2 \in \widehat{\mathbb{Z}}_K$ to the *inverse* of the matrix M_x describing multiplication by x on $\widehat{\mathbb{Z}}_K$ with respect to the basis $[\tau, 1]$, then M_x is given explicitly as in (7-10), and formula (7-7) holds for $f \in \mathcal{F}$ and $x \in \widehat{\mathbb{Z}}_K^*$ if we use the natural action of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ on $\mathcal{F}$ from (7-9).

To obtain complex multiplication by arbitrary ideles, we note that on the one hand, the idele class quotient $\mathbf{A}_K^*/(K^* \cdot \mathbb{C}^*)$ from (7-2), which is isomorphic to $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ under the Artin map, is the quotient of the unit group $\widehat{K}^*$ of the *finite adele ring*

$$\widehat{K} = \widehat{\mathbb{Z}}_K \otimes_{\mathbb{Z}} \mathbb{Q} = \prod\nolimits'_{\mathfrak{p}\,\text{finite}} K_{\mathfrak{p}} \subset \mathbf{A}_K = \widehat{K} \times \mathbb{C}$$

by the subgroup $K^* \subset \widehat{K}^*$ of principal ideles. On the other hand, not all automorphisms of $\mathcal{F}$ come from $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ as in (7-9): there is also an action of the projective linear group $\mathrm{PGL}_2(\mathbb{Q})^+ = \mathrm{GL}_2(\mathbb{Q})^+/\mathbb{Q}^*$ of rational matrices of positive determinant, which naturally act on $\mathbf{H}$ by linear fractional transformations. It does not fix j, as it maps the elliptic curve $\mathbb{C}/[\tau, 1]$ defined by $\tau \in \mathbf{H}$ not to an isomorphic, but to an isogenous curve. More precisely, if we pick $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})^+$ in its residue class modulo $\mathbb{Q}^*$ such that M^{-1} has integral coefficients, then the lattice

$$(\gamma\tau + \delta)^{-1}[\tau, 1] = \left[\frac{\tau}{\gamma\tau+\delta}, \frac{1}{\gamma\tau+\delta}\right] = M^{-1}\Big[(\alpha\tau + \beta)/(\gamma\tau + \delta), 1\Big]$$

is a sublattice of finite index $\det M^{-1}$ in $[(\alpha\tau + \beta)/(\gamma\tau + \delta), 1]$, and putting $\mu = (\gamma\tau + \delta)^{-1}$, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{C}/[\tau, 1] & \xrightarrow{\quad\mu\quad} & \mathbb{C}/[M\tau, 1] = \mathbb{C}/[(\alpha\tau + \beta)/(\gamma\tau + \delta), 1] \\ {\scriptstyle W}\downarrow{\scriptstyle \sim} & & {\scriptstyle W'}\downarrow{\scriptstyle \sim} \\ E_\tau & \xrightarrow{\quad\phi_\mu\quad} & E_{M\tau} \end{array}$$

as in (7-3). Moreover, the torsion point $u_1\tau+u_2$ having coordinates $u=(u_1,u_2)$ with respect to $[\tau,1]$ is mapped to the torsion point with coordinates uM^{-1} with respect to the basis $[M\tau,1]$.

We let $\widehat{\mathbb{Q}}=\widehat{\mathbb{Z}}\otimes_{\mathbb{Z}}\mathbb{Q}=\prod_p'\mathbb{Q}_p$ be the ring of finite $\mathbb{Q}$-ideles. Then every element in the ring $\mathrm{GL}_2(\widehat{\mathbb{Q}})$ can be written as UM with $U\in\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $M\in\mathrm{GL}_2(\mathbb{Q})^+$. This representation is not unique since $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and $\mathrm{GL}_2(\mathbb{Q})^+$ have nontrivial intersection $\mathrm{SL}_2(\mathbb{Z})$, but we obtain a well-defined action $\mathrm{GL}_2(\widehat{\mathbb{Q}})\to\mathrm{Aut}(\mathcal{F})$ by putting $f^{UM}(\tau)=f^U(M\tau)$. We now extend, for the zero $\tau\in\mathbf{H}$ of a polynomial $X^2+BX+C\in\mathbb{Q}[X]$, the map g_τ in (7-11) to

$$\begin{aligned} g_\tau:\widehat{K}^*=(\widehat{\mathbb{Q}}\tau+\widehat{\mathbb{Q}})^* &\longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Q}})\\ x=x_1\tau+x_2 &\longmapsto M_x^{-1}=\begin{pmatrix}-Bx_1+x_2 & -Cx_1\\ x_1 & x_2\end{pmatrix}^{-1}\end{aligned}\tag{7-12}$$

to obtain the complete Galois action of $\mathrm{Gal}(K_{\mathrm{ab}}/K)\cong\widehat{K}^*/K^*$ on modular function values $f(\tau)$. The result is known as *Shimura's reciprocity law*:

THEOREM 7.13. *Let $\tau\in\mathbf{H}$ be imaginary quadratic, $f\in\mathcal{F}$ a modular function that is finite at τ, and $x\in\widehat{K}^*/K^*$ a finite idele for $K=\mathbb{Q}(\tau)$. Then $f(\tau)$ is abelian over K, and the idele x acts on it via its Artin symbol by*

$$f(\tau)^x=f^{g_\tau(x)}(\tau),$$

where g_τ is defined as in (7-12).

8. Class invariants

Much work has gone into algorithmic improvements of the classical algorithms in Section 6, with the aim of reducing the size of the class polynomials obtained. Clearly the *degree* of the polynomials involved cannot be lowered, as these are the degrees of the field extensions one wants to compute. There are however methods to reduce the size of their coefficients. These already go back to Weber, who made extensive use of 'smaller' functions than j to compute class fields in his algebra textbook [Weber 1908]. The function $\mathfrak{f}_2$ that we used to compute j in (6-12), and that carries Weber's name (as does the elliptic function in (6-14)) provides a good example. A small field such as $K=\mathbb{Q}(\sqrt{-71})$, for which the class group of order 7 is easily computed by hand, already has the

sizable Hilbert class polynomial

$$\begin{aligned}\mathrm{Hil}_K(X) = {} & X^7 + 313645809715\,X^6 - 3091990138604570\,X^5 \\ & + 98394038810047812049302\,X^4 \\ & - 82353426343973077996809 1389\,X^3 \\ & + 513880036645397678032372 6329446\,X^2 \\ & - 425319473946139603274605151187659\,X \\ & + 737707086760731113357714241006081263\,.\end{aligned}$$

However, the Weber function $\mathfrak{f}_2$, when evaluated at an appropriate generator of $\mathbb{Z}_K$ over $\mathbb{Z}$, also yields a generator for H over K, with irreducible polynomial

$$X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2X - 1.$$

As Weber showed, the function $\mathfrak{f}_2$ can be used to generate H over K when 2 splits and 3 does not ramify in $\mathbb{Q} \subset K$. The general situation illustrated by this example is that, despite the content of Theorem 7.6, it is sometimes possible to use a function f of high level, like the Weber function $\mathfrak{f}_2 \in \mathcal{F}_{48}$ of level 48, to generate the Hilbert class field H of conductor 1. The attractive feature of such high level functions f is that they can be much smaller than the j-function itself. In the case of $\mathfrak{f}_2$, the extension $\mathbb{Q}(j) \subset \mathbb{Q}(\mathfrak{f}_2)$ is of degree 72 by (6-12), and this means that the size of the coefficients of class polynomials using $\mathfrak{f}_2$ is about a factor 72 smaller than the coefficients of $\mathrm{Hil}_K(X)$ itself. Even though this is only a constant factor, and complex multiplication is an intrinsically 'exponential' method, the computational improvement is considerable. For this reason, Weber's use of 'small' functions has gained renewed interest in present-day computational practice.

Shimura's reciprocity law Theorem 7.13 is a convenient tool to understand the occurrence of *class invariants*, that is, modular functions $f \in \mathcal{F}$ of higher level that generate the Hilbert class field of K when evaluated at an appropriate generator τ of $\mathbb{Z}_K$. Classical examples of such functions used by Weber are $\gamma_2 = \sqrt[3]{j}$ and $\gamma_3 = \sqrt{j - 1728}$, which have level 3 and 2. As is clear from (6-12), the j-function can also be constructed out of even smaller building blocks involving the Dedekind η-function (6-11). Functions that are currently employed in actual computations are

$$\frac{\eta(pz)}{\eta(z)} \qquad \text{and} \qquad \frac{\eta(pz)\eta(qz)}{\eta(pqz)\eta(z)}, \tag{8-1}$$

which are of level $24p$ and $24pq$. These functions, or sometimes small powers of them, can be used to generate H, and the resulting minimal polynomials have much smaller coefficients than $\mathrm{Hil}_K(X)$. We refer to [Cohen 2000, Section 6.3]

for the precise theorems, and indicate here how to use Theorem 7.13 to obtain such results for arbitrary modular functions $f \in \mathcal{F}$.

Let $f \in \mathcal{F}$ be any modular function of level m, and assume $\mathbb{Q}(f) \subset \mathcal{F}$ is Galois. Suppose we have an explicit Fourier expansion in $\mathbb{Q}(\zeta_m)((q^{1/m}))$ that we can use to approximate its values numerically. Suppose also that we know the explicit action of the generators $S : z \mapsto 1/z$ and $T : z \mapsto z + 1$ on f. Then we can determine the Galois orbit of $f(\tau)$ for an element $\tau \in \mathbf{H}$ that generates $\mathbb{Z}_K$ in the following way. First, we determine elements $x = x_1\tau + x_2 \in \mathbb{Z}_K$ with the property that they generate $(\mathbb{Z}_K/m\mathbb{Z}_K)^*/\mathbb{Z}_K^*$. Then the Galois orbit of $f(\tau)$ over H is determined using Theorem 7.13, and amounts to computing the (repeated) action of the matrices $g_\tau(x) \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ (given by the right hand side of (7-10)) on f. This involves writing $g_\tau(x)$ as a product of powers of S and T and a matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & k \end{smallmatrix}\right)$ acting on f via its Fourier coefficients. Although f may have a large $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$-orbit over $\mathbb{Q}(j)$, the matrices $g_\tau(x)$ only generate a small subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ isomorphic to $(\mathbb{Z}_K/m\mathbb{Z}_K)^*/\mathbb{Z}_K^*$, and one often finds that the orbit of f under this subgroup is quite small. In many cases, one can slightly modify f, multiplying it by suitable roots of unity or raising it to small powers, to obtain an orbit of length one. This means that $f \in \mathcal{F}$ is invariant under $g_\tau[\widehat{\mathbb{Z}}_K^*] \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$. As we have the fundamental equivalence

$$f(\tau)^x = f(\tau) \quad \Longleftrightarrow \quad f^{g_\tau(x)} = f, \tag{8-2}$$

this is equivalent to finding that $f(\tau)$ is a class invariant for $K = \mathbb{Q}(\tau)$. The verification that $g_\tau[\widehat{\mathbb{Z}}_K^*]$ stabilizes f takes place modulo the level m of f, so it follows from (7-12) that if $f(\tau)$ is a class invariant for $K = \mathbb{Q}(\tau)$, then $f(\tau')$ is a class invariant for $K' = \mathbb{Q}(\tau')$ whenever $\tau' \in \mathbf{H}$ is a generator of $\mathbb{Z}_{K'}$ that has an irreducible polynomial congruent modulo m to that of τ. In particular, a function of level m that yields class invariants does so for families of quadratic fields for which the discriminant is in certain congruence classes modulo $4m$.

If $f(\tau)$ is found to be a class invariant, we need to determine its conjugates over K to determine its irreducible polynomial over K as we did in (6-8) for $j(\tau)$. This amounts to computing $f(\tau)^{\sigma_\mathfrak{c}}$ as in Theorem 6.9, with $\mathfrak{c}$ ranging over the ideal classes of Cl_K. If we list the ideal classes of Cl_K as in Section 6 as integer triples (a, b, c) representing the reduced quadratic forms of discriminant Δ_K, the Galois action of their Artin symbols in Theorem 6.9 may be given by

$$j(\tau)^{(a,-b,c)} = j\Big(\frac{-b+\sqrt{b^2-4ac}}{2a}\Big).$$

For a class invariant $f(\tau)$ a similar formula is provided by Shimura's reciprocity law. Let $\mathfrak{a} = \mathbb{Z} \cdot ((-b + \sqrt{b^2 - 4ac})/2) + \mathbb{Z} \cdot a$ be a $\mathbb{Z}_K$-ideal in the ideal class corresponding to the form (a, b, c). Then the $\widehat{\mathbb{Z}}_K$-ideal $\mathfrak{a}\widehat{\mathbb{Z}}_K$ is principal since $\mathbb{Z}_K$-ideals are locally principal, and we let $x \in \widehat{\mathbb{Z}}_K$ be a generator. The element

x is a finite idele in $\widehat{K}^*$, and the Artin symbol of x^{-1} acts on $f(\tau)$ as the Artin symbol of the form $(a, -b, c)$. We have $U = g_\tau(x^{-1})M^{-1} \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ for the matrix $M \in \mathrm{GL}_2(\mathbb{Q})^+$ defined by

$$[\tau, 1]M = \Big[\frac{b+\sqrt{b^2-4ac}}{2}, 2a\Big],$$

since U stabilizes the $\widehat{\mathbb{Z}}_K$-lattice spanned by the basis $[\tau, 1]$. Applying Theorem 7.13 for the idele x^{-1} yields the desired formula

$$f(\tau)^{(a,-b,c)} = f^U\Big(\frac{-b+\sqrt{b^2-4ac}}{2a}\Big).$$

This somewhat abstract description may be phrased as a simple explicit recipe for the coefficients of $U \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$, which we only need to know modulo m, see [Stevenhagen 2001].

There are limits to the improvements coming from intelligent choices of modular functions to generate class fields. For any nonconstant function $f \in \mathcal{F}$, there is a polynomial relation $\Psi(j, f) = 0$ between j and f, with $\Psi \in \mathbb{C}[X, Y]$ some irreducible polynomial with algebraic coefficients. The *reduction* factor one obtains by using class invariants coming from f (if these exist) instead of the classical j-values is defined as

$$r(f) = \frac{\deg_f(\Psi(f, j))}{\deg_j(\Psi(f, j))}.$$

By [Hindry and Silverman 2000, Proposition B.3.5], this is, asymptotically, the *inverse* of the factor

$$\lim_{h(j(\tau))\to\infty} \frac{h(f(\tau))}{h(j(\tau))}.$$

Here h is the absolute logarithmic height, and we take the limit over all CM-points $\mathrm{SL}_2(\mathbb{Z}) \cdot \tau \in \mathbf{H}$. It follows from gonality estimates for modular curves [Bröker and Stevenhagen 2008, Theorem 4.1] that $r(f)$ is bounded above by $1/(24\lambda_1)$, where λ_1 is 'Selberg's eigenvalue' as defined in [Sarnak 1995]. The currently proved bounds [Kim 2003, p. 176] on λ_1 yield $r(f) \le 32768/325 \approx 100.8$, and conjectural bounds imply $r(f) \le 96$. Thus Weber's function $\mathfrak{f}_2$, which has $r(f) = 72$ and yields class invariants for a positive density subset of all discriminants, is close to being optimal.

Acknowledgements

Useful comments on earlier versions of this paper were provided by Reinier Bröker, René Schoof and Marco Streng. Bjorn Poonen provided us with the reference to [Kim 2003].

References

[Artin and Tate 1990] E. Artin and J. Tate, *Class field theory*, 2nd ed., Advanced Book Classics, Addison-Wesley, Redwood City, CA, 1990.

[Bröker and Stevenhagen 2008] R. Bröker and P. Stevenhagen, "Constructing elliptic curves of prime order", pp. 17–28 in *Computational Arithmetic Geometry*, edited by K. E. Lauter and K. A. Ribet, Contemp. Math. **463**, 2008.

[Buhler and Wagon 2008] J. P. Buhler and S. Wagon, "Basic algorithms in number theory", pp. 25–68 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Bump et al. 2003] D. Bump, J. W. Cogdell, E. de Shalit, D. Gaitsgory, E. Kowalski, and S. S. Kudla, *An introduction to the Langlands program*, Birkhäuser Boston Inc., Boston, MA, 2003. Lectures presented at the Hebrew University of Jerusalem, Jerusalem, March 12–16, 2001, Edited by Joseph Bernstein and Stephen Gelbart.

[Cassels and Fröhlich 1967] J. W. S. Cassels and A. Fröhlich (editors), *Algebraic number theory*, Academic Press, London, 1967.

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer, Berlin, 1993.

[Cohen 2000] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics **193**, Springer, New York, 2000.

[Cox 1989] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, John Wiley & Sons, New York, 1989.

[Deuring 1958] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzyklopädie der mathematischen Wissenschaften, Band I_2, Heft 10, Teil II, Teubner, Stuttgart, 1958.

[Fieker 2001] C. Fieker, "Computing class fields via the Artin map", *Math. Comp.* **70**:235 (2001), 1293–1303.

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics **201**, Springer, New York, 2000.

[Kim 2003] H. H. Kim, "Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2", *J. Amer. Math. Soc.* **16**:1 (2003), 139–183.

[Lang 1987] S. Lang, *Elliptic functions*, Second ed., Graduate Texts in Mathematics **112**, Springer, New York, 1987.

[Lang 2002] S. Lang, *Algebra*, Third ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002.

[Sarnak 1995] P. Sarnak, "Selberg's eigenvalue conjecture", *Notices Amer. Math. Soc.* **42**:11 (1995), 1272–1277.

[Schneps 1994] L. Schneps (editor), *The Grothendieck theory of dessins d'enfants* (Luminy, 1993), London Math. Soc. Lecture Note Ser. **200**, Cambridge Univ. Press, Cambridge, 1994.

[Schoof 2008] R. J. Schoof, "Computing Arakelov class groups", pp. 447–495 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Serre 1989] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Second ed., Advanced Book Classics, Addison-Wesley, Redwood City, CA, 1989.

[Shimura 1998] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series **46**, Princeton University Press, Princeton, NJ, 1998.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986.

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994.

[Stevenhagen 2001] P. Stevenhagen, "Hilbert's 12th problem, complex multiplication and Shimura reciprocity", pp. 161–176 in *Class field theory — its centenary and prospect* (Tokyo, 1998), edited by K. Miyake, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001.

[Stevenhagen 2008] P. Stevenhagen, "The arithmetic of number rings", pp. 209–266 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Stevenhagen and Lenstra 1996] P. Stevenhagen and H. W. Lenstra, Jr., "Chebotarëv and his density theorem", *Math. Intelligencer* **18**:2 (1996), 26–37.

[Völklein 1996] H. Völklein, *Groups as Galois groups: an introduction*, Cambridge Studies in Advanced Mathematics **53**, Cambridge Univ. Press, Cambridge, 1996.

[Weber 1908] H. Weber, *Lehrbuch der Algebra*, F. Vieweg und Sohn, Braunschweig, 1908. Reprinted by Chelsea Pub., New York, 1961.

HENRI COHEN
LABORATOIRE A2X, U.M.R. 5465 DU C.N.R.S.
UNIVERSITÉ BORDEAUX I
351 COURS DE LA LIBÉRATION
33405 TALENCE CEDEX
FRANCE
cohen@math.u-bordeaux1.fr

PETER STEVENHAGEN
MATHEMATISCH INSTITUUT,
UNIVERSITEIT LEIDEN, POSTBUS 9512
2300 RA LEIDEN
THE NETHERLANDS
psh@math.leidenuniv.nl