Abelian varieties with complex multiplication and modular functions, by Goro
   Shimura, Princeton Univ. Press, Princeton, NJ, 1998, xiv + 217 pp., $55.00,
   ISBN 0-691-01656-9

The subject that might be called "explicit class field theory" begins with *Kronecker's Theorem*: every abelian extension of the field of rational numbers $\mathbb{Q}$ is a
subfield of a cyclotomic field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of 1. In other
words, we get all abelian extensions of $\mathbb{Q}$ by adjoining all "special values" of

$$e(x) = \exp(2\pi i x),$$

i.e., with $x \in \mathbb{Q}$. Hilbert's twelfth problem, also called Kronecker's Jugendtraum,
is to do something similar for any number field K, i.e., to generate all abelian
extensions of K by adjoining special values of suitable special functions. Nowadays
we would add that the reciprocity law describing the Galois group of an abelian
extension L/K in terms of ideals of K should also be given explicitly.

After $K = \mathbb{Q}$, the next case is that of an imaginary quadratic number field K,
with the real torus $\mathbb{R}/\mathbb{Z}$ replaced by an elliptic curve E with complex multiplication.
(Kronecker knew what the result should be, although complete proofs were given
only later, by Weber and Takagi.) For simplicity, let $\mathcal{O}$ be the ring of integers in
K, and let $\mathfrak{A}$ be an $\mathcal{O}$-ideal. Regarding $\mathfrak{A}$ as a lattice in $\mathbb{C}$, we get an elliptic curve
$E = \mathbb{C}/\mathfrak{A}$ with $\mathrm{End}(E) = \mathcal{O}$; E has complex multiplication, or CM, by $\mathcal{O}$. If
$j = j(\mathfrak{A})$ is the j-invariant of E, then $K(j)$ is the Hilbert class field of K, i.e., the
maximal abelian unramified extension of K. In more suggestive terminology, $K(j)$
is the field of moduli of E. Here $j(\mathfrak{A})$ depends only on the ideal class of $\mathfrak{A}$, and we
realize the ideal class group H of K as the Galois group of $K(j)/K$ by the rule:
the automorphism attached to an ideal $\mathfrak{B}$ carries $j(\mathfrak{A})$ to $j(\mathfrak{A}\mathfrak{B}^{-1})$. The ramified
abelian extensions of K are obtained by adjoining the coordinates of torsion points
of E (or rather their images in the Kummer variety of E, obtained by dividing E
by its automorphism group, usually of order 2).

As Wüstholz has been telling us, it is instructive to consider Hilbert's seventh
problem together with the twelfth. The seventh says that our special functions
take transcendental values at not-so-special points. Thus $e(x)$ is transcendental
for x algebraic but not rational (Gelfond, Schneider), and $j(\Lambda)$ is transcendental if
the lattice Λ has a period ratio in the upper half-plane which is algebraic but not
quadratic, and there are many other transcendency results involving elliptic and
modular functions.

Aside from some results of Hecke in 1912, the only progress on the twelfth problem was made by Shimura and Taniyama in the 1950s. They achieved complete
results concerning the abelian extensions of number fields arising from abelian varieties, with complex multiplication, of arbitrary dimension n (the case $n = 1$ being
elliptic curves with complex multiplication, discussed above). Their results appeared in the 1961 book [1], of which the present book is the successor; roughly
speaking, the first half of the new book is an updated version of the old book, and
the second half is new material.

Let K be a CM field of degree $2n$ over $\mathbb{Q}$; i.e., K is a totally imaginary quadratic extension of a totally real number field F of degree n. Let A be an abelian variety of dimension n, in characteristic 0, such that the endomorphism ring $\mathrm{End}(A)$ of A contains the ring of integers $\mathcal{O}$ of K. (More generally, $\mathcal{O}$ could be an order in K instead of the full ring of integers.) Then we say that A has complex multiplication, or CM, by $\mathcal{O}$. The case $n > 1$ has some new features, of which we mention two.

First, the action of K on the space of invariant 1-forms on A (which space has dimension n) chooses half of the embeddings of K into C, say $\varphi_1, \ldots, \varphi_n$; there is a basis $\omega_1, \ldots, \omega_n$ of the invariant 1-forms such that

$$\alpha \cdot \omega_i = \alpha^{\varphi_i} \cdot \omega_i \qquad (\alpha \in K;\ 1 \le i \le n),$$

and the complex conjugates $\bar{\varphi}_1, \ldots, \bar{\varphi}_n$ are the other half of the embeddings. (The rational representation is the direct sum of the analytic representation and its complex conjugate.) So the proper object of study here is not the field K by itself, but the CM type $(K;\ (\varphi_1, \ldots, \varphi_n))$. Conversely, each such type comes from an abelian variety A with CM, unique up to isogeny. (Two abelian varieties are isogenous if there is a homomorphism of one onto the other, with finite kernel.) There is a test as to whether A is simple; in the Galois case, where $\mathrm{Gal}(K/\mathbb{Q}) = \{\varphi_1, \ldots, \varphi_n, \bar{\varphi}_1, \ldots, \bar{\varphi}_n\}$, A is simple if and only if the only $\gamma \in \mathrm{Gal}(K/Q)$ with $\gamma S = S = \{\varphi_1, \ldots, \varphi_n\}$ is $\gamma =$ the identity. Given K, there are 2^n corresponding CM types, or 2^{n-1} if φ_1 is fixed. A CM type is *primitive* if the associated abelian varieties are simple.

Next, a CM type $(K;\ (\varphi_1, \ldots, \varphi_n))$ has a *reflex CM type* $(K^*;\ (\psi_1, \ldots, \psi_m))$. The field K^* is the extension of $\mathbb{Q}$ obtained by adjoining the "semi-traces"

$$\sum_{i=1}^{n} \xi^{\varphi_i} \qquad (\xi \in K).$$

A reflex CM type is primitive, and a primitive CM type is its own double reflex. In the very simplest case, if $K/\mathbb{Q}$ is abelian and $(K;\ (\varphi_1, \ldots, \varphi_n))$ is primitive, then its reflex is $(K;\ (\varphi_1^{-1}, \ldots, \varphi_n^{-1}))$.

Also, when $n > l$ it is important to fix a polarization of an abelian variety, and hence a projective embedding. A polarized abelian variety of type $(K;\ (\varphi_1, \ldots, \varphi_n))$ then has a *field of moduli* which is an unramified abelian extension of K^*, generalizing the results on the values of the j-function when $n = 1$ (hence $K = K^*$). (Roughly speaking, a field of moduli for an algebro-geometric object V is a minimal field of definition k_0 of the isomorphism class of V. If V is defined over an extension k of k_0, and σ is an isomorphism of k onto another field, then V is isomorphic to V^σ if and only if σ is the identity on k_0.) Ramified class fields over K^* are given by fields of moduli of ideal section points on A, or rather their images on the Kummer variety. This does not give all abelian extensions of K^*, when $n > 1$, so Hilbert's twelfth problem is not quite solved for CM fields.

The main theorems on the class fields obtained from complex multiplication are carefully stated and proved in chapter 4 of the book. An important ingredient is the notion of reduction modulo $\mathfrak{p}$, which is the subject of chapter 3. This leads us to the second major theme, the zeta function.

Given a variety V over a number field k, it has a well-defined good reduction modulo $\mathfrak{p}$ for all but a finite number of primes $\mathfrak{p}$ of k, a variety $V(\mathrm{mod}\,\mathfrak{p})$ over the finite field $\mathcal{O}/\mathfrak{p}$ which is as nice as V. If $V = A$ is an abelian variety, this means that $A(\mathrm{mod}\,\mathfrak{p})$ is an abelian variety over $\mathcal{O}/\mathfrak{p}$ of the same dimension as A. The

Hasse-Weil zeta function is the product of the local zeta functions

$$Z(V, k; \ s) = \prod_{\mathfrak{p}} Z(V(\mathrm{mod}\,\mathfrak{p}), \ \mathcal{O}/\mathfrak{p}; \ s).$$

The product converges for $s \in \mathbb{C}$ with $\mathrm{Re}(s)$ large enough. The $\mathfrak{p}$-factors for primes $\mathfrak{p}$ of bad reduction need special treatment, which we don't go into here. While the local zeta functions are well understood, thanks to Deligne, the global one is not. The conjecture (attributed to Hasse, in the 1930s) is that $Z(V, k; s)$ extends to a function meromorphic for $s \in \mathbb{C}$, with a functional equation of the usual type. This will have to appear on any updated list of Hilbert problems and is almost as open as Hilbert's twelfth. Much progress has been made, notably by Eichler and Shimura, for varieties which arise somehow from automorphic functions. It is only with the proof by Wiles et al. that (almost all) elliptic curves over $\mathbb{Q}$ are modular, that the Hasse conjecture for (almost all) elliptic curves over $\mathbb{Q}$ without complex multiplication was proved.

However, for abelian varieties with complex multiplication, the situation is quite satisfactory, and complete results are given in chapter 5 of the book. The zeta function in this case is a product of Hecke L-functions $L(\chi; s)$ attached to Hecke characters χ of k (formerly called Grössencharaktere), for which the analytic continuation and functional equation were proved by Hecke in 1920. This also appeared in the earlier book (the case $n = 1$ was done earlier by Deuring), but the new book has a more complete treatment.

Chapter 6 contains a rapid treatment of modular forms, modular varieties, and modular functions in a rather general setting, including Hilbert and Siegel modular functions. Fiber systems of abelian varieties are emphasized over a base whose complex points are a quotient of a generalized half-plane by a discrete group of automorphisms. A point of the base represents an isomorphism class of abelian varieties, with additional structure, and the fiber over that point is such an abelian variety. There is also a brief introduction to canonical models, which Shimura introduced about 1970.

Chapter 7 begins with a study of theta functions on abelian varieties, with special attention to the CM case. Finally, there are many results giving relations among periods on abelian varieties with complex multiplication. For example, let (K, Φ) be a CM type ($\Phi = \{\varphi_1, \ldots, \varphi_n\}$). Then there is a *period*

$$p_K(\varphi, \Phi) \in \mathbb{C}^\times/\bar{\mathbb{Q}}^\times,$$

for $\varphi \in \Phi$, with values in the multiplicative group of the complex numbers modulo that of the algebraic numbers, as follows. Let A be of type (K, Φ), and let η be a $\bar{\mathbb{Q}}$-rational invariant 1-form on A with $\alpha \cdot \eta = \alpha^\varphi \cdot \eta$ for $\alpha \in K$. Then

$$p_K(\varphi, \Phi) = 1/\pi \int_c \eta \qquad \text{in } \mathbb{C}^\times/\bar{\mathbb{Q}}^\times$$

for any $c \neq 0$ in $H_1(A, \mathbb{Z})$. Let I_K be the free abelian group of the $2n$ embeddings of K into $\mathbb{C}$; Φ above is identified with $\varphi_1 + \cdots + \varphi_n \in I_K$. Then the above extends to a pairing (the *period symbol*)

$$I_K \times I_K \in \mathbb{C}^\times/\bar{\mathbb{Q}}^\times,$$

with various properties. Now, given K, we have 2^{n-1} sets $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ with φ_1 fixed, in I_K, which has rank $2n$. So, for larger values of n, there will be many $\mathbb{Z}$-linear relations among the Φ and corresponding multiplicative relations among

the $p_K(\tau, \Phi)$ for a fixed embedding τ of K into $\mathbb{C}$. Often the Φ can be chosen so that the relations are among periods of nonisogenous abelian varieties. There are also connections between periods and special values of Hecke L-functions.

The book brings us up to date on much important and interesting material and is a valuable addition to the literature. It is not easy reading, as a great deal of material has been packed into 200 pages, but it is fairly self-contained, with detailed proofs of most of the results. The background in algebraic geometry is based on Weil's *Foundations*, which younger readers may find to be a foreign language, especially in the part concerning reduction modulo $\mathfrak{p}$. But one of the aims of Grothendieck's approach was a smoother treatment of reduction modulo $\mathfrak{p}$, and those who grew up with schemes should have no trouble, on that account, in reading this book.

References

1. G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, no. 6, 1961. MR **23**:A2419

A. P. Ogg

University of California, Berkeley
E-mail address: ogg@math.berkeley.edu