Kleine AG: Complex Multiplication of Elliptic Curves

Organisation:
Timo Keller[1]
Robert Kucharczyk[2]

For abelian extensions of the rationals, the theorem of Kronecker and Weber states that every such extension is contained in a cyclotomic extension $\mathbf{Q}(\zeta_n)$, i. e. is generated by adjunction of torsion points of $\mathbf{G}_{m,\mathbf{Q}}$ or values of the complex analytic function $\exp(2\pi i z)$. There is no such construction known in general for other number fields, but for CM fields, especially for imaginary quadratic number fields, the theory of complex multiplication yields an explicit class field theory.

1. Class Field Theory and The Main Theorem of Complex Multiplication I

- State the main theorem of global class field theory [Sh], 5.2, p. 115 ff or [Si], II §3, pp. 115–120.
- State the main theorem of complex multiplication of elliptic curves [Sh], 5.3, p. 117.
- Start proving the main theorem up to [Sh], 5.3, p. 119.. 117–119, line 4.

2. The Main Theorem of Complex Multiplication II

- Finish the proof of the main theorem [Sh], 5.3, pp. 119–121.

3. Applications of The Main Theorem of Complex Multiplication: Explicit class field theory for imaginary quadratic number fields

Now we can reap the fruits of our labour constructing all abelian extensions of imaginary quadratic number fields by adjoining torsion points of CM elliptic curves:

- The j-invariant generates the Hilbert class field and is integral, [Ru], Corollary 5.12, p. 18
- Existence of a Hecke character, [Ru], Theorem 5.15, p. 19 f.
- Properties of the Hecke character, [Ru], Corollary 5.16, p. 20.
- Generation of abelian extensions, [Ru], Corollary 5.20, p. 21.

[1] `<Vorname>.<Nachname>@mathematik.uni-regensburg.de`

[2] `rak@math.uni-bonn.de`

4. The L-series

All references refer to [Si], Chapter II. Let E/L be a CM elliptic curve with complex multiplication by K and assume $L \supset K$.

- Define the (global) L-series $L(E/L, s)$ of E/L (p. 172).
- Define the Hecke L-series $L(s, \psi)$ attached to a Grössencharacter ψ and cite without proof its analytic continuation and functional equation (Theorem 10.3).
- Prove that the reduction of $\psi_{E/L}(\mathfrak{P})$ is given by the $\mathfrak{P}$-Frobenius (Proposition 10.4).
- Finally prove the main result of this talk:

$$L(E/L, s) = L(s, \psi_{E/L})L(s, \overline{\psi_{E/L}})$$

(Theorem 10.5 (a) and—referring without proof to exercises 2.30–2.32—(b)).

- If time permits, tell as much as possible from Example 10.6.

5. Computational aspects

Follow [Co], §12.A–C and E. In addition, Theorem 12.24 should be mentioned. The goal of this talk is to understand, at least in an outline, the proof of Theorem 12.34: the classification of imaginary quadratic number fields of class number one. (You may also want to look at [Cohen, *A Course in Computational Algebraic Number Theory*] and [Cohen-Stevenhagen, `http://www.math.leidenuniv.nl/~aangelakis/15cohenpsh.pdf`]).

References

[Co] Cox D.: *Primes of the Form $x^2 + ny^2$.*

[Ru] Rubin K.: *Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer*, `http://wstein.org/swc/aws/notes/files/99RubinCM.pdf`

[Sh] Shimura G.: *Introduction to the Arithmetic Theory of Automorphic Functions.*

[Si] Silverman J.: *Advanced Topics in the Arithmetic of Elliptic Curves.*