A summary of my master's thesis

Kéva Djambaé

November 2022

Contents

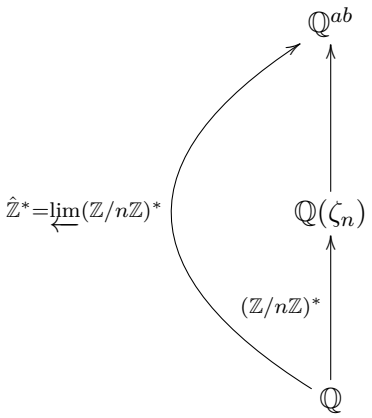
1 Summary of Master Thesis

This document is an attempt to quickly explain my master's thesis. The starting point was the Kronecker-Weber's theorem :

Théorème 1.1. *By posing $\mathbb{Q}^{ab}$ the maximal abelian extension of $\mathbb{Q}$. Then, if ζ_n is an n-th root of unity then we have :*

$$\mathbb{Q}^{ab} = \bigcup_{n\in\mathbb{N}^*} \mathbb{Q}(\zeta_n) \text{ et } \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^* = \varprojlim (\mathbb{Z}/n\mathbb{Z})^*.$$

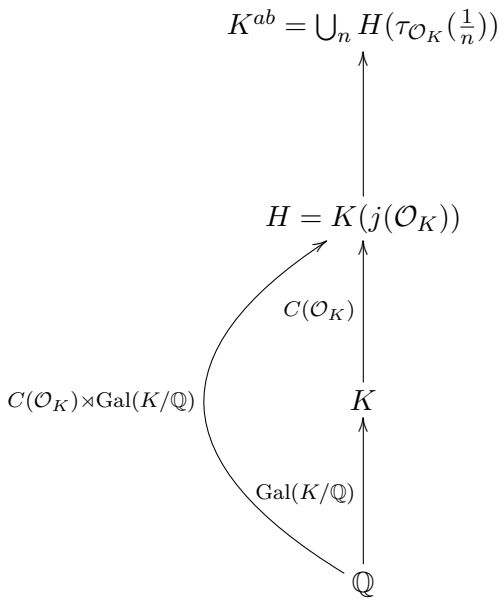
This allows to obtain the diagram below (the groups above the arrows being the associated Galois groups):



Hilbert's twelfth problem is the generalization of this theorem to all number fields which is still not solved, my thesis is interested in the case of totally imaginary quadratic fields.
Our main goal for chapter II was therefore to generalize this situation to the case of imaginary quadratic fields K. Our real goal was to establish the class field of radius $n\mathcal{O}_K$ of the field K which will play a role analogous to $\mathbb{Q}^{ab}$. To achieve this, we had to combine tools coming from two fields of mathematics (class field theory, complex analysis).
After the introduction of Weber function and show that the j-invariant is an algebraic integer, we are focus to exposes the class field of radius K for the module $n\mathcal{O}_K$. We establish the generalization of the Kronecker-Weber theorem for imaginary quadratic fields :

Théorème 1.2. *The class field of radius $n\mathcal{O}_K$ of K is $K(j(\mathcal{O}_K), \tau_{\mathcal{O}_K}(\frac{1}{n}))$. Moreover, if $\mathcal{O}$ is an order of conductor n in K then the class field of radius $n\mathcal{O}_K$ is $K(j(\mathcal{O}), \tau_{\mathcal{O}}(\omega_K))$ where $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$, d_K being the discriminant of K.*

Thus, we obtain the diagram :



2 Kronecker-Weber's Theorem

We will now try to highlight the different links we have made. Let us recall our starting point, the basic field was that of the rationals $\mathbb{Q}$, we posed $\mathbb{Q}^{ab}$ the maximal abelian extension of $\mathbb{Q}$. The first step of my internship was to understand the interest and the complexity of the Kronecker-Weber theorem. We have separated this first chapter into three parts.

The first one is a preliminary study of cyclotomic extensions, we make explicit in Corollary 1.3 and Remark 1.4 the fact that they are abelian extensions so, we have :

Corollaire 2.1. *Let ζ_n be a primitive root n-th of the unit. Then, by posing $K = \mathbb{Q}(\zeta_n)$, $K/\mathbb{Q}$ is an abelian extension and $G = Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.*

It is easily deduced that their integer ring $\mathcal{O}_K$ is a $\mathbb{Z}$-free module of rank $|Gal(K/\mathbb{Q})|$. After that, we study more particularly the rings of integers of cyclotomic extensions in order to establish in Theorem 1.7 that :

Théorème 2.2. *The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

We also study the decomposition of primes in a cyclotomic extension:

Théorème 2.3. *Let $\zeta = e^{\frac{2i\pi}{n}}, K = \mathbb{Q}(\zeta)$ and p prime. We write $n = p^k m$ with $pgcd(p, m) = 1$. Then,*

- *The ramification index of p is $\varphi(p^k) = e$.*
- *The degree of inertia f is the (multiplicative) order of $p \mod m$.*

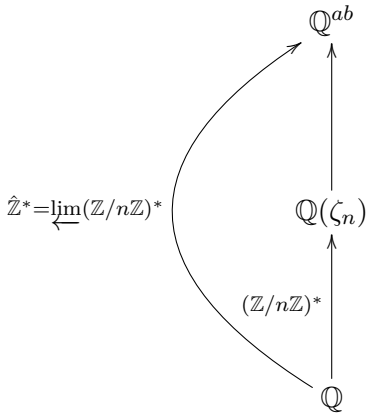
The second is a brief reminder of class field theory in the local and global cases. In the global case, we expose class field theory through ideals and adeles to try to have a complete study. We also take the opportunity to present the Kummer theory,

In third part, the Galois theory and class field theory combined with our topological knowledge studied in Appendix 11 allowed us to establish the (Kronecker-Weber) theorem:

Théorème 2.4. *By posing $\mathbb{Q}^{ab}$ the maximal abelian extension of $\mathbb{Q}$. Then, if ζ_n is an n-th root of unity then we have :*

$$\mathbb{Q}^{ab} = \bigcup_{n \in \mathbb{N}^*} \mathbb{Q}(\zeta_n) \text{ et } \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^* = \varprojlim (\mathbb{Z}/n\mathbb{Z})^*.$$

We present two demonstrations, one using adels by global arguments, the other by local arguments where we will establish the Kronecker-Weber theorem in the local case to deduce the global case. This is a great example of the use of the "local-global" principle. All this allows to obtain the diagram below (the groups above the arrows being the associated Galois groups):



3 Generalization to quadratic fields

Our main goal for chapter II was therefore to generalize this situation to the case of imaginary quadratic fields K. Our real goal was to establish the class field of radius $n\mathcal{O}_K$ of the field K which will play a role analogous to

$\mathbb{Q}^{ab}$. To achieve this, we had to combine tools coming from two fields of mathematics (class field theory, complex analysis).
To begin with, we introduced in section 4 the notion of order :

Définition 3.1. *We call $\mathcal{O}$ an order of K if it is a subring of K, a $\mathbb{Z}$-free module of rank 2 without torsion and K is the fraction field of $\mathcal{O}$.*
The number $f = [\mathcal{O}_K : \mathcal{O}]$ is the conductor of $\mathcal{O}$.

Définition 3.2. *In this case, thanks to the existence theorem, there exists L an extension of K such that $Gal(L/K) \simeq C(\mathcal{O})$.*
The extension L is called the ring class field of order $\mathcal{O}$.

Exemple 3.1. The ring of the class field of K for O_K is its Hilbert class field.

Then, the study of objects of an analytical nature in section 5 was necessary to reach our objective.

Définition 3.3. *For ω_1, $\omega_2 \in \mathbb{C}$, let $\Lambda = [\omega_1, \omega_2]$ be a lattice of $\mathbb{C}$. A complex function f is elliptic for Λ if f is meromorphic on $\mathbb{C}$ and for any $z \in \mathbb{C} \setminus \Lambda$, $f(z) = f(z + \omega_1) = f(z + \omega_2)$.*

Exemple 3.2. The $\wp$-Weierstrass function for a lattice Λ :

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega} \right).$$

We define the equivalence relation :

Définition 3.4. *If there exists $\lambda \in \mathbb{C}$ such that for two lattice Λ and Λ' we have $\Lambda' = \lambda\Lambda$ then we say that Λ and Λ' are homothetic.*

This allowed us to introduce in section 6 the function j :

Définition 3.5. *For a lattice Λ, the number $j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda) - 27 g_3(\Lambda)}$ is always defined.*

We show that this function is invariant by homothety :

Théorème 3.6. *We have the equivalence $j(\Lambda) = j(\Lambda')$ if and only if there exists $\lambda \in \mathbb{C}$ such that that $\Lambda' = \lambda\Lambda$.*

We did all this to establish that the number $j(\Lambda)$ is an algebraic integer. For that we must introduce the complex multiplication thanks to the following theorem:

Théorème 3.7. *For any $\alpha \in \mathbb{C} \setminus \mathbb{Z}$, we have the equivalences following equivalences:*
The function $\wp_\Lambda(\alpha.)$ is rational in $\wp_\Lambda(.)$ if and only if $\alpha\Lambda \subset \Lambda$ if and only if there exists an order $\mathcal{O}$ of K such that $\alpha \in \mathcal{O}$ and Λ are homothetic to an eigenideal of $\mathcal{O}$.

Définition 3.8. *The order $\mathcal{O}$ (of the last theorem) is the complex multiplication ring of the lattice Λ.*

Thus, we can link the notion of lattice to that of order with corollary 7.10 :

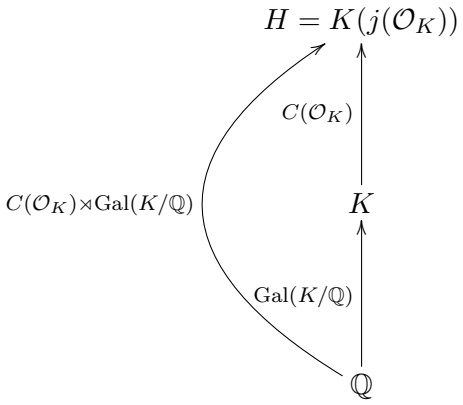
Corollaire 3.9. *There is a 1-1 correspondence between the group of classes $C(\mathcal{O})$ and the classes homothety classes of lattice of $\mathbb{C}$ which have $\mathcal{O}$ as their complex multiplication ring.*

Finally, by establishing that the j-invariant is an algebraic integer by linking it to the ring class field of an order in the theorem :

Théorème 3.10. *The number $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field of order $\mathcal{O}$.*

Remarque 3.11. *The extension $K(j(\mathcal{O}_K))$ is abelian maximal unramified on K where the complex conjugation acts on $C(\mathcal{O}_K)$ by the application $(g \mapsto g^{-1})$.*

We thus obtain the following commutative diagram:



To conclude our algebraic study, we introduced in section 8 the Weber function:

Définition 3.12. *For any lattice Λ, we will call the Weber function $\tau_\Lambda : \mathbb{C} \to \mathbb{C}$ defined by :*

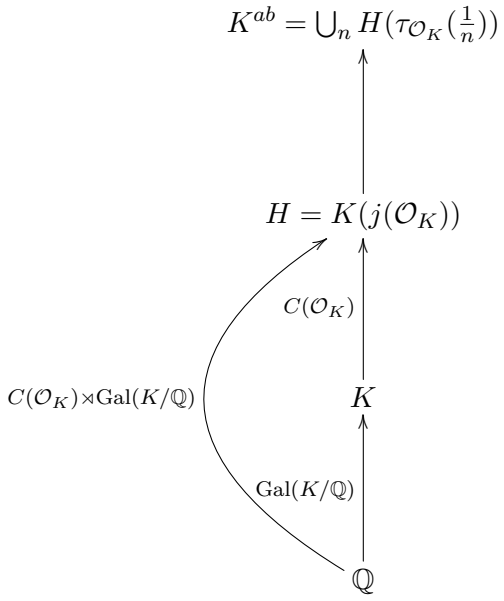
$$\tau_\Lambda(z) = \begin{cases} \dfrac{g_2(\Lambda)^2}{\Delta(\Lambda)} \wp_\Lambda(z)^2 & \text{if } g_3(\Lambda) = 0 \\ \dfrac{g_3(\Lambda)}{\Delta(\Lambda)} \wp_\Lambda(z)^3 & \text{if } g_2(\Lambda) = 0 \\ \dfrac{g_2(\Lambda) g_3(\Lambda)}{\Delta(\Lambda)} \wp_\Lambda(z)^3 & \text{else.} \end{cases}$$

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

To reach our goal which exposes the class field of radius K for the module $n\mathcal{O}_K$. We establish the generalization of the Kronecker-Weber theorem for imaginary quadratic fields :

Théorème 3.13. *The class field of radius $n\mathcal{O}_K$ of K is $K(j(\mathcal{O}_K), \tau_{\mathcal{O}_K}(\frac{1}{n}))$. Moreover, if $\mathcal{O}$ is an order of conductor n in K then the class field of radius $n\mathcal{O}_K$ is $K(j(\mathcal{O}), \tau_{\mathcal{O}}(\omega_K))$ where $\omega_K = \frac{d_K+\sqrt{d_K}}{2}$, d_K being the discriminant of K.*

Thus, we obtain the diagram :



4 Elliptic curves

Finally, since elliptic functions naturally define elliptic curves, section 9 introduces the Weierstrass equation :

Définition 4.1. *For $g_2, g_3 \in K$, if $\Delta = g_2^3 - 27g_3^2 \neq 0$ so*
$y^2 = 4x^3 - g_2x - g_3$ is a Weierstrass equation.
It defines an elliptic curve E. We will note $E(K)$ the set of solutions of $y = 0$ on K and let us notice that $\infty \in E(K)$.

We have the following theorem :

Théorème 4.2. *Let E be an elliptic curve on $\mathbb{C}$ given by the equation :*

$$y^2 = 4x^3 - g_2x - g_3 \text{ where } g_2, g_3 \in \mathbb{C} \text{ with } \Delta = g_2^3 - 27g_3^2 \neq 0.$$

So, there is a unique lattice Λ of $\mathbb{C}$ such as $g_2 = g_2(\Lambda)$ et $g_3 = g_3(\Lambda)$.

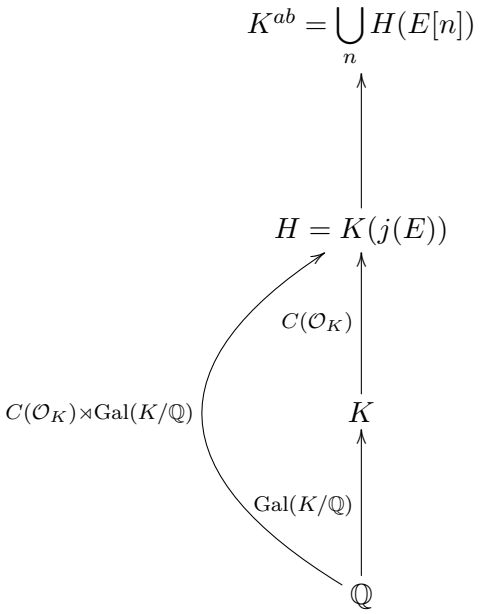
We then show that $E(K)$ is an additive group:

Proposition 4.3. *The set $E(K)$ is an additive group where ∞ is the neutral element.*

Then, we redefine the complex multiplication for an elliptic curve:

Définition 4.4. *Let $\mathrm{End}_{\mathbb{C}}(E) = \{\alpha \in \mathbb{C},\ \alpha\Lambda \subset \Lambda\}$. If $\mathbb{Z} \subsetneq \mathrm{End}_{\mathbb{C}}(E)$ then E has a complex multiplication.*

Thus all our algebraic theory applies to elliptic curves. Let E be an elliptic curve on $H = K(j(E))$ having $\mathcal{O}_K$ as the complex multiplication ring. Let $n \in \mathbb{N}^*$, we set $E[n]$ to the n-twisting points of E on an algebraic closure $\overline{K}$. Thus, we can modify the last diagram:



5 What happens next?

In spite of our initial goal, these results open new questions that would deserve and could occupy us for many years to come. The time of the internship being short, we will only be able to give a few hints in this thesis.

First, the introduction of elliptic curves strongly encourages us to generalize our results to spaces more general than the complex plane. The second appendix, which establishes the Riemmann-Roch theorem, is a beginning of work in the direction of algebraic geometry. The combination of algebraic geometry and algebraic number theory leads us to focus on arithmetic geometry which is a rich area for research. For that, I would have to reinforce

my knowledge of algebraic geometry around the notion of schemes and algebraic variety.

Also, we have established the existence of a particular class field, so its explicit construction is a natural problem. Trying to solve the global case automatically seems counterproductive and restricting oneself to the local case seems more fruitful despite some apparent difficulty. The work of Lubin-Tate supports this and deserves to be studied in depth. The local-global principle and the adelic constructs allow us to nourish the hope of understanding the global case through local constructions.
However, a marginal interest in category theory does not seem totally superfluous either and the computer implementation of these constructions, once established, is also a rich issue.

References

[1] Algèbre Corporelle, Antoine Chambert-Loir, Editions Polytechniques, 2005

[2] Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, Wiley, 1989

[3] Class Field Theory, J. Neukirch, Springer, 1986

[4] Algebraic Number Theory, J. Neukirch Springer, Springer, 1994

[5] Elliptic Curves, Diophantine Analysis, Serge Lang, Springer, 1978

[6] Elliptic Fonction, Graduate Texts in Mathematics, Serge Lang, Springer, 1987

[7] Introduction to Algebraic and Abelian Functions, Serge Lang, Springer, 1982

[8] Théorie Algébrique des nombres, P.Samuel, Hermann, 1997

[9] On the History of Hilbert's Twelfth Problem, N.Schappacher, SMF, 1999

[10] Cohomologie Galoisienne, J.P Serre, Springer, 1994

[11] The Arithmetic of Elliptic Curves, Joseph H.Silvermann, Springer, 2009

[12] Fourier Analysis on Number Fields, D.Ramakrishnan, R.Valenza, Springer, 1999

[13] Introduction to Cyclotomic Fields, Part of the Graduate Texts in Mathematics book series (GTM, volume 83), Lawrence C. Washington, Springer, 1950-2021

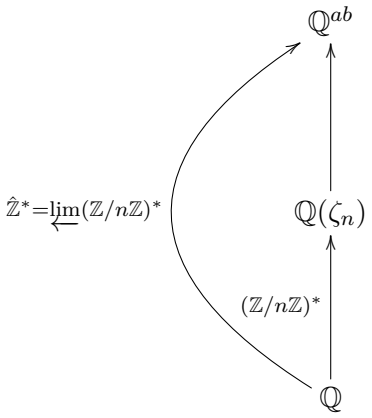
[14] Profinite groups are galois groups, W.C Waterhouse, AMS, 1974

This document is an attempt to quickly explain my master's thesis. The starting point was the Kronecker-Weber's theorem :

Théorème 5.1. *By posing $\mathbb{Q}^{ab}$ the maximal abelian extension of $\mathbb{Q}$. Then, if ζ_n is an n-th root of unity then we have :*

$$\mathbb{Q}^{ab} = \bigcup_{n\in\mathbb{N}^*} \mathbb{Q}(\zeta_n) \text{ et } \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^* = \varprojlim(\mathbb{Z}/n\mathbb{Z})^*.$$

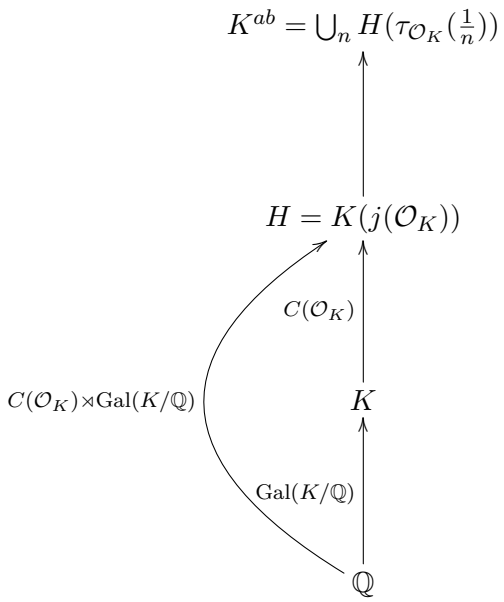
This allows to obtain the diagram below (the groups above the arrows being the associated Galois groups):



Hilbert's twelfth problem is the generalization of this theorem to all number fields which is still not solved, my thesis is interested in the case of totally imaginary quadratic fields.
Our main goal for chapter II was therefore to generalize this situation to the case of imaginary quadratic fields K. Our real goal was to establish the class field of radius $n\mathcal{O}_K$ of the field K which will play a role analogous to $\mathbb{Q}^{ab}$. To achieve this, we had to combine tools coming from two fields of mathematics (class field theory, complex analysis).
After the introduction of Weber function and show that the j-invariant is an algebraic integer, we are focus to exposes the class field of radius K for the module $n\mathcal{O}_K$. We establish the generalization of the Kronecker-Weber theorem for imaginary quadratic fields :

Théorème 5.2. *The class field of radius $n\mathcal{O}_K$ of K is $K(j(\mathcal{O}_K), \tau_{\mathcal{O}_K}(\frac{1}{n}))$. Moreover, if $\mathcal{O}$ is an order of conductor n in K then the class field of radius $n\mathcal{O}_K$ is $K(j(\mathcal{O}), \tau_{\mathcal{O}}(\omega_K))$ where $\omega_K = \frac{d_K+\sqrt{d_K}}{2}$, d_K being the discriminant of K.*

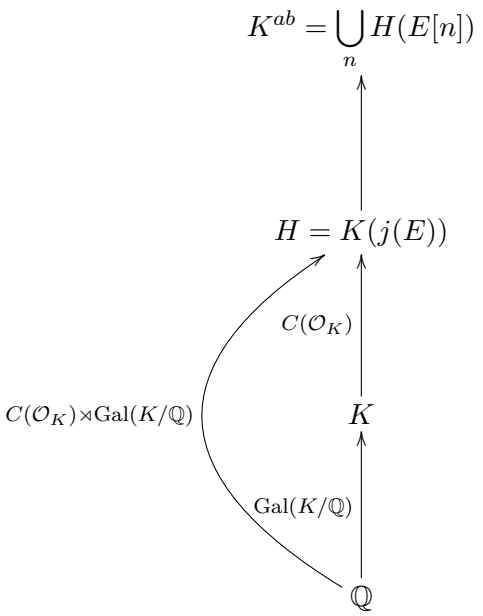
Thus, we obtain the diagram :



Finally, since elliptic functions naturally define elliptic curves, after we introduce the Weierstrass equation, we show that elliptic curves on $\mathbb{C}$ are in bijection with the lattice of $\mathbb{C}$. After that, we determine that $E(K)$ is an additive group. Then, we redefine the complex multiplication for an elliptic curve. Thus all our algebraic theory applies to elliptic curve.

Let E be an elliptic curve on $H = K(j(E))$ having $\mathcal{O}_K$ as the complex multiplication ring. Let $n \in \mathbb{N}^*$, we set $E[n]$ to the n-twisting points of E

on an algebraic closure $\overline{K}$. Thus, we can modify the last diagram:



In spite of our initial goal, these results open new questions that would deserve and could occupy us for many years to come. The time of the internship being short, we will only be able to give a few hints in this thesis.

First, the introduction of elliptic curves strongly encourages us to generalize our results to spaces more general than the complex plane. The second appendix, which establishes the Riemmann-Roch theorem, is a beginning of work in the direction of algebraic geometry. The combination of algebraic geometry and algebraic number theory leads us to focus on arithmetic geometry which is a rich area for research. For that, I would have to reinforce my knowledge of algebraic geometry around the notion of schemes and algebraic variety.

Also, we have established the existence of a particular class field, so its explicit construction is a natural problem. Trying to solve the global case automatically seems counterproductive and restricting oneself to the local case seems more fruitful despite some apparent difficulty. The work of Lubin-Tate supports this and deserves to be studied in depth. The local-global principle and the adelic constructs allow us to nourish the hope of understanding the global case through local constructions.
However, a marginal interest in category theory does not seem totally superfluous either and the computer implementation of these constructions, once established, is also a rich issue.