Galois representations and their entanglement

Riccardo Pengo

November 2023

Abstract

The aim of this mini-course, given at the University of Stellenbosch in November 2023, is to give an introduction to the theory of ℓ-adic and adelic Galois representations, with a particular emphasis on the *entanglement* phenomenon, which studies the interactions between different ℓ-adic representations when the prime ℓ varies.

Plan of the course

Each lecture will consist of one academic hour (*i.e. 45 minutes*). The plan is probably too ambitious, so don't be scared! Moreover, the program is definitely open to changes following suggestions from the audience!

Lecture 1 From $\mathbb{Z}$ to Galois representations.

Lecture 2 Reminders of finite and infinite Galois theory, and of algebraic number theory.

Lecture 3 Reminders of local fields.

Lecture 4 Local and global class field theories. Ring and ray class fields.

Lecture 5 An introduction to the Langlands program.

Lecture 6 Elliptic curves and their Galois representations.

Lecture 7 Elliptic curves with complex multiplication and ray class fields of imaginary quadratic fields: Kronecker's youth dream.

Lecture 8 Entanglement between the division fields of elliptic curves.

Warning

Given the time limitation, this course aims just at giving an overview of the themes involved. In particular, we will see essentially no proofs. I will try to use these (very brief) notes to give the appropriate references when needed. Furthermore, it could very well happen that some typo managed to sneak in these notes. I would be very glad if you signaled any mistake you may find by writing me an email.

URL: https://drive.google.com/file/d/1wKIjZTit-r3euRziu0BJPMxdVTqELnAF/view?usp=sharing

1 Introduction: from $\mathbb{Z}$ to Galois representations

The ring of rational integers $\mathbb{Z}$ is one of the simplest, but also most mysterious rings that exist in mathematical nature. In particular, the interaction between the sum and product operations on $\mathbb{Z}$ is still the object of many tantalizing conjectures, the most celebrated of which is probably due to Goldbach (who conjectured that every even integer $n \geq 4$ should be the sum of two primes).

It turns out that studying $\mathbb{Z}$ as a ring is essentially equivalent, thanks to a well known lemma of Yoneda, to studying *Diophantine equations* $f(x_1, \dots, x_n) = 0$, where $f \in \mathbb{Z}[x_1, \dots, x_n]$ is a multivariate polynomial with integer coefficients. This problem is well known to be extremely difficult. For example, a theorem of Matiyasevich, which solved the tenth of Hilbert's problems, showed that there does not exist a universal algorithm for solving such Diophantine equations. This confirms the fact that finding explicitly all the solutions of a given family of Diophantine equations is usually a very difficult task. The prototypical examples of this fact are given by Fermat's family $x^n + y^n = z^n$ and by Catalan's family $x^a - y^b = 1$.

Despite this negative news, there is a way to access the sets of integer solutions of a Diophantine equation $f(x_1, \dots, x_n) = 0$. More precisely, homogenizing the polynomial one can actually look at the set $X_f(\mathbb{Q})$ of rational solutions to this Diophantine equation. Then, such a set can be seen as the set of those algebraic solutions $X_f(\overline{\mathbb{Q}})$ which are invariant under the action of the *absolute Galois group* $\Gamma_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, the study of solutions of Diophantine equations can be reduced to the study of the absolute Galois group $\Gamma_{\mathbb{Q}}$ and of its actions.

In fact, studying a compact topological group, such as the absolute Galois group, is essentially equivalent to unraveling the mysteries behind its actions. More precisely, given a compact topological group G, the category of its complex linear representations $\Pi(G)$ can be used to reconstruct the group G in question, and its topology, thanks to a celebrated result of Tannaka. In particular, one can apply this philosophy to the absolute Galois group $G = \Gamma_F := \mathrm{Gal}(\overline{F}/F)$ of a field F.

If F is a *number field*, which is to say that F contains the field of rational numbers $\mathbb{Q}$ and is a finite dimensional vector space over it, every linear complex representation $\rho\colon \Gamma_F \to \mathrm{GL}_n(\mathbb{C})$ factors through a finite quotient $\Gamma_F \twoheadrightarrow G$. In particular, G will be the Galois group of a finite extension $L = F[x]/(f(x))$, and the resulting representation $G \to \mathrm{GL}_n(\mathbb{C})$ corresponds to the action of G on the roots of the polynomial $f(x)$.

These representations are already very rich. For example, if $F = \mathbb{Q}$, then one expects that *every* finite group G should be a quotient of $\Gamma_{\mathbb{Q}}$. This is usually known as the *inverse Galois problem*, and has been the subject of a mini-course by Angelot Behajaina, given in Stellenbosch during the spring semester of the academic year 2021/22.

During the present course, we will instead look at different fields, and even rings of coefficients. In particular, we will be interested in finite Galois representations of the form $\rho_N\colon \Gamma_F \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$. When N is a power of a single prime ℓ, one can often assemble all these representations along the quotient maps

$\mathrm{GL}_n(\mathbb{Z}/\ell^{k+1}\mathbb{Z}) \twoheadrightarrow \mathrm{GL}_n(\mathbb{Z}/\ell^k\mathbb{Z})$, and obtain a new representation $\rho_{\ell^\infty}\colon \Gamma_F \to \mathrm{GL}_n(\mathbb{Z}_\ell)$ with coefficients in the ring $\mathbb{Z}_\ell := \varprojlim_k \mathbb{Z}/\ell^k\mathbb{Z}$ of ℓ-adic integers. Taking the field of fractions of $\mathbb{Z}_\ell$, one ends up with the field of ℓ-adic numbers $\mathbb{Q}_\ell$, which can be seen as an analogue of the field of real numbers. Taking the algebraic closure $\overline{\mathbb{Q}}_\ell$ one obtains a field which is not complete any more, but taking the completion of $\overline{\mathbb{Q}}_\ell$ yields a complete and algebraically closed field $\mathbb{C}_\ell$, which is the analogue of complex numbers. Then, one can consider representations of Γ_F with coefficients in the fields $\mathbb{Q}_\ell$ and $\mathbb{C}_\ell$, which are amenable to the same Tannakian reconstruction results.

These representations are much richer than the ones with complex coefficients, thanks to the totally disconnected nature of the topology on $\mathbb{Z}_\ell$. In particular, one can associate to every algebraic variety X defined over a number field F, every pair of integers $i, j \in \mathbb{N}$, and every prime ℓ, a Galois representation

$$\rho_{X,i,j,\ell^\infty}\colon \Gamma_F \to \mathrm{GL}(H^i_{\text{ét}}(X_{\overline{F}}; \mathbb{Q}_\ell(j))) \cong \mathrm{GL}_n(\mathbb{Q}_\ell),$$

where $H^i_{\text{ét}}(X_{\overline{F}}; \mathbb{Q}_\ell(j))$ denotes the i-th *étale cohomology group* of the base change of X to the algebraic closure $\overline{F}$ of F, with coefficients in the *Tate twist* $\mathbb{Q}_\ell(j)$. In particular, the vector spaces $H^i_{\text{ét}}(X_{\overline{F}}; \mathbb{Q}_\ell(j))$ can be related to the singular cohomology of the topological space given by the complex points of X (taken along any embedding $F \hookrightarrow \mathbb{C}$), and this relation allows one to compute the dimension $n = \dim_{\mathbb{Q}_\ell}(H^i_{\text{ét}}(X_{\overline{F}}; \mathbb{Q}_\ell(j)))$ of such vector spaces.

Class field theory

Particularly interesting examples of these kinds of representations arise when $n = 1$ or $n = 2$. In the first case, one obtains the characters of the absolute Galois group Γ_F, which completely determine the abelianization $\Gamma_F^{\mathrm{ab}} := \Gamma_F / [\Gamma_F, \Gamma_F]$. This is the subject of *class field theory*, which provides a surjective map

$$[F, \cdot]\colon \mathbb{A}_F^\times \twoheadrightarrow \Gamma_F^{\mathrm{ab}},$$

known as the *Artin map*, whose kernel can be explicitly determined. Here, $\mathbb{A}_F^\times$ denotes the group of units of the *ring of adèles* $\mathbb{A}_F$ associated to the number field F, which is obtained by putting together all its different completions F_v.

The first part of the present course will consist in giving a presentation of the main results of class field theory, while recalling some basics from Galois theory and algebraic number theory.

Elliptic curves and their entanglement

In the second part of our course, we will look at two dimensional Galois representations, focusing on those that come from elliptic curves. More precisely, for every elliptic curve E defined over a number field F, one

has an isomorphism

$$H^1_{\text{ét}}(E_{\overline{F}}; \mathbb{Z}_\ell(1)) \cong T_\ell(E) := \varprojlim_k E[\ell^k](\overline{F})$$

between the first étale cohomology group of E, with coefficients in $\mathbb{Z}_\ell(1)$, and the *Tate module* $T_\ell(E)$, which is given by assembling together the different groups of torsion points $E[\ell^k](\overline{F}) \cong (\mathbb{Z}/\ell^k\mathbb{Z})^2$ along the multiplication-by-ℓ maps $[\ell]\colon E[\ell^{k+1}] \to E[\ell^k]$. In particular, this gives rise to a Galois representation

$$\rho_{E,\ell^\infty}\colon \Gamma_F \to \mathrm{GL}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell) \cong \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty](\overline{F})),$$

where $E[\ell^\infty](\overline{F})$ denotes the abelian group of those torsion points of E that have ℓ-power order. Through this isomorphism, ρ_{E,ℓ^∞} can actually be seen as the Galois representation induced by the natural action of Γ_F on the abelian group $E[\ell^\infty]$. This approach can actually be "globalized", and yields the *adelic* Galois representation

$$\rho_E\colon \Gamma_F \to \mathrm{Aut}_{\mathbb{Z}}(E_{\text{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

where $\widehat{\mathbb{Z}} := \varprojlim_N \mathbb{Z}/N\mathbb{Z}$ denotes the ring of profinite integers, and $E_{\text{tors}} := E(\overline{F})_{\text{tors}}$ denotes the group of torsion points of E.

It turns out that the Galois representation ρ_E is intimately related to the arithmetic properties of the elliptic curve E. In particular, if E does not have *complex multiplication*, a celebrated theorem of Jean-Pierre Serre shows that the image of ρ_E has finite index inside $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Finding this index, and computing this image, turn out to be two highly non-trivial tasks, which have attracted a lot of attention in the past years. In particular, it has been observed that in several cases the aforementioned image is not given by the product of the images of the ℓ-adic representations ρ_{E,ℓ^∞}. When such a phenomenon occurs, one poetically says that these representations are *entangled*.

On the other hand, when the elliptic curve E has *complex multiplication* by an order $\mathcal{O}$, the image of ρ_E is much smaller, as it is essentially contained inside the group of automorphisms of E_{tors} which respect its structure of $\mathcal{O}$-module. This group of automorphisms is abelian, and is in fact isomorphic to the units $\widehat{\mathcal{O}}^\times$ inside the profinite completion $\widehat{\mathcal{O}} := \varprojlim_N \mathcal{O}/N\mathcal{O}$ of the ring $\mathcal{O}$. The simplicity of these Galois representations allows one to study the entanglement between the division fields of elliptic curves with complex multiplication more in detail, which is what we did in two joint works with Francesco Campagna [5, 6]. Moreover, elliptic curves with complex multiplication allow one to answer affirmatively Hilber's 12th problem for imaginary quadratic fields, as given by Kronecker's insight.

In the second part of my course, I will give an overview of these results, with a focus on explicit examples.

2 A gist of Galois theory and algebraic number theory

The aim of the present lecture is to recall the essentials of Galois theory and algebraic number theory that we will need in future lectures of this course. We invite the interested reader to read the necessary proofs in [22, Chapter VI, § 1] (for the Galois theory part) and [32] (for the algebraic number theory part).

Basics on field extensions

First of all, let us recall that Galois theory deals with field extensions $K \subseteq L$, and builds a correspondence between sub-extensions of such a field extension and subgroups of the group $\mathrm{Aut}_K(L)$ of those field automorphisms $L \to L$ which fix K pointwise.

Such a correspondence does not hold always, but only under suitable assumptions. More precisely, let us recall that a field extension $K \subseteq L$ is *finite* if L is a finite dimensional K-vector space, and *algebraic* if for every $\alpha \in L$ the evaluation map

$$\Psi_\alpha \colon K[x] \to L$$
$$P(x) \mapsto P(\alpha)$$

is not injective. Since $K[x]$ is a principal ideal domain, the ideal $\ker(\Psi_\alpha)$ is always generated by a unique monic, irreducible polynomial $f_\alpha(x) \in K[x]$, which is usually referred to as the *minimal polynomial* of α.

It may happen that these minimal polynomials have actually repeated roots inside L. If this is not the case, which means that $\gcd(f_\alpha, f'_\alpha) = 1$, one says that α is *separable*. Moreover, we will call the entire extension $K \subseteq L$ *separable* if every element $\alpha \in L^\times$ is itself separable.

The notion of separability is especially important because of the so-called *primitive element theorem*, which states that every *finite* separable extension of fields $K \subseteq L$ admits a primitive element, which is an element $\alpha \in L$ such that Ψ_α is surjective. In other words, in these cases we have that $L = K(\alpha)$, where $K(\alpha) \subseteq L$ is the smallest subfield which contains both K and α.

On the other hand, it may happen that the minimal polynomial of an element of L does not have all its possible roots inside L. If this does not happen, *i.e.* if every irreducible polynomial $P \in K[x]$ which has a root in L actually splits completely in $L[x]$, we say that the extension $K \subseteq L$ is *normal*.

Finally, we say that $K \subseteq L$ is *Galois* if it is both separable and normal. When $K \subseteq L$ is also finite, being Galois is actually equivalent to being the *splitting field* of a separable polynomial $P \in K[x]$, which is the smallest field extension of K over which the polynomial splits into linear factors, and is unique up to isomorphism.

The fundamental theorem(s) of Galois theory

Let us fix any Galois extension $K \subseteq L$. Then, the group $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ admits a canonical *pro-finite* topology. More precisely, if $K \subseteq L$ is finite, we endow this group with the discrete topology. On the other hand, if $K \subseteq L$ is infinite, we observe that an automorphism $L \to L$ is determined by its restrictions on the fields $K(\alpha)$, for α varying over L. In more fancy terms, we have a group homomorphism

$$\mathrm{Gal}(L/K) \cong \varprojlim_{\substack{K \subseteq M \subseteq L \\ K \subseteq M \text{ finite Galois}}} \mathrm{Gal}(M/K), \tag{1}$$

where the inverse limit on the right hand side runs over all sub-extensions $K \subseteq M \subseteq L$ such that $K \subseteq M$ is finite and Galois. Then, the right hand side of (1) admits a canonical *inverse limit* topology, which is the coarsest topology such that for every finite sub-extension $K \subseteq M$ the projection map

$$\left(\varprojlim_{\substack{K \subseteq M \subseteq L \\ K \subseteq M \text{ finite Galois}}} \mathrm{Gal}(M/K) \right) \twoheadrightarrow \mathrm{Gal}(M/K)$$

is continuous. Therefore, (1) allows us to transfer this topology to $\mathrm{Gal}(L/K)$.

Using this topology, we can finally state the *fundamental theorem of Galois theory*, which asserts that given any Galois extension $K \subseteq L$ (which may be infinite) the following two maps

$$\begin{aligned} \{K \subseteq M \subseteq L\} &\leftrightarrow \{G \subseteq \mathrm{Gal}(L/K) \colon G \text{ is closed}\} \\ M &\mapsto \mathrm{Aut}_M(L) \\ L^G &\hookleftarrow G \end{aligned}$$

establish a bijection between closed subgroups of the *Galois group* $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ and the sub-extensions of $K \subseteq L$. Here, $L^G := \{\alpha \in L \colon \sigma(\alpha) = \alpha, \text{ for each } \sigma \in G\}$ represents the field of those elements $\alpha \in L$ which are fixed by every automorphism that belongs to the subgroup G. Under this correspondence, closed subgroups which are also open are precisely those of finite index, and hence correspond to finite extensions of K, whose degree equals the corresponding index. Moreover, normal subgroups correspond to Galois extensions of K.

Finally, let us mention that Galois groups behave well with respects to towers and composites of number fields. More precisely, if $K \subseteq M \subseteq L$ is a tower of Galois extensions, then we have an exact sequence

$$1 \to \mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \to 1,$$

where the first map is the obvious inclusion and the second map is given by restricting an automorphism from L to M. Moreover, if $K \subseteq M_1, M_2 \subseteq L$ and $K \subseteq M_1$ is Galois, then $M_2 \subseteq M_1 M_2$ is Galois, and the natural restriction map induces an isomorphism $\mathrm{Gal}(M_1 M_2/M_2) \xrightarrow{\sim} \mathrm{Gal}(M_1/M_1 \cap M_2)$. Finally, if $K \subseteq M_2$

is also Galois, then $K \subseteq M_1M_2$ is Galois, and the natural restriction maps $\mathrm{Gal}(M_1M_2/K) \to \mathrm{Gal}(M_1/K)$ and $\mathrm{Gal}(M_1M_2/K) \to \mathrm{Gal}(M_2/K)$ induce an isomorphism

$$\mathrm{Gal}(M_1M_2/K) \xrightarrow{\sim} \mathrm{Gal}(M_1/K) \times_{\mathrm{Gal}(M_1\cap M_2/K)} \mathrm{Gal}(M_2/K)$$

where the *fiber product* on the right is the group given by those pairs $(\sigma, \tau) \in \mathrm{Gal}(M_1/K) \times \mathrm{Gal}(M_2/K)$ whose restrictions to $M_1 \cap M_2$ coincide.

Algebraic number theory

In this course, we will mainly be interested in finite extensions of the rational numbers $\mathbb{Q}$, known as *number fields*. These extensions can be studied by Galois theory, but they share the unique feature that they contain some "integral" elements. More precisely, given a number field K, any element $\alpha \in K$ admits a unique monic minimal polynomial $f_\alpha(x) \in \mathbb{Q}[x]$, and α is called *integral* if $f_\alpha(x) \in \mathbb{Z}[x]$. The set of all integral elements of K forms a ring, denoted by $\mathcal{O}_K$, which goes under the name of *ring of integers* of the number field K. Sometimes, it is also interesting to study sub-rings $\mathcal{O} \subseteq \mathcal{O}_K$. When such a sub-ring has finite index, we call it an *order*.

The ring of integers $\mathcal{O}_K$ has the very important property of being a *Dedekind domain*. This means in particular that every non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ is maximal, and give rise to a finite quotient field $\mathcal{O}_K/\mathfrak{p}$. Moreover, every ideal $I \subseteq \mathcal{O}_K$ admits a unique factorization (up to permutations) $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}_K$ are prime ideals. This property fails for any other order $\mathcal{O} \subsetneq \mathcal{O}_K$, which is not a Dedekind domain anymore.

Class groups

Such a unique factorization property generalizes the usual fundamental theorem of arithmetic. However, the exact analogue of this theorem, which would predict the unique factorization of *elements* of $\mathcal{O}_K$, is not true in general, as one can see already in the case of $K = \mathbb{Q}(\sqrt{-5})$, where $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and the element 6 admits two factorizations into irreducible elements of $\mathbb{Z}[\sqrt{-5}]$, given by $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

This failure of unique factorization is particularly relevant in the case of *cyclotomic fields*, which are finite extensions of $\mathbb{Q}$ generated by *roots of unity*. In particular, any root of unity ζ_n of exact order n generates the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$, which is Galois over $\mathbb{Q}$ with Galois group given by $(\mathbb{Z}/n\mathbb{Z})^\times$, where an element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ corresponds to the unique automorphism $\sigma_a \colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ which fixes $\mathbb{Q}$ and sends ζ_n to ζ_n^a. Moreover, cyclotomic fields are *monogenic*, which means that their ring of integers is simply given by $\mathbb{Z}[\zeta_n]$. Finally, Kummer has shown that if $\mathbb{Z}[\zeta_n]$ does admit unique factorization (of elements), then the only integer solutions to $x^n + y^n = z^n$ are those for which $xyz = 0$.

In fact, one can do slightly better. To do so, we observe that there is another way of measuring when the ring of integers of a number field is not a unique factorization domain. More precisely, a Dedekind domain is

a unique factorization domain if and only if it is a principal ideal domain. Therefore, to measure how far $\mathcal{O}_K$ is from being a unique factorization domain, one can consider the *class group* $\mathrm{Cl}(\mathcal{O}_K)$, which is defined as the quotient of the group of *fractional ideals* of $\mathcal{O}_K$, which are $\mathcal{O}_K$-submodules $I \subseteq K$ such that there exists $\lambda \in K$ with the property that $\lambda I \subseteq \mathcal{O}_K$, modulo the principal ones, which have the form $\alpha \cdot \mathcal{O}_K$ for some $\alpha \in K$. It turns out that this group $\mathrm{Cl}(\mathcal{O}_K)$ is always finite. Moreover, if p is a *regular* rational prime, *i.e.* a rational prime such that $p \nmid \#\mathrm{Cl}(\mathbb{Z}[\zeta_p])$, then the only integer solutions to the Fermat equation $x^p + y^p = z^p$ are once again the trivial ones. Unfortunately, the class groups of cyclotomic fields can be quite big, and there are infinitely many primes p which are *irregular* (see [42, Theorem 5.17]), the smallest of which is $p = 37$.

Decomposition of primes

Going back to general number fields, one can ask if it is possible to compute $\mathrm{Cl}(\mathcal{O}_K)$, or at least to bound its size, in terms of other invariants of K.

To this end, let us take an extension of number fields $K \subseteq L$, which induces an extension of rings of integers $\mathcal{O}_K \subseteq \mathcal{O}_L$. Then, given a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, one can consider the extended ideal $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. It turns out that every element of this factorization can be computed in a very explicit way, thanks to a result of Kummer and Dedekind. More precisely, suppose that there exists $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$ and $\mathfrak{p} \nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]\mathcal{O}_K$, and let $\phi \in \mathcal{O}_K[x]$ denote the minimal polynomial of α over K. Then, the reduction of ϕ modulo $\mathfrak{p}$ factorizes as $\phi = g_1^{e_1} \cdots g_r^{e_r}$, and $\mathfrak{P}_j = \mathfrak{p}\mathcal{O}_K + g_j(\alpha)$ for every $j \in \{1, \dots, r\}$. Finally, we also have that $\deg(g_j) = |\mathcal{O}_L/\mathfrak{P}_j : \mathcal{O}_K/\mathfrak{p}|$ for each $j \in \{1, \dots, r\}$.

The invariants $e_1, \dots, e_r$ are the *ramification indices* of $\mathfrak{p}$ in the extension $K \subseteq L$, while the other invariants $f_j := |\mathcal{O}_L/\mathfrak{P}_j : \mathcal{O}_K/\mathfrak{p}|$ are the *inertia degrees* of the prime $\mathfrak{p}$ inside the aforementioned extension. These invariants satisfy the formula $e_1 f_1 + \cdots + e_r f_r = [L : K]$. When the extension $K \subseteq L$ is Galois, the group $\mathrm{Gal}(L/K)$ acts *transitively* on the set $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$, which implies that $e_1 = \cdots = e_r =: e$, and analogously that $f_1 = \cdots = f_r =: f$. Therefore, in this case we see that $efr = [L : K]$.

These definitions allow us to say that a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ is *ramified* in the extension $K \subseteq L$ if there exists a prime $\mathfrak{P} \subseteq \mathcal{O}_L$ such that $e(\mathfrak{P} \mid \mathfrak{p}) > 1$. One can prove that this happens if and only if $\mathfrak{P}$ divides the *different ideal* $\mathfrak{D}_{L/K} \subseteq \mathcal{O}_L$, which is the inverse of the *complementary module* $\mathfrak{C}_{L/K} := \{\alpha \in L \mid \mathrm{Tr}(\alpha\mathcal{O}_L) \subseteq \mathcal{O}_K\}$. In particular, the norm of $\mathfrak{D}_{L/K}$ is the so-called *relative discriminant* $\Delta_{L/K} \subseteq \mathcal{O}_K$ of $K \subseteq L$. When $K = \mathbb{Q}$, we have a preferred generator of $\Delta_{L/\mathbb{Q}}$, given by the *absolute discriminant*

$$\Delta_L := \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \cdots & \sigma_n(b_n) \end{pmatrix}^2,$$

where $n = [L\colon \mathbb{Q}]$ and $\sigma_1, \dots, \sigma_n\colon L \hookrightarrow \mathbb{C}$ denote all the possible embeddings of L in $\mathbb{C}$, while $b_1, \dots, b_n$ denotes a $\mathbb{Z}$-basis of $\mathcal{O}_L$.

This invariant is quite powerful. In particular, a famous theorem of Hermite tells us that there are only finitely many isomorphism classes of number fields K such that the absolute value of Δ_K is bounded. Finally, we are able, thanks to the absolute discriminant of a number field, to answer the question we asked in the beginning. More precisely, one can prove that every class $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_K)$ admits a representative I whose absolute norm $\mathrm{N}(I) := |\mathcal{O}_K/I|$ is bounded above by $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}$, where $n = [K\colon \mathbb{Q}]$ is the degree of K, and r_2 denotes the number of complex embeddings of K which are not real, counted up to complex conjugation.

Unit groups

Another crucial invariant of a number field is given by its group of units $\mathcal{O}_K^\times$, which is a finitely generated abelian group, thanks to a theorem of Dirichlet. Even better, if we write

$$\{\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \dots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}\}$$

for all the embeddings $K \hookrightarrow \mathbb{C}$, the map

$$\begin{aligned} \mathcal{O}_K^\times &\to \mathbb{R}^{r_1+r_2} \\ x &\mapsto (\log|\sigma_j(x)|)_{j=1}^{r_1+r_2} \end{aligned}$$

embeds $\mathcal{O}_K^\times$ as a lattice inside the hyperplane $\{(v_1, \dots, v_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2}\colon v_1 + \cdots + v_{r_1+r_2} = 0\}$.

3 Local fields

The aim of this lecture is to recall some basic notions about local fields, which can be found (with all the necessary proofs) in Serre's seminal account [39].

Let K be a field. Then, an *absolute value* on K is a map of sets $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ such that $|x| = 0$ if and only if $x = 0$, while $|xy| = |x| \cdot |y|$ and $|x + y| \leq |x| + |y|$ for every $x, y \in K$. Such an absolute value clearly induces a metric on K, by setting the distance between $x \in K$ and $y \in K$ to be $|x - y|$. This in turn induces a topology on K, and two absolute values $|\cdot|$ and $|\cdot|'$ are said to be *equivalent* if they induce the same topology. This turns out to be equivalent to the fact that $|\cdot|' = |\cdot|^t$ for some $t \in \mathbb{R}_{>0}$, or to the fact that $\{x \in K\colon |x| < 1\} = \{x \in K\colon |x|' < 1\}$. Equivalence classes of absolute values are called *places*, and the set of places of a given field K will be denoted by $\mathfrak{M}_K$.

Examples of absolute values include:

- the *trivial absolute value* $|\cdot|_{\mathrm{triv}}$, defined as $|x|_{\mathrm{triv}} = 1$ for every $x \in K^\times$ (and as $|x|_{\mathrm{triv}} = 0$ when $x = 0$);

- the usual absolute values $|\cdot|_{\mathbb{R}}\colon \mathbb{R} \to \mathbb{R}_{\geq 0}$ and $|\cdot|_{\mathbb{C}}\colon \mathbb{C} \to \mathbb{R}_{\geq 0}$;
- the $\mathfrak{p}$-adic absolue values $|\cdot|_{\mathfrak{p}}$ on a number field K. More precisely, if $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal, we define $|x|_{\mathfrak{p}} = \#(\mathcal{O}_K/\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)}$, where $\mathrm{ord}_{\mathfrak{p}}(x) \in \mathbb{Z}$ denotes the unique integer such that $x \cdot \mathcal{O}_K = \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x)} \cdot \mathfrak{a}$ for some fractional ideal $\mathfrak{a}$ which is coprime to $\mathfrak{p}$.

Archimedean and non-Archimedean absolute values

The last family of absolute values are all *non-Archimedean*, which means that $|x+y| \leq \max(|x|, |y|)$. The name comes from the fact that, for these fields, we have that $|nx| \leq |x|$ for every $n \in \mathbb{N}$, which implies that we cannot get arbitrarily big just by taking multiples of a given element $x \in K^\times$. It is easy to see that if a given absolute value is Archimedean or non-Archimedean, so is any absolute value equivalent to it. Therefore, given a field K, it is reasonable to partition the set of places $\mathfrak{M}_K$ into the set of non-Archimedean places $\mathfrak{M}_K^\infty$ and the set of Archimedean places $\mathfrak{M}_{K,\infty}$.

In a non-Archimedean valued field $(K, |\cdot|)$, the closed unit ball $\mathcal{O}_K = \{x \in K\colon |x| \leq 1\}$ is a local ring, with maximal ideal $\mathfrak{m}_K$ given by the open unit ball. In the case of the $\mathfrak{p}$-adic absolute values defined on a number field F, this local ring coincides with the localization of $\mathcal{O}_F$ at $\mathfrak{p}$, given by all the fractions $x/y \in F$ with $x \in \mathcal{O}_F$ and $y \in \mathcal{O}_F \setminus \mathfrak{p}$.

It turns out that the classes of the absolute values $|\cdot|_{\mathfrak{p}}$ yield all the possible non-Archimedean places of a number field F. On the other hand, the Archimedean ones are given by the equivalence classes of the absolute values induced by the complex embeddings $F \hookrightarrow \mathbb{C}$, taken up to the action of complex conjugation. Thanks to this result, which is due to Ostrowski, we can partition $\mathfrak{M}_K$ into the set of non-Archimedean places $\mathfrak{M}_K^\infty$, which is in bijection with prime ideals, and the set of Archimedean places $\mathfrak{M}_{K,\infty}$. The latter can be partitioned again into the set of real places $\mathfrak{M}_{K,\mathbb{R}}$, corresponding to real embeddings $K \hookrightarrow \mathbb{R}$, and the set of complex places $\mathfrak{M}_{K,\mathbb{C}}$, which correspond to embeddings $K \hookrightarrow \mathbb{C}$, taken up to complex conjugation, whose image is not contained in $\mathbb{R}$.

Since valued fields are metric spaces, we have the notions of convergence and completeness of such metric spaces. In particular, if K is a valued field, one can consider its completion $K^\wedge$, given by the set of Cauchy sequences in K modulo those sequences that converge to zero. Endowing $K^\wedge$ with pointwise addition and multiplication allows us to see $K^\wedge$ as the complete valued field which is closest to K. In particular, we have a canonical inclusion $K \hookrightarrow K^\wedge$ whose image is dense in $K^\wedge$.

In the Archimedean case, the only complete valued fields (up to isomorphism) are $\mathbb{R}$ and $\mathbb{C}$. On the other hand, we have many possible non-Archimedean complete valued fields. First of all, for any subgroup $H \subseteq \mathbb{R}_{>0}$ there exists a complete valued field K such that $|K^\times| = H$. Moreover, even if we restrict to complete valued fields K such that $|K^\times|$ is discrete, which implies that the maximal ideal $\mathfrak{m}_K$ of the valuation ring $\mathcal{O}_K$

is principal, we get a plethora of possibilities.

Such examples include for instance the field of p-adic numbers $\mathbb{Q}_p$, obtained as the completion of the field of rational numbers $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$. Similarly, we have the fields of formal Laurent series $\mathbb{F}_p((T))$ over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In fact, these are all the possible complete, non-Archimedean, non-trivially valued fields which are also locally compact topological spaces.

Let us recall that, if K is a complete, non-Archimedean and non-trivially valued field then

$$\mathcal{O}_K = \left\{ \sum_{n=0}^{+\infty} a_n \pi^n : a_n \in S \right\} \cong \varprojlim_n \frac{\mathcal{O}_K}{\mathfrak{m}_K^n}$$

where $S \subseteq \mathcal{O}_K$ is any set of representatives for the residue field $\mathcal{O}_K/\mathfrak{m}_K$, and $\pi \in A$ denotes any *uniformizer*, *i.e.* any generator of $\mathfrak{m}_K$. In particular, if $K = \mathbb{Q}_p$ then we have that

$$\mathcal{O}_K = \mathbb{Z}_p = \left\{ \sum_{n=0}^{+\infty} a_n p^n : a_n \in \{0, \dots, p-1\} \right\} \cong \varprojlim_n \frac{\mathbb{Z}_p}{p^n \mathbb{Z}_p} \cong \varprojlim_n \frac{\mathbb{Z}}{p^n \mathbb{Z}}$$

with maximal ideal $\mathfrak{m}_K = p\mathbb{Z}_p$.

Hensel's lemma

The notion of complenetess of a non-Archimedean field K is important because it allows one to find the roots of a polynomial $f \in \mathcal{O}_K[x]$ by Newton's method. More precisely, for every element $\alpha_0 \in K$ such that $|f(\alpha_0)| < |f'(\alpha_0)|^2$, there exists a unique $\alpha \in K$ such that $f(\alpha) = 0$ and $|\alpha - \alpha_0| < |f'(\alpha_0)|$, which can be constructed as the limit of the sequence $\{\alpha_n\}$ defined recursively by setting $\alpha_{n+1} = \alpha_n - f(\alpha_n)/f'(\alpha_n)$. In particular, as in the classical case, Newton's method allows us to double the precision of our guessed answer at every step, thanks to the estimate $|\alpha_{n+1} - \alpha_n| \leq |f'(\alpha_0)| \cdot |f(\alpha_0)/f'(\alpha_0)^2|^{2^{n-1}}$. This allows in particular to find the roots of f by finding its roots in one of the finite rings $\mathcal{O}_K/\mathfrak{m}_K^n$, which can then be lifted to the required α_0.

Extension of absolute values

Moreover, completeness helps also when one wants to study finite dimensional vector spaces over a valued field, because if this field is complete than all the norms on a given finite dimensional vector space are equivalent.

This allows one to show that given a finite field extension $K \subseteq L$, any absolute value $|\cdot|_K : K \to \mathbb{R}_{\geq 0}$ which makes K into a complete valued field admits a *unique* extension to L, given by $|x|_L = \sqrt[d]{|\mathrm{N}_{L/K}(x)|_K}$, which makes L into a complete valued field as well. Moreover, in the non-Archimedean case the ring $\mathcal{O}_L$ is the integral closure of the ring $\mathcal{O}_K$ inside L.

A similar statement holds true for valued fields which are not complete. More precisely, if $K \subseteq L$ is a finite extension of fields, there exists a unique sub-extension $K \subseteq M \subseteq L$ such that $K \subseteq M$ is separable and $M \subseteq L$ is purely inseparable. In this second case, it is easy to see that any absolute value on M extends uniquely to L. Looking at the extension $K \subseteq M$, we know that $M = K(\alpha)$ for some $\alpha \in M$ with minimal polynomial $f_\alpha \in K[x]$. Then, the possible extensions to M of a given absolute value $|\cdot|_v$ on K, representing a place $v \in \mathfrak{M}_K$ are in bijection with the irreducible factors of f_α over the completion K_v of K with respect to this absolute value. Moreover, we have a canonical isomorphism $K_v \otimes_K L \cong \prod_{w|v} L_w$.

Unramified and totally ramified extensions

Using these notions, one can say that an extension of non-Archimedean valued fields $K \subseteq L$ is *unramified* if $|K^\times|_K = |L^\times|_L$, and *totally ramified* if $\mathcal{O}_K/\mathfrak{m}_K = \mathcal{O}_L/\mathfrak{m}_L$. In general, any algebraic extension $K \subseteq L$ has a maximal sub-extension $K \subseteq M \subseteq L$ such that $K \subseteq M$ is unramified and $M \subseteq L$ is totally ramified, because the compositum of two unramified extensions is again unramified.

Finite unramified extensions of complete, discretely valued fields are known to be in bijection with the finite and separable extensions of their residue fields. Moreover, this bijection preserves the automorphism groups. In other words, if $K \subseteq L$ is a finite unramified extension of a complete, discretely valued field K then $\mathrm{Aut}_K(L) \cong \mathrm{Aut}_{\kappa_K}(\kappa_L)$, where $\kappa_K = \mathcal{O}_K/\mathfrak{m}_K$ and $\kappa_L = \mathcal{O}_L/\mathfrak{m}_L$.

On the other hand, any finite and totally ramified extension $K \subseteq L$ of a complete, discretely valued field K is generated by any of its uniformizers $\pi \in \mathcal{O}_L$. Moreover, the minimal polynomial $f(x) = \sum_{j=0}^{d} a_j x^j \in \mathcal{O}_K[x]$ of any such uniformizer is *Eisenstein*, which means that $a_0, \dots, a_{n-1} \in \mathfrak{m}_K$ while $a_n \notin \mathfrak{m}_K$ and $a_0 \notin \mathfrak{m}_K^2$. Finally, given such a finite, totally ramified extension $K \subseteq L$ whose degree $d = [L\colon K]$ is coprime with the residual characteristic of K, we can take the uniformizer of L to be the d-th root of some uniformizer of K.

Ramification filtration

Something quite interesting happens if we combine Galois theory with the theory of complete and non-Archimedean fields. Namely, if $K \subseteq L$ is a finite, Galois extension of complete and discretely valued fields, we can define a filtration $\{G_n(L/K)\}_{n\in\mathbb{Z}}$ on $\mathrm{Gal}(L/K)$, which is given by

$$G_n(L/K) := \{\sigma \in \mathrm{Gal}(L/K)\colon |x - \sigma(x)|_L \leq |\pi_L|_L^{n+1} \text{ for all } x \in \mathcal{O}_L\},$$

where $\pi_L \in \mathcal{O}_L$ is any uniformizer. Clearly $G_n(L/K) = \mathrm{Gal}(L/K)$ for every $n \leq -1$.

The first ramification group $G_0(L/K)$ is the so-called *inertia group* of the extension $K \subseteq L$. It is not difficult to see that, if the extension of residue fields $\kappa_K \subseteq \kappa_L$ is separable, then it is Galois, and moreover reducing modulo the maximal ideal induces a surjective map

$$\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(\kappa_L/\kappa_K),$$

whose kernel is precisely $G_0(L/K)$. This implies that the invariant field $L^{G_0(L/K)}$ is precisely the maximal unramified extension of $K \subseteq L$. Therefore, $G_0(L/K) = \{1\}$ if and only if $K \subseteq L$ is unramified.

The higher ramification groups $\{G_n(L/K)\}_{n=1}^{+\infty}$ are related to the unit groups

$$U_L^{(n)} := \{x \in \mathcal{O}_L^\times \mid x - 1 \in \mathfrak{m}_L^n\},$$

thanks to the maps

$$\begin{aligned} G_n(L/K) &\to \frac{U_L^{(n)}}{U_L^{(n+1)}} \\ \sigma &\mapsto \frac{\sigma(\pi_L)}{\pi_L} \end{aligned}$$

which do not depend on the choice of the uniformizer π_L, and whose kernel is $G_{n+1}(L/K)$.

This implies that the invariants $L^{G_1(L/K)}$ under the *wild inertia group* $G_1(L/K)$ coincide with the largest sub-extension of $K \subseteq L$ that is tamely ramified, *i.e.* whose ramification index $(|L^{G_1(L/K)}| : |K^\times|)$ is co-prime with the residual characteristic of K. Moreover, the quotient $G_0(L/K)/G_1(L/K)$ is a cyclic group of order prime to p, whereas for every $n \geq 1$ the quotient $G_n(L/K)/G_{n+1}(L/K)$ is a product of cyclic groups of order p.

In order to define the ramification filtration for infinite extensions, it is useful to change the numbering a little bit. More precisely, the ramification filtration that we just defined are not compatible with quotients. More precisely, suppose that $K \subseteq L$ is a finite Galois extension of local fields, and that $H \trianglelefteq G := \mathrm{Gal}(L/K)$ is a normal subgroup, corresponding to the finite Galois extension $K \subseteq M := L^H$. Then, a theorem of Herbrand allows us to compute the ramification filtration $\{G_n(M/K)\}_{n\in\mathbb{Z}}$ in terms of the ramification filtration $\{G_n(L/K)\}_{n\in\mathbb{Z}}$. More precisely, $(G_n(L/K) \cdot H)/H = G_{\phi_{L/M}(n)}(M/K)$ for every $n \in \mathbb{Z}$, where $\phi_{L/M} \colon [-1, +\infty[\to \mathbb{R}$ is the function defined by $\phi_{L/M}(u) := u$ for $u \in [-1, 0]$ and by setting

$$\phi_{L/M}(u) := \int_0^u \frac{dt}{(G_0(L/M) : G_{\lceil t \rceil}(L/M))}$$

whenever $u \geq 0$. In particular, for every finite Galois extension $K \subseteq L$, the function $\phi_{L/K}$ is continuous and strictly increasing. Therefore, it admits a continuous inverse $\psi_{L/K} \colon [-1, +\infty[\to \mathbb{R}$ which allows us to define the ramification filtration in upper numbering by setting $G^u(L/K) := G_{\lceil \psi_{L/K}(u) \rceil}(L/K)$ for every real number $u \geq -1$. Thanks to Herbrand's theorem, we see that $G^u(L^H/K) = (G^u(L/K) \cdot H)/H$ for every $u \in [-1, +\infty[$, which allows one to define the ramification filtration in upper numbering of an infinite Galois extension $K \subseteq L$ by setting

$$G^u(L/K) := \varprojlim_{\substack{K \subseteq M \subseteq L \\ K \subseteq M \text{ finite Galois}}} G^u(M/K)$$

for every $u \in [-1, +\infty[$.

Exercises

- Prove that, given any prime p, the p-adic expansion of $\alpha \in \mathbb{Q}_p$ is eventually periodic if and only if $\alpha \in \mathbb{Q}$.
- What are the roots of unity contained in $\mathbb{Q}_p$?
- Given any discretely valued field K, there is an associated *valuation* $v_K \colon K \to \mathbb{Z} \cup \{+\infty\}$, defined as $v_K(x) := \log|x|_K / \log|\pi_K|_K$. Prove that, if $K \subseteq L$ is a finite extension of complete and discretely valued fields, then $(|L^\times|_L \colon |K^\times|_K) = v_L(\pi_K)$.
- Show that the ramification filtration $G_n(L/K)$ becomes trivial for $n \gg 1$.
- Fix a prime p and an element $c \in \mathbb{Z}_p^\times$. Let $\mathbb{Q}_p \subseteq K$ be the splitting field of $x^p - c$. Compute the ramification filtration on $\mathrm{Gal}(K/\mathbb{Q}_p)$.

4 Class field theory

The aim of this lecture is to address the problem of describing the abelian extensions of different kinds of fields. This description, which goes under the name of *class field theory*, is due to the great efforts of many mathematicians in the beginning of the twentieth century, such as Artin, Chevalley, Hasse, Takagi, *etc.*... For a complete account with proofs we refer the interested reader to Neukirch's book [32, Chapter VI].

Finite fields

First of all, let us start with the finite field $\mathbb{F}_p$. In this case, we know that *every* finite extension of $\mathbb{F}_p$ is abelian, and that in fact there is exactly one for each degree d, whose Galois group is cyclic. A distinguished generator of this group is given by the Frobenius element $\mathrm{Frob}(x) = x^p$. Therefore, we get a family of isomorphisms

$$\begin{aligned} \mathbb{Z}/d\mathbb{Z} &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \\ a &\mapsto \mathrm{Frob}^a, \end{aligned}$$

which in turn induces an isomorphism $\widehat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)^{\mathrm{ab}} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. More generally, given a finite field κ, the map $a \mapsto \mathrm{Frob}_\kappa^a$, where $\mathrm{Frob}_\kappa(x) = x^{|\kappa|}$, induces a map of groups

$$[\kappa, \cdot] \colon \mathbb{Z} \to \mathrm{Gal}(\overline{\kappa}/\kappa)^{\mathrm{ab}} = \mathrm{Gal}(\overline{\kappa}/\kappa), \tag{2}$$

which yields an isomorphism $\widehat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Gal}(\overline{\kappa}/\kappa)^{\mathrm{ab}} = \mathrm{Gal}(\overline{\kappa}/\kappa)$.

Local fields

In the case of local fields K, it turns out that there exists a unique continuous group homomoprphism

$$[K,\cdot]\colon K^\times \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

such that $[K,\mathcal{O}_K^\times] = \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{unr}})$ and the induced map $\mathbb{Z} \cong K^\times/\mathcal{O}_K^\times \to \mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \mathrm{Gal}(\overline{\kappa}_K/\kappa_K)$ coincides with the map (2), while for every finite extension $K \subseteq L$ we get a commutative diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{[L,\cdot]} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}_{L/K}} \\ K^\times & \xrightarrow[[K,\cdot]]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

which involves the norm map $\mathrm{N}_{L/K}\colon L^\times \to K^\times$ and the restriction map $\mathrm{res}_{L/K}\colon \mathrm{Gal}(L^{\mathrm{ab}}/L) \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

The continuous group homomorphism $[K,\cdot]$, which goes under the name of *local Artin map*, induces an isomorphism $\widehat{K^\times} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$ between the profinite completion of $K^\times$ and the abelianization of the absolute Galois group of K. Therefore, the finite abelian extensions $K \subseteq L$ inside a fixed separable closure are in bijection with open subgroups $U \subseteq K^\times$ of finite index. More precisely, for every finite abelian extension $K \subseteq L$ there exists a unique open subgroup of finite index $U \subseteq K^\times$ such that $L = (K^{\mathrm{ab}})^{[K,U]}$, which can be recovered from the finite abelian extension $K \subseteq L$ because $U = \mathrm{N}_{L/K}(L^\times)$. Moreover, it turns out that for every abelian extension $K \subseteq L$, the unit groups $1+\mathfrak{m}_K^n$ map to the higher ramification groups in upper numbering $G^n(L/K)$ via the Artin map.

To prove the main statements of local class field theory exposed in this section, one can construct explicitly the abelian extensions of K that correspond to the unit groups $1+\mathfrak{m}_K^n$, and then assemble the information obtained from those to conclude. This construction proceeds by adding to K the roots of the iterates of some polynomial $f(x) \in \mathcal{O}_K[x]$ which is congruent to $x^{|\kappa_K|}$ modulo $\mathfrak{m}_K$. Such an idea is due to *Lubin* and *Tate*, and allows one to obtain a rather easy and constructive proof of local class field theory.

Global fields

Let K be a global field, *i.e.* a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(T)$. Then, we can glue together all the local Artin maps $[K_v,\cdot]\colon K_v^\times \to \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)$ associated to the completions K_v of K into a *global Artin map*.

As in the local case, this map will emanate from a group of units. However, instead of taking the units of our number field K, we need to take the group of units of the much bigger ring of adèles

$$\mathbb{A}_K := \prod_{v\in\mathfrak{M}_K}{}' (K_v\colon \mathcal{O}_{K_v}),$$

which consists of sequences $(x_v)_v \in \prod_{v\in\mathfrak{M}_K} K_v$ such that $x_v \in \mathcal{O}_{K_v}$ for all but finitely many places $v \in \mathfrak{M}_K$. Pointwise addition and multiplication make $\mathbb{A}_K$ into a ring, which admits also a canonical topology, whose

basis of open sets is given by products of the form $\prod_{v\in\mathfrak{M}_K} U_v$ where each $U_v \subseteq K_v$ is open, and $U_v = \mathcal{O}_{K_v}$ for all but finitely many places $v \in \mathfrak{M}_K$. Moreover, the diagonal map $K \hookrightarrow \mathbb{A}_K$ includes K as a discrete and co-compact subgroup of $\mathbb{A}_K$. The unit group

$$\mathbb{A}_K^\times = \prod_{v\in\mathfrak{M}_K}{}' (K_v^\times : \mathcal{O}_{K_v}^\times),$$

goes under the name of *idèle group*, and is the domain of the *global Artin map*.

More precisely, there exists a unique surjective, continuous group homomorphism

$$[K,\cdot]\colon \mathbb{A}_K^\times \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \tag{3}$$

such that for every place $v \in \mathfrak{M}_K$ we have a commutative diagram

$$\begin{array}{ccc} K_v^\times & \xrightarrow{[K_v,\cdot]} & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \\ \downarrow & & \downarrow \\ \mathbb{A}_K^\times & \xrightarrow{[K,\cdot]} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

which relates the local and global Artin maps, and for every finite extension $K \subseteq L$ we have a commutative diagram

$$\begin{array}{ccc} \mathbb{A}_L^\times & \xrightarrow{[L,\cdot]} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}_{L/K}} \\ \mathbb{A}_K^\times & \xrightarrow[[K,\cdot]]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

where $\mathrm{N}_{L/K}\colon \mathbb{A}_L^\times \to \mathbb{A}_K^\times$ is the *idelic norm map*, defined as $\mathrm{N}_{L/K}((x_w)_{w\in\mathrm{M}_L}) = \left(\prod_{w|v} \mathrm{N}_{L_w/K_v}(x_w)\right)_{v\in\mathfrak{M}_K}$.

In fact, one can define explicitly the global Artin map $[K,\cdot]$ as a combination of the local Artin maps $[K_v,\cdot]$. More precisely, for every finite abelian extension $K \subseteq L$ and every idéle $(x_v)_v \in \mathbb{A}_K^\times$, the expression $\prod_{v\in\mathfrak{M}_K}[K_v, x_v]$ makes sense as an element of $\mathrm{Gal}(L/K)$, because $[K_v, x_v] = 1$ whenever v is unramified in $K \subseteq L$ and $x_v \in \mathcal{O}_{K_v}^\times$. Passing to the inverse limit along all possible finite abelian extensions $K \subseteq L$, we obtain a map

$$\begin{aligned} \mathbb{A}_K^\times &\to \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ (x_v)_v &\mapsto \prod_{v\in\mathfrak{M}_K} [K_v, x_v] \end{aligned}$$

which can be seen to satisfy all the required conditions above, and therefore coincides with the global Artin map $[K,\cdot]$.

The global Artin map can also be used to obtain an explicit description of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. More precisely, the kernel of the global Artin map can be described as the inverse image of the connected component of the identity of the idelic class group $\mathbb{A}_K^\times/K^\times$. More explicitly, the kernel of the global Artin map is the topological closure of the product $K^\times \cdot K_\infty^+$, where $K_\infty := \prod_{v|\infty} K_v$ denotes the product of the Archimedean completions of K, and $K_\infty^+ = \left(\prod_{v\in\mathfrak{M}_{K,\mathbb{R}}} \mathbb{R}_{>0}\right) \times \left(\prod_{v\in\mathfrak{M}_{K,\mathbb{C}}} \mathbb{C}^\times\right)$ denotes the connected component of the identity of $K_\infty^\times$.

Hilbert and ray class fields

The previous notions of global class field theory allow one to define a family of finite abelian extensions of any number field K whose union equals the whole maximal abelian extension K^{ab}. In particular, when $K = \mathbb{Q}$ we will see in the next paragraph that these extensions coincide with the cyclotomic fields.

These fields will be associated to *moduli*, which are formal linear combinations $\mu = \sum_{v \in \mathfrak{M}_K} \mu_v[v]$ of the places of K, with coefficients in the natural numbers $\mathbb{N}$, such that $\mu_v = 0$ for all but finitely many places. More precisely, given any such formal linear combination, one can define a subgroup $U_K^\mu \subseteq \mathbb{A}_K^\times$ by setting

$$U_K^\mu := \prod_{v \in \mathfrak{M}_K} U_K^\mu(v)$$

where $U_K^\mu(v) := 1 + \mathfrak{m}_{K_v}^{\mu_v}$ if $v \in \mathfrak{M}_K^\infty$, while $U_K^\mu(v) := \mathbb{R}_{>0}$ if $K_v \cong \mathbb{R}$ and $\mu_v \neq 0$, whereas $U_K^\mu(v) := \mathbb{R}^\times$ if $K_v \cong \mathbb{R}$ and $\mu_v = 0$, and $U_K^\mu(v) := \mathbb{C}^\times$ whenever $K_v \cong \mathbb{C}$. This allows us to define the *ray class field* H_μ associated to μ by setting $H_\mu := (K^{\mathrm{ab}})^{[K, U_K^\mu]}$. By definition, this is an abelian extension of K, whose Galois group is given by

$$\mathrm{Gal}(H_\mu / K) \cong \frac{\mathbb{A}_K^\times}{K^\times \cdot U_K^\mu},$$

as follows from the fact that $K^\times \cdot U_K^\mu$ contains the kernel of the Artin map $[K, \cdot]$.

The reason why these fields are called *ray class fields* stems from the classical description of class field theory. More precisely, to every modulus μ one can associate a *ray* of principal ideals

$$\mathcal{P}_K^\mu := \left\{ \alpha \mathcal{O}_K \colon \alpha \in \bigcap_{v \in \mathfrak{M}_K} (U_K^\mu(v) \cap \mathcal{O}_K) \right\},$$

whose name comes from the fact that if $\alpha \mathcal{O}_K \in \mathcal{P}_K^\mu$ then $\iota_v(\alpha) > 0$ for every $v \in \mathfrak{M}_K^\infty$ such that $K_v \cong \mathbb{R}$ and $\mu_v \neq 0$. Then, we can also define the group of ideals associated to μ by setting

$$\mathcal{I}_K^\mu := \left\{ I \subseteq \mathcal{O}_K \colon I + \prod_{v \in \mathfrak{M}_K^\infty} \mathfrak{p}_K^{\mu_v} = \mathcal{O}_K \right\},$$

and we have an isomorphism $\mathrm{Gal}(H_\mu / K) \cong \mathcal{I}_K^\mu / \mathcal{P}_K^\mu$.

As said before, ray class fields "exhaust" all the possible finite abelian extensions of a number field. More precisely, the groups U_K^μ form a basis of open neighborhoods of the identity inside $\mathbb{A}_K^\times$. This means in particular that given any finite abelian extension $K \subseteq L \subseteq K^{\mathrm{ab}}$, there exists a modulus μ such that $L \subseteq H_\mu$. The minimal such μ that is possible is usually called the *conductor* of the abelian extension $K \subseteq L$.

Finally, if we let $\mathbf{0}$ denote the modulus such that $\mathbf{0}_v = 0$ for every $v \in \mathfrak{M}_K$, the associated ray class field goes under the name of *Hilbert class field* for the number field K, and is usually denoted by H. It is easy to see that the only places v that ramify in a ray class field $K \subseteq H_\mu$ are those such that $\mu_v \neq 0$. Therefore, nothing ramifies in the Hilbert class field, which is indeed the maximal abelian unramified extension of a number

field K. Moreover, the above description of the Galois group of a ray class field in terms of ideals implies that $\mathrm{Gal}(H/K) \cong \mathrm{Pic}(\mathcal{O}_K)$, which gives a way to realize the class group of a number field as the Galois group of one of its extensions.

The Kronecker-Weber theorem

What happens to these general statements when we specialize them to $K = \mathbb{Q}$? In this case, to every modulus μ we can associate an integer $n_\mu := \prod_p p^{\mu_p}$. Then, one can prove that $H_\mu = \mathbb{Q}(\zeta_{n_\mu})$ if $\mu_\infty \neq 0$, and that $H_\mu = \mathbb{Q}(\zeta_{n_\mu} + \zeta_{n_\mu}^{-1})$ otherwise. This implies that every finite abelian extension of $\mathbb{Q}$ is contained inside a cyclotomic extension, which is a theorem due to *Kronecker* and *Weber*.

5 An introduction to the Langlands program

In the previous lecture we have seen how one can explicitly describe the abelianization of the absolute Galois group $\Gamma_F := \mathrm{Gal}(\overline{F}/F)$ of a finite, local or global field F in terms of other explicitly definable groups, such as the units of F (in the case of local fields) or the units of the adèle ring associated to F (in the case of a global field).

The absolute Galois group of a local field

A natural question is whether one can obtain a similar description of the whole Galois group Γ_F. This is possible when F is a local field. More precisely, if F is has positive characteristic, then Γ_F is a semi-direct product between the Galois group $\mathrm{Gal}(F^{\mathrm{tame}}/F)$ of the maximal tamely ramified extension of F together with a free group on infinitely many generators, as shown by Koch [21]. When F is a finite extension of $\mathbb{Q}_p$ we also know an explicit presentation of Γ_F, thanks to work of Jannsen and Wingberg [18]. More precisely, the Galois group Γ_F has $[F\colon \mathbb{Q}_p] + 3$ generators. One of these, commonly denoted by σ, lifts the Frobenius endomorphism which generates $\mathrm{Gal}(F^{\mathrm{unr}}/F) \cong \mathrm{Gal}(\overline{\kappa}/\kappa)$, where κ is the residue field of F, and F^{unr} denotes the maximal unramified extension of F. Another generator, commonly denoted by τ, lifts the generator of $\mathrm{Gal}(F^{\mathrm{tame}}/F^{\mathrm{unr}})$, where F^{tame} denotes the maximal tamely ramified extension of F. In particular, the two elements σ and τ satisfy the "tame relation" $\sigma\tau\sigma^{-1} = \tau^{|\kappa|}$. The remaining generators $x_0, \dots, x_{[F\colon \mathbb{Q}_p]}$ generate the subgroup $\mathrm{Gal}(\overline{F}/F^{\mathrm{tame}})$ which gives the wildly ramified extensions of F. To complete the presentation of Γ_F, one should impose that the normal subgroup generated by $x_0, \dots, x_{[F\colon \mathbb{Q}_p]}$ is a pro-p group, and one should add only one extra relation, which expresses $\sigma x_0 \sigma^{-1}$ in terms of the commutators between the different elements $x_1, \dots, x_{[F\colon \mathbb{Q}_p]}$.

Langlands's vision

Giving a similar presentation for the absolute Galois group Γ_F when F is a global field seems, at the moment, to be out of reach. However, there is another possible way to describe the group Γ_F, by describing its representations. As we explained in the first section, this is enough to determine Γ_F up to isomorphism, thanks to Tannaka and Krein's reconstruction theorem. The *Langlands program*, which is the subject of this lecture, aims at describing the continuous representations of Γ_F in terms of *automorphic representations*, which are of an analytic nature.

To be more precise, we will focus our attention on Galois representations $\rho\colon \Gamma_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$, and we will only briefly mention the case of other algebraic groups towards the end of this lecture. In the case of GL_n, the gargantuan program put forward by Langlands predicts that irreducible, n-dimensional Galois representations should be in bijective correspondence with cuspidal, automorphic representations of $\mathrm{GL}_n(\mathbb{A}_F)$.

Establishing such a correspondence would allow one to prove non-abelian analogues of the classical reciprocity laws in number theory. More precisely, one of the consequences of class field theory is that, if we want to describe the splitting behavior of prime ideals $\mathfrak{p} \subseteq \mathcal{O}_F$ inside a finite abelian extension $F \subseteq L$, we just need to look at the classes represented by the idèles associated to these prime ideals inside a suitable finite quotient of the group of idèles $\mathbb{A}_F^\times$. When $F = \mathbb{Q}$, this boils down to studying congruence classes of primes modulo the smallest integer N such that $L \subseteq \mathbb{Q}(\zeta_N)$, which is the *conductor* of the abelian extension $\mathbb{Q} \subseteq L$. As we mentioned, when the extension $F \subseteq L$ is not abelian, one can still hope to obtain such reciprocity laws, by studying representations of Γ_F. For instance, one can take $F = \mathbb{Q}$ and L to be the splitting field of the polynomial $f(x) = x^5 + 10x^3 - 10x^2 + 35x - 18$, which gives rise to an icosahedral Galois group $\mathrm{Gal}(L/\mathbb{Q}) \cong A_5$. Then, one can describe explicitly the splitting of primes in this extension by looking at a corresponding modular form of weight one, as explained by Langlands in his very accessible survey paper [25].

Automorphic forms and representations

What is such a cuspidal, automorphic representation? To define them, we need to recall that a function $\phi\colon \mathrm{GL}_n(\mathbb{A}_F) \to \mathbb{C}$ is *smooth* if there exists a compact and open subgroup $K \subseteq \mathrm{GL}_n(\mathbb{A}_F^\infty)$ for which ϕ is right-invariant, *i.e.* such that $\phi(gk) = \phi(g)$ for each $g \in \mathrm{GL}_n(\mathbb{A}_F)$, and such that for every $g^\infty \in \mathrm{GL}_n(\mathbb{A}_F^\infty)$ the associated function $\mathrm{GL}_n(F \otimes_{\mathbb{Q}} \mathbb{R}) \to \mathbb{C}$ defined by $g_\infty \mapsto \phi(g^\infty, g_\infty)$ is smooth. Among smooth functions, one singles out the class of automorphic forms, which are smooth functions $\phi\colon \mathrm{GL}_n(\mathbb{A}_F) \to \mathbb{C}$ such that:

- $\phi(g_0 g) = \phi(g)$ for every $g \in \mathrm{GL}_n(\mathbb{A}_F)$ and $g_0 \in \mathrm{GL}_n(F)$;
- the complex vector space spanned by the functions $\mathrm{GL}_n(\mathbb{A}_F) \to \mathbb{C}$ of the form $g \mapsto \phi(gk)$, where k varies among the elements of the group $K_\infty := \prod_{v \in \mathfrak{M}_{F,\mathbb{R}}} O_n(\mathbb{R}) \times \prod_{v \in \mathfrak{M}_{F,\mathbb{C}}} U_n(\mathbb{C})$, is finite dimensional;

- the complex vector space spanned by the orbit of ϕ under the center of the universal enveloping algebra of $\mathfrak{g}_{\mathbb{C}} := \prod_{v \in \mathfrak{M}_{F,\infty}} \mathrm{Mat}_n(F_v) \otimes \mathbb{C}$ is finite dimensional;
- there exist two constants $c_1, c_2 > 0$ such that $|\phi(g)| \leq c_1 \|g\|^{c_2}$, where the norm $\|g\|$ of an element $g = (g_{i,j})_{i,j=1}^n \in \mathrm{GL}_n(\mathbb{A}_F)$ is defined to be

$$\|g\| := \prod_{v \in \mathfrak{M}_F} \max\left(|\det(g)^{-1}|_v, \max\{|g_{i,j}|_v : i,j \in \{1,\dots,n\}\}\right).$$

These conditions may be a lot to digest, therefore it might be nice to look at some examples. First of all, let us recall that the universal enveloping algebra $U(\mathfrak{g})$ of a complex Lie algebra $\mathfrak{g}$ is the universal unitary and associative algebra that admits a map $\iota : \mathfrak{g} \to U(\mathfrak{g})$ such that $\iota([x,y]) = \iota(x)\iota(y) - \iota(y)\iota(x)$ for every $x, y \in \mathfrak{g}$. More explicitly, if $\mathfrak{g}$ is generated by $X_1, \dots, X_n$, then $U(\mathfrak{g})$ is the associative algebra with unity generated by elements $x_1, \dots, x_n$ which satisfy the unique relations $x_i x_j - x_j x_i = \sum_{k=1}^n c_{i,j}^k x_k$, where the constants $c_{i,j}^k$ are the structure constants of $\mathfrak{g}$, defined by the equality $[x_i, x_j] = \sum_{k=1}^n c_{i,j}^k X_k$. For example, for $n = 2$, we see that the complexified Lie algebra of $\mathrm{GL}_2(\mathbb{R})$ is generated by the four elements

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad H = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Y_+ = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix} \quad Y_- = \begin{pmatrix} 1 & -i \\ -i & -1 \end{pmatrix},$$

which implies that the corresponding universal enveloping algebra has four generators z, h, y_+, y_-, subject to the relations that correspond to the fact that $[Z, H] = [Z, Y_+] = [Z, Y_-] = 0$, and to the three relations $[H, Y_+] = 2Y_+$ and $[H, Y_-] = -2Y_-$ and $[Y_+, Y_-] = 4H$. Under these conditions, it is not difficult to show that the center of this universal enveloping algebra is given by $\mathbb{C}[z, h^2 - 2h + y_+ y_-]$. Furthermore, let us recall that the action of the universal enveloping algebra on functions $\phi : \mathrm{GL}_n(\mathbb{A}_F) \to \mathbb{C}$ comes from the usual action of the Lie algebra $\mathfrak{g}_{\mathbb{C}} := \prod_{v \in \mathfrak{M}_{F,\infty}} \mathrm{Mat}_n(F_v) \otimes \mathbb{C}$ on functions $\mathrm{GL}_n(F \otimes_{\mathbb{Q}} \mathbb{R}) \to \mathbb{C}$, given by

$$(X * \phi)(g_\infty) = \frac{d}{dt}(\phi(g_\infty \exp(t \cdot X)))\Big|_{t=0},$$

and is obtained by deriving the standard right action of $\mathrm{GL}_n(F \otimes_{\mathbb{Q}} \mathbb{R})$ on $\mathrm{GL}_n(\mathbb{A}_F)$.

Automorphic forms and modular forms

Now, let us fix $n = 2$ and $F = \mathbb{Q}$. Then, the theory of automorphic forms is intimately related to the theory of modular forms. More precisely, recall that a *modular form* of weight k for a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a holomorphic function $f : \mathfrak{h} \to \mathbb{C}$ defined on the complex upper half plane $\mathfrak{h} := \{z \in \mathbb{C} : \Im(z) > 0\}$, such that $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ for every $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $z \in \mathfrak{h}$, and such that for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the function $z \mapsto (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$ stays bounded when $\Im(z) \to \infty$. It turns out that if Γ has finite index inside $\mathrm{SL}_2(\mathbb{Z})$, then $\Gamma \supseteq \Gamma(N)$ for some $N \geq 1$, where $\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$. This implies

that $\Gamma = K \cap \mathrm{SL}_2(\mathbb{Z})$ for some compact open subgroup $K \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. Now, let us suppose for simplicity that the determinant map $\det\colon K \to \widehat{\mathbb{Z}}^\times$ is surjective, which can be achieved for the classical congruence subgroups $\Gamma = \Gamma_0(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \colon c \equiv 0 (N) \right\}$ and $\Gamma = \Gamma_1(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) \colon a, d \equiv 1 (N) \right\}$. Then, the strong approximation lemma for SL_2 guarantees that the map

$$\begin{aligned} \mathrm{GL}_2(\mathbb{R})^+ \times K &\to \mathrm{GL}_2(\mathbb{Q}) \backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}) \\ (g, k) &\mapsto g \cdot k \end{aligned}$$

is a continuous surjection, where $\mathrm{GL}_2(\mathbb{R})^+$ denotes the subgroup of those $g \in \mathrm{GL}_2(\mathbb{R})$ such that $\deg(g) > 0$. If we take the quotient by the right action of K, the aforementioned map yields a homeomorphism

$$\Gamma \backslash \mathrm{GL}_2(\mathbb{R})^+ \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Q}) \backslash \left(\mathrm{GL}_2(\mathbb{R}) \times \mathbb{GL}_2(\mathbb{A}_\mathbb{Q}^\infty) / K \right), \tag{4}$$

which allows us to see a modular form as an automorphic form on the right hand side. More precisely, to any modular form $f\colon \mathfrak{h} \to \mathbb{C}$ one can associate a smooth function $\tilde{f}\colon \mathrm{GL}_2(\mathbb{R})^+ \to \mathbb{C}$ by setting

$$\tilde{f}\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \right) := (ci + d)^{-k} f\left(\frac{ai + b}{ci + d} \right),$$

where $i \in \mathbb{C}$ is a chosen square root of -1. It is not difficult to see from the definition that this function $\tilde{f}$ will be invariant under the left action of Γ on $\mathrm{GL}_2(\mathbb{R})^+$. Therefore, $\tilde{f}$ induces a function

$$\tilde{f}\colon \mathrm{GL}_2(\mathbb{Q}) \backslash \left(\mathrm{GL}_2(\mathbb{R}) \times \mathbb{GL}_2(\mathbb{A}_\mathbb{Q}^\infty) / K \right) \to \mathbb{C},$$

thanks to the isomorphism (4). This function turns out to be an automorphic form in the sense that we defined above. More specifically, the fact that f is holomorphic translates to the property that $Y_- \tilde{f} = 0$. Moreover, f is a *cusp form* (which means that for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the function $(cz + d)^{-k} f\left(\frac{az+b}{cz+d}\right)$ tends to zero as $\Im(z) \to +\infty$) if and only if $\int_{\mathbb{Q} \backslash \mathbb{A}_\mathbb{Q}} \tilde{f}(\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \cdot g) dx = 0$ for every $g \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$.

Automorphic representations

Now, what are automorphic forms good for? Well, they form a complex vector space $\mathcal{A}(\mathrm{GL}_{n,F})$ which has a natural action of $\mathrm{GL}_n(\mathbb{A}_F^\infty)$, given by $(g * \phi)(h) = \phi(h \cdot g)$. This action is *smooth*, meaning that every $\phi \in \mathcal{A}(\mathrm{GL}_{n,F})$ is fixed by a compact open subgroup of $\mathrm{GL}_n(\mathbb{A}_F^\infty)$. Moreover, the space $\mathcal{A}(\mathrm{GL}_{n,F})$ admits also a natural structure of $(\mathfrak{g}_\mathbb{C}, K_\infty)$-*module*. This means that $\mathcal{A}(\mathrm{GL}_{n,F})$ has an action of $\mathfrak{g}_\mathbb{C} := \prod_{v \in \mathfrak{M}_{F,\infty}} \mathrm{Mat}_n(F_v) \otimes \mathbb{C}$, as we described above, and also a canonical action of $K_\infty := \prod_{v \in \mathfrak{M}_{F,\mathbb{R}}} O_n(\mathbb{R}) \times \prod_{v \in \mathfrak{M}_{F,\mathbb{C}}} U_n(\mathbb{C})$, with the property that:

- $\mathcal{A}(\mathrm{GL}_{n,F})$ is a direct sum of continuous, finite-dimensional representations of K_∞;
- for every $X \in \mathfrak{g}_\mathbb{C}$ and $\phi \in \mathcal{A}(\mathrm{GL}_{n,F})$ we have that $X * \phi = \frac{d}{dt}(\exp(tx) * \phi)\Big|_{t=0}$;

- for every $X \in \mathfrak{g}_{\mathbb{C}}$ and $k \in K_\infty$, and every $\phi \in \mathcal{A}(\mathrm{GL}_{n,F})$ we have that

$$k * (X * (k^{-1} * \phi)) = \mathrm{Ad}(k)(X) * \phi,$$

  where $\mathrm{Ad}\colon \mathrm{GL}_n(F \otimes_{\mathbb{Q}} \mathbb{R}) \to \mathrm{Aut}(\mathfrak{g})$ denotes the adjoint representation, which in this case can be written down explicitly as $\mathrm{Ad}(g)(X) := gXg^{-1}$ for every $g \in \mathrm{GL}_n(F \otimes_{\mathbb{Q}} \mathbb{R})$ and $X \in \mathfrak{g}$.

In fact, these properties of the space of automorphic forms $\mathcal{A}(\mathrm{GL}_{n,F})$ are so important that they have been used to define the notion of *admissible representation*. More precisely, an admissible representation of $\mathrm{GL}_n(\mathbb{A}_F)$ is a complex vector space V equipped with an action of $\mathrm{GL}_n(\mathbb{A}_F^\infty)$ which is smooth, and with the structure of a $(\mathfrak{g}_{\mathbb{C}}, K_\infty)$-module, such that the two actions commute and each irreducible, continuous, finite-dimensional representation of $K = K_\infty \times \mathrm{GL}_n(\mathcal{O}_F)$ occurs only finitely many times, up to isomorphism, inside V. Moreover, an admissible representation is said to be *automorphic* if it is irreducible (*i.e.* it has exactly two sub-representations) and is isomorphic to a sub-quotient of $\mathcal{A}(\mathrm{GL}_{n,F})$.

Finally, one can introduce the notion of cuspidal automorphic representation, which are those automorphic representations that are isomorphic to a sub-quotient of the space of *cuspforms* $\mathcal{A}_0(\mathrm{GL}_{n,F}) \subseteq \mathcal{A}(\mathrm{GL}_{n,F})$. These are those automorphic forms $\phi \in \mathcal{A}(\mathrm{GL}_{n,F})$ such that for every *standard parabolic subgroup* $P \subseteq \mathrm{GL}_n$ and every $g \in \mathrm{GL}_n(\mathbb{A}_F)$ we have that

$$\int_{N(\mathbb{A}_F)} f(g \cdot x)dx = 0,$$

where $P = M \cdot N$ denotes the *Levi decomposition* of P. More precisely, let us recall that the standard parabolic subgroups P of GL_n are those of the form

$$P = \begin{pmatrix} A_{n_1} & * & * & * \\ & A_{n_2} & * & * \\ & & \ddots & * \\ & & & A_{n_r} \end{pmatrix}$$

where $(n_1, \dots, n_r)$ is a partition of n, and $A_{n_j} \in \mathrm{GL}_{n_j}$ for every $j \in \{1, \dots, r\}$. In this situation, the decomposition $P = M \cdot N$ is given by taking $M = \mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r}$, embedded diagonally, and

$$N = \begin{pmatrix} \mathrm{Id}_{n_1} & * & * & * \\ & \mathrm{Id}_{n_2} & * & * \\ & & \ddots & * \\ & & & \mathrm{Id}_{n_r} \end{pmatrix}.$$

The global Langlands conjectures for the general linear groups

We are almost able to describe what the global Langlands conjectures for GL_n predict. To do so, we need the notion of *algebraic* automorphic representation, which is an automorphic representation such that the action

of the center of the universal enveloping algebra $U(\mathfrak{g}_{\mathbb{C}})$ of $\mathfrak{g}_{\mathbb{C}}$ is "integral". More precisely, a theorem of Harish-Chandra shows that this center is isomorphic to the ring of symmetric polynomials $\mathbb{C}[X_1, \dots, X_n]^{\mathfrak{S}_n}$. Therefore, to every automorphic representation π one can associate an n-tuple of complex numbers, which correspond to the images of the elementary symmetric polynomials under the central character associated to the action of $U(\mathfrak{g}_{\mathbb{C}})$. Then, one says that π is *algebraic* if these complex numbers are all integers.

Finally, let us come to the *global Langlands conjecture*, which predicts that, having fixed a number field F, a prime number ℓ and an isomorphism $\iota\colon \mathbb{C} \xrightarrow{\sim} \overline{\mathbb{Q}}_\ell$, one should be able to associate to any algebraic cuspidal automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_F)$ a semi-simple Galois representation $\rho_\pi\colon \Gamma_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ such that for every place $v \in \mathfrak{M}_F$ with the property that ρ_π is unramified at v, and such that $v \nmid \ell\mathcal{O}_F$, the matrix $\rho_\pi(\mathrm{Frob}_v) \in \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ should belong to the conjugacy class $\iota(\phi_{\pi_v})$, where π_v denotes the v-th component of π, which is a representation of $\mathrm{GL}_n(F_v)$, and ϕ_{π_v} denotes the *Satake parameter* of π_v. This is a conjugacy class in $\mathrm{GL}_n(\mathbb{C})$, that comes from the *Satake isomorphism*, which describes the Hecke algebra $\mathcal{H}(\mathrm{GL}_n(F_v), \mathrm{GL}_n(\mathcal{O}_{F_v}))$ as the algebra of symmetric Laurent polynomials.

The aforementioned conditions, which deal with all but finitely many places of F, in fact determine the Galois representation ρ_π, thanks to *Chebotarev's density theorem*, and the automorphic representation π, by the so-called *strong multiplicity one* theorem, which says that a cuspidal automorphic representation π is determined by the class of its local restrictions $\{\pi_v\colon v \in \mathfrak{M}_F \setminus S\}$, where S denotes any finite set of places. In particular, the aforementioned conditions imply that one should have an equality $L(\pi, s) = L(\rho_\pi, s)$ between the *L-functions* associated to the automorphic representation π and the Galois representation ρ_π. It is this equality of L-functions that can be seen a non-abelian analogue of the so-called *Artin reciprocity law*, which lies at the core of class field theory. In particular, since spaces of automorphic representations are often finite dimensional, the Langlands program can be seen as an attempt to give an explicit description of the sequences of rational primes that have a given splitting behavior in a given number field F.

Known results

To conclude this very brief introduction to the Langlands program, let us mention several known partial results. First of all, there is a local version of the Langlands program, which relates representations of the absolute Galois group Γ_K of a local field K to automorphic representations of $\mathrm{GL}_n(K)$. This conjecture has been proven by Laumon, Rapoport and Stuhler [26] when K has positive characteristic, and by Harris and Taylor [14] for local fields of characteristic zero. Alternative proofs were later found by Henniart [16] and by Scholze [37]. Moreover, both in the local and in the global cases, the Langlands conjectures can be formulated for more general reductive algebraic groups. In this context, one can predict a certain kind of *functoriality* of the Langlands correspondence, which is in fact a crucial part of Langlands's conjectures.

Finally, when $\pi = \tilde{f}$ is the cuspidal automorphic form of GL_2 associated to a cuspidal modular form

f of weight $k = 2$ and level $\Gamma_0(N)$, which is an eigenform for the Hecke operators, the representation ρ_π corresponds to the Galois representation attached to the rationalized Tate module $V_\ell(E) := (\varprojlim_n E[\ell^n]) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ associated to the elliptic curve E obtained as a quotient of the Jacobian $J(\Gamma_0(N))$ of the modular curve $X(\Gamma_0(N))$ associated to the modular group $\Gamma_0(N)$ by the idempotent of the Hecke algebra

$$\mathcal{H} = \mathbb{Q}[\{T_p \colon p \text{ rational prime}\}] \subseteq \mathrm{End}(J(\Gamma_0(N))) \otimes \mathbb{Q}$$

corresponding to the eigenform f. The deep *modularity theorem*, proved by combining the work of Breuil, Conrad, Diamond, Taylor [4] and Wiles [43] asserts that in this case the image of the association $\pi \mapsto \rho_\pi$ contains *all* the Galois representations associated to elliptic curves defined over $\mathbb{Q}$. In general, the Fontaine-Mazur conjecture [13] predicts that all the Galois representations of geometric origin should lie in the image of the Langlands correspondence.

6 Elliptic curves and their Galois representations

The aim of the second part of this course, which starts with the present lecture, is to concentrate our attention on the Galois representations associated to elliptic curves. More precisely, let F be a number field, and let E denote an elliptic curve defined over F. Then, for every integer $N \geq 1$, one can consider the group $E[N] := E(\overline{F})[N]$ of those points $P \in E(\overline{F})$ defined over the algebraic closure $\overline{F}$ of F which are annihilated by the multiplication-by-N map $[N] \colon E(\overline{F}) \to E(\overline{F})$. It turns out that $E[N]$ is a finite abelian group, isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$, as follows from the fact that the isogeny $[N] \colon E \to E$ is a finite separable map of degree N^2, which necessarily implies that $\#E[M] = M^2$ for every $M \geq 1$, and leaves $(\mathbb{Z}/N\mathbb{Z})^2$ as the only possibility for the group $E[N]$.

Therefore, the action of Γ_F on $E[N]$ yields a family of Galois representations

$$\rho_{E,N} \colon \Gamma_F \to \mathrm{Aut}_{\mathbb{Z}}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

parametrized by the integers $N \geq 1$. These Galois representations can be assembled together in two different ways. First of all, one can fix a prime ℓ and consider the torsion subgroups $E[\ell^n]$, for $n \geq 0$. These finite groups are related by natural inclusion maps $E[\ell^n] \hookrightarrow E[\ell^{n+1}]$ and by multiplication-by-ℓ maps $[\ell] \colon E[\ell^{n+1}] \to E[\ell^n]$. These two families of maps yield two different Galois representations

$$\rho_{E,\ell^\infty} \colon \Gamma_F \to \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty]) \quad \text{and} \quad \tilde{\rho}_{E,\ell^\infty} \colon \Gamma_F \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E))$$

where $E[\ell^\infty] := \varinjlim_n E[\ell^n]$ denotes the set of all those points $P \in E(\overline{F})$ which are annihilated by a power of ℓ, while $T_\ell(E) := \varprojlim_n E[\ell^n]$ denotes the *ℓ-adic Tate module* of E. Despite the fact that these two groups may look rather different, we have a canonical identification

$$\frac{T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell}{T_\ell(E)} = \bigcup_{n=1}^{+\infty} \frac{\ell^{-n} T_\ell(E)}{T_\ell(E)} = \bigcup_{n=1}^{+\infty} E[\ell^n] = E[\ell^\infty],$$

which provides a canonical isomorphism $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)) \xrightarrow{\sim} \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty])$ that identifies ρ_{E,ℓ^∞} with $\tilde{\rho}_{E,\ell^\infty}$.

Therefore, in these notes, we will mostly concentrate on the Galois representations $\rho_{E,N}$ and ρ_{E,ℓ^∞}. Moreover, all these representations can be put together inside one adelic Galois representation

$$\rho_E \colon \Gamma_F \to \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \varprojlim_N \mathrm{Aut}_{\mathbb{Z}}(E[N])$$

where $E_{\mathrm{tors}} := E(\overline{F})_{\mathrm{tors}}$ denotes the group of all torsion points of E defined over $\overline{F}$. In particular,

$$\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \prod_\ell \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty]) = \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

and under this isomorphism the adelic Galois representation ρ_E decomposes as the product of the ℓ-adic Galois representations ρ_{E,ℓ^∞}.

Serre's open image theorem

These Galois representations are arguably the simplest examples of Galois representations which land in a non-abelian group. In fact, one knows that their image is actually non-abelian, unless the elliptic curve E has *complex multiplication*. More precisely, recall that given an elliptic curve E defined over a number field F there are only two possibilities for the endomorphism ring $\mathrm{End}_F(E)$. More precisely, either $\mathrm{End}_F(E) \cong \mathbb{Z}$ or $\mathrm{End}_F(E) \cong \mathcal{O}$ where $\mathcal{O}$ is an order inside an imaginary quadratic field K. In this second case, each element in the image $\rho_E(\Gamma_F)$ of the Galois representation associated to E commutes with the action of $\mathcal{O}$ induced on E_{tors}. Therefore, we get a Galois representation

$$\rho_E \colon \Gamma_F \to \mathcal{G}(E/F) := \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}),$$

and one can show that $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathcal{O}}^\times$ is an abelian group. This follows from the fact that for every $N \geq 1$ we have an isomorphism $\mathrm{Aut}_{\mathcal{O}}(E[N]) \cong (\mathcal{O}/N\mathcal{O})^\times$, because the group of N-torsion points $E[N]$ is a free $\mathcal{O}/N\mathcal{O}$-module of rank one. It can also happen that $\mathrm{End}_F(E) \cong \mathbb{Z}$ but $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$. In this case, it turns out that $\mathrm{End}_{FK}(E) \cong \mathcal{O}$, which implies that $\rho_E(\Gamma_F)$ is contained in the subgroup $\mathcal{G}(E/F) \subseteq \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ generated by $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ and by $\rho_E(\sigma)$, where $\sigma \in \Gamma_F$ is any lift of the generator of $\mathrm{Gal}(FK/F) \cong \mathbb{Z}/2\mathbb{Z}$. In both cases, as we will see in one of the following lectures, classical results of Kronecker and Deuring imply that $\rho_E(\Gamma_F)$ is open inside $\mathcal{G}(E/F)$.

A similar result, with a much more difficult proof, holds true when $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$. More precisely, in this case $\rho_E(\Gamma_F)$ is open inside $\mathcal{G}(E/F) := \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$. This theorem is due to Serre, and its proof is divided into the book [40] (originally published in 1968) and the seminal paper [38]. We will devote the rest of this lecture to give a sketch of the proof of this theorem, and also a brief survey of subsequent developments.

The local open image theorem

First of all, showing that $\rho_E(\Gamma_F)$ is open inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ is equivalent to showing that for every prime ℓ the ℓ-adic image $\rho_{E,\ell^\infty}(\Gamma_F)$ is open inside $\mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty])$, and that in fact $\rho_{E,\ell^\infty}(\Gamma_F) = \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty])$ for every ℓ sufficiently large. The first result is proven in [40, Chapter IV, Section 2.2]. To do so, Serre shows first of all that for every prime ℓ the rationalized Tate module $V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is an irreducible $\mathbb{Q}_\ell[\Gamma_F]$-module. Indeed, if by contradiction this was not the case then there would exist a one dimensional $\mathbb{Q}_\ell$-subspace $W \subseteq V_\ell(E)$ stable under the action of Γ_F, which would yield a submodule $M := W \cap T_\ell(E)$ of $T_\ell(E)$ with the property that both M and $T_\ell(E)/M$ are free $\mathbb{Z}_\ell$-modules of rank one. Taking the image M_n of M inside $E[\ell^n] = T_\ell(E)/\ell^n$ yields a finite cyclic subgroup of $E(\overline{F})$ of order ℓ^n, to which corresponds a cyclic isogeny $E \twoheadrightarrow E/M_n$ of order ℓ^n. It is easy to see, using the fact that $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$, that all the curves E/M_n will not be isomorphic, which yields a contradiction thanks to *Shafarevich's theorem*, which asserts that the isogeny class of an elliptic curve defined over a number field is finite. This irreducibility result implies that $V_\ell(E)$ is also irreducible as a module over the Lie algebra $\mathfrak{g}_\ell := \mathrm{Lie}(\tilde{\rho}_{E,\ell^\infty}(\Gamma_F)) \subseteq \mathrm{End}(V_\ell(E))$. By Schur's lemma, the center $Z(\mathfrak{g}_\ell)$ of $\mathfrak{g}_\ell$ must be a field, of degree $[Z(\mathfrak{g}_\ell)\colon \mathbb{Q}_\ell] \leq 2$ because $\dim_{\mathbb{Q}_\ell}(V_\ell(E)) = 2$. In the first case, we have either that $\mathfrak{g}_\ell = \mathrm{End}(V_\ell(E))$, or that $\mathfrak{g}_\ell = \mathfrak{sl}(V_\ell(E))$ consists of those endomorphisms having trace zero. However, this second case would imply that $\rho_{E,\ell^\infty}(\Gamma_F) \subseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$, which would contradict the fact that $\det(\rho_{E,\ell^\infty}(\Gamma_F)) \subseteq \mathbb{Z}_\ell^\times$ has finite index, as follows from the compatibility between the Weil pairing and the action of Γ_F. Moreover, one can also exclude the eventuality that $Z(\mathfrak{g}_\ell)$ is a quadratic extension of $\mathbb{Q}_\ell$, because in this case one would have (up to replacing F by a finite extension, which does not affect $\mathfrak{g}_\ell$) that $\rho_{E,\ell^\infty}(\Gamma_F)$ is abelian. One can exclude this by looking at the local theory of the representation $V_\ell(E)$, which (using several results of Tate) implies that such a Galois representation could not possibly be irreducible, as we have shown before. Therefore, the only possibility is that $\mathfrak{g}_\ell = \mathrm{End}(V_\ell(E))$, which implies that $\rho_{E,\ell^\infty}(\Gamma_F)$ is open inside $\mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty])$.

The global open image theorem

Now, let us briefly mention how one proves that $\rho_{E,\ell^\infty}(\Gamma_F) = \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty])$ for all but finitely many primes ℓ. First of all, this is equivalent to the fact that $\rho_{E,\ell}(\Gamma_F) = \mathrm{Aut}_{\mathbb{Z}}(E[\ell])$ for all but finitely many primes ℓ, as follows from some group-theoretic arguments. Now, the image $G_\ell(E) := \rho_{E,\ell}(\Gamma_F)$ is a subgroup of $\mathrm{Aut}_{\mathbb{Z}}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$, where $\mathbb{F}_\ell := \mathbb{Z}/\ell\mathbb{Z}$, which has the property that $\det(G_\ell(E)) = \mathbb{F}_\ell^\times$, at least for every ℓ such that $F \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$. Therefore, for these primes ℓ, which are all but finitely many primes, the group $G_\ell(E)$ is either:

- contained in a *Borel subgroup*, which has the form $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ after a suitable choice of basis;
- contained in the normalizer of a *Cartan subgroup*, which is either a *split Cartan subgroup*, which has the

form $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$ after a suitable choice of basis, or is a *non-split Cartan subgroup*, given by the units κ^* of some sub-field $\kappa \subseteq \mathrm{End}(E[\ell])$ with ℓ^2 elements;

- contained in an *exceptional group*, which maps to A_4, S_4 or A_5 inside $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$;
- equal to $\mathrm{End}_{\mathbb{Z}}(E[\ell])$.

Now, we would like to exclude the eventuality that the first three cases occur for infinitely many primes ℓ. To do so, we can first of all enlarge F, and therefore assume that E has semi-stable reduction (*i.e.* either good or split multiplicative reduction) at every prime of $\mathcal{O}_F$, that F has no real embeddings and that $\mathbb{Q} \subseteq F$ is a Galois extension. Moreover, we can take a prime ℓ such that E has good reduction at ℓ, and ℓ is unramified in $\mathbb{Q} \subseteq F$, because this excludes only a finite number of primes.

Under the above assumptions, we exclude first of all the eventuality that $G_\ell(E)$ is contained in an exceptional subgroup. This can be done by looking at the image $I_\mathfrak{l}(E) := \rho_{E,\ell}(I_\mathfrak{l}) \subseteq G_\ell(E)$ of the inertia subgroup $I_\mathfrak{l} \subseteq \Gamma_F$ relative to a prime $\mathfrak{l} \subseteq \mathcal{O}_F$ lying above ℓ. More precisely, the image $\overline{I_\mathfrak{l}(E)}$ of $I_\mathfrak{l}(E)$ inside the projective general linear group $\mathrm{PGL}_2(\mathbb{F}_\ell)$ turns out to have always cardinality $\#\overline{I_\mathfrak{l}(E)} \geq \ell - 1$, which clearly implies that $G_\ell(E)$ can be contained inside an exceptional subgroup only if $\ell \leq 61$. To show the aforementioned claim about the cardinality of $\overline{I_\mathfrak{l}(E)}$, one should consider the two possibilities for the reduction $\tilde{E}$ of E modulo $\mathfrak{l}$. If $\tilde{E}$ is ordinary, we have that $E[\ell] \twoheadrightarrow \tilde{E}[\ell]$, which implies that $I_\ell(E)$ contains all the elements of the form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$, where $a \in \mathbb{F}_\ell^\times$ and $b \in \mathbb{F}_\ell$. In the supersingular case, the group of ℓ-torsion points $E[\ell]$ identifies with the group of ℓ-torsion points of the *formal group law* $\widehat{E}$ attached to E. By the theory of formal groups, the reduction of $\widehat{E}$ modulo $\mathfrak{l}$ has height two, which implies that $I_\mathfrak{l}(E)$ is a non-split Cartan subgroup of $\mathrm{Aut}_{\mathbb{Z}}(E[\ell])$, which has therefore cardinality $\ell^2 - 1$.

Now, we need to exclude that $G_\ell(E)$ is contained in a Borel subgroup or in the normalizer of a Cartan subgroup for infinitely many primes ℓ. First of all, one can show that there exists an extension $F \subseteq F'$ with $[F' \colon F] \leq 2$, such that $\rho_{E,\ell}(\mathrm{Gal}(\overline{F}/F'))$ is contained in a Borel or in a Cartan subgroup for infinitely many primes ℓ. Indeed, the only other eventuality that could occur is that $G_\ell(E)$ is contained in the normalizer of a Cartan subgroup, but not in the Cartan subgroup itself, for infinitely many primes ℓ. However, Cartan subgroups have index two inside their normalizers, which implies that for every such prime ℓ we indeed get an extension $F \subseteq F'_\ell$ such that $[F'_\ell \colon F] \leq 2$ and $\rho_{E,\ell}(\mathrm{Gal}(\overline{F}/F'_\ell))$ is contained in a Cartan subgroup. To conclude, we need to show that infinitely many of these extensions F'_ℓ coincide, and to do so it suffices to show that the extension $F \subseteq F'_\ell$ is unramified everywhere. Indeed, if $\mathfrak{p} \subseteq \mathcal{O}_F$ is a prime ideal lying over ℓ, then E has good reduction at $\mathfrak{p}$. Therefore, we know that $I_\mathfrak{p}(E)$ is either of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ (when the reduction of E modulo $\mathfrak{p}$ is ordinary), or that we have $\#I_\mathfrak{p}(E) = \ell^2 - 1$ (when the reduction of E modulo $\mathfrak{p}$ is supersingular). In both cases, these facts combined with the assumption that $I_\mathfrak{p}(E)$ is contained in the normalizer of a Cartan subgroup, implies that $I_\mathfrak{p}(E)$ is in fact contained in the Cartan subgroup itself, and

therefore that $\mathfrak{p}$ is unramified in $F \subseteq F'_\ell$. When $\mathfrak{p} \nmid \ell$, the Néron-Ogg-Shafarevich criterion implies that $F \subseteq F'_\ell$ can be ramified at $\mathfrak{p}$ only when E has split multiplicative reduction at $\mathfrak{p}$. However, in this case we can use Tate's uniformization for the base change $E_{F_\mathfrak{p}}$, which yields a short exact sequence

$$0 \to \mu_\ell(\overline{\mathbb{Q}}_p) \to E[\ell] \to q^{\mathbb{Z}}/q^{\ell\mathbb{Z}} \to 0,$$

where $q = |\mathcal{O}_F/\mathfrak{p}|$. Since this is a sequence of Galois modules, we see once again that $I_\mathfrak{p}(E) = \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, which allows us to conclude as before that $I_\mathfrak{p}(E)$ is contained in the Cartan subgroup, and therefore that $F \subseteq F'_\ell$ is unramified at $\mathfrak{p}$. Therefore, in what follows we can replace F with the extension F' that we just constructed.

To conclude, we need to show that there cannot exist infinitely many primes ℓ such that $G_\ell(E)$ is contained in a Borel or in a Cartan subgroup. First of all, one can also show, by looking at the semi-simplification of $\rho_{E,\ell}$, that if $G_\ell(E)$ is contained in a non-split Cartan subgroup for infinitely many primes ℓ, then in fact one can assume that there are infinitely many primes ℓ for which $G_\ell(E)$ is contained inside a split Cartan subgroup. Since a split Cartan subgroup is always contained in a Borel subgroup, we can assume that there exist infinitely many primes ℓ such that $G_\ell(E)$ is contained in a Borel subgroup. Once again, this yields infinitely many ℓ-isogenies $E \twoheadrightarrow E_\ell$. Since the isogeny class of any given elliptic curve defined over F is finite, we have that $E_\ell \cong E_{\ell'}$ for some $\ell \neq \ell'$, which yields an endomorphism $E \to E_\ell \cong E_{\ell'} \to E$ of degree $\ell\ell'$. However, this is absurd, because the degree of every endomorphism of an elliptic curve without complex multiplication is a square.

Subsequent developments

The aforementioned theorem of Serre prompts naturally several questions. First of all, the openness of the image $\rho_E(\Gamma_F)$ implies that the index $\mathcal{I}(E/F) := [\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \colon \rho_E(\Gamma_F)]$ is finite. How big can it be? In fact, a celebrated question asked by Serre in [38], which became known as *Serre's uniformity conjecture*, implies that $\mathcal{I}(E/F)$ should be bounded solely in terms of the number field F, or even in terms of its degree $[F \colon \mathbb{Q}]$. In particular, Zywina [44] has recently given an explicit finite set of natural numbers which should give all the possible indices $\mathcal{I}(E/\mathbb{Q})$ for elliptic curves defined over $\mathbb{Q}$. Moreover, the aforementioned conjecture about the boundedness of $\mathcal{I}(E/F)$ implies in particular that for every number field F there should exist a finite list of rational primes S_F such that for $\ell \notin S_F$ we have that $\rho_{E,\ell^\infty}(\Gamma_F) = \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty])$ for every elliptic curve E defined over F such that $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$. In particular, one should have $S_\mathbb{Q} = \{2, 3, 5, 7, 11, 13, 17, 37\}$.

This uniformity conjecture is probably out of the current technology, because the only current approaches which are available to study it require a deep understanding of rational points on modular curves. Via such an understanding, one can in particular prove that for every prime $\ell > 37$ and every elliptic curve E defined over $\mathbb{Q}$, the image $G_\ell(E)$ is not contained in any group which is not the normalizer of a non-split Cartan subgroup. Doing so, however, requires some deep understanding of rational points on curves,

exemplified by the works of Bilu and Parent [2] and Balakrishnan, Dogra, Müller, Tuitman and Vonk [1]. However, some completely different techniques allowed Conjocaru and Hall [9] to prove an analogue of Serre's uniformity conjecture over function fields of positive characteristic, and Cojocaru [10] to provide an explicit lower bound, in terms of the conductor $N_E \in \mathbb{N}$ of the elliptic curve E, for the smallest prime $\ell_0(E)$ such that $\rho_{E,\ell^\infty}(\Gamma_F) = \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty])$ for every $\ell \geq \ell_0(E)$. More precisely, under the assumption of the existence of a modular parametrization of E which has small degree, she proves that

$$\ell_0(E) \leq a \cdot (\log(N_E))^\gamma,$$

where γ is a constant introduced in earlier work of Masser and Wüstholz [30]. Finally, Lombardo [28] has shown that

$$\mathcal{I}(E/F) \leq \exp(1.9 \cdot 10^{10}) \cdot ([F\colon \mathbb{Q}] \cdot \max\{1, h(E), \log[K\colon \mathbb{Q}]\})^{12395}$$

for every elliptic curve E defined over a number field F, such that $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$. Here $h(E) \in \mathbb{R}$ denotes the *stable Faltings height* of E, which is defined by the formula

$$[F'\colon \mathbb{Q}]h(E) = \frac{1}{12}\left(\log|\mathrm{N}_{F'/\mathbb{Q}}(\Delta_{E/F'})| - \sum_{v \in \mathfrak{M}_{F',\infty}} [F'_v\colon \mathbb{R}] \cdot \log(|\Delta(\tau_v)|(\mathrm{Im}(\tau_v))^6)\right)$$

where $F' \supseteq F$ denotes any field over which E attains semi-stable reduction, and for every infinite place $v \in \mathfrak{M}_{F',\infty}$ the number $\tau_v \in \mathfrak{h}$ is the unique one such that $E_{F'_v}(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau_v)$.

7 Complex multiplication and explicit class field theory

As we have seen in the previous lecture, the image of the Galois representation attached to an elliptic curve without complex multiplication tends to be quite big. However, when we have an elliptic curve E defined over a number field F such that $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ inside an imaginary quadratic field K, the image of the Galois representation $\rho_E\colon \Gamma_F \to \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ is contained in the closed, non-open subgroup

$$\mathcal{G}(E/F) := \begin{cases} \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}), \text{ if } K \subseteq F \\ \langle \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}), \rho_E(\sigma)\rangle, \text{ if } K \not\subseteq F, \end{cases}$$

where $\sigma \in \Gamma_F$ is any lift of the generator of the Galois group $\mathrm{Gal}(FK/F)$. In particular, this closed subgroup $\mathcal{G}(E/F) \subseteq \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ is quite small.

Nevertheless, one can show that the image $\rho_E(\Gamma_F)$ of the Galois representation attached to E is *open* inside $\mathcal{G}(E/F)$. To do so, one can first of all assume without loss of generality that $K \subseteq F$. Then, this theorem follows from the main results in the theory of complex multiplication, which we would like to recall in this lecture.

Hilbert's twelfth problem

The classical theory of complex multiplication is intimately related to the problem of finding an explicit description of the abelian extensions of a given number field K. When $K = \mathbb{Q}$, this can be achieved by the classical theorem of Kronecker and Weber, which asserts that every abelian extension of $\mathbb{Q}$ is contained inside a cyclotomic field. In modern terms, this follows from the fact that the ray class fields of $\mathbb{Q}$ are given by cyclotomic fields or by their maximal real sub-fields.

In general, one can ask how to obtain explicit polynomials, or generators, for the ray class fields of a number field K. This was the twelfth problem in the celebrated list presented by Hilbert at the International Congress of Mathematicians held in Paris in 1900 [17]. Despite several efforts to attack this problem, it remains unsolved to this day. However, this problem has been completely solved for imaginary quadratic fields, thanks to the theory of complex multiplication, even if the history of this solution has been quite tortuous [35]. Moreover, in recent years Hilbert's twelfth problem has been related by Borger and de Smit to the arithmetic significance of certain dynamical systems [3], and it has been essentially solved for totally real number fields by Dasgupta and Kakde [12], albeit their solution involves the use of infinitely many p-adic analytic functions to describe the maximal abelian extension of a totally real number field.

Ray class fields for orders

The main result that we are going to explain in this lecture shows that the ray class fields of an imaginary quadratic field K can be generated by the j-invariants and the x-coordinates of torsion points of an elliptic curve E with complex multiplication by the ring of integers $\mathcal{O}_K$. This will imply immediately that the image of the Galois representation ρ_E is open inside $\mathcal{G}(E/F)$.

In fact, a similar statement holds true when one considers elliptic curves E which have complex multiplication by an arbitrary order $\mathcal{O} \subseteq \mathcal{O}_K$. To formulate it, we need to introduce the notion of ray class fields relative to an order, which is due to Söhngen [41]. A more recent exposition is given in Schertz's book [36], and in our work [5, § 4] (see also [33, Chapter 6]).

Let K be a general number field, and $\mathcal{O} \subseteq K$ be an order. Then, for every rational prime p, we can consider the completion $\mathcal{O}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$, which embeds into the ring of adèles

$$\mathbb{A}_K = \mathbb{A}_{\mathbb{Q}} \otimes_{\mathbb{Q}} K = \prod_p (K_p : \mathcal{O}_{K_p}),$$

where $K_p := \prod_{\mathfrak{p}|p} K_{\mathfrak{p}} = \mathbb{Q}_p \otimes_{\mathbb{Q}} K$ and $\mathcal{O}_{K_p} := \prod_{\mathfrak{p}|p} \mathcal{O}_{K_{\mathfrak{p}}}$. Analogously, we have the decomposition

$$\mathbb{A}_K^\times := \prod_p (K_p^\times : \mathcal{O}_{K_p}^\times) \tag{5}$$

for the group of idèles $\mathbb{A}_K^\times$. Now, given an ideal $I \subseteq \mathcal{O}$, one can define the *ray class field* of $\mathcal{O}$ associated to I

as $H_{I,\mathcal{O}} := (K^{\mathrm{ab}})^{[K,U_{I,\mathcal{O}}]}$, where $[K,\cdot]\colon \mathbb{A}_K^\times \to \Gamma_K^{\mathrm{ab}} := \mathrm{Gal}(K^{\mathrm{ab}}/K)$ denotes the global Artin map, and

$$U_{I,\mathcal{O}} := \left\{ s \in \mathbb{A}_K^\times \colon s_p \in (\mathcal{O}_p^\times \cap (1 + I\mathcal{O}_p)),\ \forall p \right\},$$

where $s_p \in K_p^\times$ denotes the p-th component of an idèle $s \in \mathbb{A}_K^\times$ under the decomposition (5). If $I = \mathcal{O}$, we get the group $U_{\mathcal{O}} := \prod_p \mathcal{O}_p^\times$, which corresponds to the so-called *ring class field* $H_{\mathcal{O}}$, which has the property that $\mathrm{Gal}(H_{\mathcal{O}}/K) \cong \mathrm{Cl}(\mathcal{O})$. In general, the Galois group $\mathrm{Gal}(H_{I,\mathcal{O}}/K)$ can be described in terms of ideals of $\mathcal{O}$ modulo principal ideals, as in the classical case. In particular, we have that $H_{\mathcal{O}} \subseteq H_{I,\mathcal{O}}$ for every ideal $I \subseteq \mathcal{O}$, and $\mathrm{Gal}(H_{I,\mathcal{O}}/H_{\mathcal{O}}) \cong (\mathcal{O}/I)^\times/\pi_I(\mathcal{O}^\times)$, where $\pi_I\colon \mathcal{O} \twoheadrightarrow \mathcal{O}/I$ denotes the canonical projection map. Finally, it is not difficult to show that for every order $\mathcal{O}$ we have that $\bigcap_I U_{I,\mathcal{O}} = \{1\}$, which implies that $\bigcup_I H_{I,\mathcal{O}} = K^{\mathrm{ab}}$.

The explicit class field theory of imaginary quadratic fields

Now, let K be an imaginary quadratic field, and $\mathcal{O} \subseteq \mathcal{O}_K$ be an order. In this case, the ray class fields $H_{I,\mathcal{O}}$ can be described explicitly in terms of the torsion points of an elliptic curve E with complex multiplication by $\mathcal{O}$.

More precisely, let E be any such elliptic curve, defined over the complex numbers. For instance, one can take $E(\mathbb{C}) = \mathbb{C}/\iota(\mathcal{O})$, where $\iota\colon K \hookrightarrow \mathbb{C}$ denotes any of the two possible complex embeddings. Such an elliptic curve will have a short Weierstrass model $E\colon \{y^2 = x^3 + Ax + B\} \subseteq \mathbb{A}^2$ and an associated j-invariant

$$j(E) := -\frac{2^8(3A)^3}{4A^3 + 27B^2},$$

which in fact does not depend on the particular Weierstrass equation that we have chosen. Moreover, we can associate to E the so-called *Weber function* $\mathfrak{h}_E\colon E \twoheadrightarrow E/\mathrm{Aut}(E) = E/\mathcal{O}^\times \cong \mathbb{P}^1$. If we fix a projective short Weierstrass model $E\colon \{y^2z = x^3 + Axz^2 + Bz^3\} \subseteq \mathbb{P}^2$, this function is simply given by

$$\mathfrak{h}_E(x\colon y\colon z) = \begin{cases} (x\colon z), \text{ if } AB \neq 0, \\ (x^2\colon z^2), \text{ if } B = 0, \\ (x^3\colon z^3), \text{ if } A = 0. \end{cases}$$

Now, suppose that $I \subseteq \mathcal{O}$ is invertible with respect to the tensor product of ideals. In other words, this means that $I \cdot (\mathcal{O}\colon I) = \mathcal{O}$ where $(\mathcal{O}\colon I) := \{\alpha \in K\colon \alpha I \subseteq \mathcal{O}\}$. Then, we have that

$$H_{I,\mathcal{O}} = K(j(E), \mathfrak{h}_E(E[I] \setminus \{0\})), \tag{6}$$

where $E[I] := \bigcap_{\alpha \in I} \ker([\alpha]\colon E(\mathbb{C}) \to E(\mathbb{C}))$. In particular, we have that $H_{\mathcal{O}} = K(j(E))$.

Let us note that one cannot generate the entire maximal abelian extension K^{ab} by means of only one transcendental function. This is in contrast with what happens when $K = \mathbb{Q}$. More precisely, in that case

the values of the transcendental function $\tau \mapsto e^{2\pi i \tau}$ at rational numbers suffice to generate the whole $\mathbb{Q}^{\mathrm{ab}}$. Similarly, one could expect that there exists a single transcendental function $f_K \colon \mathbb{C} \to \mathbb{C}$ such that the values $f_K(\tau)$ for $\tau \in \iota(K)$ would suffice to generate K^{ab}. In particular, it was expected that one could take $f_K = j$ for every imaginary quadratic field K. In other words, one could ask whether $K_j := K(\{j(E) \colon E \in \mathcal{E}_K\})$ equals K^{ab}, where $\mathcal{E}_K$ denotes the set of elliptic curves E (defined say over the complex numbers) with the property that $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}$ for some order $\mathcal{O} \subseteq \mathcal{O}_K$. Thanks to (6), we know that K_j equals the union of all the ring class fields $H_{\mathcal{O}}$, where $\mathcal{O}$ varies among the orders of $\mathcal{O}_K$. Using this, one can show that $\mathrm{Gal}(K^{\mathrm{ab}}/K_j\mathbb{Q}^{\mathrm{ab}})$ is an infinite Galois group of exponent two. Therefore, adding the values of the Weber functions is really necessary. Moreover, it turns out that using a finite number of modular functions $f \colon \mathfrak{h} \to \mathbb{C}$ (of any level) will also not be sufficient to obtain the full maximal abelian extension K^{ab}, as was proven by Söhngen in [41].

Some ideas about the proof

How does one prove that (6) holds? First of all, one proves that $H_{\mathcal{O}} = K(j(E))$. To do so, one uses the fact that the natural multiplication between ideals $I \subseteq \mathcal{O}$ and lattices $\Lambda \subseteq K$ induces a simply transitive action of the class group $\mathrm{Cl}(\mathcal{O})$ on the set of isomorphism classes of elliptic curves E defined over the complex numbers which have the property that $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}$. In particular, there are only finitely many of these isomorphism classes, which are therefore defined over the algebraic numbers, and admit an action of Γ_K. It turns out that the natural quotient map $\Gamma_K \twoheadrightarrow \mathrm{Gal}(H_{\mathcal{O}}/K) \cong \mathrm{Cl}(\mathcal{O})$ is compatible with the action of Γ_K and $\mathrm{Cl}(\mathcal{O})$ on the set of isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}$. Therefore, we get a similar compatibility between the actions of Γ_K and $\mathrm{Cl}(\mathcal{O})$ on the set of j-invariants $j(E)$ of elliptic curves with complex multiplication by $\mathcal{O}$, which finally implies that $H_{\mathcal{O}} = K(j(E))$.

Then, it remains to show that $H_{I,\mathcal{O}} = H_{\mathcal{O}}(\mathfrak{h}_E(E[I]))$ for every invertible ideal $I \subseteq \mathcal{O}$. A proof of this result which uses the standard language of class field theory is essentially available in Söhngen's thesis [41] (see also [36, Theorem 6.2.3]). We have also given a proof which uses the idelic language of class field theory in [5, Theorem 4.7].

The main theorem of complex multiplication

The key fact which is used in all the proofs is the so-called *main theorem of complex multiplication*. This asserts that, given a number field $F \supseteq K$ and an elliptic curve E defined over F such that $\mathrm{End}_F(E) \cong \mathcal{O}$, if we fix an embedding $F \subseteq \mathbb{C}$ then there exists a unique continuous group homomorphism $\mu_E \colon \mathbb{A}_F^{\times} \to K^{\times}$ such that for

every $s \in \mathbb{A}_F^\times$ and every complex uniformization $\xi\colon \mathbb{C} \twoheadrightarrow E(\mathbb{C})$, the following diagram commutes

$$\begin{array}{ccc} K/\ker(\xi) & \xrightarrow{(\mu(s)\mathrm{N}_{F/K}(s^{-1}))\cdot} & K/\ker(\xi) \\ \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \xi} \\ E_{\mathrm{tors}} & \xrightarrow{\rho_E([F,s])} & E_{\mathrm{tors}} \end{array} \quad . \tag{7}$$

Here, the map $(\mu(s)\cdot \mathrm{N}_{F/K}(s^{-1}))\colon K/\ker(\xi) \to K/\ker(\xi)$ is defined as follows. First of all, one should recall that any idèle $s \in \mathbb{A}_K^\times$ acts on the set of lattices $\Lambda \subseteq K$, which are the free additive subgroups of rank $[K\colon \mathbb{Q}]$, by setting $s\cdot\Lambda$ to be the unique lattice of K such that $(s\cdot\Lambda)\otimes_{\mathbb{Z}}\mathbb{Z}_p = s_p\cdot(\Lambda\otimes_{\mathbb{Z}}\mathbb{Z}_p)$ for every rational prime p. Moreover, we also have a multiplication map $K/\Lambda \xrightarrow{s\cdot} K/(s\cdot\Lambda)$, defined by the following diagram

$$\begin{array}{ccc} K/\Lambda & \xrightarrow{s\cdot} & K/(s\cdot\Lambda) \\ \wr\downarrow & & \wr\downarrow \\ \bigoplus_p K_p/(\Lambda_p) & \longrightarrow & \bigoplus_p K_p/(s_p\Lambda_p) \end{array}$$

where the map on the bottom is defined as $(x_p)_p \mapsto (s_p x_p)_p$, and $\Lambda_p := \Lambda\otimes_{\mathbb{Z}}\mathbb{Z}_p$.

Going back to the diagram (7), we see in particular that the action of $\mu(s)\mathrm{N}_{F/K}(s^{-1})$ stabilizes $\ker(\xi)$, which is an invertible fractional ideal of $\mathcal{O}$. Therefore, $\mu(s)\mathrm{N}_{F/K}(s^{-1})$ stabilizes $\mathcal{O}$ as well, which in turn implies that $(\mu(s)\mathrm{N}_{F/K}(s^{-1}))^\infty \in \widehat{\mathcal{O}}^\times$, where, as before, we denote by $s^\infty = (s_v)_{v\in\mathfrak{M}_K^\infty}$ the finite part of an idèle. Combining this observation with the diagram (7), we see that the map $\theta_E(s) := (\mu(s)\mathrm{N}_{F/K}(s^{-1}))^\infty$ yields a continuous group homomorphism $\theta_E\colon \mathbb{A}_F^\times \to \widehat{\mathcal{O}}^\times$ which fits in the following commutative diagram:

$$\begin{array}{ccc} \mathbb{A}_F^\times & \xrightarrow{\theta_E} & \widehat{\mathcal{O}}^\times \\ {\scriptstyle \mathrm{res}_{F^{\mathrm{ab}}/F(E_{\mathrm{tors}})}\circ[F,\cdot]}\downarrow\!\!\downarrow & & \wr\downarrow \\ \mathrm{Gal}(F(E_{\mathrm{tors}})/F) & \xhookrightarrow{\rho_E} & \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \end{array} \quad , \tag{8}$$

where $F(E_{\mathrm{tors}}) \subseteq F^{\mathrm{ab}}$ denotes the field obtained by adjoining to F all the coordinates of the torsion points of E. This diagram allows us to see that the Galois representation ρ_E is in fact compatible with the Artin map $[K,\cdot]$. More precisely, let $\psi_E\colon \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}})$ denote the composition of the isomorphism $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathcal{O}}^\times$ with the map $\mathfrak{a}_{\mathcal{O}}\colon \widehat{\mathcal{O}}^\times \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}})$ given by $\mathfrak{a}_{\mathcal{O}}(s) := [K, s^{-1}]$. This map ψ_E fits into the square

$$\begin{array}{ccc} \mathrm{Gal}(F(E_{\mathrm{tors}})/F) & \xhookrightarrow{\rho_E} & \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow{\scriptstyle \psi_E} \\ \mathrm{Gal}(K^{\mathrm{ab}}/F\cap K^{\mathrm{ab}}) & \xhookrightarrow{\iota} & \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \end{array} \tag{9}$$

where the map on the left is defined as $\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \twoheadrightarrow \mathrm{Gal}(FK^{\mathrm{ab}}/F) \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/F\cap K^{\mathrm{ab}})$, while the map on the bottom is the natural inclusion induced by the fact that $H_{\mathcal{O}} = K(j(E)) \subseteq F\cap K^{\mathrm{ab}}$, because E is defined over F. One can easily see that (9) is commutative, because when we glue the diagram (8), whose

vertical maps are surjective, on top of (9) we obtain the diagram

$$\begin{array}{ccc} \mathbb{A}_F^\times & \xrightarrow{\theta_E} & \widehat{\mathcal{O}}^\times \\ \Big\downarrow{\scriptstyle \mathrm{res}_{F^{\mathrm{ab}}/K^{\mathrm{ab}}}\circ[F,\cdot]} & & \Big\downarrow{\scriptstyle \mathfrak{a}_{\mathcal{O}}} \\ \mathrm{Gal}(K^{\mathrm{ab}}/F\cap K^{\mathrm{ab}}) & \xhookrightarrow{\iota} & \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \end{array}$$

which commutes because $\mathfrak{a}_{\mathcal{O}}(\theta_E(s)) = [K,((\mu_E(s)\mathrm{N}_{F/K}(s^{-1}))^\infty)^{-1}] = [K,\mathrm{N}_{F/K}(s)] = \iota(\mathrm{res}_{F^{\mathrm{ab}}/K^{\mathrm{ab}}}([F,s]))$ for every idèle $s \in \mathbb{A}_F^\times$, as follows from the fact that $K^\times \cdot K_\infty^\times \subseteq \ker([K,\cdot])$ and from the functoriality of class field theory. Therefore, dividing $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathcal{O}}^\times$ by the subgroup $U_{I,\mathcal{O}}$, we see easily from (9) that $H_{I,\mathcal{O}} = H_{\mathcal{O}}(\mathfrak{h}_E(E[I]))$, because the map ψ_E fits into the exact sequence

$$1 \to \mathrm{Aut}_F(E) \to \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \xrightarrow{\psi_E} \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \to 1, \tag{10}$$

as follows from the fact that $\ker([K,\cdot]) \cap \widehat{\mathcal{O}}^\times = K^\times \cap \widehat{\mathcal{O}}^\times = \mathcal{O}^\times$.

A formula for the index of the image of Galois representations

To conclude this lecture, let us show how one can apply the considerations above to prove an explicit formula for the index $\mathcal{I}(E/F) := [\mathcal{G}(E/F)\colon \rho_E(\Gamma_F)]$ of the image of the Galois representation ρ_E attached to an elliptic curve E which has complex multiplication by an imaginary quadratic order $\mathcal{O}$ and is defined over a number field F. To do so, one can observe first of all that $\mathcal{I}(E/F) = \mathcal{I}(E/FK)$, which allows us to assume that $K \subseteq F$, which implies that $\mathcal{G}(E/F) = \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$. Then, one can combine the exact sequence (10) with the diagram (9) to obtain the following diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(F(E_{\mathrm{tors}})/FK^{\mathrm{ab}}) & \longrightarrow & \mathrm{Gal}(F(E_{\mathrm{tors}})/F) & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/F\cap K^{\mathrm{ab}}) & \longrightarrow & 1 \\ & & \Big\downarrow{\scriptstyle \iota'} & & \Big\downarrow{\scriptstyle \rho_E} & (9) & \Big\downarrow{\scriptstyle \iota} & & \\ 1 & \longrightarrow & \mathrm{Aut}_F(E) & \longrightarrow & \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) & \xrightarrow[\psi_E]{} & \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) & \longrightarrow & 1 \end{array}$$

whose rows are exact. Therefore, we see by the snake lemma that

$$\mathcal{I}(E/F) = |\mathrm{coker}(\rho_E)| = |\mathrm{coker}(\iota)| \cdot |\mathrm{coker}(\iota')| = [F\cap K^{\mathrm{ab}}\colon H_{\mathcal{O}}] \cdot \frac{|\mathcal{O}^\times|}{[F(E_{\mathrm{tors}}) : FK^{\mathrm{ab}}]}, \tag{11}$$

which gives us a completely explicit formula for the index of the Galois representation attached to E, that was proven in [6, Theorem 1.1]. This formula can in fact be rewritten as

$$\mathcal{I}(E/F) = \frac{\#\mathcal{O}^\times \cdot [L\cap K^{\mathrm{ab}}\colon K]}{\#\mathrm{Cl}(\mathcal{O}) \cdot [L\colon F]},$$

where $F \subseteq L$ is any finite extension such that $F(E_{\mathrm{tors}}) = LK^{\mathrm{ab}}$. For instance, one can take $L = F(E[N])$ for any $N > 3$. This allows one to compute explicitly the index $\mathcal{I}(E/F)$, and gives a completely effective analogue of Serre's open image theorem in the complex multiplication case.

URL: https://drive.google.com/file/d/1wKIjZTit-r3euRziu0BJPMxdVTqELnAF/view?usp=sharing

8 Entanglement between the division fields of elliptic curves

The aim of this final lecture is to give some ideas about the phenomenon of *entanglement* inside the family of division fields associated to an elliptic curve. Recall that, if E is an elliptic curve defined over a number field F, and $I \subseteq \mathrm{End}_{\overline{F}}(E)$ is an ideal, the I-th division field of E is the number field $F(E[I])$, where we let $E[I] := \bigcap_{\alpha \in I} \ker\left([\alpha]\colon E(\overline{F}) \to E(\overline{F})\right)$ denote the I-th torsion subgroup. Moreover, we will usually consider the infinite division fields $F(E[N^\infty]) := \bigcup_{n=0}^{+\infty} F(E[N^n])$.

Entanglement

The protagonist of this lecture will be the *entanglement* between these division fields. More precisely, if F is a number field and $\mathcal{F}$ is a family of Galois sub-extensions of a fixed algebraic closure $F \subseteq \overline{F}$, we say (following Lenstra) that $\mathcal{F}$ is *entangled* (over F) if the canonical injective restriction map

$$\mathrm{Gal}\left(\prod_{L\in\mathcal{F}} L \Big/ F\right) \hookrightarrow \prod_{L\in\mathcal{F}} \mathrm{Gal}(L/F)$$

is not surjective, where $\prod_{L\in\mathcal{F}} L$ denotes the compositum of all the fields belonging to the family $\mathcal{F}$. With a terminology that is perhaps more familiar to the reader, we say that $\mathcal{F}$ is *linearly disjoint* (over F) if the aforementioned map *is* injective.

Clearly, the presence of entanglement in a family of number fields is heavily dependent on how we index the fields in question. For instance, we could take $\mathcal{F}$ to be the family of all the division fields $F(E[N])$, where N varies over all the non-zero natural numbers. However, this family is clearly going to be entangled, because $F(E[N]) \subseteq F(E[M])$ whenever $N \mid M$. Therefore, it is better to consider the family of infinite division fields $\mathcal{F}_E = \{F(E[\ell^\infty])\colon \ell \in \mathbb{N} \text{ prime}\}$ indexed over primes, which has a better chance of being linearly disjoint over F. In terms of Galois representations, we are asking whether the adelic image

$$\rho_E(\Gamma_F) \subseteq \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \prod_{\ell} \mathrm{Aut}_{\mathbb{Z}}(E[\ell^\infty])$$

has any change of being equal to the product $\prod_\ell \rho_{E,\ell^\infty}(\Gamma_F)$ of the ℓ-adic images.

More generally, a foundational problem in the theory of Galois representations (introduced by Mazur) consists in classifying the possible adelic images $\rho_E(\Gamma_F)$. The aforementioned problem can be divided into the question of classification of the possible ℓ-adic images $\rho_{E,\ell^\infty}(\Gamma_F)$, and then the problem of knowing how these different local images interact inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$. In particular, when $F = \mathbb{Q}$ we know that for every fixed prime ℓ there are only finitely many possibilities for the ℓ-adic image $\rho_{E,\ell^\infty}(\Gamma_F)$, which were classified in various recent works, culminating with the work of Rouse, Sutherland and Zureick-Brown [34]. A similar classification for the possible images of the ℓ-adic representations attached to elliptic curves with complex multiplication which are defined over the minimal field of definition $\mathbb{Q}(j(E))$ has been recently completed

by Lozano-Robledo [29]. Moreover, as we already mentioned, recent work of Zywina [44] provides a finite list of integers which should conjecturally exhaust all the possible indices of the images of adelic Galois representations associated to elliptic curves without complex multiplication, while our formula (11) provides a similar explicit list of possible indices for elliptic curves with complex multiplication (defined over any number field). Despite these finiteness results, the images $\rho_E(\Gamma_F)$ can take infinitely many possible values, as we will see by looking at elliptic curves with complex multiplication.

The Lang-Trotter conjecture

Before moving to the classification of the possible types of entanglement for the families of division fields of elliptic curves defined over a number field, we would like to explain a possible application related to the study of this entanglement problem.

Let E be an elliptic curve defined over a number field F. Given a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_F$ at which E has good reduction $\tilde{E}$, we write $a_\mathfrak{p}(E) := |\mathcal{O}_F/\mathfrak{p}| + 1 - \#\tilde{E}(\mathcal{O}_F/\mathfrak{p})$ for the trace of the action of Frobenius on the étale cohomology of E. Then, Lang and Trotter [23] conjectured that

$$\#\{\mathfrak{p} \subseteq \mathcal{O}_F \colon |\mathcal{O}_F/\mathfrak{p}| \leq x,\ a_\mathfrak{p}(E) = r\} \sim C_{E,r} \cdot \frac{\sqrt{x}}{\log(x)}$$

when $x \to +\infty$, unless E has some *congruence obstruction*. This can be expressed in terms of the Galois representations $\rho_{E,N}$, by saying that there exists some integer N such that $\rho_{E,N}(\Gamma_F)$ does not contain any element of trace equal to r modulo N.

One can give an explicit conjectural expression for the constant $C_{E,r}$ by studying the adelic image $\rho_E(\Gamma_F)$. More precisely, if E does not have complex multiplication then $C_{E,r} = C'_{E,r} \cdot \mathcal{LT}_\mathbb{Z}$, where

$$\mathcal{LT}_\mathbb{Z} = \frac{2}{\pi} \cdot \prod_\ell \left(1 - \frac{1}{(\ell-1)(\ell^2-1)}\right)$$

denotes the *Lang-Trotter constant* (for $\mathbb{Z}$), while $C'_{E,r} \in \mathbb{Q}$ is an *entanglement correction factor*. To define it, let N_E denote the smallest positive integer N such that $\rho_E(\Gamma_F)$ equals the inverse image of $\rho_{E,N}(\Gamma_F)$ under the canonical projection map $\mathrm{Aut}_\mathbb{Z}(E_{\mathrm{tors}}) \twoheadrightarrow \mathrm{Aut}_{\mathbb{Z}/N\mathbb{Z}}(E[N])$, which exists thanks to Serre's open image theorem. Then

$$C'_{E,r} = \frac{N_E \cdot \#\{g \in \rho_{E,N_E}(\Gamma_F) \colon \mathrm{Tr}(g) \equiv r(N_E)\}}{\#\rho_{E,N_E}(\Gamma_F)} \cdot \prod_{\substack{\ell \mid r \\ \ell \nmid N_E}} \left(1 + \frac{1}{\ell^2-1}\right) \cdot \prod_{\ell \mid r N_E} \left(1 - \frac{1}{(\ell-1)(\ell^2-1)}\right)^{-1},$$

which allows us to give a precise asymptotic for the function $x \mapsto \#\{\mathfrak{p} \subseteq \mathcal{O}_F \colon |\mathcal{O}_F/\mathfrak{p}| \leq x,\ a_\mathfrak{p}(E) = r\}$ if we know N_E and the finite image $\rho_{E,N_E}(\Gamma_F)$, which amounts to knowing the adelic image $\rho_E(\Gamma_F)$.

On the other hand, if E has complex multiplication by an imaginary quadratic order $\mathcal{O}$, Lang and Trotter conjectured that $C_{E,r} = C'_{E,r} \cdot \mathcal{LT}_\mathcal{O}$, where

$$\mathcal{LT}_\mathcal{O} = \frac{1}{2\pi} \prod_\ell \left(1 - \frac{\chi_\mathcal{O}(\ell)}{(\ell-1)(\ell - \chi_\mathcal{O}(\ell))}\right)$$

is the *Lang-Trotter constant* of the order $\mathcal{O}$, defined in terms of the character

$$\chi_{\mathcal{O}}(\ell) := \begin{cases} 1, & \text{if } \ell \text{ splits in } \mathcal{O} \\ -1, & \text{if } \ell \text{ is inert } \mathcal{O} \\ 0, & \text{if } \ell \text{ ramifies in } \mathcal{O}, \end{cases}$$

while once again $C'_{E,r} \in \mathbb{Q}$ is an *entanglement correction factor*. This can be explicitly defined as

$$C'_{E,r} = \frac{N_E \cdot \#\{g \in \rho_{E,N_E}(\Gamma_F) \colon \mathrm{Tr}(g) \equiv r(N_E)\}}{\#\rho_{E,N_E}(\Gamma_F)} \cdot \prod_{\substack{\ell \mid r \\ \ell \nmid N_E}} \left(1 + \frac{\chi_{\mathcal{O}}(\ell)}{\ell - \chi_{\mathcal{O}}(\ell)}\right) \cdot \prod_{\ell \mid r N_E} \left(1 - \frac{\chi_{\mathcal{O}}(\ell)}{(\ell-1)(\ell - \chi_{\mathcal{O}}(\ell))}\right)^{-1},$$

where once again N_E denotes the minimal integer N such that $\rho_E(\Gamma_F)$ equals the pre-image of $\rho_{E,N}(\Gamma_F)$ under the canonical reduction map $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \twoheadrightarrow \mathrm{Aut}_{\mathbb{Z}/N\mathbb{Z}}(E[N])$.

Artin's primitive root conjecture

Let us mention another application of the study of entanglements to arithmetic statistics.

To do so, let us look at the division fields of the algebraic group $\mathbb{G}_m$ (over $\mathbb{Q}$), which are given by the cyclotomic fields $\mathbb{Q}(\zeta_N)$ for $N \geq 1$. Moreover, given a fixed integer $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$, one can look at the field $\mathbb{Q}(\zeta_N, \sqrt[N]{a})$, which is Galois over $\mathbb{Q}$ because it is the splitting field of $x^N - a$. Then, it turns out that the entanglement in the family $\{\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a}) \colon \ell \in \mathbb{N} \text{ prime}\}$ is closely related to the problem of determining the density of the primes ℓ such that the reduction of a modulo ℓ generates the group $\mathbb{F}_\ell^\times$. In particular, Hooley has shown that this density exists and is non-negative if one assumes the validity of the Generalized Riemann Hypotheses for the Dedekind zeta functions of the number fields $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})$. Moreover, Lenstra, Moree and Stevenhagen [27] have shown that this density should be a rational multiple of Artin's constant $\mathcal{A} = \prod_p (1 - (p^2 - p)^{-1})$, and that this rational multiple can be detected by studying the entanglement in the aforementioned family $\{\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a}) \colon \ell \in \mathbb{N} \text{ prime}\}$. More precisely, the expected density of the set of primes ℓ such that the reduction of a modulo ℓ generates $\mathbb{F}_\ell^\times$ can be written as

$$\delta(a) := \mathcal{A} \cdot \prod_{p \mid h} \frac{p^2 - 2p}{p^2 - p - 1} \cdot \left(1 - \prod_{\substack{p \mid D \\ p \mid h}} \frac{1}{2 - p} \cdot \prod_{\substack{p \mid D \\ p \nmid h}} \frac{1}{1 - p - p^2}\right),$$

where h is the biggest number such that a is an h-power in $\mathbb{Q}$, while $D = 1$ unless the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{a})$ is quadratic of odd discriminant D. This is due to the fact that, when the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{a})$ is quadratic of odd discriminant, the field $\mathbb{Q}(\sqrt{a})$ is contained in the compositum of all the fields $\mathbb{Q}(\zeta_\ell)$, where ℓ runs over the prime divisors of D. This inclusion gives us a non-trivial entanglement in the aforementioned family $\{\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a}) \colon \ell \in \mathbb{N} \text{ prime}\}$, and yields the second correction factor in the product defining $\delta(a)$.

This picture can be generalized to the context of elliptic curves. More precisely, let E be an elliptic curve defined over a number field F, and fix a point $P \in E(F)$. Then, Lang and Trotter [24] conjectured that the set of prime ideals $\mathfrak{p} \subseteq \mathcal{O}_F$ such that the reduction of P modulo $\mathfrak{p}$ generates the group $\tilde{E}(\mathcal{O}_F/\mathfrak{p})$ has positive density. However, in this case the group $\tilde{E}(\mathcal{O}_F/\mathfrak{p})$ may not be cyclic, and in fact the density of those primes $\mathfrak{p} \subseteq \mathcal{O}_F$ such that $\tilde{E}(\mathcal{O}_F/\mathfrak{p})$ is cyclic can again be expressed as the product of a fixed "Artin constant" $\mathcal{A}_E$ multiplied by a rational correction factor, which is related to the entanglement in the family $\{F(E[\ell])\colon \ell \in \mathbb{N} \text{ prime}\}$. When $F = \mathbb{Q}$, these considerations are due to Serre, who dedicated to them one of his courses at the Collège de France. Campagna and Stevenhagen [7] have recently written down these considerations in the general case, and they have studied in particular those cases in which the expected density of the set of primes of cyclic reduction can vanish.

Entanglement for elliptic curves without complex multiplication

In order to answer this question, Campagna and Stevenhagen provided an explicit upper bound for the set of primes that one has to exclude in order to have a linearly disjoint family of division fields. More precisely, let E be an elliptic curve defined over a number field F, such that $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$. Then, one can define an integer $B_E := 2 \cdot 3 \cdot 5 \cdot \Delta_F \cdot \mathrm{N}_{F/K}(\mathfrak{f}_E)$, where Δ_F denotes the absolute discriminant of F, and $\mathfrak{f}_E \subseteq \mathcal{O}_F$ denotes the conductor of the elliptic curve E. Moreover, let S'_E denote the set of primes ℓ such that $\rho_{E,\ell}(\Gamma_F) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which is finite by Serre's open image theorem. Then, the family

$$\{F(E[\ell])\colon \ell \in \mathbb{N} \setminus (\{\ell \mid B_E\} \cup S'_E) \text{ prime}\}$$

is linearly disjoint over the number field F.

Apart from these explicit bounds on the set of primes which can be entangled, a great amount of work has been done in recent years to understand the possible types of entanglement, especially when $F = \mathbb{Q}$. From the point of view of Galois representations, this means once again that one would like to classify all the possible images $\rho_E(\Gamma_F)$. This question, especially when $F = \mathbb{Q}$, appeared as the *Program B* in a seminal paper of Mazur [31]. When $F = \mathbb{Q}$, it turns out that the image $\rho_E(\Gamma_F)$ cannot be equal to $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$. This is due to the fact that if the second division field $\mathbb{Q}(E[2])$ does not collapse, which happens when the discriminant Δ_E is not a square in $\mathbb{Q}^\times$, we have an entanglement between $\mathbb{Q}(E[2])$, which contains $\mathbb{Q}(\sqrt{\Delta_E})$ as its unique quadratic sub-extension, and the field $\mathbb{Q}(E[\Delta_E|])$, which contains $\mathbb{Q}(\zeta_{|\Delta_E|})$ thanks to the Weil pairing. As was shown by Jones [19], 100% of elliptic curves defined over $\mathbb{Q}$, when ordered by naive height, are *Serre curves*, which means that $\mathcal{I}(E/\mathbb{Q}) = 2$, *i.e.* that the image $\rho_E(\Gamma_{\mathbb{Q}})$ is as big as possible.

Nevertheless, classifying all the possible images $\rho_E(\Gamma_F)$ of the Galois representations associated to elliptic curves E defined over a fixed number field F remains an interesting and challenging problem. A recent paper by Daniels, Lozano-Robledo and Morrow [11] aims at providing a first step towards a complete classification

of the possible types of entanglement between the division fields of an elliptic curve. In particular, this work uses a group theoretic approach to study entanglements, by looking at certain subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. More precisely, given two divisors $a, b \mid N$, one says that a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ represents an (a,b)-entanglement if $\langle \ker(\pi_a) \cap G', \ker(\pi_b) \cap G' \rangle \subsetneq \ker(\pi_d) \cap G'$, where $c = \mathrm{lcm}(a,b)$ and $d = \gcd(a,b)$, while $G' \subseteq \mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z})$ denotes the image of G under the natural quotient map $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z})$, and for every divisor $n \mid c$ we let $\pi_n \colon \mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ denote the canonical quotient map. In terms of division fields, the subgroup $\mathrm{Im}(\rho_{E,N}(\Gamma_F)) \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ represents a non-trivial (a,b)-entanglement if $\mathbb{Q}(E[d]) \subsetneq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$, where once again $d = \gcd(a,b)$. The aforementioned paper of Daniels, Lozano-Robledo and Morrow [11] then proceeds to describe several different types of *abelian* entanglements, *i.e.* those cases in which $\mathbb{Q}(E[d]) \cap \mathbb{Q}^{\mathrm{ab}} \subsetneq (\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])) \cap \mathbb{Q}^{\mathrm{ab}}$. More precisely, they classify this type of entanglement into four types (*Weil*, *discriminant*, *CM* and *fake CM*), and they show that if an elliptic curve E defined over $\mathbb{Q}$ exhibits an abelian entanglement that is not of these types then its j-invariant $j(E)$ belongs to the union between a certain finite set J and one of three explicit families of j-invariants, parametrized by rational maps $j_1, j_2, j_3 \in \mathbb{Q}(t)$. Their proof proceeds by classifying some modular curves which parametrize elliptic curves whose division fields have a certain type of entanglement. When these modular curves have genus zero or one, we can explicitly determine their set of rational points. For example, the rational maps j_1, j_2, j_3 correspond to those modular curves that have genus zero. On the other hand, when these modular curves have genus two or higher, it is quite challenging to determine their set of rational points, which leads to the inexplicit nature of the finite set J. Finally, let us mention that a similar investigation for elliptic curves with non-abelian entanglements has been carried out by Jones and McMurdy [20].

Entanglement for elliptic curves with complex multiplication

Let us see what happens when an elliptic curve E defined over a number field F has complex multiplication by an order $\mathcal{O} \subseteq K$. For simplicity, let us also assume that the complex multiplication is defined over F, *i.e.* that $K \subseteq F$. In this case, we proved in [5] that the family of division fields $\{F(E[\ell^\infty]) \colon \ell \in \mathbb{N} \setminus \{\ell \mid B_E\} \text{ prime}\}$ is linearly disjoint, where $B_E := \Delta_F \cdot |\mathcal{O}_F/\mathfrak{f}_E| \cdot [\mathcal{O}_K \colon \mathcal{O}]$. The proof of this result proceeds along three steps. First of all, we prove a slight generalization of the Néron-Ogg-Shafarevich criterion, which shows that for every ideal $I \subseteq \mathcal{O}$ the extension $F \subseteq F(E[I])$ is unramified outside $(I \cdot \mathcal{O}_F) \cdot \mathfrak{f}_E$. Moreover, we show that for any prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ coprime with $B_E \cdot \mathcal{O}$ and any $n \in \mathbb{N}$, the extension $F \subseteq F(E[\mathfrak{p}^n])$ is totally ramified at every prime ideal of $\mathcal{O}_F$ which divides $\mathfrak{p} \cdot \mathcal{O}_F$. This implies that for every rational prime ℓ each sub-extension of $F \subseteq F(E[\ell^n])$ is ramified at some prime ideal of $\mathcal{O}_F$ which divides $\ell\mathcal{O}_F$, and allows us to conclude.

It is then interesting to try addressing Mazur's *program B* for elliptic curves with complex multiplication, *i.e.* to give a complete classification of all the possible images $\rho_E(\Gamma_F)$ of the adelic Galois representations associated to such elliptic curves. It turns out that the nature of these images depends crucially on whether

or not the maximal division field $F(E_{\text{tors}})$ is an abelian extension of the imaginary quadratic field K^{ab}. More generally, if the extension $FK^{\text{ab}} \subseteq F(E_{\text{tors}})$ is not trivial and $j(E) \notin \{0, 1728\}$, we know from (11) that the image $\rho_E(\Gamma_F)$ has the smallest possible index. When $F = H_{\mathcal{O}}$, this implies that $\rho_E(\Gamma_F) = \text{Aut}_{\mathcal{O}}(E_{\text{tors}})$, and therefore that the family of division fields $\{H_{\mathcal{O}}(E[\ell^\infty])\colon \ell \in \mathbb{N} \text{ prime}\}$ is linearly disjoint. When the class group $\text{Cl}(\mathcal{O})$ is not trivial, it turns out that 100% of the elliptic curves with complex multiplication by $\mathcal{O}$ have this property. However, one can also show that for any given elliptic curve E with this property, infinitely many of its quadratic twists E' of E will *not* have this property, which means that the maximal division fields $H_{\mathcal{O}}(E'_{\text{tors}})$ will be abelian extensions of K. It is still not clear to us under what conditions there exists an elliptic curve E defined over the smaller field $\mathbb{Q}(j(E))$ for which the maximal division field is an abelian extension of K.

Finally, let us mention what happens when $\text{Cl}(\mathcal{O})$ is trivial. In this case $H_{\mathcal{O}} = K$, which implies that for every elliptic curve E defined over K which has complex multiplication by $\mathcal{O}$, the maximal division field $K(E_{\text{tors}})$ is an abelian extension of K. Moreover, when E is the base change of a curve defined over $\mathbb{Q}$, we were able to describe explicitly the image $\rho_E(\Gamma_F)$ of the Galois representation associated to E. More precisely, if E belongs to a finite list of thirty elliptic curves of "minimal conductor", and p denotes the unique prime which ramifies in $\mathbb{Q} \subseteq K$, we have that $\rho_{E,p^\infty}(\Gamma_K) \subseteq \text{Aut}_{\mathcal{O}_p}(E[p^\infty])$ has index two. Since the index of $\rho_E(\Gamma_K)$ inside $\text{Aut}_{\mathcal{O}}(E_{\text{tors}})$ is also two, this implies that $\rho_{E,\ell^\infty}(\Gamma_K) = \text{Aut}_{\mathcal{O}_\ell}(E[\ell^\infty])$ for every $\ell \neq p$, and that the family $\{K(E[\ell^\infty])\colon \ell \in \mathbb{N} \text{ prime}\}$ is linearly disjoint over K. Note that the family $\{\mathbb{Q}(E[\ell^\infty])\colon \ell \in \mathbb{N} \text{ prime}\}$ can never be linearly disjoint over $\mathbb{Q}$, because when $N \geq 3$ the division field $\mathbb{Q}(E[N])$ contains the imaginary quadratic field K. To conclude, let us see what happens when E does not have minimal conductor. In this case, E will be the d-th quadratic twist of an elliptic curve E_0 of minimal conductor. Using this fact, one can show that the family $\{K(E[\ell^\infty])\colon \ell \in \mathbb{N} \setminus \{\ell \mid pd\} \text{ prime}\}$ is linearly disjoint, and that $\rho_{E,\ell^\infty}(\Gamma_K) = \text{Aut}_{\mathcal{O}_\ell}(E[\ell^\infty])$ for every rational prime ℓ. Since the index of $\rho_E(\Gamma_K)$ inside $\text{Aut}_{\mathcal{O}}(E_{\text{tors}})$ is always two, this last fact implies that we must have some non-trivial entanglement. Indeed, it happens that $K(E[p^n]) = H_{p^n,\mathcal{O}}(\sqrt{d})$, which yields a non-trivial entanglement between the p-adic and d-adic towers of division fields of E. In particular, $K(E[N]) = H_{N,\mathcal{O}}$ whenever $pd \mid N$.

We expect that a similar classification should hold true for the images of the Galois representations attached to elliptic curves E defined over $H_{\mathcal{O}}$ which are base-changes of curves defined over $\mathbb{Q}(j(E))$, have complex multiplication by $\mathcal{O}$ and for which the maximal division field $H_{\mathcal{O}}(E_{\text{tors}})$ is an abelian extension of K. In general, we know that for these curves the image $\rho_E(\Gamma_{H_{\mathcal{O}}})$ will never be maximal, and we can provide an explicit bound for the minimal integer N such that $H_{\mathcal{O}}(E[N]) = H_{N,\mathcal{O}}$. This bound, which is related to the conductor of the elliptic curve E, generalizes a result of Coates and Wiles [8, Lemma 5].

References

[1] Balakrishnan, J., Dogra, N., Müller, J. S., Tuitman, J., & Vonk, J. (2019). *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*. Annals of Mathematics. Second Series, 189(3), 885–944. doi:10.4007/annals.2019.189.3.6

[2] Bilu, Yu., & Parent, P. (2011). *Serre's uniformity problem in the split Cartan case*. Annals of Mathematics, 173(1), 569–584. doi:10.4007/annals.2011.173.1.13

[3] Borger, J., & de Smit, B. (2018). *Explicit class field theory and the algebraic geometry of Λ-rings*. arXiv:1809.02295

[4] Breuil, C., Conrad, B., Diamond, F., & Taylor, R. (2001). *On the modularity of elliptic curves over* **Q***: Wild 3-adic exercises*. Journal of the American Mathematical Society, 14(4), 843–939. doi:10.1090/S0894-0347-01-00370-8

[5] Campagna, F., & Pengo, R. (2022). *Entanglement in the family of division fields of elliptic curves with complex multiplication*. Pacific Journal of Mathematics, 317(1), 21–66. doi:10.2140/pjm.2022.317.21

[6] Campagna, F., & Pengo, R. (2022). *How big is the image of the Galois representations attached to CM elliptic curves?* In: Arithmetic, geometry, cryptography, and coding theory 2021 (Vol. 779, pp. 41–56). Amer. Math. Soc., [Providence], RI. 10.1090/conm/779/15670

[7] Campagna, F., & Stevenhagen, P. (2023). *Cyclic reduction densities for elliptic curves*. Research in Number Theory, 9(3), 61. doi:10.1007/s40993-023-00463-9

[8] Coates, J., & Wiles, A. (1977). *On the conjecture of Birch and Swinnerton-Dyer*. Inventiones Mathematicæ, 39(3), 223–251. doi:10.1007/BF01402975

[9] Cojocaru, A. C., & Hall, C. (2005). *Uniform results for Serre's theorem for elliptic curves*. International Mathematics Research Notices, 50, 3065–3080. doi:10.1155/IMRN.2005.3065

[10] Cojocaru, A. C. (2005). *On the Surjectivity of the Galois Representations Associated to Non-CM Elliptic Curves*. With an appendix by E. Kani. Canadian Mathematical Bulletin, 48(1), 16–31. doi:10.4153/CMB-2005-002-x

[11] Daniels, H. B., Lozano-Robledo, A., & Morrow, J. S. (2023). *Towards a classification of entanglements of Galois representations attached to elliptic curves*. Revista Matemática Iberoamericana, 39(3), 803–844. doi:10.4171/rmi/1424

[12] Dasgupta, S., & Kakde, M. (2021). *Brumer-Stark Units and Explicit Class Field Theory*. To appear in Duke Mathematical Journal. arXiv:2103.02516.

[13] Fontaine, J.-M., & Mazur, B. (1995). *Geometric Galois representations*. In Elliptic curves, modular forms, & Fermat's last theorem. Proceedings ot the conference on elliptic curves and modular forms held at the Chinese University of Hong Kong, December 18-21, 1993 (pp. 41–78). International Press.

[14] Harris, M., Taylor, R., & Berkovich, V. G. (2001). *The Geometry and Cohomology of Some Simple Shimura Varieties*. (AM-151). Princeton University Press. ISBN:978-0-691-09090-0

[15] Hazewinkel, M. (1975). Local class field theory is easy. Advances in Mathematics, 18(2), 148–181. doi:10.1016/0001-8708(75)90156-5

[16] Henniart, G. (2000). *Une preuve simple des conjectures de Langlands pour $GL(n)$ sur un corps p-adique*. Inventiones mathematicae, 139(2), 439–455. doi:10.1007/s002220050012

[17] Hilbert, D. (1902). *Mathematical problems*. Bulletin of the American Mathematical Society, 8(10), 437–479. doi:10.1090/S0002-9904-1902-00923-3

[18] Jannsen, U., & Wingberg, K. (1982). *Die Struktur der Absoluten Galoisgruppe* $\mathfrak{p}$*-Zahlkörper*. Inventiones mathematicae, 70(1), 71–98. doi:10.1007/BF01393199

[19] Jones, N. (2010). *Almost all elliptic curves are Serre curves*. Transactions of the American Mathematical Society, 362(3), 1547–1570. doi:10.1090/S0002-9947-09-04804-1

[20] Jones, N., & McMurdy, K. (2022). *Elliptic curves with non-abelian entanglements*. The New York Journal of Mathematics, 28, 182–229. url:https://nyjm.albany.edu/j/2022/28-9.html

[21] Koch, H. (1967). *Über die Galoissche Gruppe der algebraischen Abschließung eines Potenzreihenkörpers mit endlichem Konstantenkörper*. Mathematische Nachrichten, 35(5–6), 323–327. doi:10.1002/mana.19670350509

[22] Lang, S. (2002). *Algebra (3rd ed.)*. Springer-Verlag. 10.1007/978-1-4613-0041-0

[23] Lang, S., & Trotter, H. (1976). *Frobenius distributions in* GL_2*-extensions*. Springer-Verlag, Berlin-New York. doi:10.1007/BFb0082087

[24] Lang, S., & Trotter, H. (1977). *Primitive points on elliptic curves*. Bulletin of the American Mathematical Society, 83(2), 289–292. doi:10.1090/S0002-9904-1977-14310-3

[25] Langlands, R. P. (1990). *Representation theory: Its rise and its role in number theory*. Proceedings of the Gibbs Symposium (New Haven, CT, 1989), 181–210.

URL: https://drive.google.com/file/d/1wKIjZTit-r3euRziu0BJPMxdVTqELnAF/view?usp=sharing

[26] Laumon, G., Rapoport, M., & Stuhler, U. (1993). *D-elliptic sheaves and the Langlands correspondence*. Inventiones Mathematicae, 113(1), 217–338. 10.1007/BF01244308

[27] Lenstra, H. W., Stevenhagen, P., & Moree, P. (2014). *Character sums for primitive root densities*. Mathematical Proceedings of the Cambridge Philosophical Society, 157(3), 489–511. doi:10.1017/S0305004114000450

[28] Lombardo, D. (2015). *Bounds for Serre's open image theorem for elliptic curves over number fields*. Algebra & Number Theory, 9(10), 2347–2395. doi:10.2140/ant.2015.9.2347

[29] Lozano-Robledo, Á. (2022). *Galois representations attached to elliptic curves with complex multiplication*. Algebra & Number Theory, 16(4), 777–837. doi:10.2140/ant.2022.16.777

[30] Masser, D. W., & Wüstholz, G. (1993). *Galois properties of division fields of elliptic curves*. The Bulletin of the London Mathematical Society, 25(3), 247–254. doi:10.1112/blms/25.3.247

[31] Mazur, B. (1977). *Rational points on modular curves*. In: J.-P. Serre & D. B. Zagier (Eds.), Modular Functions of one Variable V (pp. 107–148). Springer. doi:10.1007/BFb0063947

[32] Neukirch, J. (1999). *Algebraic Number Theory* (Vol. 322). Springer Berlin Heidelberg. doi:10.1007/978-3-662-03983-0

[33] Pengo, R. (2020). *Mahler measures, special values of L-functions and complex multiplication*. PhD thesis, University of Copenhagen. url:http://web.math.ku.dk/noter/filer/phd20rp.pdf

[34] Rouse, J., Sutherland, A. V., & Zureick-Brown, D. (2022). *ℓ-adic images of Galois for elliptic curves over* $\mathbb{Q}$. With an appendix by John Voight. Forum of Mathematics, Sigma, 10, e62. doi:10.1017/fms.2022.38

[35] Schappacher, N. (1998). *On the history of Hilbert's twelfth problem: A comedy of errors*. In: Matériaux pour l'histoire des mathématiques au XX^e siècle (Nice, 1996) (Vol. 3, pp. 243–273). Soc. Math. France, Paris. url:https://smf.emath.fr/publications/history-hilberts-twelfth-problem

[36] Schertz, R. (2010). *Complex multiplication*. Cambridge University Press, Cambridge. doi:10.1017/CBO9780511776892

[37] Scholze, P. (2013). *The Local Langlands Correspondence for* GL_n *over p-adic fields*. Inventiones Mathematicæ, 192(3), 663–715. doi:10.1007/s00222-012-0420-5

[38] Serre, J.-P. (1971). *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Inventiones mathematicae, 15(4), 259–331. doi:10.1007/BF01405086

[39] Serre, J.-P. (1979). *Local fields* (Vol. 67). Springer-Verlag, New York-Berlin. doi:10.1007/978-1-4757-5673-9

URL: https://drive.google.com/file/d/1wKIjZTit-r3euRziu0BJPMxdVTqELnAF/view?usp=sharing

[40] Serre, J.-P. (1998). Abelian l-adic representations and elliptic curves (Vol. 7). A K Peters, Ltd., Wellesley, MA. ISBN:978-1-56881-077-5

[41] Söhngen, H. (1935). *Zur komplexen Multiplikation*. Mathematische Annalen, 111(1), 302–328. doi:10.1007/BF01472223

[42] Washington, L. C. (1997). *Introduction to cyclotomic fields*. Second edition. Springer-Verlag, New York. doi:10.1007/978-1-4612-1934-7

[43] Wiles, A. (1995). *Modular Elliptic Curves and Fermat's Last Theorem*. Annals of Mathematics, 141(3), 443–551. doi:10.2307/2118559

[44] Zywina, D. (2022). *Explicit open images for elliptic curves over* $\mathbb{Q}$. arXiv:2206.14959

About the author

At the time of writing, I was a postdoc at the Leibniz Universität in Hannover, working in the group of Ziyang Gao. My institutional email address was pengo@math.uni-hannover.de, and my personal email address was riccardopengo@gmail.com. This personal address will probably be still the same when you will be reading this document. For some more updated information about me, you can look at my website https://sites.google.com/view/riccardopengo/.