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.

1 Introduction

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

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

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. 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 Plan of the course

Each lecture will consist of one hour.

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

Lecture 2 Tannaka's reconstruction theorem.

Lecture 3 Reminders of finite and infinite Galois theory, with examples.

Lecture 4 Reminders of algebraic number theory, with examples.

Lecture 5 Reminders of local fields.

Lecture 6 The local and global Kronecker-Weber theorem. The cyclotomic character.

Lecture 7 Local and global class field theories. Ring and ray class fields.

Lecture 8 Reminders on elliptic curves and their Galois representations.

Lecture 9 Serre's open image theorem.

Lecture 10 Elliptic curves with complex multiplication and ray class fields of imaginary quadratic fields: Kronecker's youth dream.

Lecture 11 Entanglement: definition and examples.

Lecture 12 Entanglement between the division fields of elliptic curves with complex multiplication (based on joint work with Francesco Campagna).