Introduction to the Langlands programme

Judith Ludwig
Department of Mathematics, Imperial College London

Imperial College London

Introduction

The Langlands programme is one of the hottest reseach areas of modern number theory.
It relates Galois representations (algebraic objects) and automorphic representations (analytic objects) of reductive algebraic groups.

On this poster you can catch a glimpse on some of the wonders and mysteries of the subject, you do NOT have to know what any of the objects from the previous sentence mean.

Automorphic side

Adeles

- The field of real numbers $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|_\infty$.
- The field of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ w.r.t. the p-adic absolute value $|\cdot|_p$: For $a, b \in \mathbb{Z}$ let m (resp. n) denote the highest power of p that divides a (resp.b), then $|\frac{a}{b}|_p := p^{n-m}$. So e.g. $|15|_3 = 1/3$. The unit ball $B(0,1) := \{x \in \mathbb{Z}_p : |x|_p \leq 1\} \subset \mathbb{Q}_p$ is called $\mathbb{Z}_p$. It is a ring which is isomorphic to the projective limit $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. $\mathbb{Q}_p$ and $\mathbb{R}$ are so called *local* fields, in contrast to the *global* field $\mathbb{Q}$.
- $\mathbb{A} := \prod_p' \mathbb{Q}_p \times \mathbb{R} := \{x \in \prod_p \mathbb{Q}_p \times \mathbb{R} : x \in \mathbb{Z}_p$ for all but finitely many $p\}$ is a locally compact topological ring called the **Adeles**. $\mathbb{A}^\times$ is called the **Ideles**. $\mathbb{Q}$ embeds diagonally into $\mathbb{A}$.
- **The Product Formula**:
$$\forall x \in \mathbb{Q}^\times : \ |x| := \prod_p |x|_p \times |x|_\infty = 1$$
Define $\mathbb{A}^1 = \{x \in \mathbb{A} \mid |x| = 1\}$. So $\mathbb{Q}^\times \subset \mathbb{A}^1$ and $\mathbb{Q}^\times \backslash \mathbb{A}^1 \cong \prod_p \mathbb{Z}_p$
- There is an isomorphism
$$\mathbb{Q}^\times \backslash \mathbb{A}^\times \cong \mathbb{Q}^\times \backslash \mathbb{A}^1 \times \mathbb{R}_{>0}$$
which allows one to identify the characters of $\mathrm{GL}_1(\mathbb{Q})\backslash \mathrm{GL}_1(\mathbb{A}) = \mathbb{Q}^\times \backslash \mathbb{A}^\times$ that have finite image with the characters of $\mathbb{Q}^\times \backslash \mathbb{A}^1$. These characters are examples of automorphic forms of $\mathrm{GL}_1/\mathbb{Q}$.

Reciprocity

Theorem 1
$$\mathbb{Q}^\times \backslash \mathbb{A}^1 \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab}$$

This follows from the Theorem of Kronecker–Weber which says that
$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}),$$
where $\mathbb{Q}(\zeta_\infty)$ is the field extension of $\mathbb{Q}$ obtained by adjoining all n-th roots of unity for all n. In particular
$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab} \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}_p.$$

Theorem 1 allows us to identify the one dimensional representations of $\mathrm{GL}_1(\mathbb{Q})\backslash \mathrm{GL}_1(\mathbb{A})$ that factor through $\mathbb{Q}^\times \backslash \mathbb{A}^1$ with one-dimensional Galois representations.

Galois side

The absolute Galois group of the rationals
$G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is

- a *profinite* group or equivalently a *compact* Hausdorff totally disconnected group,
- one of the most *mysterious* groups in mathematics.

We hope to understand it better by understanding its continuous representations
$$\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\mathbb{C}) \ \text{ or more generally } \ \rho : G_\mathbb{Q} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p).$$
We call these representations *Galois representations*.
Start with the one-dimensional representations. As $\mathbb{C}^\times$ and $\overline{\mathbb{Q}}_p$ are abelian these will factor through the maximal abelian quotient $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab}$ of $G_\mathbb{Q}$.

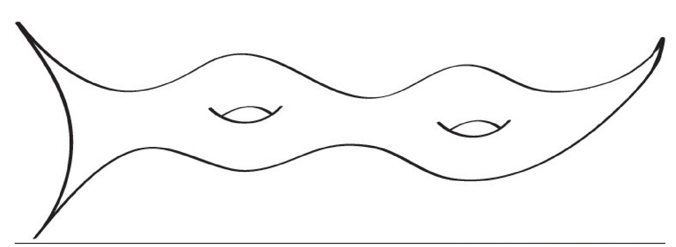
$\mathrm{GL}_1/\mathbb{Q}$

Automorphic side: Cusp Forms $\subset$ Automorphic Forms for $\mathrm{GL}_2/\mathbb{Q}$

- Let $\mathbb{H} := \{z \in \mathbb{C} : Im(z) > 0\}$ be the upper half plane and
$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c = 0, a = d = 1 \bmod N \right\} \subset \mathrm{SL}_2(\mathbb{Z}).$$
$\Gamma_1(N)$ acts on $\mathbb{H}$ by Moebius transformations: $z \mapsto \frac{az+b}{cz+d}$. Note $\Gamma_1(1) = SL_2(\mathbb{Z})$.
- A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called a cusp form of weight k and level N if f satisfies
$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$
for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ and some technical growth conditions. These conditions imply that f has a Fourier expansion of the form
$$f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}.$$
- The space of cusp forms of weight k and level N is a finite dimensional complex vector space which we denote by $S_k(\Gamma_1(N))$. For each p there is a so called *Hecke operator* T_p acting on $S_k(\Gamma_1(N))$. There exist cusp forms f that are eigenvectors for all the T_p simultanously. We call them Hecke eigenforms. After suitable normalization $T_p(f) = a_p f$.
- Example: $S_{12}(SL_2(\mathbb{Z}))$ is one dimensional and spanned by
$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24}, \quad \text{where } q = e^{2\pi i z}.$$

Reciprocity via Modular Curves

$\Gamma_1(N)$ also acts on $\mathbb{P}^1(\mathbb{Q})$. The quotient
$$X_N := \Gamma_1(N) \backslash \mathbb{H} \times \mathbb{P}^1(\mathbb{Q})$$
is called a *modular curve*. It is a compact Riemann surface. Even better: One can prove that there exists a variety $X_1(N)/\mathbb{Q}$ such that
$$X_1(N)(\mathbb{C}) \cong X_N.$$



Complex points of modular curves

One can now use the theory of étale cohomology of these varieties to attach Galois representations to eigenforms:

Theorem 2 (Deligne, Serre)
Let f be a Hecke eigenform of weight k and level N. Then there exists a Galois representation
$$\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$$
unramified outside pN such that $Tr(\rho_f(Frob_l)) = a_l$ for all $l \nmid pN$.

AMAZING!

Galois side

Fixing embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ gives (via restriction) embeddings $G_{\mathbb{Q}_p} \hookrightarrow G_\mathbb{Q}$.

- $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is a cyclic group. Pick a generator $Frob_p$. Any lift of $Frob_p$ under the surjection
$$G_{\mathbb{Q}_p} \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$$
will be called a Frobenius element and denoted by $Frob_p$. The kernel I_p of the above surjection is called the *Inertia* subgroup.
- A Galois representation ρ is called *unramified* at a prime p, if $I_p \subset ker(\rho)|_{G_{\mathbb{Q}_p}}$. For an unramified representation $\rho(Frob_p)$ makes sense and we define
$$Tr(\rho(Frob_p)) =: a_p$$
- Example: Let $E/\mathbb{Q}$ be an elliptic curve. For each $n > 0$ the Galois group $G_\mathbb{Q}$ acts on the group $E[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^2$ of p^n-torsion points and on the Tate module $T_p(E) := \varprojlim E[p^n] \cong \mathbb{Z}_p^2$. So we get Galois representations
$$\rho_{E,p} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_p) \subset \mathrm{GL}_2(\mathbb{Q}_p)$$
They are unramified outside pN_E where N_E is the conductor of E.

$\mathrm{GL}_2/\mathbb{Q}$

Automorphic side

- Assume $F = \mathbb{Q}$. In this general setting one studies certain representations of the $G(\mathbb{A})$, called automorphic representations. Certain cusp forms will give rise to such representations in the case of $G/F = \mathrm{GL}_2/\mathbb{Q}$.. All automorphic represenations are of the following form
$$\pi = \bigotimes_p \pi_p \otimes \pi_\infty,$$
where π_p is a represenation of $G(\mathbb{Q}_p)$ and π_∞ is a representation of the Lie algebra $\mathfrak{g}$ and of $K_\infty \subset G(\mathbb{R})$ a maximal compact subgroup.
- A lot of representation theoretic research is centered around questions adressing the interplay between these *local* representations π_p and the *global* ones π.
- If one starts with two groups $G.G'$ that are related in certain ways, e.g. if one embeds into the other like $\mathrm{GL}_1 \times \mathrm{GL}_2$ into GL_3, one can ask whether the automorphic representations are related. These questions have only been answered in specific cases. There is an extremely powerful analytic machine, the Arthur-Selberg Trace formula, that can be used to explore these relationships.

?
?
?

Galois side

- A good source for Galois representations is algebraic geometry, more precisely the étale cohomology of varieties (actually the example above involving elliptic curves belongs to this class of representations). A lot of reseach is concerned with classifying those Galois representation that come from geometry.
- For topological reasons the restriction of $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ to $G_{\mathbb{Q}_p}$ is much more interesting but also much more complicated than the restriction to $G_{\mathbb{Q}_l}$ for $l \neq p$. There is a lot of research trying to understand these local representations better. There is a huge amount of interesting unsolved questions waiting to be tackled.

G/F connected reductive linear algebraic group over a number field F, e.g. GL_n, SL_n, unitary groups, symplectic groups, orthogonal groups