An introduction to Langlands' reciprocity conjecture

Gaëtan Chenevier

CNRS, LMO

October 10th, 2019

Reciprocity laws

Fix Q a monic irreducible polynomial in $\mathbb{Z}[t]$.

For each prime p, we may reduce Q mod p and factor it into irreducible polynomials

$$Q \bmod p \;=\; Q_1^{e_1} \cdots Q_g^{e_g} \qquad \text{in } \mathbb{Z}/p\mathbb{Z}[t].$$

One of the most classical unsolved problems is alg. number theory is:

Problem: Understand the recipe $p \mapsto$ **shape** of Q mod p (e.g. defined as the collection of $\deg Q_i$ and e_i).

Historical examples : Euler and Gauss

$$Q = t^2 + 1 \ (Euler)$$

Q mod p has shape $Q_1^2 = (t+1)^2$ if $p = 2$,

$Q_1 Q_2 = (t-a)(t+a)$ with $a^2 \equiv -1 \bmod p$ if -1 is a square mod p,

Q_1 (irred.) otherwise.

Euler : -1 is a square mod p iff $p = 2$ or $p \equiv 1 \mod 4$.

$$Q = t^2 - q, \text{ for } q \text{ say an odd prime}$$

Answer given by Gauss's famous **quadratic reciprocity law** : q is a square mod odd p iff $(-1)^{(p-1)/2} p$ is a square mod q (a congruence mod $4q$).

QRL gives recipe more generally whenever $\deg Q = 2$.

Other (still classical) examples:

$$Q = t^3 - 2 \ \ (Gauss)$$

Q mod p has a single root in $\mathbb{Z}/p\mathbb{Z}$ iff $p \equiv 2 \bmod 3$,
shape $Q_1 Q_2 Q_3$ iff $p \equiv 1 \bmod 3$ and $p = a^2 + 27b^2$,
shape Q_1 iff $p \equiv 1 \bmod 3$ and is not of the form $a^2 + 27b^2$.

$$Q = t^3 - t^2 + t + 1 \ \ (Kronecker)$$

Q mod p has a single root in $\mathbb{Z}/p\mathbb{Z}$ iff $p \equiv 2, 6, 7, 8, 10 \bmod 11$,
shape $Q_1 Q_2 Q_3$ iff $p \equiv 1, 3, 4, 5, 9 \bmod 11$ and $p = a^2 + 11b^2$.

Remark: Interestingly, in both cases, no congruence on p allows to distinguish between the cases "split mod p" and "irreducible mod p".

Reciprocity laws

Answer's like this are called **reciprocity laws**. We find several examples of them in the works of Euler, Gauss, Jacobi, Eisenstein (sometimes more complicated)... for very specific polynomials Q.

(a very special case of) **Langlands' reciprocity conjecture:** *A reciprocity law should exist for each polynomial Q in a sense involving automorphic forms and Hecke operators.*

My main goal will be to try to state this conjecture more precisely. Before, I need to refine it and talk about more elementary structures that were discovered mainly by Galois, Frobenius and E. Artin.

The discriminant

Write $Q = \prod_i (t - x_i)$ in $\mathbb{C}[t]$, the discriminant of Q is

$$D = \prod_{i,j} (x_i - x_j)^2.$$

It is actually in $\mathbb{Z}$, and nonzero.

Fact : $p \nmid D$ iff Q mod p is multiplicity free (i.e $e_i = 1$ for each i).

For such a p, by the shape of Q mod p we just mean the collection of $\deg Q_i$. This is a partition of $\deg Q$.

Philosophy: (i) Primes dividing D always have an exceptional behaviour.

(ii) In degree ≤ 2 the reciprocity law only depends on p mod D as we saw. Although this seems wrong in general, this will be true in some sophisticated sense, as we shall see later.

(Note we have $D = -2^2 \cdot 3^3$ in case $t^3 - 2$ and $D = -44$ in case $t^3 - t^2 + t + 1$).

Galois groups

Let K be the subfield of $\mathbb{C}$ generated by the roots x_i of Q, so $K = \mathbb{Q}(x_1, ..., x_n)$ with $n = \deg Q$.

Any field automorphism of K permutes the roots x_i of Q hence defines a permutation of $\{1, \ldots, n\}$. Those automorphisms form a subgroup

$$\mathrm{Gal}(Q) \subset \mathfrak{S}_n$$

called the Galois group of P ("allowed permutations of the roots x_i preserving all the rational polynomial identities between the x_i").

In practice, very often $\mathrm{Gal}(Q) = \mathfrak{S}_n$, but not always. It may be any subgroup of $\mathfrak{S}_n$ acting transitively on $\{1, ..., n\}$.

Frobenius conjugacy classes 1

Frobenius : For each prime p not dividing D, there is a natural conjugacy class

$$\mathrm{Frob}_p \subset \mathrm{Gal}(Q)$$

whose cycle-decomposition in $\mathfrak{S}_n$, a partition of n, is the shape of Q mod p.

1. The possible shapes of Q mod p depend thus strongly on $\mathrm{Gal}(Q)$. We shall see after it is the only constraint.

2. Mod p analogue of $\mathrm{Frob}_\infty =$ conjugacy class of complex conjugation.

3. A slightly finer version of main problem is thus to understand the recipe $p \mapsto \mathrm{Frob}_p$.

Frobenius conjugacy classes 2

Dirichlet-Cebotarev : any conjugacy class C in $G = \mathrm{Gal}(Q)$ is Frob_p for infinitely many primes p, with probability $|C|/|G|$.

Altough beautiful, this result does not make the recipe precise, and does not count as a reciprocity law. It however allows to show the following:

Kronecker-Weber : The reciprocity law for Q is determined by congruences on p iff $\mathrm{Gal}(Q)$ is abelian. If so, it is determined by p mod D.

All other classical examples actually cases with solvable $\mathrm{Gal}(Q)$. Until Langlands' proposal : no example with non solvable $\mathrm{Gal}(Q)$.

Euclidean lattices

Let $V = \mathbb{R}^n$ be the standard Euclidean space of dimension $n \geq 1$.

A lattice in V is a discrete subgroup of finite covolume, i.e. of the form

$$\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n$$

where $e_1, ..., e_n$ is a suitable $\mathbb{R}$-basis of V. The standard lattice is $\mathbb{Z}^n$, generated by the canonical basis.

Definition: We denote by $\mathcal{L}_n$ the set of all lattices in V.

$\mathcal{L}_n$ as a homogenous space

The general linear group $\mathrm{GL}_n(\mathbb{R}) = \mathrm{GL}(V)$ acts on V, sending lattices to lattices. It acts transitively on $\mathcal{L}_n$.

The stabilizer of $\mathbb{Z}^n$ is the discrete subgroup $\mathrm{GL}_n(\mathbb{Z})$ of integral matrices with determinant ± 1, we have thus an identification

$$\mathcal{L}_n \xrightarrow{\sim} \mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}).$$

This allows us to see $\mathcal{L}_n$ as a smooth manifold (of dimension n^2) with a smooth transitive action of the Lie group $\mathrm{GL}_n(\mathbb{R})$.

The symmetric space

The compact orthogonal group $\mathrm{O}(n) = \mathrm{O}(V)$ acts on V, hence on $\mathcal{L}_n$ in a natural way. The stabilizer of any L in $\mathrm{O}(n)$ is a finite group (it is discrete and compact). The orbit space

$$\mathcal{X}_n = \mathrm{O}(n)\backslash\mathcal{L}_n$$

is a locally symmetric space ("isometry classes of lattices of rank n"). It helps understanding the geometry of $\mathcal{L}_n$.

Example: $n = 2$, the classical action of $\mathrm{SL}_2(\mathbb{R})$ on the (hyperbolic) upper-half plane $\mathbb{H} = \{\tau \in \mathbb{C},\ \mathrm{Im}\,\tau > 0\}$ is transitive and induces an isomorphism $\mathcal{X}_2 \simeq \mathbb{R}_{>0} \times \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$.

An important variant : level structures

Fix $D \geq 1$ and consider the set $\mathcal{L}_n(D)$ of pairs (L, e) where L is in $\mathcal{L}_n$ and $e : L/DL \simeq (\mathbb{Z}/D\mathbb{Z})^n$ is an additive isomorphism.

Then $\mathrm{GL}_n(\mathbb{R})$ acts on $\mathcal{L}_n(D)$ by $g.(L, e) = (g(L), e \circ g^{-1})$ and we have

$$\mathcal{L}_n(D) \simeq \coprod_{i \in (\mathbb{Z}/D\mathbb{Z})^\times/\{\pm 1\}} \mathrm{GL}_n(\mathbb{R})/\Gamma_n(D)$$

with $\Gamma_n(D) = \{\gamma \in \mathrm{GL}_n(\mathbb{Z}),\ \gamma \equiv 1 \bmod D\}$ (*principal congruence subgroup modulo* D).

Example: For $n = 1$ we have $\mathcal{L}_1(D) \simeq \mathbb{R}_{>0} \times (\mathbb{Z}/D\mathbb{Z})^\times$.

Automorphic forms for GL_n

An automorphic form of level $D \geq 1$ for GL_n is a smooth function $f : \mathcal{L}_n(D) \to \mathbb{C}$ such that :

(i) f generates a finite-dimensional representation of $\mathrm{O}(n)$ by left-translations,

(ii) f is an eigenvector for all the $\mathrm{GL}_n(\mathbb{R})$-invariant differential operators acting on $\mathrm{GL}_n(\mathbb{R})$,

(iii) f is of moderate growth.

I omit the discussion of moderate growth. (i) and (ii) say f is very symmetric w.r.t. $\mathrm{GL}_n(\mathbb{R})$.

Brief explanation of (ii)

Action by left-translations of $\mathrm{GL}_n(\mathbb{R})$ on $\mathcal{L}_n(D)$ defines an action of the universal enveloping algebra $\mathrm{U}(\mathfrak{gl}_n(\mathbb{R}))$ on $\mathcal{C}^\infty(\mathcal{L}_n(D))$: we ask that f is an eigenform of all elements in the center $\mathfrak{z}$ of $\mathrm{U}(\mathfrak{gl}_n(\mathbb{R}))$ (e.g. for the Casimir operator).

Structure of $\mathfrak{z}$ is actually known : it is a commutative polynomial algebra in n variables, so f essentially satisfies n independent differential equations.

Automorphic forms of level D form a vector space with a natural action of $\mathfrak{gl}_n(\mathbb{R})$ and of $\mathrm{O}(n)$ (Harish-Chandra module).

Definition: $\mathcal{A}(D, \rho, \lambda)$ is the space of level D automorphic forms generating ρ under the action of $\mathrm{O}(n)$ and with a certain character $\lambda : \mathfrak{z} \to \mathbb{C}$ under the action of $\mathfrak{z}$.

Harish-Chandra finiteness theorem

Harish-Chandra: For all n, D, ρ and λ, then $\mathcal{A}(D, \rho, \lambda)$ is a finite dimensional vector space.

1. Reminiscent to finite dimensionality of spaces of classical modular forms of fixed weight and level, of sections of holomorphic vector bundles on projectives complex varieties, etc... Analysis of elliptic PDE's here.

2. n and D being given, for all but very specific (and unknown a priori) pairs (ρ, λ) we have $\mathcal{A}(D, \rho, \lambda) = 0$. Subspace of cusp-form (not defined here) is especially interesting.

Examples:

(i) ($n = 2$) Classical elliptic modular or Mass forms, viewed as lattice functions, are automorphic forms.

(ii) ($n = 1$) all functions $(\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{C}$.

(iii) ($n > 2$) no other (nicer) description. Very hard to construct concrete examples (especially cuspforms), although we know there are many.

Hecke operators

The **Hecke operators** are natural correspondences on $\mathcal{L}_n$.

If $f : \mathcal{L}_n \to \mathbb{C}$ is any map, and if A is a finite abelian group, we define a map $\mathrm{T}_A(f) : \mathcal{L}_n \to \mathbb{C}$ by the formula

$$\mathrm{T}_A(f)(L) = \sum_{N \subset L \mid L/N \simeq A} f(N).$$

1. Most important one $\mathrm{T}_p := \mathrm{T}_{\mathbb{Z}/p\mathbb{Z}}$ for p a prime : corresponds to all index p lattices.

2. If $f : \mathcal{L}_n(D) \to \mathbb{C}$ and $|A|$ is prime to n, then $\mathrm{T}_A(f)$ still makes sense as a funtion on $\mathcal{L}_n(D)$ (restrict level structure to N).

General properties of Hecke operators

(i) Hecke operators commute : $\mathrm{T}_A \circ \mathrm{T}_B = \mathrm{T}_B \circ \mathrm{T}_A$,

(ii) $\mathrm{T}_A \circ \mathrm{T}_B$ is a (universal) integer linear combination of the T_C with $|C|$ dividing $|A||B|$; it is just $\mathrm{T}_{A\times B}$ if $|A|$ and $|B|$ are coprime,

(iii) The T_A with $|A|$ prime to D preserve each $\mathcal{A}(D, \rho, \lambda)$.

Leads to the notion of automorphic **eigenform** of level D : an automorphic form which is furthermore an eigenform for all T_A with $|A|$ prime to D. Those forms have a maximal number of symmetries.

Linear algebra shows that eigenforms exist as soon as $\mathcal{A}(D, \rho, \lambda)$ is nonzero. Actually, the subspace of *cuspforms* in $\mathcal{A}(D, \rho, \lambda)$ has a basis made of eigenforms.

Philosophy behind Hecke operators

1. Hecke operators such as T_p may be viewed as discrete Laplace operators, associated to each prime p, with a similar role as the elements of $\mathfrak{z}$ ("archimedean prime").

2. Define $\mathfrak{z}_p$ as the $\mathbb{C}$-algebra generated by all T_A with $|A|$ a power of p. Satake showed this is a polynomial ring in n variables, and Langlands observed that

$$\mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathfrak{z}_p, \mathbb{C})$$

is in can. bijection with the set of diagonalizable conjugacy classes in $\mathrm{GL}_n(\mathbb{C})$.

Langlands view : *Eigenvalues of Hecke operators on automorphic forms have to be thought as automorphic analogues of Frobenius elements.*

Example :

(i) $n = 1$, automorphic eigenforms are essentially the *Dirichlet characters* $(\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{C}^\times$.

(ii) For modular forms, this is Hecke theory. It actually goes back to Mordell, who showed using this $\tau(mn) = \tau(m)\tau(n)$ for $(m, n) = 1$, where

$$q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n.$$

The reciprocity conjecture

Let Q be an irreducible monic polynomial in $\mathbb{Z}[t]$ of discriminant D.

We want to understand the recipe $p \mapsto \mathrm{Frob}_p$ for p not dividing D.

By Fourier theory on $\mathrm{Gal}(Q)$, enough to understand the recipe

$$p \mapsto \mathrm{trace}\, \rho(\mathrm{Frob}_p)$$

for each irreducible representation $\rho : \mathrm{Gal}(Q) \to \mathrm{GL}_n(\mathbb{C})$.

Langlands reciprocity conjecture: For any Q as above, and any irreducible $\rho : \mathrm{Gal}(Q) \to \mathrm{GL}_n(\mathbb{C})$, there is a (cuspidal) automorphic form f of level D for GL_n which is an eigenform for the Hecke operators T_p for each p not dividing D, with eigenvalue $\mathrm{trace}\, \rho(\mathrm{Frob}_p)$.

Some examples

If $\mathrm{Gal}(Q)$ abelian, then ρ has dimension $n = 1$: recover Kronecker-Weber.

Assume $n = 2$ and complex conjugation acts non trivially in ρ, then existence of f is known by rather recent work of Khare and Wintenberger (2008), in the lead of results of Wiles and Taylor. In this case, f is a classical modular form of weight 1.

When $\mathrm{Gal}(Q) \simeq \mathfrak{S}_3 \subset \mathrm{GL}_2(\mathbb{C})$, get classical theta series and recover Gauss and Kronecker examples.

When $\mathrm{Gal}(Q) \simeq \widetilde{A_5} \subset \mathrm{GL}_2(\mathbb{C})$, a really new reciprocity law for Q.

Essentially no other general case known (including $n = 2$ and real complex conjugation).