CIMPA School at Makerere University
Galois representations and the LMFDB

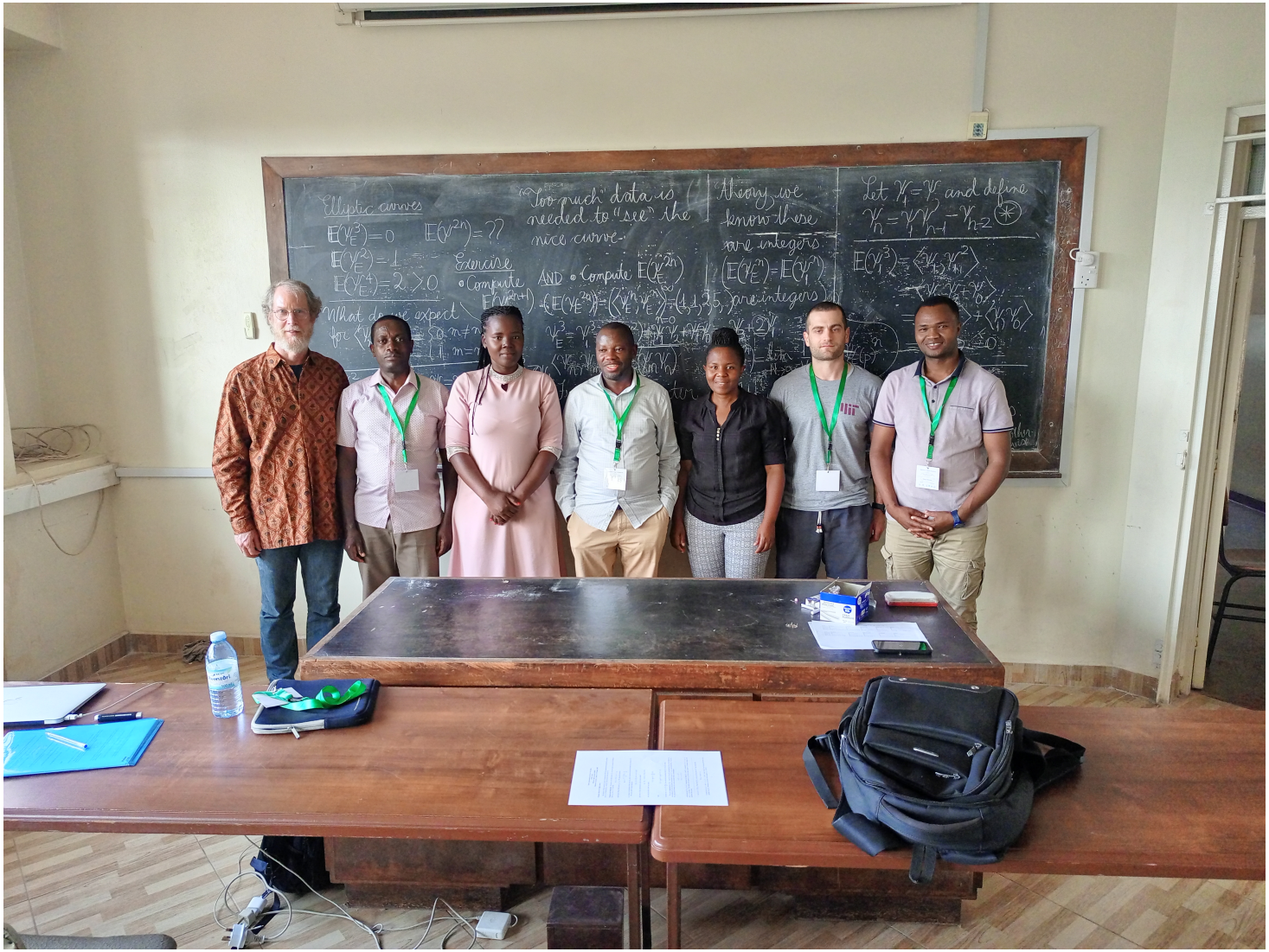
Galois representations and Sato-Tate

Research group members:
Flugence Bunani Gabiro, Philly Ivan Kimuli,
Annet Kyomuhangi, Patrick Masaba, Caroline Namanya

Research group leaders:
Leonardo Colò and David Kohel

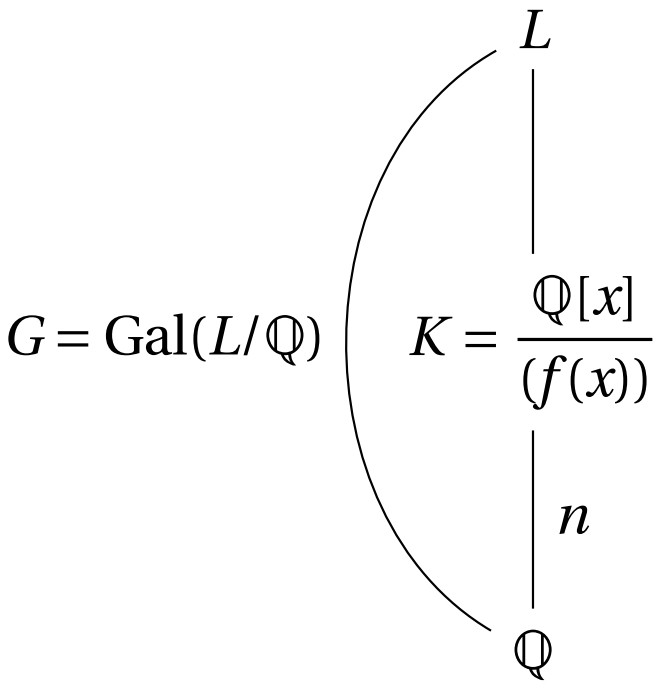
Makerere University
January 24, 2025

Group photo


Elliptic curves
"Too much" data is needed to "see" the nice curve.
Theory we know these are integers
Let $\gamma_1 = \gamma$ and define
Exercise
AND • Compute

Number fields

Let $K = \mathbb{Q}[x]/(f(x))$ be a number field defined by a polynomial $f(x) \in \mathbb{Z}[x]$, and L is the splitting field of $K/\mathbb{Q}$.



We are interested in studying the Galois groups of these fields, from the perspective of character theory of groups.

Character theory of number fields

Consider the number field defined by

$$f(x) = x^n + c_1 x^{n-1} + \cdots + c_0 \in \mathbb{Z}[x],$$

and suppose that $(p, \mathrm{disc}(f)) = 1$.

- The factorization type $f(x) \equiv f_1(x) \cdots f_r(x) \in \mathbb{F}_p[x]$, determines the cycle type $(d_1, \ldots, d_r) = (\deg(f_i))$ of the Frobenius lift in $\mathrm{Gal}(L/\mathbb{Q})$, up to conjugation.
- In the associated permutation representation $\rho\colon \mathrm{Gal}(L/\mathbb{Q}) \to S_n$, the Frobenius lift has characteristic polynomial

$$P(x) = (x^{d_1} - 1) \cdots (x^{d_r} - 1) = x^n - a_1 x^{n-1} + \cdots + (-1)^r = \sum_{i=0}^{n} (-1)^i a_i x^{n-i}$$

Let $V = \mathbb{R}^n$ whose canonical basis is identified with the roots of f, and define $V_0 = \mathbb{R}(1, 1, \ldots, 1)$.

- The representation decomposes into $V = V_0 \bigoplus V_0^{\perp}$, and the representation on $V_0^{\perp}$ is the *standard representation*.

- The characteristic polynomial of the Frobenius on $V_0^{\perp}$ is

$$Q(x) = \frac{P(x)}{x-1} \in \mathbb{Z}[x] = x^{n-1} - a_1 x^{n-2} + \cdots + (-1)^{n-1} a_{n-1}$$

  and $x-1$ on V_0.

- The coefficients $(a_0, a_1, \ldots, a_{n-1})$ are class invariants on the set $C(G) = \{C_0, \ldots, C_t\}$ of conjugacy classes in $G = C_0 \cup \cdots \cup C_t$.

- The coefficients are character values, that is,

$$(\chi_0(p), \ldots, \chi_{n-1}(p)) = (a_0, a_1, \ldots, a_{n-1}).$$

Example (Galois group S_3)

Let $f(x) = x^3 + 2x + 2$. We obtain the polynomials

$$Q(x) \in \{x^2 - 2x + 1, x^2 - 1, x^2 + x + 1\}$$

with corresponding vector sequences $\{(1,2,1),(1,0,-1),(1,-1,1)\}$.
Thus we obtain the character table:

	C_0	C_1	C_2
a_0	1	1	1
a_1	2	0	-1
a_2	1	-1	1

The conjugacy classes are $C_0 = C(1), C_1 = C((1\,2)), C_2 = C((1\,2\,3))$.

Remark

For S_n, all of these characters are irreducible, but the situation is much more complicated in general.

Characters and Expectation

- Let G be a finite group, then if χ, ψ are irreducible characters over $\mathbb{C}$,

$$\langle \chi, \psi \rangle = \begin{cases} 0 & \text{if } \chi \neq \psi, \\ 1 & \text{if } \chi = \psi \end{cases} \quad \text{where } \langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} (\chi \bar{\psi})(g)$$

- Let $G = \mathrm{Gal}(L/\mathbb{Q})$. We define the expectation of a character as an average over its values at the first N primes:

$$\mathbb{E}(\chi) = \lim_{N \to \infty} \frac{1}{N} \sum_{p \in \mathscr{P}_N} \chi(p),$$

where $\chi(p)$ is the character value at the Frobenius lift. This allows us to compute the inner product as the expectation

$$\langle \chi, \psi \rangle = \mathbb{E}(\chi \bar{\psi}).$$

For S_3, using primes $\leq 2^{12}$, an explicit computation in Sage, with respect to the characters $(1, \psi, \chi)$, such that

$$(1(p), \psi(p), \chi(p)) = (a_0, a_1, a_2),$$

gives the inner product matrix

```
[ 1.00000000   -0.0285204991 -0.0231729055]
[-0.0285204991  0.948306595  -0.0285204991]
[-0.0231729055 -0.0285204991  1.00000000  ]
```

This gives a good approximation of the identity matrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

This confirms that the characters $1, \psi, \chi$ are irreducible and distinct.

Example (Galois group D_4)

Let $f(x) = x^4 + x^3 - 2x - 1$. We obtain the polynomials

$$Q(x) \in \{x^3 - 3x^2 + 3x - 1, x^3 + x^2 - x - 1, x^3 - x^2 - x + 1, x^3 + x^2 + x + 1\}$$

with corresponding vector sequences

$$\{(1,3,3,1),(1,-1,-1,1),(1,1,-1,-1),(1,-1,1,-1)\}$$

Thus we obtain the character table:

	C_0	C_1	C_2	C_4
a_0	1	1	1	1
a_1	3	-1	1	-1
a_2	3	-1	-1	1
a_3	1	1	-1	-1

where $C_0 = C(1), C_1 = C((1\,2)), C_2 = C((1\,2)(3\,4)), C_4 = C((1\,2\,3\,4))$.

For D_4, using primes $\leq 2^{12}$, an explicit computation in Sage, with respect to the characters $(\chi_0, \chi_1, \chi_2, \chi_3)$, gives the inner product matrix

```
[    1.00000000 -0.0284697509 -0.0533807829 -0.0213523132]
[-0.0284697509     1.89679715    0.875444840 -0.0533807829]
[-0.0533807829    0.875444840     1.89679715 -0.0284697509]
[-0.0213523132 -0.0533807829 -0.0284697509     1.00000000]
```

This approximates

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

From the inner product matrix, we can conclude:

- χ_0 and χ_3 are irreducible and distinct
- χ_1 and χ_2 are reducible, and moreover

$$\chi_1 = \psi + \xi_1 \quad \text{and} \quad \chi_2 = \psi + \xi_2$$

for irreducible characters ψ, ξ_1 and ξ_2.

Question: How do we find ψ, ξ_1 and ξ_2?

The End

Thank you for your attention!