Galois representations and Sato–Tate groups
CIMPA School
Effective Algebra and the LMFDB
Makerere University, Uganda, 13–24 January 2025

Character theory for number fields.

Notation and background. Let $K/\mathbb{Q}$ be a number field, and $\mathrm{Gal}(K/\mathbb{Q})$ the Galois group of its normal closure. A representation will be most often be denoted by ρ:

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(F),$$

where F is the base field of the representation, or by χ when linear ($n = 1$). A character on a Galois group, the trace of a representation, will be typically denoted by Greek letters χ, ψ, ξ, where χ is most often a linear representation (thus both a representation and a character).

Quadratic fields.

Let $\chi_n : \mathbb{Z} \to \{\pm 1\}$ be the quadratic character associated to the Galois extension $K/\mathbb{Q} = \mathbb{Q}(\sqrt{n})/\mathbb{Q}$. For squarefree n, the character χ_n is defined on primes by

$$\chi_n(p) = \begin{cases} 1 & p \text{ is split in } K, \\ -1 & p \text{ is inert in } K, \\ 0 & p \mid n \text{ or } p = 2 \text{ and } n \neq 3 \bmod 4 \end{cases}$$

Let $\mathscr{P}_N$ denote of the set consisting of the first N primes. The Chebotarev density theorem gives the following *orthogonality relations* for (quadratic) characters:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{p \in \mathscr{P}_N} \chi_m(p)\chi_n(p) = \begin{cases} 1 & \text{if } mn \in (\mathbb{Q}^*)^2, \\ 0 & \text{otherwise.} \end{cases}$$

1. Justify the orthogonality relations, describe a computational model to test the relations, and verify their consistency in Sage.

Cubic fields.

Cyclic cubics. A cubic extension $K/\mathbb{Q}$ can be Galois (cylic of order 3) or non-Galois whose Galois closure is an S_3-extension. A universal cubic polynomial with cyclic Galois group is given by:

$$x^3 - sx^2 - (s+3)x - 1$$

for $s \in \mathbb{Q}$, of discriminant $(s^2+3s+9)^2$. Such a cubic is called a Morton cubic. The roots α_0, α_1, α_2, permuted by the transformation

$$\sigma(\alpha_i) = \frac{-1}{(\alpha_i + 1)} = \alpha_{i+1}.$$

2. Verify that Galois group is generated by the above transformation, and show that the Galois group induces a 2-dimensional representation ρ on the subspace of trace zero elements (generated by $\alpha_i - \alpha_j$).

3. Show that the character group on $G = \mathrm{Gal}(K/\mathbb{Q})$ is generated by a character $\chi : G \to \mathbb{Q}(\zeta_3)$ such that $\chi(\sigma) = \zeta_3$, and that the trace of χ is the character $\psi = \chi + \overline{\chi}$, in particuler:

$$\psi(\sigma) = \psi(\sigma^{-1}) = -1, \text{ and } \psi(1) = 2.$$

4. Denote by $\psi(p)$ the value of the Frobenius automorphism. Show that this character value is determined, for all p not dividing the discriminant of f, by the character values:

$$\psi(p) = \begin{cases} 2 & \text{if } f(x) \equiv (x-a_1)(x-a_2)(x-a_3) \bmod p, \\ -1 & \text{if } f(x) \text{ is inert mod } p. \end{cases}$$

5. Suggest a method to define the character values $\chi(p)$ for primes p. In particular, how does one differentiate the inert primes p such that $\chi(p)=\zeta_3$ from the inert primes q such that $\chi(q)=\zeta_3^2$?

Generic cubics. A universal cubic polynomial with Galois group S_3 is $f(x)=x^3+sx+s\in\mathbb{Q}[x]$, with discriminant $-(4s+27)s^2$; in particular, the normal closure contains the extension $F=\mathbb{Q}(\sqrt{4s+27})$ whose Galois group is the quotient group $S_3/A_3\cong\{\pm1\}$. Denote the quadratic character on F by ξ and let ψ be the degree-2 character associated to the standard representation of $K=\mathbb{Q}[x]/(f(x))$.

6. Develop explicit formulas for the characters values of ψ at primes p, in terms of the factorization of $f(x)$ mod p, and for the

7. Show that the virtual character ring for $S_3\cong\mathrm{Gal}(K/\mathbb{Q})$ is $\mathbb{Z}[\xi,\psi]$ and deduce relations for the characters.

The permutation representation and the standard representation of a number field

Suppose that $K=\mathbb{Q}[x]/(f(x))$ of degree n, and let p be a prime, coprime to $\mathrm{disc}(f)$, and let $L\subset\overline{\mathbb{Q}}$ be a splitting field of K. Then $\mathscr{O}_K/p\mathscr{O}_K$ is isomorphic to a product of fields:

$$\mathscr{O}_K/p\mathscr{O}_K\cong\mathbb{F}_{p^{d_1}}\times\cdots\times\mathbb{F}_{p^{d_t}},$$

where $n=d_1+\cdots+d_t$. This corresponds to a factorization

$$\bar{f}=g_1\cdots g_t\in\mathbb{F}_p[x]\text{ where }d_i=\deg(g_i).$$

Equivalently the Frobenius automorphism

$$\begin{array}{ccc}\mathscr{O}_K/p\mathscr{O}_K & \xrightarrow{\ \phi\ } & \mathscr{O}_K/p\mathscr{O}_K\\ \alpha & \longmapsto & \alpha^p\end{array}$$

lifts to a permutation of the roots $\alpha_1,\ldots,\alpha_n\in L$ with cycle structure $(d_1,\ldots,d_t)$. The characteristic polynomial of ϕ is then

$$P(x)=(x^{d_1}-1)\cdots(x^{d_t}-1)=x^n-a_1x^{n-1}+\cdots+(-1)^t=\sum_{i=0}^{n}(-1)^ia_ix^{n-i},$$

referred to as *permutation representation* of $G=\mathrm{Gal}(L/\mathbb{Q})=\mathrm{Gal}(K/\mathbb{Q})$. In particular the character (= trace) of this representation is the number $a_1=N_f(p)$ of roots of $\bar{f}\in\mathbb{F}_p[x]$ in $\mathbb{F}_p$.

8. Let e_d be the number of irreducible divisors of degree d of $\bar{f}\in\mathbb{F}_p[x]$: $e_d=|\{d_i:1\le i\le n,d_i=d\}|$. Express the numbers $N_f(p^r)$ of roots of $\bar{f}$ over $\mathbb{F}_{p^r}$ in terms of the numbers $(e_1,\ldots,e_n)$.

This permutation representation is the induced action on $V=L\otimes_{\mathbb{Q}}K\cong L^n$, in the canonical base for L^n. To make the isomorphism $V\cong L^n$ explicit, we note that the canonical isomorphism:

$$L\otimes_{\mathbb{Q}}K=L\otimes_{\mathbb{Q}}\frac{\mathbb{Q}[x]}{(f(x))}\cong\frac{L[x]}{(f(x))}$$

follow from the definitions of K and of the tensor product. Next, the evaluation map

$$\begin{array}{ccc}\dfrac{L[x]}{(f(x))} & \longrightarrow & L\times\cdots\times L\\ g(x) & \longmapsto & (g(\alpha_1),\ldots,g(\alpha_n))\end{array}$$

is an isomorphism by the Chinese remainder theorem, and its inverse is given by Lagrange interpolation

$$(\gamma_1,\ldots,\gamma_n)\longmapsto\sum_{i=1}^{n}\gamma_ie_i\text{ where }e_i=\prod_{j\neq i}\frac{(x-\alpha_j)}{(\alpha_i-\alpha_j)}.$$

Clearly G acts by permutation on $(e_1,\ldots,e_n)$, and e_i maps to the i-th canonical basis element for L^n under the evaluation map.

9. Justify the assertions regarding the images of the e_i, the form of the inverse to the evaluation map, and show that $e_i \in L \otimes_{\mathbb{Q}} K$ are primitive idempotents:

$$\begin{aligned} &e_1 + \cdots + e_n = 1, \\ &e_i^2 = e_i \text{ for all } 1 \leq i \leq n, \\ &e_i e_j = e_j e_i = 0 \text{ for } 1 \leq i < j \leq n, \end{aligned}$$

and any idempotent is a sum of a subset of $\{e_1, \ldots, e_n\}$.

We now observe that the vector $e = e_1 + \cdots + e_n \in V$ is fixed by the permutation action, and its orthogonal complement V_0, generated by the differences $e_i - e_j$, is stablized by G. The G-module decomposition $Le + V_0$, shows that the permutation character decomposes as $1 + \psi$, where 1 is the constant linear character. We call ψ the *standard representation* of $G \subset S_n$, which is irreducible for $G = S_n$. The restriction of a Frobenius lift to V_0 has characteristic polynomial

$$P_0(x) = \frac{P(x)}{(x-1)} = \sum_{i=0}^{n-1} (-1)^i c_i x^{n-i-1}.$$

The coefficients $(c_1, \ldots, c_{n-1})$ are class invariants of the conjugacy class of Frobenius. More specifically they are values of characters at Frobenius, on the exterior module $\bigwedge^i(V_0)$, giving $|c_i| \leq \binom{n-1}{i}$, with equality for all i if and only if the conjugacy class of Frobenius is the identity class.

10. Determine the characteristic polynomial $P_0(x)$ for each conjugacy class in S_3 and S_4.

Characters and expectation.

Identifying the set $\mathscr{P}$ of primes with their associated Frobenius conjugacy classes in G, we obtain by restriction a map $\psi : \mathscr{P} \longrightarrow \mathbb{Z}$ such that $\psi(p) = N_f(p) - 1$. This perspective permits us to analyze arbitrary characters in the virtual character ring $\mathfrak{R}(G)$ — whose additive structure is defined to be the free abelian group on the irreducible characters of G — in terms of values at the discrete set of primes.

The Chebotarev density theorem asserts that the Frobenius classes in a Galois group G are equistributed among the conjugacy classes, with probability distribution $|C|/|G|$ for the class $C \subset G$. A given character ψ determines a sequence $(\psi(p))$ indexed by $\mathscr{P}$, equidistributed with respect to this probability. This lets us define the expectation of the character in terms of this sequence:

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

where $\mathscr{P}_N$ is the initial segment of N primes. An inner product on complex-valued characters can be defined in terms of this expectation:

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

The principle characters we will study are real-valued for which $\overline{\chi} = \chi$. The Schur orthogonality relations assert that for ψ and χ irreducible:

$$\langle \psi, \chi \rangle = \begin{cases} 1 & \text{if } \psi = \chi \\ 0 & \text{otherwise.} \end{cases}$$

11. For each of the polynomials $f(x)$, let $K = \mathbb{Q}[x]/(f(x))$. Determine a set of real irreducible characters on the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ and identify the Galois group from the statistics of its character values.

- $f(x) = x^4 + x^3 + x^2 + x + 1$,
- $f(x) = x^4 + x^3 - 2x - 1$,
- $f(x) = x^4 - x^3 - 3x + 4$
- $f(x) = x^4 - x + 1$

Let $f(x)$ be a monic irreducible polynomial of degree n. Let $\psi(p) = N_f(p) - 1$ be the character of the standard representation, for p coprime to $\mathrm{disc}(f)$. Observe that

$$\psi(p) \in \{-1, \ldots, n-3\} \cup \{n-1\}.$$

12. Define polynomials $\delta_s(x) \in \mathbb{Q}[x]$, for $s \in \mathrm{Im}(\psi)$, such that $\delta_s(t) = 1$ for $t = s$ and otherwise $\delta_s(t) = 0$.

13. Determine the polynomials $\delta_s(x)$ for $n = 3$ and $n = 4$, assuming $\mathrm{Im}(\psi) = \{-1, \ldots, n-3\} \cup \{n-1\}$. What is $\mathrm{Im}(\psi)$ for $G = C_n$, and what is the form of the resulting $\delta_s(x)$?

14. Define $C_s(\psi) = \{\sigma \in G : \psi(\sigma) = s\}$. Observe that $C_s(\psi)$ is a union of conjugacy classes of G, and prove that the expectation of the composition $\delta_s \circ \psi$ is the density of the class $C_s(\psi)$ in G:

$$\mathbb{E}(\delta_s \circ \psi) = \lim_{N\to\infty} \frac{1}{N} \sum_{p \in \mathscr{P}_N} \delta_s(\psi(p)) = \frac{|C_s(\psi)|}{|G|}.$$

15. While one character may be insufficient to separate conjugacy classes in G, one can use multiple characters ψ, χ to construct intersections,

$$C = C_s(\psi) \cap C_t(\chi) = \{\sigma \in G : \psi(\sigma) = s \text{ and } \chi(\sigma) = t\}.$$

Show that the density of C is the expectation of the product $\mathbb{E}\big((\delta_s \circ \psi)(\delta_t \circ \chi)\big) = \dfrac{|C|}{|G|}$.

N.B. The interpolation polynomials δ_s and δ_t can be defined independently with respect to $\mathrm{Im}(\psi)$ and $\mathrm{Im}(\chi)$, or (with higher degree polynomials) with respect to their union.

Remark. The above examples are finite groups, of rank 0, in which the character ring is spanned by finitely many characters. Next, we consider elliptic curves, which give rise to groups of rank 1. In particular, the Sato–Tate group is $\mathrm{SU}(2)$ if non CM or $\mathrm{O}(2)$ (containing $\mathrm{SO}(2)$ of index 2). Both $\mathrm{SU}(2)$ and $\mathrm{SO}(2)$ are compact connected Lie groups of rank 1, whose virtual character rings are isomorphic to $\mathbb{Z}[x]$.