Computing groups of Hecke characters

Aurel Page
joint work with Pascal Molin

08/08/2022
ANTS XV, Bristol

Inria / IMB Bordeaux

Plan

Hecke characters

Finite order: ray class group characters

F number field with ring of integers $\mathbb{Z}_F$.

Ray class groups of modulus $\mathfrak{M} \subset \mathbb{Z}_F$:

$$\mathrm{Cl}_F(\mathfrak{M}) = \frac{\{\text{ideals coprime to } \mathfrak{M}\}}{\{(\alpha) \text{ with } \alpha = 1 \bmod \mathfrak{M}\}}.$$

Finite order Hecke characters:

$$\chi \colon \mathrm{Cl}_F(\mathfrak{M}) \to \mathbb{C}^\times.$$

- Smallest modulus: **conductor** of χ;
- **evaluations** $\chi(\mathfrak{a}) \in \mathbb{C}^\times$ for $\mathfrak{a}$ coprime to $\mathfrak{M}$;
- **restriction** through the map $(\mathbb{Z}_F/\mathfrak{M})^\times \to \mathrm{Cl}_F(\mathfrak{M})$;
- correspond to finite order **Galois characters** $\mathrm{Gal}(L/F) \to \mathbb{C}^\times$ (class field theory).

Algebraic Hecke characters

Algebraic Hecke characters χ have

- a **conductor** $\mathfrak{M}$,
- an **infinity type** (an integer for each complex embedding of F);
- **evaluations** $\chi(\mathfrak{a}) \in \overline{\mathbb{Q}}^\times$ for $\mathfrak{a}$ coprime to $\mathfrak{M}$;
- a **restriction** $(\mathbb{Z}_F/\mathfrak{M})^\times \to \mathbb{C}^\times$;
- attached **Galois characters** $\mathrm{Gal}(\overline{F}/F) \to \overline{\mathbb{Q}_p}^\times$.

General Hecke characters

Group of idèles $\mathbb{A}_F^\times = \prod'_v F_v^\times$ (v place, also denoted $\mathfrak{p}$ or σ).

A **Hecke quasi-character** is a multiplicative and continuous map

$$\chi \colon \mathbb{A}_F^\times / F^\times \to \mathbb{C}^\times.$$

A **Hecke character** is a Hecke quasi-character χ such that $|\chi(a)| = 1$ for all $a \in \mathbb{A}_F^\times$.

Example: the **norm** $\|\cdot\|$ defined by

$$\|a\| = \prod_v |a_v|_v \in \mathbb{R}_{>0}.$$

is a Hecke quasi-character (product formula) but not a Hecke character.

Basic decompositions

Hecke quasi-character χ: **unique decomposition**

$$\chi = \chi_0 \| \cdot \|^s$$

with χ_0 Hecke character trivial on diagonal $\mathbb{R}_{>0} \subset \prod_\sigma F_\sigma^\times$ (σ complex embedding) and $s \in \mathbb{C}$.

The quasi-character χ is a character if and only if $s \in i\mathbb{R}$.

Characters of $\mathbb{A}_F^\times/(F^\times \cdot \mathbb{R}_{>0})$ form a **discrete group.**

Modulus and conductor

A Hecke quasi-character has **modulus** $\mathfrak{M}$ if it is trivial on

$$U(\mathfrak{M}) = \prod_{\mathfrak{p}|\mathfrak{M}} (1 + \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{M})}) \times \prod_{\mathfrak{p}\nmid\mathfrak{M}} \mathbb{Z}_\mathfrak{p}^\times .$$

Every Hecke quasi-character has a modulus.

Smallest modulus: **conductor** of the quasi-character.

Characters of $C^1_\mathfrak{M} = \mathbb{A}_F^\times/(F^\times \cdot \mathbb{R}_{>0} \cdot U(\mathfrak{M}))$ form a **finitely generated abelian group.**

Local components

Recall $\mathbb{A}_F^\times = \prod'_v F_v^\times$.

A Hecke character χ has **local components** $\chi_v \colon F_v^\times \to \mathbb{C}^\times$. In particular:

- **infinity type** for real and complex embeddings σ:

$$\chi_\sigma(z) = \left(\frac{z}{|z|}\right)^{k_\sigma} |z|_\sigma^{i\varphi_\sigma} \text{ for } k_\sigma \in \mathbb{Z} \text{ and } \varphi_\sigma \in \mathbb{R};$$

- **evaluations** $\chi(\mathfrak{p}) = \chi_\mathfrak{p}(\pi_\mathfrak{p})$ for $\mathfrak{p} \nmid \mathfrak{M}$ ($\pi_\mathfrak{p} \in \mathbb{Z}_\mathfrak{p}$ uniformiser);
- **restrictions** $(\mathbb{Z}_\mathfrak{p}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{M})})^\times \to \mathbb{C}^\times$ of $\chi_\mathfrak{p}$.

L-function

Let $\chi \colon \mathbb{A}_F^\times/(F^\times \cdot \mathbb{R}_{>0}) \to \mathbb{C}^\times$ be a Hecke character.

The **completed L-function**

$$\Lambda(\chi, s) = \gamma(\chi, s)L(\chi, s), \text{ where } L(\chi, s) = \prod_{\mathfrak{p} \nmid \mathfrak{M}} (1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}$$

and $\gamma(\chi, s)$ depends only on the conductor and infinity type, satisfies

$$\Lambda(\chi, 1 - s) = w \cdot \Lambda(\bar{\chi}, s)$$

for some $w \in \mathbb{C}^\times$.

Algorithms

Explicit description and dual logarithm maps

Theorem (Molin–P.)

There exists integers $\ell, n \geq 0$*, a full rank lattice* $\Lambda \subset \mathbb{Z}^\ell \times \mathbb{R}^n$*, and isomorphisms*

$$\mathcal{L}\colon C^1_{\mathfrak{M}} \xrightarrow{\sim} (\mathbb{Z}^\ell \times \mathbb{R}^n)/\Lambda \text{ and } \mathcal{L}^*\colon \operatorname{Hom}(C^1_{\mathfrak{M}}, \mathbb{C}^\times) \xrightarrow{\sim} \Lambda^\vee/\mathbb{Z}^\ell,$$

where $\Lambda^\vee = \{x \in \mathbb{Z}^\ell \times \mathbb{R}^n \mid \langle x, \lambda\rangle \in \mathbb{Z} \text{ for all } \lambda \in \Lambda\}$*, such that* $\chi(x) = \exp(2\pi i \langle \mathcal{L}^*(\chi), \mathcal{L}(x)\rangle)$ *for all* $x \in \mathbb{A}_F^\times$*, and*

- *a basis of the lattice* Λ*, and*
- *evaluations of* $\mathcal{L}$

are computable at given precision in polynomial time from $\mathbb{Z}_F^\times$ *and discrete logarithms in* Cl_F *and* $(\mathbb{Z}_F/\mathfrak{M})^\times$*.*

Algebraic characters and CM fields

A Hecke quasi-character is **algebraic** if its **infinity type** on the connected component of every real or complex completion is of the form

$$z \mapsto z^p \bar{z}^q \text{ with } p, q \in \mathbb{Z}.$$

A **CM field** is a purely imaginary quadratic extension of a totally real number field.

Either F does not contain a CM subfield, or it contains a **maximal CM subfield** F^{CM}.

The group of algebraic Hecke quasi-characters can be simply determined from knowledge of F^{CM} (Artin–Weil).

Computing the maximal CM subfield

For $\varepsilon \in \{\pm\}$, let

$$F^{\varepsilon} = \{x \in F \mid \sigma(x) = \varepsilon\bar{\sigma}(x) \text{ for all } \sigma \in \mathrm{Hom}(F, \mathbb{C})\}.$$

Proposition

F admits a CM subfield iff $F^{-} \neq 0$, and $F^{CM} = \mathbb{Q}(F^{-})$.

Theorem (Molin–P.)

There is a polynomial time algorithm that, given F, determines whether F has a CM subfield and computes F^{CM}.

Examples

Pari/GP implementation

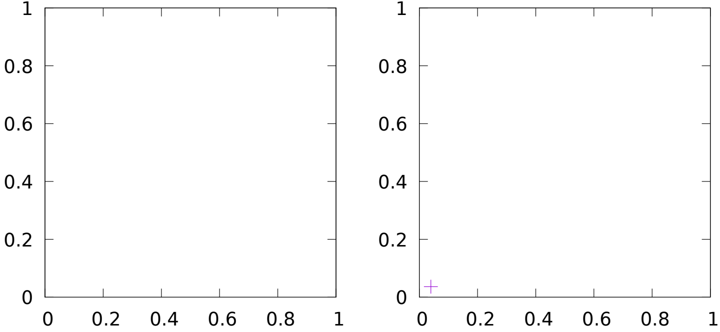
Our implementation is available on the **master branch** of Pari/GP and will be included in the **next release**.

```
? bnf = bnfinit(x^3+4*x-1,1);
? gc = gcharinit(bnf,1);
? gc.cyc
% = [2, 0, 0, 0.E-57] \\ Z/2 * Z * Z * C
? chi = [0,1,0,0]~;
? gcharlocal(gc,chi,2)
% = [2, 0.718193] \\ z -> (z/|z|)^2 * |z|^{2*0.718193*i}
? pr = idealprimedec(bnf,2)[1];
? chareval(gc,chi,pr)
% = -0.458755 \\ chi(pr) = exp(2*pi*i*(-0.458755))
? lfun([gc,chi],2)
% = 0.874082 - 0.029990*I
```

Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

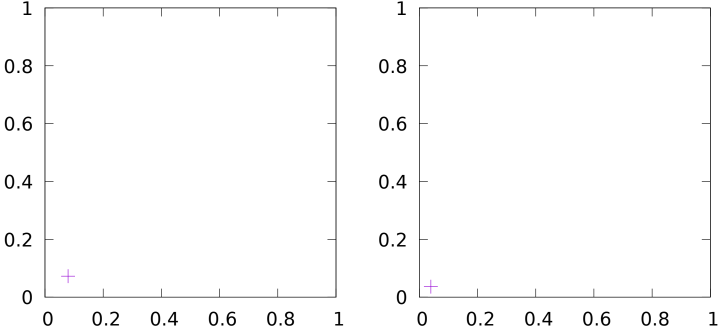
Values $\arg \chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C_{\mathfrak{m}}^1$.

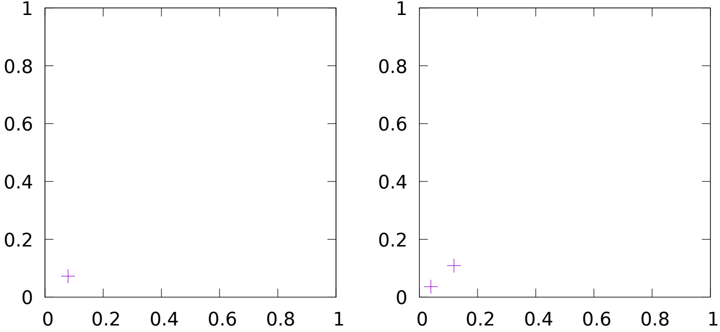
Values $\arg\chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

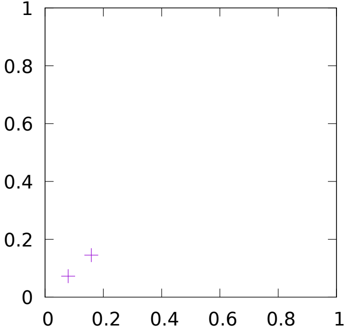
Values $\arg \chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:

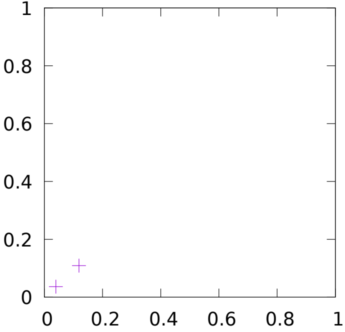


Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

Values $\arg\chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:

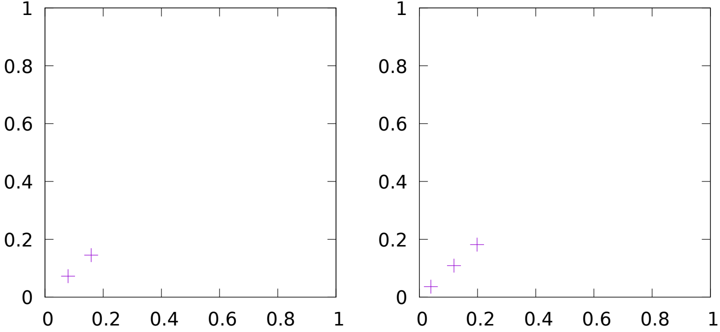




Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

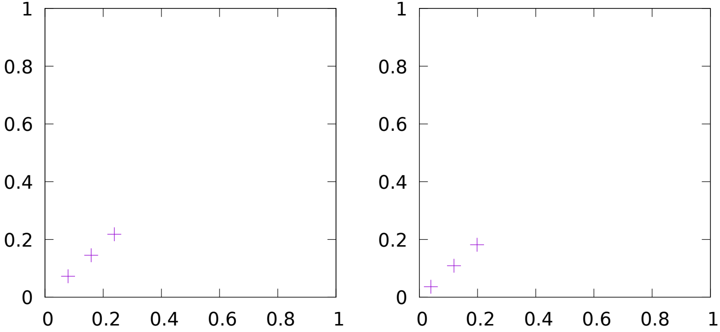
Values $\arg\chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

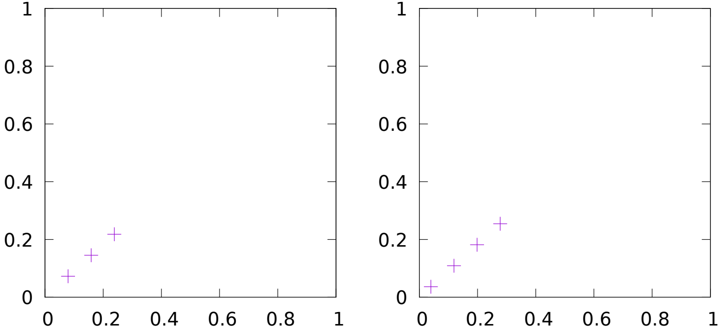
Values $\arg \chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

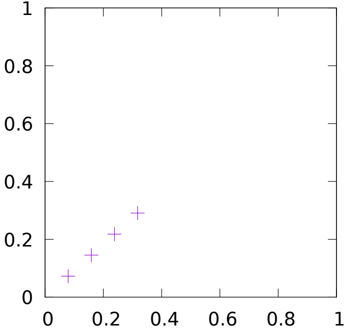
Values $\arg \chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:

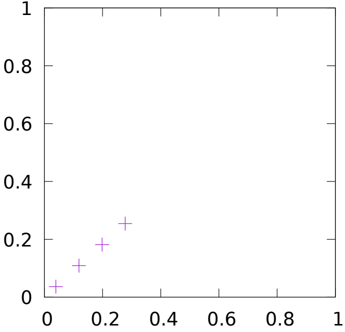


Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

Values $\arg \chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:

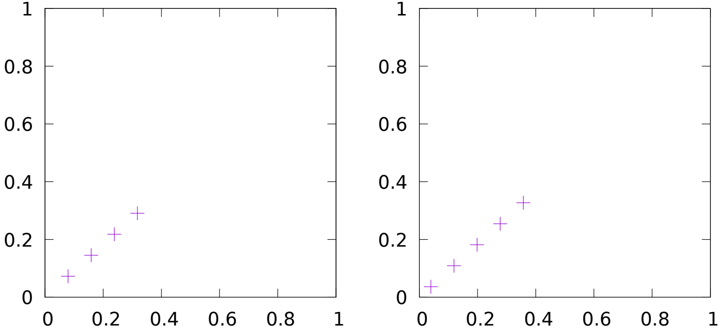




Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

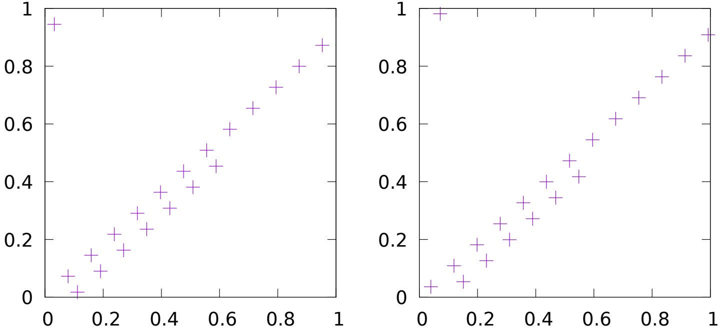
Values $\arg\chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

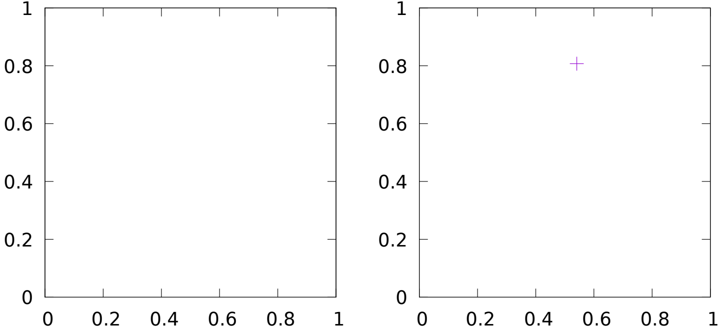
Values $\arg\chi(\mathfrak{p}^k)/2\pi$ for $k \geq 1$:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

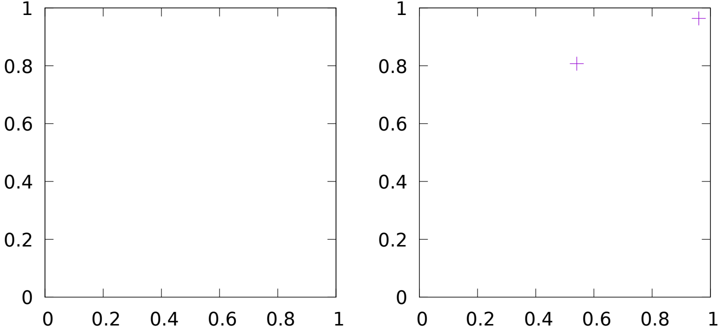
Values $\arg \chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

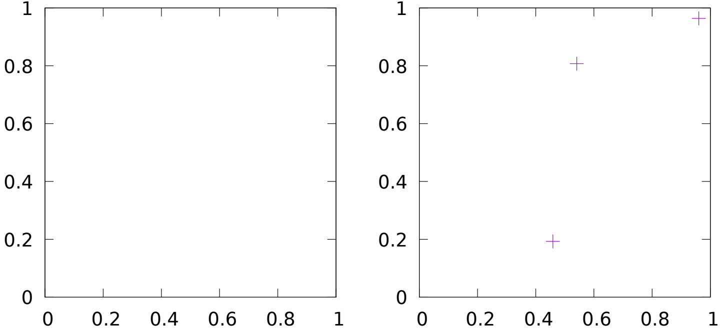
Values $\arg\chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

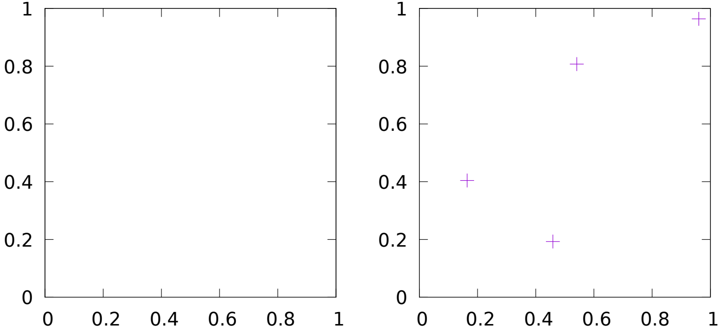
Values $\arg\chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

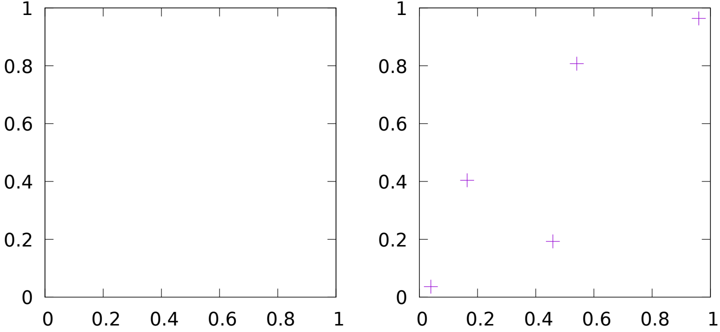
Values $\arg\chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

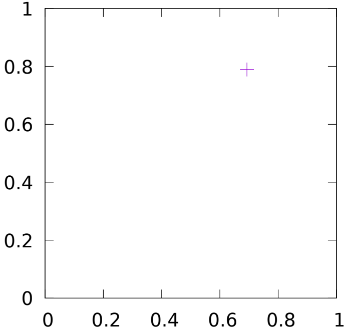
Values $\arg \chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:

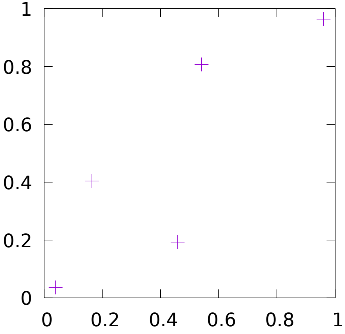


Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

Values $\arg \chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:

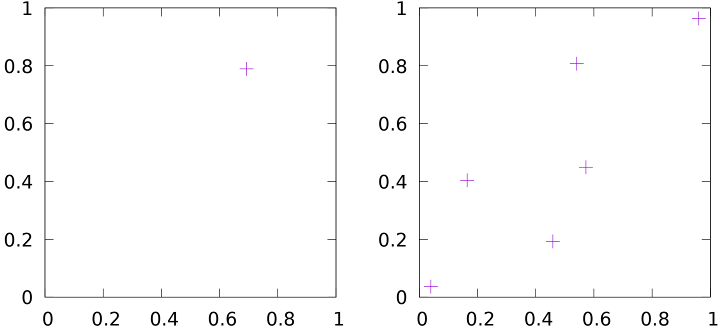




Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

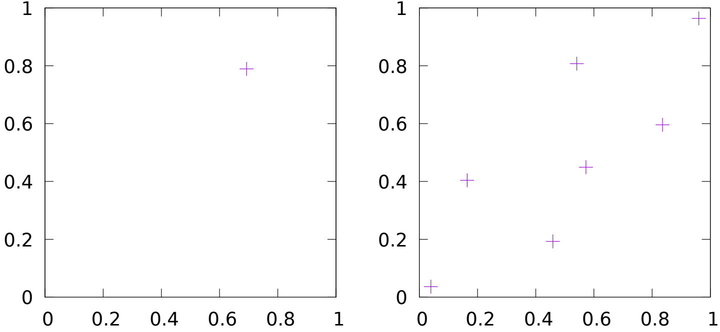
Values $\arg\chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:



Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

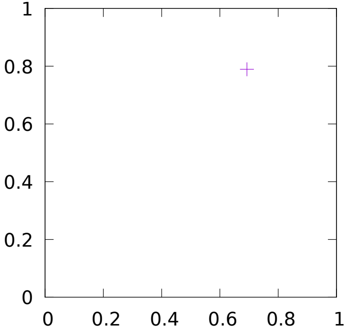
Values $\arg \chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:

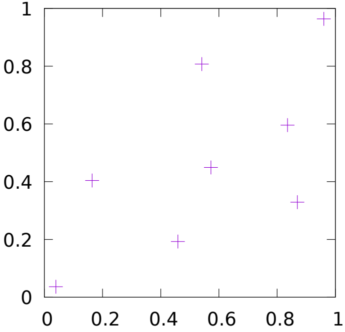


Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

Values $\arg\chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:

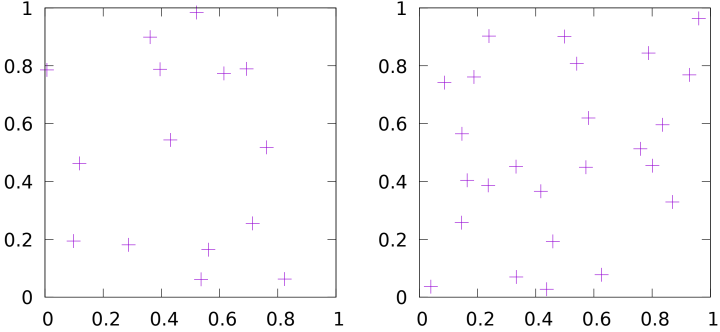




Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{M}}$.

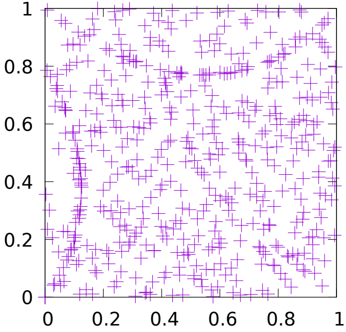
Values $\arg \chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:

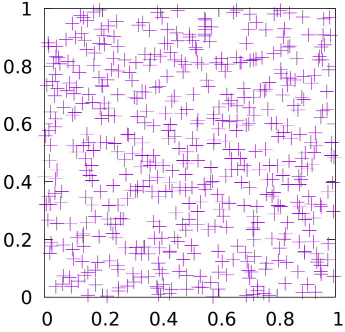


Coordinates on idèle class groups

A basis of the group of Hecke characters provides coordinates on the idèle class group $C^1_{\mathfrak{m}}$.

Values $\arg \chi(\mathfrak{q})/2\pi$ for primes $\mathfrak{q}$ sorted by norm:





CM varieties

Let A be the Jacobian of the genus 3 curve `3.9-1.0.3-9-9.6`

$$C : y^3 = x(x^3 - 1).$$

Let $K = \mathbb{Q}(\zeta_9)$, so that A has CM by K.

Shimura: there exists an algebraic Hecke character χ of K such that

$$L(A, s) = L(\chi, s).$$

- **Infinity type** and **conductor** bound: finite number of candidates.
- **Coefficients** of L-function: elimination of all but one candidate.
- **Question**: efficient elimination if many candidates?

CM varieties

prime $\mathfrak{p}$	$\chi(\mathfrak{p}) \in \mathbb{C}$	$\chi(\mathfrak{p}) \in K$
3.1	$\langle\exp(\frac{i\pi}{9})\rangle 1.7320\ldots i$	$\langle-\zeta_9\rangle\sqrt{-3} = \langle-\zeta_9\rangle(1+2\zeta_9^3)$
19.1	$4.3400\ldots+0.4052\ldots i$	$2\zeta_9^5+2\zeta_9^4+2\zeta_9^3+\zeta_9^2-2\zeta_9+2$
19.2	$-4.1172\ldots+1.4312\ldots i$	$-\zeta_9^5+2\zeta_9^4+2\zeta_9^3-2\zeta_9^2+4\zeta_9+2$
19.3	$4.3400\ldots-0.4052\ldots i$	$4\zeta_9^5+\zeta_9^4-2\zeta_9^3+2\zeta_9^2-\zeta_9$
19.4	$-4.1172\ldots-1.4312\ldots i$	$-2\zeta_9^5+\zeta_9^4-2\zeta_9^3-4\zeta_9^2+2\zeta_9$
19.5	$2.7771\ldots+3.3596\ldots i$	$-\zeta_9^5-4\zeta_9^4+2\zeta_9^3+\zeta_9^2-2\zeta_9+2$
19.6	$2.7771\ldots-3.3596\ldots i$	$-2\zeta_9^5-2\zeta_9^4-2\zeta_9^3+2\zeta_9^2-\zeta_9$
37.1	$4.3400\ldots-4.2619\ldots i$	$4\zeta_9^5+4\zeta_9^4-2\zeta_9^3+5\zeta_9^2+2\zeta_9$
37.2	$2.7771\ldots-5.4117\ldots i$	$-5\zeta_9^5-2\zeta_9^4-2\zeta_9^3-\zeta_9^2-4\zeta_9$
37.3	$-4.1172\ldots-4.4775\ldots i$	$-4\zeta_9^5+5\zeta_9^4+2\zeta_9^3-2\zeta_9^2+4\zeta_9+2$
37.4	$4.3400\ldots+4.2619\ldots i$	$2\zeta_9^5-\zeta_9^4+2\zeta_9^3-2\zeta_9^2-5\zeta_9+2$
37.5	$2.7771\ldots+5.4117\ldots i$	$2\zeta_9^5-4\zeta_9^4+2\zeta_9^3+4\zeta_9^2+\zeta_9+2$
37.6	$-4.1172\ldots+4.4775\ldots i$	$\zeta_9^5-2\zeta_9^4-2\zeta_9^3-4\zeta_9^2+2\zeta_9$
64.1	-8	-8

Density of gamma shifts

The gamma shifts μ_j of an L-function appearing in its gamma factor

$$\prod_{j=1}^{r_1} \Gamma_{\mathbb{R}}(s+\mu_j) \prod_{j=r_1+1}^{r_1+r_2} \Gamma_{\mathbb{C}}(s+\mu_j)$$

are expected to satisfy $\Re(\mu_j) \in \{0,1\}$ for $j \leq r_1$ and $\Re(\mu_j) \in \frac{1}{2}\mathbb{Z}_{\geq 0}$ for $j > r_1$.

- Satisfied by L-functions of Hecke characters.
- Set of corresponding gamma shifts is **dense** in the family of possible ones.
- Proof is effective!

Density of gamma shifts

Example: parameters φ near π and *e*.

```
? gc=gcharinit(x^3-3*x+1,2^20);
? chi = [0,-2033118, 694865]~;
? gcharlocal(gc,chi,1)
% = [0, 3.14159238551138]
? gcharlocal(gc,chi,2)
% = [0, 2.71828314775293]
```

Partially algebraic Hecke characters

Up to finite index:
algebraic Hecke characters $\iff \varphi_\sigma = 0$ for all σ.

Are there **partially algebraic** Hecke characters, i.e. such that $\varphi_\sigma = 0$ for a subset of the infinite places?

Proposition (Molin–P.)

Let F/F_0 be a quadratic extension and R the set of complex places of F that are real in F_0. There exists a group of Hecke characters of F of rank $[F_0 : \mathbb{Q}]$ for which $\varphi_\sigma = 0$ for all $\sigma \in R$.

Question: is this the only way to construct partially algebraic characters?

Such characters play an important role in an upcoming paper with A. Bartel on Vignéras's isospectral manifolds.

Partially algebraic characters

Example: consider $F_0 = \mathbb{Q}(\sqrt{5}) \subset F = \mathbb{Q}(5^{1/4})$.

```
? gc=gcharinit(x^4-5,1);
? chi = [1,0,0]~;
? gcharlocal(gc,chi,1)
% = [0, -0.72908519629282042564585827345932876864]
? gcharlocal(gc,chi,2)
% = [0, 0.72908519629282042564585827345932876864]
? gcharlocal(gc,chi,3)
% = [2, 0]
```

The character χ satisfies

$\chi_{\sigma_1} : x \mapsto |x|^{-i\times 0.729\ldots}$, $\chi_{\sigma_2} : x \mapsto |x|^{i\times 0.729\ldots}$, and $\chi_{\sigma_3} : z \mapsto (z/|z|)^2$.

Thank you! Questions?

- **Hecke characters** generalise ray class group characters.
- **Algorithm** to compute groups of Hecke characters of **given modulus** via explicit **dual logarithm maps.**
- **Algorithm** to compute the subgroup of **algebraic** characters, via the **maximal CM subfield.**
- Pari/GP **implementation.**
- **Examples**: coordinates on idèle class groups, CM varieties, gamma shifts of L-functions, partially algebraic characters, . . .