Computing groups of Hecke characters

Pascal Molin* and Aurel Page†

July 19, 2022

Abstract

We describe algorithms to represent and compute groups of Hecke characters. We make use of an idèlic point of view and obtain the whole family of such characters, including transcendental ones. We also show how to isolate the algebraic characters, which are of particular interest in number theory. This work has been implemented in Pari/GP, and we illustrate our work with a variety of explicit examples using our implementation.

1 Introduction

Hecke characters are, from the modern point of view, continuous characters of idèle class groups, in other words automorphic forms for GL_1. They were introduced by Hecke [8] who proved the functional equation of their L-function, and are the starting point of many developments that blossom in modern number theory: automorphic L-functions via Tate's thesis [28], ℓ-adic Galois representations via Weil's notion of algebraic characters [31], Shimura varieties via CM theory [27], and the Langlands programme via class field theory and the global Weil group [32]. Despite their fundamental role, Hecke characters have not received a full algorithmic treatment, perhaps due to the fact that they are considered well-understood compared to automorphic forms on higher rank groups. The existing literature only describes how to compute with finite order characters, since they are characters of ray class groups [4], and algebraic Hecke characters [30]. As part of a collective effort to enumerate and compute L-functions, automorphic representations and Galois representations, we believe that the GL_1 case also deserves close scrutiny, and this is the goal of the present paper.

We describe algorithms to compute, given a number field F and a modulus $\mathfrak{m}$ over F, a basis of the group of Hecke quasi-characters of modulus $\mathfrak{m}$ (Algorithm 18) and its subgroup of algebraic characters (Algorithm 30), in

*Université Paris Cité, IMJ-PRG, CNRS and INRIA Paris
†INRIA Bordeaux

a form suitable for evaluation at arbitrary ideals and decomposition into local characters (Algorithm 17). In particular, we describe a polynomial time algorithm to compute the maximal CM subfield of F (Algorithm 28). It is sometimes believed that the adélic point of view is not suitable for computational purposes; we claim the contrary, and adopt an adélic setting throughout the paper. Our implementation [18] in Pari/GP [22] is available in the master branch of the software. We provide examples that illustrate the use of our algorithms and showcase some interesting features of Hecke characters: a presentation of the software interface, small degree examples, illustrations of automorphic induction from quadratic fields, examples of CM abelian varieties with emphasis on the rigorous identification of the corresponding Hecke character, illustration of the density of the gamma shifts of Hecke L-functions in the conjectured space of possible ones (Proposition 44), examples of provably partially algebraic Hecke characters (Proposition 46) and of twists of L-functions by Hecke characters.

The only previous work on computation of infinite order Hecke characters is that of Watkins [30], so we give a short comparison: only algebraic characters were considered, and only over a CM field, whereas we treat arbitrary Hecke characters over arbitrary number fields; the values of characters were represented exactly by algebraic numbers, whereas we represent values by approximations since this is forced in the transcendental case; the emphasis was on individual Hecke characters, which the user had to construct by hand, whereas our emphasis is on groups of Hecke characters, which we construct for the user, simply from the modulus.

Our implementation makes it possible to tabulate Hecke characters and their L-functions systematically by increasing analytic conductor; we think that this is a valuable project but we leave it for future work.

The paper is organized as follows. In Section 2 we recall the definitions and basic properties of Hecke characters and their L-functions. In Section 3 we describe our algorithms to compute groups of Hecke characters and evaluate them. In Section 4 we present our algorithms to compute the maximal CM subfield and groups of algebraic Hecke characters. Finally, Section 5 contains a variety of examples.

2 Hecke characters

We recall the definition of Hecke characters in the adèlic setting. This material is standard and can be found in [10, chap. XIV] or [25].

Let F be a number field of degree $[F : \mathbb{Q}] = n$ and discriminant Δ_F. When K/F is a finite extension, we denote by $N_{K/F}$ the norm from K to F; we also denote $N = N_{F/\mathbb{Q}}$ when F is clear from the context. For every prime ideal $\mathfrak{p}$ of F, we consider the completion $F_\mathfrak{p}$ and its ring of integers $\mathbb{Z}_\mathfrak{p}$. We choose a uniformizer $\pi_\mathfrak{p} \in \mathbb{Z}_\mathfrak{p}$ and denote by $v_\mathfrak{p} \colon F_\mathfrak{p}^\times \twoheadrightarrow \mathbb{Z}$ the $\mathfrak{p}$-

adic valuation. For every place v, let $n_v = [F_v : \mathbb{Q}_v]$, and let $|\cdot|_v$ be the normalised absolute value, i.e. $n_\sigma = 1$ and $|\cdot|_\sigma = |\cdot|$ for a real embedding σ, $n_\sigma = 2$ and $|\cdot|_\sigma = |\cdot|^2$ for a complex embedding σ, and $|\pi_\mathfrak{p}|_\mathfrak{p} = N(\mathfrak{p})^{-1}$ for a prime ideal $\mathfrak{p}$. We denote by $\mathbb{A}_F^\times = \prod' F_v^\times$ the group of idèles of F. We write $F_\mathbb{R} = F \otimes_\mathbb{Q} \mathbb{R} \cong \prod_\sigma F_\sigma \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where r_1 (resp. r_2) is the number of real embeddings (resp. pairs of nonreal complex embeddings) of F.

Let $\mathbb{U}$ denote the group of complex numbers of absolute value 1. For G a topological group, G° will denote the connected component of 1 in G.

2.1 Pontryagin duality

We recall some definitions and properties of locally compact abelian groups that will be used later. See [19, 20] for general reference.

Let G be a locally compact abelian group. A *quasi-character* of G is a continuous morphism

$$\chi\colon G \to \mathbb{C}^\times.$$

A *character* of G is a continuous morphism

$$\chi\colon G \to \mathbb{U}.$$

The group of characters of G, which we denote by $\widehat{G}$, is the Pontryagin dual $\mathrm{Hom}_{\mathsf{cont}}(G, \mathbb{U})$ of G, and is a locally compact abelian group. The canonical map

$$G \to \widehat{\widehat{G}}$$

given by $g \mapsto (\chi \mapsto \chi(g))$ is an isomorphism. Let $H \subset G$ be a subgroup. Let

$$H^\perp = \{\chi \in \widehat{G} \mid \chi(h) = 1 \text{ for all } h \in H\}$$

be the Pontryagin orthogonal of H in $\widehat{G}$. Then $H^\perp$ is a closed subgroup of $\widehat{G}$, and $(H^\perp)^\perp$ is the closure of H, where the second orthogonal is taken in G. If H is a closed subgroup of G, then we have canonical isomorphisms

$$\widehat{G/H} \cong H^\perp \text{ and } \widehat{G}/(H^\perp) \cong \widehat{H}.$$

The group G is compact if and only if $\widehat{G}$ is discrete.

Pontryagin duality is an exact contravariant functor on the category of locally compact abelian groups.

Let $(x, y) \mapsto x \cdot y$ denote a nondegenerate $\mathbb{R}$-bilinear form on a finite dimensional $\mathbb{R}$-vector space V. The pairing $V \times V \to \mathbb{U}$ defined by $(x, y) \mapsto \exp(2i\pi x \cdot y)$ induces an isomorphism $V \cong \widehat{V}$. We will use this isomorphism to identify characters on V with elements of V.

Let Λ be a full rank lattice in V. The pairing above identifies the dual lattice $\Lambda^\vee = \mathrm{Hom}(\Lambda, \mathbb{Z})$ with the subgroup

$$\Lambda^\perp = \{x \in V \mid x \cdot y \in \mathbb{Z} \text{ for all } y \in \Lambda\},$$

which is canonically isomorphic to $\widehat{V/\Lambda}$ by the above, and we have $\widehat{\Lambda} \cong V/\Lambda^{\perp}$. In particular for $V = \mathbb{R}$ and $\Lambda = \mathbb{Z}$ we consider the standard bilinear form and we have $\widehat{\mathbb{R}/\mathbb{Z}} = \mathbb{Z}^{\perp} = \mathbb{Z}$ and $\widehat{\mathbb{Z}} = \mathbb{R}/\mathbb{Z}$.

The dual $\mathbb{V} = \widehat{\mathbb{Q}}$ of the group of rationals equipped with the discrete topology, is the compact topological group $\varprojlim_{n} \mathbb{R}/n\mathbb{Z}$, called the *solenoid.*

2.2 General Hecke characters

A Hecke quasi-character is a quasi-character of $C_F = \mathbb{A}_F^{\times}/F^{\times}$, and a Hecke character is a character of C_F.

The *norm* is the Hecke quasi-character

$$\|\cdot\| \colon C_F \to \mathbb{C}^{\times}$$

defined by

$$x = (x_v)_v \mapsto \|x\| = \prod_v |x_v|_v.$$

This is a well-defined Hecke quasi-character by the product formula.

Every Hecke quasi-character χ is of the form $\chi = \chi_0 \|\cdot\|^s$ for a unique Hecke character χ_0 and a unique $s \in \mathbb{R}$. We refer to χ_0 as the *unitary component* of χ. In the algebraic setting, the value $w = -2s$ is the *weight* of χ.

We also define $C_F^1 = \ker(\|\cdot\| \colon C_F \to \mathbb{R}_{>0})$ to be the kernel of the norm, which is a compact group. We have a canonical embedding

$$\mathbb{R}_{>0} \to C_F,$$

by sending $t \in \mathbb{R}_{>0} \mapsto ((t^{1/n})_{\sigma}, 1, \dots) \in \mathbb{A}_F^{\times}$, and a canonical decomposition

$$C_F \cong C_F^1 \times \mathbb{R}_{>0}.$$

As a consequence, it suffices to compute the characters of C_F^1 to deduce the full groups of Hecke characters and Hecke quasi-characters.

$$\mathrm{Hom}_{\mathrm{cont}}(C_F, \mathbb{C}^{\times}) = \widehat{C}_F \|\cdot\|^{\mathbb{R}} = \widehat{C}_F^1 \|\cdot\|^{\mathbb{C}} \tag{1}$$

Every quasi-character χ of $\mathbb{A}_F^{\times}$ (and in particular Hecke quasi-characters) admits a factorization $\chi = \prod_v \chi_v$, where χ_v is a quasi-character of $F_v^{\times}$. We therefore describe quasi-characters of local fields.

2.3 Local characters

- Every quasi-character χ of $\mathbb{C}^{\times}$ is of the form

$$\chi(z) = \left(\frac{z}{|z|}\right)^k |z|_{\mathbb{C}}^s = \left(\frac{z}{|z|}\right)^k |z|^{2s}$$

  for a unique pair $(k, s) \in \mathbb{Z} \times \mathbb{C}$. The quasi-character χ is a character if and only if $\mathrm{Re}(s) = 0$, i.e. $s = i\varphi$ for some $\varphi \in \mathbb{R}$.

- Every quasi-character χ of $\mathbb{R}^\times$ is of the form

$$\chi(x) = \mathrm{sgn}(x)^k |x|^s$$

for a unique pair $(k, s) \in \{0, 1\} \times \mathbb{C}$. We say that χ is *unramified* if $k = 0$. The quasi-character χ is a character if and only if $\mathrm{Re}(s) = 0$, i.e. $s = i\varphi$ for some $\varphi \in \mathbb{R}$.

- Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_F$. Every quasi-character χ of $F_\mathfrak{p}^\times$ is of the form

$$\chi(x) = \chi_0(x\pi_\mathfrak{p}^{-v_\mathfrak{p}(x)} \bmod \mathfrak{p}^m)\chi(\mathfrak{p})^{v_\mathfrak{p}(x)}$$

for a unique $m \geq 0$ and a unique primitive character χ_0 of $(\mathbb{Z}_\mathfrak{p}/\mathfrak{p}^m)^\times$, and where we write $\chi(\mathfrak{p}) = \chi(\pi_\mathfrak{p}) \in \mathbb{C}^\times$. Note that in general $\chi(\mathfrak{p})$ depends on the choice of uniformizer $\pi_\mathfrak{p}$, but $\chi(\mathfrak{p})$ is well defined up to the roots of unity of the same order as χ_0. We call $\mathfrak{p}^m$ the conductor of χ and m its conductor exponent. If $m = 0$ we call χ *unramified*; in this case, $\chi(\mathfrak{p})$ does not depend on the choice of uniformizer, and the character χ only depends on $\chi(\mathfrak{p})$. Regardless of m, the quasi-character χ is a character if and only if $\chi(\mathfrak{p}) \in \mathbb{U}$.

Whenever we write a global idèle character χ as a product of local characters χ_v, we write its local parameters k_σ, φ_σ, and $m_\mathfrak{p}$, and we let $\mathfrak{f}_\chi = \prod_\mathfrak{p} \mathfrak{p}^{m_\mathfrak{p}}$ be the conductor of χ. Note that for a complex place, the pair $(k_\sigma, \varphi_\sigma)$ depends on the choice of a complex embedding among the two conjugate ones, or equivalently on the choice of an isomorphism between the completion of F and $\mathbb{C}$: we have $\varphi_{\bar\sigma} = \varphi_\sigma$ and $k_{\bar\sigma} = -k_\sigma$.

2.4 L-function

Let χ be a Hecke character such that $\sum_\sigma n_\sigma \varphi_\sigma = 0$, i.e. that is trivial on the embedded $\mathbb{R}_{>0}$ as above. Let $N_\chi = |\Delta_F| \cdot \mathrm{N}(\mathfrak{f}_\chi)$. Let

$$L(\chi, s) = \prod_{\mathfrak{p} \nmid \mathfrak{f}_\chi} (1 - \chi(\mathfrak{p}) \, \mathrm{N}(\mathfrak{p})^{-s})^{-1}$$

and

$$\gamma(\chi, s) = \prod_{\sigma \text{ real}} \Gamma_\mathbb{R}(s + i\varphi_\sigma + k_\sigma) \cdot \prod_{\sigma \text{ complex}} \Gamma_\mathbb{C}(s + i\varphi_\sigma + |k_\sigma|/2).$$

where $\Gamma_\mathbb{R}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$ and $\Gamma_\mathbb{C}(s) = 2(2\pi)^{-s}\Gamma(s)$. Then

$$\Lambda(\chi, s) = N_\chi^{s/2} \gamma(\chi, s) L(\chi, s)$$

satisfies the functional equation

$$\Lambda(\chi, 1 - s) = W(\chi)\Lambda(\bar\chi, s)$$

for some complex number $W(\chi)$ of absolute value 1.

2.5 Algebraic Hecke characters

Warning: an algebraic Hecke character is usually not a Hecke character, it is only a quasi-character.

Let χ be a Hecke quasi-character. It is called *algebraic* if for every archimedean place σ of F, there exists integers $p_\sigma, q_\sigma \in \mathbb{Z}$ such that for all $z \in (F_\sigma^\times)^\circ$ we have [1]

$$\chi_\sigma(z) = z^{-p_\sigma}(\bar{z})^{-q_\sigma}.$$

Note: if σ is complex, then p_σ and q_σ are uniquely determined; if σ is real then only their sum is well-defined. We refer to the data $(p_\sigma, q_\sigma)_\sigma$ as the *type* of χ.

Example 1. The norm $\|\cdot\|$ is an algebraic character, of type $(p_\sigma, q_\sigma) = (-1, -1)$ if σ is complex. We have $\|\mathfrak{p}\| = N(\mathfrak{p})^{-1}$ for every prime ideal $\mathfrak{p}$.

Definition 2. We call a Hecke character *almost-algebraic* if $\varphi_\sigma = 0$ for all σ. We denote by $\left(\widehat{C}_F\right)^{\text{a.a.}}$ the subgroup of almost-algebraic characters.

Thus the group of unitary components χ_0 of algebraic Hecke characters $\chi = \chi_0\|\cdot\|^{-w/2}$ is a finite index subgroup of the group of almost-algebraic Hecke characters.

Remark 3. Algebraic characters correspond to *type* A_0 and almost-algebraic to *type* A with trivial norm component in Weil's terminology [31]. By a theorem of Waldschmidt [29], these definitions coincide with the fact that *type* A are the characters whose values are algebraic, and *type* A_0 the quasi-characters whose values belong to a finite extension.

2.5.1 Parameters at infinity of algebraic Hecke characters

It is known that if F has a real embedding, then every algebraic Hecke character is an integral power of the norm times a Hecke character of finite order. So from now on we assume that F is totally complex. We recall the following well-known lemma.

Lemma 4. *Let χ_0 be a Hecke character such that all φ_σ are 0 and all the k_σ have the same parity.*

Let $w \in \mathbb{Z}$ be such that $k_\sigma + w$ is even for all σ. Then $\chi = \chi_0\|\cdot\|^{-\frac{w}{2}}$ is an algebraic Hecke character of infinity-type $((p_\sigma, q_\sigma))_\sigma$, where $p_\sigma = \frac{w-k_\sigma}{2} \in \mathbb{Z}$ and $q_\sigma = \frac{w+k_\sigma}{2} \in \mathbb{Z}$.

Conversely, an algebraic character of infinity-type $((p_\sigma, q_\sigma))_\sigma$ must have constant value $p_\sigma + q_\sigma = w$, in which case its parameters are $k_\sigma = q_\sigma - p_\sigma$.

[1] The choice of sign in the exponents is such that the values of χ at integral ideals are algebraic integers if and only if all p_σ and q_σ are nonnegative.

Proof. Assume $\chi = \chi_0 \|\cdot\|^s$ is an algebraic character, with χ_0 a Hecke character and $s \in \mathbb{R}$, and let χ_σ denote the local component of χ_0 at a complex place σ. We solve

$$\chi_\sigma(z)|z|_\sigma^s = \left(\frac{z}{|z|}\right)^{k_\sigma} |z|^{2(i\varphi_\sigma+s)} = z^{k_\sigma/2+i\varphi_\sigma+s}(\bar{z})^{-k_\sigma/2+i\varphi_\sigma+s} = z^{-p_\sigma}(\bar{z})^{-q_\sigma}.$$

as

$$p_\sigma = -k_\sigma/2 - i\varphi_\sigma - s \text{ and } q_\sigma = k_\sigma/2 - i\varphi_\sigma - s.$$

This implies that $\varphi_\sigma = 0$ and that $2s \in \mathbb{Z}$, so we write $w = -2s$. We obtain

$$2p_\sigma = -k_\sigma + w,\ 2q_\sigma = k_\sigma + w,\ w = p_\sigma + q_\sigma, \text{ and } k_\sigma = q_\sigma - p_\sigma,$$

so all the k_σ must have the same parity. □

2.5.2 L-function of an algebraic Hecke character

Let $\chi = \chi_0 \|\cdot\|^{-w/2}$ be an algebraic Hecke character as above. Let $\mathfrak{f}_\chi = \mathfrak{f}_{\chi_0}$ be its conductor and $N_\chi = N_{\chi_0}$. Let

$$L(\chi, s) = \prod_{\mathfrak{p} \nmid \mathfrak{f}_\chi} (1 - \chi(\mathfrak{p}) \operatorname{N}(\mathfrak{p})^{-s})^{-1} = L(\chi_0, s - w/2),$$

and

$$\gamma(\chi, s) = \prod_\sigma \Gamma_{\mathbb{C}}(s - \min(p_\sigma, q_\sigma)) = \gamma(\chi_0, s - w/2).$$

Then

$$\Lambda(\chi, s) = N_\chi^{s/2} \gamma(\chi, s) L(\chi, s)$$

satisfies the functional equation

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

for some complex number $W(\chi) = W(\chi_0)$ of absolute value 1.

3 Computing the group of Hecke characters

3.1 Filtration by modulus

We have a non-canonical isomorphism

$$\widehat{C}_F \cong T \times \mathbb{Q}^{r_1+r_2-1} \times \mathbb{Z}^{r_2} \times \mathbb{R},$$

where T is an infinite torsion abelian group. Indeed, we have the classical decomposition [32]

$$1 \to C_F^\circ \to C_F \to \pi_0(C_F) \to 1, \text{ where } C_F^\circ \cong \mathbb{V}^{r_1+r_2-1} \times (\mathbb{R}/\mathbb{Z})^{r_2} \times \mathbb{R},$$

where $\mathbb{V} = \widehat{\mathbb{Q}}$ is the solenoid, and $\pi_0(C_F)$ is profinite; by Pontryagin duality, we get

$$0 \to T \to \widehat{C}_F \to \mathbb{Q}^{r_1+r_2-1} \times \mathbb{Z}^{r_2} \times \mathbb{R} \to 0,$$

and this exact sequence splits. Since we cannot give a finite description of the whole group T, we will filter $\widehat{C}_F$ according to moduli.

Let $\mathfrak{m} = \mathfrak{m}_f \mathfrak{m}_\infty$ be a modulus, meaning that $\mathfrak{m}_f$ is an integral ideal and $\mathfrak{m}_\infty$ is a set of real embeddings of F. We write

$$(\mathbb{Z}_F/\mathfrak{m})^\times = (\mathbb{Z}_F/\mathfrak{m}_f)^\times \times \prod_{\sigma \in \mathfrak{m}_\infty} \{\pm 1\}\,.$$

A Hecke character χ is said to have modulus $\mathfrak{m}$ if χ is trivial on the group $U(\mathfrak{m})$ of idèles congruent to 1 mod $\mathfrak{m}$:

$$U(\mathfrak{m}) = \prod_{\mathfrak{p} \mid \mathfrak{m}_f} (1 + \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}\mathbb{Z}_\mathfrak{p}) \times \prod_{\mathfrak{p} \nmid \mathfrak{m}_f} \mathbb{Z}_\mathfrak{p}^\times \times \prod_{\sigma \in \mathfrak{m}_\infty} \{1\} \times \prod_{\substack{\sigma \notin \mathfrak{m}_\infty \\ \sigma \text{ real}}} \{\pm 1\} \times \prod_{\sigma \text{ complex}} \{1\}\,.$$

Equivalently, the conductor of χ divides $\mathfrak{m}_f$ and χ is unramified at all the real places not dividing $\mathfrak{m}_\infty$.

The character group of modulus $\mathfrak{m}$ is the dual of

$$C_\mathfrak{m} = \mathbb{A}_F^\times / (F^\times \cdot U(\mathfrak{m})),$$

and we have

$$\widehat{C}_F = \bigcup_\mathfrak{m} \widehat{C}_\mathfrak{m}.$$

In the remainder of this section, we fix a modulus $\mathfrak{m}$.

3.2 Explicit description

The character group $\widehat{C}_\mathfrak{m}$ is isomorphic to $T_\mathfrak{m} \times \mathbb{Z}^{n-1} \times \mathbb{R}$ where $T_\mathfrak{m}$ is finite. Our goal in the next paragraphs is to prove the following

Proposition 5. *There exist an integer $\ell \geq 0$, an explicit lattice Λ of rank $\ell + n - 1$, and two explicit isomorphisms*

$$\mathcal{L}\colon C_\mathfrak{m} \xrightarrow{\sim} (\mathbb{Z}^\ell \times \mathbb{R}^n)/\Lambda$$
$$\mathcal{L}^*\colon \widehat{C}_\mathfrak{m} \xrightarrow{\sim} \Lambda^\perp / \mathbb{Z}^\ell$$

where $\Lambda^\perp$ is the Pontryagin orthogonal of Λ in $\mathbb{R}^{\ell+n}$, and such that for all $\chi \in \widehat{C}_\mathfrak{m}$ and $x \in \mathbb{A}_F^\times$ we have

$$\chi(x) = \exp(2i\pi \mathcal{L}^*(\chi) \cdot \mathcal{L}(x)). \tag{2}$$

3.3 Idèle class groups

Definition 6. Let $x \in \mathbb{A}_F^\times$. We define the *ideal attached to* x to be

$$\prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})}.$$

Let S be a finite set of primes of F. Define the group of S*-idèles* to be

$$U_S = \prod_{\mathfrak{p} \in S} F_\mathfrak{p}^\times \times \prod_{\mathfrak{p} \notin S} \mathbb{Z}_\mathfrak{p}^\times \times F_\mathbb{R}^\times,$$

and the group of S*-units* $\mathbb{Z}_{F,S}^\times = F^\times \cap U_S$.

Lemma 7. *Let $x \in \mathbb{A}_F^\times$. Then $x \in U_S$ if and only if the ideal attached to x belongs to the group $\langle S \rangle$ generated by S. If S generates the class group of F, then $\mathbb{A}_F^\times = U_S \cdot F^\times$.*

Proof. The first property follows from rewriting the definition of U_S as $U_S = \{x \in \mathbb{A}_F^\times \mid v_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}$. Let $x \in \mathbb{A}_F^\times$ and $\mathfrak{a}$ the ideal attached to x. Assuming S generates the class group, let α be such that $\mathfrak{a}(\alpha^{-1}) \in \langle S \rangle$. Then $x\alpha^{-1} \in U_S$. □

Definition 8. Let S be a set of primes generating the class group of F. Let

$$\mathcal{D}_S \colon U_S \to \mathbb{Z}^S \times (\mathbb{Z}_F/\mathfrak{m})^\times \times (F_\mathbb{R}^\times)^\circ$$

be defined by

$$\mathcal{D}_S(x) = \big(v_\mathfrak{p}(x_\mathfrak{p})_{\mathfrak{p} \in S}, (u \bmod \mathfrak{m}_f), (\operatorname{sgn}(x_\sigma))_{\sigma \in \mathfrak{m}_\infty}, (|x_\sigma|)_{\sigma \text{ real}}, (x_\sigma)_{\sigma \text{ complex}}\big),$$

where $u \in \prod_\mathfrak{p} \mathbb{Z}_\mathfrak{p}^\times$ is defined by $u_\mathfrak{p} = x_\mathfrak{p} \pi_\mathfrak{p}^{-v_\mathfrak{p}(x_\mathfrak{p})}$.

Let

$$\mathcal{D} \colon \mathbb{A}_F^\times \to \Big[\mathbb{Z}^S \times (\mathbb{Z}_F/\mathfrak{m})^\times \times (F_\mathbb{R}^\times)^\circ\Big] / \mathcal{D}_S(\mathbb{Z}_{F,S}^\times)$$

be defined by $\mathcal{D}(x) = \mathcal{D}_S(x\alpha^{-1})$ where $\alpha \in F^\times$ is such that $x\alpha^{-1} \in U_S$.

Lemma 9. *Let S be a finite set of primes generating the class group. Then $\mathcal{D}$ is well-defined and induces an isomorphism*

$$C_\mathfrak{m} \cong \Big[\mathbb{Z}^S \times (\mathbb{Z}_F/\mathfrak{m})^\times \times (F_\mathbb{R}^\times)^\circ\Big] / \mathcal{D}_S(\mathbb{Z}_{F,S}^\times). \tag{3}$$

Proof. If $x\alpha^{-1}$ and $x\beta^{-1}$ belong to U_S with $\alpha, \beta \in F^\times$, then $\beta/\alpha \in F^\times \cap U_S = \mathbb{Z}_{F,S}^\times$, so $\mathcal{D}$ is well-defined. The map $\mathcal{D}_S$ is onto and $\ker \mathcal{D}_S = U(\mathfrak{m}) \subset U_S$. Moreover by definition $\mathcal{D}(F^\times) = 1$. This proves that $\ker \mathcal{D} = F^\times \cdot U(\mathfrak{m})$ and therefore $\mathcal{D}$ induces an isomorphism from $C_\mathfrak{m} = \mathbb{A}_F^\times/(F^\times \cdot U(\mathfrak{m}))$ to its codomain. □

3.4 Logarithm maps

In this section we fix a finite set S of primes that generates the class group of F.

Definition 10. Consider the usual archimedean logarithm $\log_\infty : (F_\mathbb{R}^\times)^\circ \to \mathbb{R}^{r_1+r_2} \times (\mathbb{R}/\mathbb{Z})^{r_2} = \mathbb{R}^n/\mathbb{Z}^{r_2}$

$$\log_\infty(z) = \left(\left(\frac{n_\sigma}{2\pi} \log |z_\sigma| \right)_\sigma, \left(\frac{\arg(z_\sigma)}{2\pi} \right)_\sigma \right), \tag{4}$$

and choose an isomorphism

$$\log_\mathfrak{m} : (\mathbb{Z}_F/\mathfrak{m})^\times \xrightarrow{\sim} \mathbb{Z}^{r(\mathfrak{m})}/\Lambda_\mathfrak{m} \tag{5}$$

with $\Lambda_\mathfrak{m} \subset \mathbb{Z}^{r(\mathfrak{m})}$ a full sublattice.

Let $\ell = \#S + r(\mathfrak{m})$, and let

$$\mathcal{L}_S \colon U_S \to \frac{\mathbb{Z}^\ell \times \mathbb{R}^n}{\Lambda_\mathfrak{m} + \mathbb{Z}^{r_2}}$$

be the composition of $\mathcal{D}_S$ with

$$\mathrm{Id}_{\mathbb{Z}^S} \times \log_\mathfrak{m} \times \log_\infty .$$

We identify $\Lambda_\mathfrak{m}$ and $\mathbb{Z}^{r_2}$ with their embedding in $\mathbb{Z}^\ell \times \mathbb{R}^n$.

Let

$$\Lambda = \mathcal{L}_S(\mathbb{Z}_{F,S}^\times) + \Lambda_\mathfrak{m} + \mathbb{Z}^{r_2}, \tag{6}$$

and let

$$\mathcal{L} \colon \mathbb{A}_F^\times \to \frac{\mathbb{Z}^\ell \times \mathbb{R}^n}{\Lambda}$$

be defined by $\mathcal{L}(x) = \mathcal{L}_S(x\alpha^{-1})$ where $\alpha \in F^\times$ is such that $x\alpha^{-1} \in U_S$.

Definition 11. We define the dual logarithm $\mathcal{L}^* \colon \widehat{C}_\mathfrak{m} \to (\mathbb{R}/\mathbb{Z})^\ell \times \mathbb{R}^n$ by

$$\mathcal{L}^*(\chi) = \left(\left(\frac{\arg \chi(\mathfrak{p})}{2\pi} \right)_{\mathfrak{p} \in S}, \left(\frac{\arg \chi(\log_\mathfrak{m}^{-1}(g_i))}{2\pi} \right)_{i=1}^{r(\mathfrak{m})}, (\varphi_\sigma)_\sigma, (k_\sigma)_\sigma \right), \tag{7}$$

where $(g_i)_{i=1}^{r(\mathfrak{m})}$ is the image in $\mathbb{Z}^{r(\mathfrak{m})}/\Lambda_\mathfrak{m}$ of the standard basis of $\mathbb{Z}^{r(\mathfrak{m})}$ and φ_σ, k_σ are the parameters at infinity of χ.

We now prove Proposition 5 in the following precise form.

Proposition 12. *Let $\Lambda^\perp$ be the Pontryagin orthogonal of Λ in $\mathbb{R}^{\ell+n}$. The homomorphisms $\mathcal{L}$ and $\mathcal{L}^*$ induce isomorphisms*

$$\mathcal{L} \colon C_\mathfrak{m} \longrightarrow \frac{\mathbb{Z}^\ell \times \mathbb{R}^n}{\Lambda} \text{ and } \mathcal{L}^* \colon \widehat{C}_\mathfrak{m} \longrightarrow \Lambda^\perp/\mathbb{Z}^\ell.$$

Let $\chi \in \widehat{C}_\mathfrak{m}$ be a character of modulus $\mathfrak{m}$ and let $x \in \mathbb{A}_F^\times$, then

$$\chi(x) = \exp(2i\pi \mathcal{L}^*(\chi) \cdot \mathcal{L}(x)). \tag{8}$$

Proof. The fact that $\mathcal{L}$ is well-defined and induces an isomorphism follows immediately from Lemma 9. Applying Pontryagin duality to the sequence

$$0 \to C_{\mathfrak{m}} \to \mathbb{R}^{\ell+n}/\Lambda \to (\mathbb{R}/\mathbb{Z})^{\ell} \to 0$$

gives $\widehat{C}_{\mathfrak{m}} = \Lambda^{\perp}/\mathbb{Z}^{\ell}$.

Let $x \in \mathbb{A}_F^{\times}$ and write $x = \alpha \cdot x\alpha^{-1}$ with $\alpha \in F^{\times}$ and $x\alpha^{-1} \in U_S$ by Lemma 7, and let u be as in Definition 8. We have

$$x = \alpha \prod_{\mathfrak{p}\in S} \pi_{\mathfrak{p}}^{v_{\mathfrak{p}}(x_{\mathfrak{p}}\alpha^{-1})} \cdot u \cdot \prod_{\sigma} (x_{\sigma}\sigma(\alpha)^{-1}),$$

and therefore

$$\chi(x) = \chi(\alpha) \cdot \prod_{\mathfrak{p}\in S} \chi_{\mathfrak{p}}(\pi_{\mathfrak{p}}^{v_{\mathfrak{p}}(x_{\mathfrak{p}}\alpha^{-1})}) \cdot \chi(u) \cdot \prod_{\sigma} \chi_{\sigma}(x_{\sigma}\sigma(\alpha)^{-1}),$$

where $\chi(\alpha) = 1$ and $\chi(u) = \prod_{\mathfrak{p}|\mathfrak{m}_f} \chi_{\mathfrak{p}}(u_{\mathfrak{p}} \bmod \mathfrak{p}^{m_{\mathfrak{p}}})$. By definition the product of local character evaluations is $\exp(2i\pi\mathcal{L}^*(\chi) \cdot \mathcal{L}(x))$. This also proves that the image of $\mathcal{L}^*$ lies in $\Lambda^{\perp}$ and that $\mathcal{L}^*$ induces an isomorphism as claimed. □

Remark 13. At this point Λ is not cocompact in $\mathbb{R}^{\ell+n}$: the Pontryagin orthogonal contains a $\mathbb{R}$ factor corresponding to the norm, and cannot be identified with a dual lattice (see Section 2.1). We obtain a nicer description in the next section.

3.5 Characters modulo the norm

Let $C_{\mathfrak{m}}^1 = C_F^1 \cap C_{\mathfrak{m}} = \ker(C_{\mathfrak{m}} \to \mathbb{R}_{>0})$ be the kernel of the norm, which is compact. We have a canonical splitting inherited from (1)

$$C_{\mathfrak{m}} \cong C_{\mathfrak{m}}^1 \times \mathbb{R}_{>0},$$

and the corresponding decomposition

$$\widehat{C}_{\mathfrak{m}} \cong \widehat{C}_{\mathfrak{m}}^1 \times \|\cdot\|^{\mathbb{R}}$$

where $\widehat{C}_{\mathfrak{m}}^1$ is a discrete finitely generated abelian group.

Proposition 14. *Let $v_0 \in \mathbb{R}^{\ell+n}$ be the vector having coordinate n_{σ} at the components corresponding to φ_{σ} and 0 elsewhere, and $p_0 : \mathbb{R}^{\ell+n} \to (\mathbb{R}v_0)^{\perp}$ the orthogonal projection.*

Then $p_0 \circ \mathcal{L}$ induces an isomorphism

$$\widehat{C}_{\mathfrak{m}}^1 \cong p_0(\Lambda)^{\vee}/\mathbb{Z}^{\ell}.$$

Proof. Let $H = (\mathbb{R}v_0)^\perp = \{x \mid \sum n_\sigma x_\sigma = 0\}$, we have an exact sequence

$$0 \to C^1_{\mathfrak{m}} \to H/p_0(\Lambda) \to (\mathbb{R}/\mathbb{Z})^\ell \to 0,$$

where $p_0(\Lambda)$ has full rank in H, so that we identify $p_0(\Lambda)^\perp = p_0(\Lambda)^\vee$ in the dual sequence. □

Remark 15. By an appropriate choice of basis of the lattice Λ, we naturally obtain a structured basis of $C_{\mathfrak{m}}$ according to the filtration

$$\widehat{\mathrm{Cl}(\mathfrak{m})} \subset \widehat{C}^1_{\mathfrak{m}} \subset \widehat{C}_{\mathfrak{m}}.$$

It is even possible to obtain a basis exhibiting the filtration

$$\widehat{\mathrm{Cl}_F} \subset \widehat{\mathrm{Cl}(\mathfrak{m})} \subset (\widehat{C}^1_{\mathfrak{m}})_{k=0} \subset \widehat{C}^1_{\mathfrak{m}} \subset \widehat{C}_{\mathfrak{m}},$$

but our implementation makes a different choice of basis, using an SNF basis for the torsion subgroup and exhibiting the subgroup of almost-algebraic characters, as explained in Section 4.

3.6 Algorithms

Since a precise discussion of the complexity is not the main point of the paper, we delegate the difficult operations to oracles.

Definition 16. Let F be a number field and I_F the set of fractional ideals of $\mathbb{Z}_F$. We say that F is *strongly computable* if it is equipped with

- algorithms to compute field operations in F, factorizations into prime ideals and valuations in I_F;
- a finite set S of prime ideals generating the class group;
- generators of the S-units $\mathbb{Z}_{F,S}^\times$;
- a principalization oracle $p_S \colon I_F \to F^\times \times \mathbb{Z}^S$ such that for every ideal $\mathfrak{a} \in I_F$ the output $p_S(\mathfrak{a}) = (\alpha, (a_\mathfrak{p})_{\mathfrak{p}\in S})$ satisfies $\mathfrak{a} = (\alpha)\prod_{\mathfrak{p}\in S}\mathfrak{p}^{a_\mathfrak{p}}$;
- for each modulus $\mathfrak{m}$, a lattice $\Lambda_\mathfrak{m}$ of rank $r(\mathfrak{m})$ and a logarithm oracle $\log_\mathfrak{m} \colon \mathbb{Z}_F \to \mathbb{Z}^{r(\mathfrak{m})}$ inducing an isomorphism $(\mathbb{Z}_F/\mathfrak{m})^\times \cong \mathbb{Z}^{r(\mathfrak{m})}/\Lambda_\mathfrak{m}$.

Algorithm 17.

- Input: a strongly computable number field F, a modulus $\mathfrak{m}$ and an ideal $\mathfrak{a} \in I_F$.
- Output: a vector z in $\mathbb{R}^{\ell+n}$ such that $\mathcal{L}(\mathfrak{a}) \equiv z \bmod \Lambda$.

1. Let $(\alpha, (a_\mathfrak{p})_\mathfrak{p}) = p_S(\mathfrak{a})$.

2. Let $u \in \mathbb{Z}_F$ such that $\alpha\pi_{\mathfrak{p}}^{-v_{\mathfrak{p}}(\alpha)} \equiv u \bmod \mathfrak{p}$ for all $\mathfrak{p} \mid \mathfrak{m}$.

3. Return $z = ((a_{\mathfrak{p}})_{\mathfrak{p}\in S}, -\log_{\mathfrak{m}}(u), -\log_{\infty}(\alpha))$.

Algorithm 18.

- Input: a strongly computable number field F and a modulus $\mathfrak{m}$.
- Output: a matrix B whose rows generate $\widehat{C}^1_{\mathfrak{m}}$ in $\mathbb{R}^{\ell+n}$.

1. Let A be a matrix whose columns form a basis of $\mathcal{L}_S(\mathbb{Z}_{F,S}^{\times}) + \Lambda_{\mathfrak{m}} + \mathbb{Z}^{r_2} + \mathbb{Z}v_0$ in $\mathbb{R}^{\ell+n}$.
2. Let $B_0 = A^{-1}$.
3. Let B be the $(\ell+n-1)\times(\ell+n)$ matrix whose rows are the orthogonal projections of those of B_0 on $(\mathbb{R}v_0)^{\perp}$.
4. Return B.

Remark 19. These algorithms output numerical approximations in $\mathbb{R}^{\ell+n}$: their validity to any prescribed accuracy can be certified as follows. In both cases, the numerical approximations come from log embeddings of number field elements, which can be obtained to arbitrary accuracy in polynomial time. All subsequent numerical operations come from linear algebra and can be implemented using certified numerical algorithms with automatic precision increase until a target precision is reached.

Theorem 20. *Algorithm 18 and Algorithm 17 are correct. They are polynomial time, meaning a polynomial number of calls to the oracles with polynomial size input and a polynomial number of other operations.*

Proof. Algorithm 18 is correct by Proposition 14.

We verify that the value z computed in Algorithm 17 equals $\mathcal{L}(\mathfrak{a}) \bmod \Lambda$: let $x = (\pi_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{a})})$ be an idèle defining $\mathfrak{a}$, we have $\mathcal{L}(\mathfrak{a}) = \mathcal{L}(x) = \mathcal{L}_S(x\alpha^{-1})$ by definition of $\mathcal{L}$. Now we have $v_{\mathfrak{p}}(x\alpha^{-1}) = a_{\mathfrak{p}}$ for $\mathfrak{p} \in S$ by definition of p_S, and $x\alpha^{-1} \equiv u^{-1} \bmod \mathfrak{m}$ by definition of u. At infinite places $(x\alpha^{-1})_{\sigma} = \alpha_{\sigma}^{-1}$. Hence $\mathcal{L}_S(x\alpha^{-1}) = z \bmod \Lambda$, and Algorithm 17 is correct. All operations not provided by the oracles can clearly be performed in polynomial time. □

4 The subgroup of algebraic characters

Among Hecke quasi-characters, we would like to exhibit the subgroup of algebraic Hecke characters. It is equivalent to compute the subgroup of almost-algebraic characters inside the group of Hecke characters. More precisely, let $H_0^\perp \subset \mathbb{R}^{\ell+n}$ be the subgroup of characters defined by $H_0^\perp = \{\varphi_\sigma = 0 \text{ for all } \sigma\}$, then

$$\begin{aligned}\left(\widehat{C}_{\mathfrak{m}}\right)^{\text{a.a.}} &= \widehat{C}_{\mathfrak{m}} \cap \left(\widehat{C}_F\right)^{\text{a.a.}} \\ &\cong \Lambda^\perp \cap H_0^\perp/\mathbb{Z}^\ell = \left\{\lambda \in \Lambda^\perp \mid \lambda(h) = 1 \text{ for all } h \in H_0\right\}/\mathbb{Z}^\ell.\end{aligned}$$

However, we do not want to solve the equation $\varphi_\sigma = 0$ since the components φ_σ on $\Lambda^\perp$ are only known approximately. We are therefore going to use the known structure of algebraic characters.

Recall that a number field K is *CM* if it is a totally complex quadratic extension of a totally real field, denoted K^+. In this case, the automorphism corresponding to this quadratic extension induces complex conjugation on every complex embedding of K, and we therefore denote it by $x \mapsto \bar{x}$.

A classical theorem of Weil and Artin states that the type of every algebraic Hecke character factors through the norm to the maximal CM subfield of F [31, 23]. Equivalently, every almost-algebraic Hecke character, up to a finite order character, factors through the norm $N_{F/K}$ of the maximal CM subfield K of F.

4.1 Determining the subgroup of algebraic characters from the maximal CM subfield

Let $G = \mathbb{R}^{\ell+n}$ be equipped with its standard inner product and $\Lambda = \mathcal{L}_S(\mathbb{Z}_{F,S}^\times) + \Lambda_{\mathfrak{m}} + \mathbb{Z}^{r_2} + \mathbb{Z}v_0$, so that $\widehat{C}_{\mathfrak{m}}^1 \times \|\cdot\|^{i\mathbb{Z}} \cong \Lambda^\perp/\mathbb{Z}^\ell$, with $\Lambda^\perp = \Lambda^\vee$ in G.

Our strategy is to capture the algebraic characters in a smaller subspace $H^\perp \subset G$ by using the additional known constraints on almost-algebraic characters, in order to apply the following lemma.

Lemma 21. *Let G be a finite dimension $\mathbb{R}$-vector space, let $H \subset G$ be an $\mathbb{R}$-vector subspace and let $\Lambda \subset G$ a lattice such that $H \cap \Lambda$ has full rank in H. Then*

$$\Lambda^\perp \cap H^\perp = \left\{\lambda \in \Lambda^\perp, \lambda \cdot h = 0 \text{ for all } h \in H \cap \Lambda\right\}.$$

Proof. We use the facts that H is an $\mathbb{R}$-subspace generated by $H \cap \Lambda$ to write

$$\begin{aligned}\Lambda^\perp \cap H^\perp &= \left\{x \in \Lambda^\perp, x \cdot h \in \mathbb{Z} \text{ for all } h \in H\right\} \\ &= \left\{x \in \Lambda^\perp, x \cdot h = 0 \text{ for all } h \in H\right\} \\ &= \left\{x \in \Lambda^\perp, x \cdot h = 0 \text{ for all } h \in H \cap \Lambda\right\},\end{aligned}$$

proving the claim. □

Remark 22. The point of Lemma 21 is that since the inner products between elements of Λ and $\Lambda^\perp$ are in $\mathbb{Z}$, the given expression for $\Lambda^\perp \cap H^\perp$ can be computed exactly as a subgroup of $\Lambda^\perp$ by linear algebra over $\mathbb{Z}$.

Example 23. When $H_0^\perp = \{\varphi_\sigma = 0\}$ as above, we have $H_0 = \mathbb{R}^{r_2}$. Then $H_0 \cap \Lambda$ is $\mathcal{L}_S(\mathbb{Z}_{K^+}^\times) + \mathbb{Z}v_0$, which has rank $r_1(K^+) = r_2(K)$. This has full rank in H_0 if and only if $K = F$.

This example shows that using H_0 is sufficient when F itself is CM. In the general case, we proceed as follows.

Proposition 24. *Let K be the maximal CM subfield of F, let*

$$H^\perp = \{\varphi_\sigma = 0 \text{ for all } \sigma, \text{ and } (k_\sigma)_\sigma \text{ factors through } K\}$$

and $\Lambda = \mathcal{L}_S(\mathbb{Z}_{F,S}^\times) + \Lambda_\mathfrak{m} + \mathbb{Z}^{r_2} + \mathbb{Z}v_0$. Then

$$\left(\widehat{C}_\mathfrak{m}\right)^{\text{a.a.}} = (\Lambda^\perp \cap H^\perp)/\mathbb{Z}^\ell.$$

where $\Lambda \cap H$ has full rank in H. More precisely, the group $U \subset \Lambda$ generated by v_0, the kernel $\ker(N_{F/K}\colon \mathbb{Z}^{r_2} \to \mathbb{Z}^{r_2(K)})$ and $\mathcal{L}_S(u)$ for all $u \in \ker(\mathbb{Z}_F^\times \to (\mathbb{Z}_F/\mathfrak{m})^\times)$ such that $N_{F/K}(u) \in K^+$, is contained in H and has full rank.

Proof. Algebraic characters are contained in $H^\perp$ since their infinity types factor through $N_{F/K}$, and we have $H = \mathbb{R}^{r_2} \times \ker(N_{F/K} : \mathbb{R}^{r_2} \to \mathbb{R}^{r_2(K)})$. The group U described in the Proposition is clearly contained in $H \cap \Lambda$. The kernel $\ker(N_{F/K}\colon \mathbb{Z}^{r_2} \to \mathbb{Z}^{r_2(K)})$ has rank $r_2 - r_2(K)$ and the units described form a finite index subgroup of $\mathbb{Z}_F^\times$, so the group U has full rank in H. □

4.2 The maximal CM subfield

In this section we reformulate the problem of determining the maximal CM subfield in a way that is suitable for an efficient algorithm. Indeed enumerating all subfields, regardless of the algorithm used, could not lead to a polynomial time algorithm since the number of subfields is not polynomially bounded. One may consider a pure Galois-theoretic approach, but it is currently not known whether one can compute in polynomial time, given a number field F, the Galois group of the Galois closure of F. Our method relies on the following Lemma.

Lemma 25. *Let F be a number field. For $\varepsilon \in \{\pm\}$, let*

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

The following are equivalent:

(i) F admits a CM subfield;

(ii) $F^- \neq 0$;

(iii) $\dim_{\mathbb{Q}} F^+ = \dim_{\mathbb{Q}} F^-$.

If those conditions are satisfied, then the largest CM subfield of F is $F^+ + F^-$; it also equals $\mathbb{Q}(a)$ for every $a \in F^-$ having minimal polynomial of degree $2\dim_{\mathbb{Q}} F^-$, and such an element exists.

Proof. First note that F^+ is the largest totally real subfield of F. It is clear than (i) implies (ii). Since $\dim_{\mathbb{Q}} F^+ \geq 1$, (iii) implies (ii). Let $a, b \in F^-$ be nonzero; then $a/b \in F^+$ and therefore F^- is a one-dimensional vector space over F^+, so (ii) implies (iii). Let $a \in F^-$ be nonzero; then $a^2 \in F^+$ is totally negative, so $F^+(a) = F^+ + F^-$ is a CM subfield of F, so that (ii) implies (i). If the conditions are satisfied, then the maximal CM subfield K of F is a quadratic extension of its totally real subfield F^+ containing $F^+ + F^-$, so there is equality as claimed. Let $a \in F^- \subset K$ have minimal polynomial of degree $2\dim_{\mathbb{Q}} F^- = [K : \mathbb{Q}]$; then it generates K over $\mathbb{Q}$. For every subfield $L \subset K$, if $F^- \subset L$ then $F^+ \subset L$ by taking ratios, so $K \subset L$ and therefore $L = K$. The set of elements of F^- lying in a proper subfield of K is therefore a finite union of proper subspaces, and is therefore nonempty. □

It is therefore enough to compute F^-. Proposition 26 below gives a meta-algorithm to solve this type of problem.

Proposition 26. *Let F be a number field. Let Ω be a field of characteristic 0, let $R \subset \mathrm{Hom}(F, \Omega)^2$ be a subset and let $(\lambda_r)_{r\in R} \in \mathbb{Q}^R$ be a family of rational numbers. Define*

$$F_{R,\lambda} = \{x \in F \mid \sigma_1(x) = \lambda_r \sigma_2(x) \text{ for all } r = (\sigma_1, \sigma_2) \in R\}.$$

Write $F \otimes_{\mathbb{Q}} F \cong \prod_{i=1}^k L_i$ where each L_i is a field. Let $p_i \colon F \otimes_{\mathbb{Q}} F \to L_i$ be the projection onto L_i. For each $r \in R$, let $i(r) \in \{1, \dots, k\}$ be the index such that r corresponds to an element of $\mathrm{Hom}(L_i, \Omega)$ under the natural bijection

$$\mathrm{Hom}(F, \Omega)^2 \cong \mathrm{Hom}(F \otimes_{\mathbb{Q}} F, \Omega) \cong \bigsqcup_{i=1}^k \mathrm{Hom}(L_i, \Omega),$$

where the last union is disjoint. Let $f : F \to \bigoplus_{r\in R} L_{i(r)}$ be the $\mathbb{Q}$-linear map defined by

$$f(x)_r = p_{i(r)}\big(x \otimes 1 - \lambda_r(1 \otimes x)\big) \text{ for all } r \in R.$$

Then $F_{R,\lambda} = \ker f$.

Proof. Let $i \in \{1, \dots, k\}$ and $\varphi \in \mathrm{Hom}(L_i, \Omega)$ correspond to $(\sigma_1, \sigma_2) \in \mathrm{Hom}(F, \Omega)^2$. Then, for all $x \in F$, we have $\sigma_1(x) = \varphi(p_i(x \otimes 1))$ and $\sigma_2(x) = \varphi(p_i(1 \otimes x))$. Noting that φ is injective since L_i is a field, we obtain for every $\lambda \in \mathbb{Q}$ the equivalence

$$\sigma_1(x) = \lambda\sigma_2(x) \Leftrightarrow \varphi\left(p_i\big(x \otimes 1 - \lambda(1 \otimes x)\big)\right) = 0 \Leftrightarrow p_i\big(x \otimes 1 - \lambda(1 \otimes x)\big) = 0.$$

This proves the claim. □

The advantage of rewriting the equations this way is that instead of having conditions in Ω (which might be a field in which we cannot compute exactly such as $\Omega = \mathbb{C}$ or $\Omega = \overline{\mathbb{Q}}_p$), the conditions take place in the number fields L_i and f is a linear map between finite-dimensional $\mathbb{Q}$-vector spaces.

Remarks 27.

- There are obvious generalisations to conditions expressed with more than two embeddings, but they become more and more expensive as the number of embeddings increases; eventually one may have to compute the full Galois closure of F.
- The application to the maximal CM subfield can be generalized to other natural conditions, such as the maximal real subfield, the maximal subfield fixed by some ramification group, or the maximal subfield in which the residue degree of a certain prime divides a given integer.
- When $\lambda_r = 1$ for all $r \in R$, Proposition 26 expresses the subfields of interest as intersections of *principal subfields* in the terminology of van Hoeij, Klüners and Novocin [9].

4.3 Algorithms

Section 4.2 leads to the following algorithm to compute the maximal CM subfield.

Algorithm 28.

- Input: an irreducible monic $P \in \mathbb{Q}[X]$ representing $F = \mathbb{Q}[X]/(P(X))$.
- Output: an element $a \in F$ such that $\mathbb{Q}(a)$ is the maximal CM subfield of F, or $\perp$ if F does not contain a CM subfield.

1. Let $P(Y) = \prod_i Q_i(X, Y) \bmod P(X)$ be the irreducible factorization of P over F.
2. Let J be the set of indices i such that there exists a complex root α of P such that $Q_i(\alpha, \bar{\alpha}) = 0$.
3. Let $V \subset F$ be the $\mathbb{Q}$-subspace of $a(X) \bmod P(X)$ such that for all $i \in J$, $a(X) + a(Y) = 0 \bmod (P(X), Q_i(X, Y))$.
4. If $V = 0$, return $\perp$.
5. Let $a \in V$ be such that the minimal polynomial of a has degree $2 \dim_{\mathbb{Q}} V$. Return a.

Theorem 29. *Algorithm 28 is a deterministic polynomial-time algorithm that, given a number field F, computes the maximal CM subfield of F.*

Proof. Algorithm 28 is correct by Lemma 25 and Proposition 26 since $F \otimes_{\mathbb{Q}} F \cong \mathbb{Q}[X,Y]/(P(X),P(Y))$. It runs in polynomial time because factorization of polynomials over number fields can be performed in polynomial time [12]. □

We obtain the following algorithm to compute the group of almost-algebraic characters.

Algorithm 30.

- Input: a strongly computable number field F and a modulus $\mathfrak{m}$.
- Output: the group of almost-algebraic characters of modulus $\mathfrak{m}$.

1. Let K be the maximal CM subfield of F, as computed by Algorithm 28.
2. If $K = \perp$, return the group of finite order characters.
3. Let A, B be the matrices computed by Algorithm 18.
4. Let U be the subgroup described in Proposition 24.
5. Let C be the subgroup of the span of the row of B consisting of elements c such that $u \cdot c = 0$ for all $u \in U$.
6. Output C.

Theorem 31. *Algorithm 30 is correct. It is polynomial time, meaning a polynomial number of calls to the oracles with polynomial size input and a polynomial number of other operations.*

Proof. If F does not contain a CM subfield, then almost-algebraic characters are exactly finite order characters by the Artin–Weil theorem. The group U can be computed by linear algebra using the oracles. The group C can be computed by linear algebra over $\mathbb{Q}$ since all the inner products that occur are in $\mathbb{Z}$. The group C is the correct output by the Artin–Weil theorem and Lemma 21 in combination with Proposition 24. All operations not provided by the oracles or Theorem 29 can clearly be performed in polynomial time. □

5 Examples

We illustrate the interface of our Pari/GP package with a list of examples of mathematical interest.

5.1 Pari/GP interface

The gcharinit(F,m) function initializes a group structure gc from a number field F and a modulus $\mathfrak{m}$. The character group structure $\widehat{C_\mathfrak{m}} \cong \prod_{i=1}^k \mathbb{Z}/c_i\mathbb{Z} \times \mathbb{Z}^{n-1} \times \mathbb{R}$ is obtained via the vector gc.cyc $= [c_1, \dots c_k, 0, \dots, 0, 0.]$.

As an example,

```
> gc = gcharinit(x^2+23,3);
> gc.cyc
[6, 0, 0.E-57]
```

expresses the group of Hecke quasi-characters of modulus $\mathfrak{m} = (3)$ over $F = \mathbb{Q}(\sqrt{-23})$

$$\mathrm{Hom}_{\mathrm{cont}}(C_3, \mathbb{C}^\times) = \chi_3^{\mathbb{Z}/6\mathbb{Z}} \times \chi_{CM}^{\mathbb{Z}} \times \|\cdot\|^{\mathbb{C}},$$

where χ_3 is a character of the ray class group $\mathrm{Cl}_F(3)$ and χ_{CM} is an infinite order character of CM type.

Characters are described as columns of coordinates in this basis, and their evaluations are given in $\mathbb{R}/\mathbb{Z}$.

```
> chareval(gc,[1,0,0]~,idealprimedec(gc.nf,3)[1])
-1/3 \\ the prime above 3 is not principal
> gcharconductor(gc,[2,0,0]~)
[1, []] \\ a class group character
```

The maps $\mathcal{L}$ and $\mathcal{L}^*$ are accessible as gcharlog and gcharduallog. For example the character χ_{CM} has the following parameters in $(\mathbb{R}/\mathbb{Z})^2 \times \mathbb{R} \times \mathbb{Z} \times \mathbb{C}$.

```
> gcharduallog(gc,[0,1,0]~)
[0.11298866677205092301511538301498585720, 1/2, 0, 1, 0]
```

For closer scrutiny we retrieve the local characters of $\chi = \chi_{CM}\|\cdot\|$. In particular for a prime $\mathfrak{p}_3$ dividing the conductor $\mathfrak{m} = 3$ we obtain an idealstar character in addition to the exponent of $\chi(\mathfrak{p}_3)$.

```
> gcharlocal(gc,[0,1,1]~,1) \\ complex place
[1, -I] \\ k = 1, phi = -I
> gcharlocal(gc,[0,1,1]~,idealprimedec(gc.nf,3)[2],&grp)
[1, 0.1042940216...+ 0.1748495762...*I] \\ [grp char, expo]
> grp.cyc
[2] \\structure of (ZF/p3)^*
```

The interface gives a basis of the subgroup of algebraic characters. We can work with these characters via their type.

```
> Vec(gcharalgebraic(gc))
[[1, 0, 0]~, [0, 1, -1/2]~, [0, 0, -1]~]
> gcharisalgebraic(gc,[2,-3,5/2]~,&t); t
[[-1, -4]] \\ it has type (-1,-4)
> gcharalgebraic(gc,[[-1,2]]))
[[0,3,-1/2]~] \\ a character of type (-1,2)
```

The L-function machinery is readily accessible

```
> lfunzeros([gc,[1,3,0]~],5)
[2.34520501265099..., 3.90705697239550...]
> lfunan([gc,[0,3,-3/2]~],8)
[1, 4.795...*I, 2+4.795...*I, -15, 0, -23+9.591...*I, 0, -33.570...*I]
> [ algdep(an,2) | an <- % ] \\ check algebraicity
[x-1, x^2+23, x^2 - 4*x+27, x+15, x, x^2+46*x+621, x, x^2+1127]
```

5.2 Small degree examples

We describe explicitly the form taken by infinite order Hecke characters and our choice of basis for low degree fields.

We denote $z = (z_1, \dots, z_{r_1+r_2})$ the elements of $F_\mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. The characters of $(F_\mathbb{R}^\times)^\circ$ are of the form

$$\chi_\infty(z) = \prod_{j=1}^{r_1+r_2} |z_j|^{in_j\varphi_j} \prod_{j=r_1+1}^{r_1+r_2} \left(\frac{z_j}{|z_j|}\right)^{k_j}$$

and conversely, such a character χ_∞ can be extended to a global Hecke character if it is trivial on a finite index subgroup of $\mathbb{Z}_F^\times$.

Taking apart the norm character, we therefore consider the characters of

$$G_\infty^1 = (F_\mathbb{R}^\times)^\circ / (\mathbb{Z}_F^\times \cdot \mathbb{R}_{>0})$$

where $\mathbb{R}_{>0}$ is embedded diagonally. The group $\widehat{G_\infty^1}$ is free of rank $n-1$ and is a full rank lattice in the $\mathbb{Q}$-vector space of all possible parameters at infinity.

When F has class number one and totally positive fundamental units, $\widehat{G_\infty^1}$ is precisely the lattice of infinite order characters of modulus $\mathfrak{m} = 1$.

Example 32. For $F = \mathbb{Q}$, infinite order characters are powers of the norm, and finite order characters are Dirichlet characters.

Example 33 (real quadratic)**.** Let $F = \mathbb{Q}(\sqrt{D})$ be real quadratic with fundamental unit $\eta_1 > 1$ and regulator $R_F = \log(\eta_1)$. Then $\widehat{G_\infty^1}$ is generated by

$$\chi(z) = \left|\frac{z_1}{z_2}\right|^{i\frac{\pi}{R_F}}.$$

Example 34 (imaginary quadratic)**.** Let $F = \mathbb{Q}(\sqrt{D})$ be imaginary quadratic with torsion units of order m. Then $\widehat{G_\infty^1}$ is generated by

$$\chi(z) = \left(\frac{z_1}{|z_1|}\right)^m.$$

Example 35 (complex cubic)**.** Let F be complex cubic, and consider a fundamental unit whose complex embeddings are $e^{-\frac{R_F}{2}\pm 2i\pi\alpha}$, where $R_F > 0$ is the regulator and $\alpha \in \mathbb{R}/\mathbb{Z}$ is an angle.

Then $\widehat{G_\infty^1}$ is generated by

$$\chi_1(z) = \left|\frac{z_1}{z_2}\right|^{2i\pi\frac{2}{3R_F}}$$

and

$$\chi_2(z) = \left|\frac{z_1}{z_2}\right|^{-2i\pi\frac{4\alpha}{3R_F}}\left(\frac{z_2}{|z_2|}\right)^2.$$

Example 36 (real cubic)**.** Let F be real cubic, and $(\pm e^{\alpha_i})_i, (\pm e^{\beta_i})_i \in F_\mathbb{R}$ the embeddings of two fundamental units, so that the regulator is $R_F = |\alpha_1\beta_2 - \alpha_2\beta_1|$. Then $\widehat{G_\infty^1}$ is generated by

$$\chi_1(z) = |z_1|^{2i\pi\frac{\alpha_1+2\alpha_2}{3R_F}}|z_2|^{2i\pi\frac{-2\alpha_1-\alpha_2}{3R_F}}|z_3|^{2i\pi\frac{\alpha_1-\alpha_2}{3R_F}}$$

and

$$\chi_2(z) = |z_1|^{2i\pi\frac{\beta_1+2\beta_2}{3R_F}}|z_2|^{2i\pi\frac{-2\beta_1-\beta_2}{3R_F}}|z_3|^{2i\pi\frac{\beta_1-\beta_2}{3R_F}}.$$

5.3 Modular forms

By automorphic induction, Hecke characters of an extension F/K are expected to induce automorphic representations of $\mathrm{GL}_{[F:K]}$ over K. This is known in a number of cases. Here we provide some explicit examples for quadratic fields, where converse theorems prove the existence of a global automorphic form.

5.3.1 Classical forms over GL_2

Let $F = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field of discriminant $-D < 0$ and $k > 0$. To an algebraic character χ of type $(k, 0)$ and conductor $\mathfrak{m}$ we associate the q-series

$$f_\chi(z) = \sum_{(\mathfrak{a},\mathfrak{m})=1} \chi(\mathfrak{a}) q^{N(\mathfrak{a})}, q = e^{2i\pi z}, \mathrm{Im}(z) > 0$$

where the sum runs over integral ideals $\mathfrak{a}$ coprime to $\mathfrak{m}$.

Theorem 37 (Hecke, Weil, Shimura)**.** *Let χ be an algebraic character of type $(k, 0)$ and conductor $\mathfrak{m}$ over $F = \mathbb{Q}(\sqrt{-D})$, then*

$$f_\chi \in S_{k+1}(\Gamma_0(N, \psi_F \psi_\chi))$$

is a newform of weight $k + 1$, level $N = DN_{F/\mathbb{Q}}(\mathfrak{m})$ and character $\psi_F \psi_\chi$ where $\psi_F = \left(\frac{-D}{\cdot}\right)$ is the quadratic character of F and $\psi_\chi(a) = a^{-k}\chi((a))$ is the Dirichlet character of modulus $N_{F/\mathbb{Q}}(\mathfrak{m})$ attached to χ.

In the other direction, Ribet proved that all CM newforms come from Hecke characters [24, Theorem 4.5].

Example 38. Consider $F = \mathbb{Q}(\sqrt{-19})$ and $\mathfrak{m} = 3$. Up to integral powers of the norm, the algebraic characters are of the form $\chi_3^i \chi_\infty^k$ where χ_3 generates $\widehat{\mathrm{Cl}(\mathfrak{m})}$ and χ_∞ is trivial on $\mathrm{Cl}(\mathfrak{m})$ and of type $(2, 0)$. In Table 1 we list the first characters and the corresponding CM modular forms referenced in [13].

5.3.2 Maass waveforms

Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field of discriminant D and fundamental unit $\eta_1 > 1$, and χ_m a Hecke character of conductor $\mathfrak{m} = (\infty_1\infty_2)^\epsilon$ for $\epsilon \in \{0, 1\}$ whose restriction to $F_\mathbb{R}^\times$ is

$$\chi_m(z) = \mathrm{sgn}(z_1 z_2)^\epsilon \left|\frac{z_1}{z_2}\right|^{ir_m}, r_m = \frac{m\pi}{2\log(\eta_1)}.$$

where $\epsilon \equiv m \bmod 2$.

Again by converse theorems it corresponds to a CM Maass form [5, section 15.3.10].

Proposition 39. *Let $\cos^{(0)}(x) = \cos(x)$ and $\cos^{(-1)}(x) = \sin(x)$, and K_{ir} denote the modified Bessel function of the second kind of parameter ir. The function*

$$f(x + iy) = \sqrt{y} \sum_{\mathfrak{a}} \chi_m(\mathfrak{a}) K_{ir_m}(2\pi N(\mathfrak{a})y) \cos^{(-\epsilon)}(2\pi N(\mathfrak{a})x) \qquad (9)$$

is a cusp form of weight 0 and character ψ_F on $\Gamma_0(D)$ with Laplace eigenvalues $\lambda_m = \frac{1}{4} + r_m^2$, where $\psi_F = \left(\frac{D}{\cdot}\right)$ is the quadratic character of F.

(i,k)	character	modular form	first zero
$(1,0)$	`[1,0,0]`	`171.1.c.a.37.1`	2.55662379...
$(2,0)$	`[2,0,0]`	Dirichlet `57.56`	2.40313422...
$(3,0)$	`[3,0,0]`	`171.1.c.a.37.1`	2.55662379...
$(0,1)$	`[0,-1,-1/2]`	`171.2.d.a.170.3`	1.19761556...
$(1,1)$	`[1,-1,-1/2]`	`171.2.d.a.170.1`	3.03101717...
$(2,1)$	`[2,-1,-1/2]`	`171.2.d.a.170.2`	2.19220898...
$(3,1)$	`[3,-1,-1/2]`	`171.2.d.a.170.4`	0.57935987...
$(0,2)$	`[0,-2,-1]`	`171.3.c.d.37.2`	1.76815328...
$(1,2)$	`[1,-2,-1]`	`171.3.c.a.37.1`	1.84559250...
$(2,2)$	`[2,-2,-1]`	`171.3.c.d.37.1`	1.54865425...
$(3,2)$	`[3,-2,-1]`	`19.3.b.a.18.1`	3.78194741...
$(0,3)$	`[0,-3,-3/2]`	`171.4.d.a.170.4`	1.59003776...
$(1,3)$	`[1,-3,-3/2]`	`171.4.d.a.170.3`	1.36085197...
$(2,3)$	`[2,-3,-3/2]`	`171.4.d.a.170.1`	0.08123213...
$(3,3)$	`[3,-3,-3/2]`	`171.4.d.a.170.2`	0.70404412...

Table 1: Some modular forms with CM by $\mathbb{Q}(\sqrt{-19})$

Example 40. Let $F=\mathbb{Q}(\sqrt{5})$, this field has trivial class group and fundamental unit $\eta=\frac{1+\sqrt{5}}{2}$. The character χ_m above is an actual Hecke character of modulus $\mathfrak{m}=(\infty_1\infty_2)^\epsilon$. Using the L-function facilities in Pari/GP we compute the first zero $0<\gamma_1$ such that $L(\chi_m,\frac{1}{2}+i\gamma_1)=0$. Results are shown in Table 2.

Note that we obtain arbitrary large imaginary spectral parameters: this raises computational issues on the L-function side which are currently not addressed in Pari/GP. See [1] for the case of degree 2 Maass forms.

5.4 CM abelian varieties

In this section we give examples of CM abelian varieties and the corresponding algebraic Hecke characters. We insist on proving equalities of L-functions rather than observing a numerical coincidence, as this is possible thanks to CM theory. For the general terminology of CM theory, we refer to [11, 16]. The following is a special case of [11, Chapter 4 Theorem 6.2].

Theorem 41 (Shimura [26], Milne [17])**.** *Let $A/\mathbb{Q}$ be a simple abelian variety of dimension g. Let K be a CM field of degree $2g$ and $\iota\colon K\to\mathrm{End}^0(A)$ an embedding, and let Φ be the corresponding CM type on K. Let F be the field of definition of $\iota(K)$, and let Φ^* be the dual type on F. Then $F/\mathbb{Q}$ is Galois; let $G=\mathrm{Gal}(F/\mathbb{Q})$. Let π be the injective morphism $\pi\colon G\to\mathrm{Aut}(K)$ such that $\iota(\lambda)^\sigma=\iota(\lambda^{\pi(\sigma)})$ for all $\lambda\in K$ and $\sigma\in G$. Then there exists an algebraic*

m	$r_m = \frac{\pi m}{2\log(\eta_1)}$	first zero
1	3.2642513026 ...	7.4947673145 ...
2	6.5285026053 ...	1.9926333454 ...
3	9.7927539079 ...	1.3437292832 ...
4	13.0570052105 ...	1.3684744255 ...
5	16.3212565132 ...	0.9723034858 ...
6	19.5855078158 ...	1.2974789657 ...
7	22.8497591185 ...	0.7849215584 ...
8	26.1140104211 ...	1.1328362023 ...
9	29.3782617237 ...	0.8591419101 ...
10	32.6425130264 ...	0.8952928125 ...
11	35.9067643290 ...	0.7861064128 ...
12	39.1710156316 ...	1.1315449163 ...
13	42.4352669343 ...	0.5067080421 ...
14	45.6995182369 ...	0.9758042566 ...
15	48.9637695395 ...	0.8620736129 ...

Table 2: First zero of Maass form L-functions of real quadratic field $\mathbb{Q}(\sqrt{5})$.

Hecke character χ over F of type Φ^* and valued in K such that

$$L(A, s) = \prod_{\tau \in \mathrm{Hom}(K,\mathbb{C})/\pi(G)} L(\chi^\tau, s).$$

Example 42. Let A be the Jacobian of the genus 2 curve `28561.a.371293.1` [14]

$$y^2 + x^3 y = -2x^4 - 2x^3 + 2x^2 + 3x - 2.$$

Let $K = \mathbb{Q}[x]/(x^4 - x^3 + 2x^2 + 4x + 3) = \mathbb{Q}(\alpha)$ be the unique degree 4 subfield of $\mathbb{Q}(\zeta_{13})$. The surface A is simple, has CM by K, and all endomorphisms of A are defined over K: we have $F = K$ in the notation of Theorem 41. Since $K/\mathbb{Q}$ is Galois, $\pi(G)$ acts transitively on $\mathrm{Hom}(K, \mathbb{C})$. All CM types of K are in the same Galois orbit; let $\Phi^* = \{\alpha \mapsto -0.65\ldots + 0.52\ldots i, \alpha \mapsto 1.15\ldots + 1.72\ldots i\}$. By Theorem 41, there exists an algebraic Hecke character χ of K of type Φ^* such that

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

The conductor of A is $28561 = 13^4$, and the discriminant of K is $2197 = 13^3$. Moreover, K has a unique prime $\mathfrak{p}$ above 13, so the conductor of χ must be $\mathfrak{p}$.

Using our implementation we compute the group of characters of modulus $\mathfrak{p}$. The subgroup of finite order characters has order 3, and there exists an algebraic character, unique up to multiplication by a finite order character, of type Φ^*. Among the three characters of this type, two have a non real

L-function coefficient a_3, and therefore cannot be χ. So χ is the remaining one, which is uniquely characterised by its type and the approximate value

$$\chi(\mathfrak{q}) = -1.65138\ldots - 0.52241\ldots i$$

where $\mathfrak{q} = (3, \alpha)$ (label `3.1` as defined in [6]). The restriction of χ to $(\mathbb{Z}_K/\mathfrak{p})^\times$ has order 2. The values of χ at some prime ideals are given in Table 3.

prime $\mathfrak{r}$	$\chi(\mathfrak{r}) \in \mathbb{C}$	$\chi(\mathfrak{r}) \in K$
`3.1`	$-1.65138\ldots - 0.52241\ldots i$	$-\frac{1}{3}\alpha^3 - \frac{2}{3}\alpha - 2$
`3.2`	$0.15138\ldots - 1.72542\ldots i$	$-\frac{1}{3}\alpha^3 + \alpha^2 - \frac{5}{3}\alpha - 1$
`3.3`	$-1.65138\ldots + 0.52241\ldots i$	$\alpha - 1$
`3.4`	$0.15138\ldots + 1.72542\ldots i$	$\frac{2}{3}\alpha^3 - \alpha^2 + \frac{4}{3}\alpha + 1$
`13.1`	$\pm 3.60555\ldots$	$\pm\sqrt{13} = \pm(\frac{2}{3}\alpha^3 - \frac{2}{3}\alpha + 3)$
`16.1`	-4	-4
`29.1`	$-3.45416\ldots - 4.13143\ldots i$	$-\frac{5}{3}\alpha^3 + 3\alpha^2 - \frac{7}{3}\alpha - 5$
`29.2`	$1.95416\ldots + 5.01809\ldots i$	$2\alpha^3 - 2\alpha^2 + 5\alpha + 5$
`29.3`	$-3.45416\ldots + 4.13143\ldots i$	$\frac{2}{3}\alpha^3 - 3\alpha^2 + \frac{10}{3}\alpha - 1$
`29.4`	$1.95416\ldots - 5.01809\ldots i$	$-\alpha^3 + 2\alpha^2 - 6\alpha - 2$

Table 3: Values of the algebraic character χ attached to an abelian surface

Example 43. Let A be the Jacobian of the genus 3 curve `3.9-1.0.3-9-9.6` [15]

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

Let $K = \mathbb{Q}(\zeta_9)$. The curve C has an automorphism of order 9, defined over K and given by $(x, y) \mapsto (\zeta_9^3 x, \zeta_9 y)$. In particular, the threefold A has CM by K defined over K. By point counting, the Euler polynomial of A at $p = 7$ is

$$1 + pT^3 + p^3T^6,$$

which is irreducible over $\mathbb{Q}$, proving that A is simple. Since $K/\mathbb{Q}$ is Galois, $\pi(G)$ acts transitively on $\mathrm{Hom}(K, \mathbb{C})$ in the notations of Theorem 41. There are two Galois orbits of CM types on K: one lifted from the CM subfield $\mathbb{Q}(\zeta_3) \subset K$, and a primitive one. Let $\Phi^* = \{\zeta_9 \mapsto \exp(2i\pi\frac{4}{9}), \zeta_9 \mapsto \exp(2i\pi\frac{1}{9}), \zeta_9 \mapsto \exp(2i\pi\frac{2}{9})\}$, which is primitive. By Theorem 41, there exists an algebraic Hecke character χ of K of type Φ^* with values in K such that

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

Let $\mathfrak{p}$ be the unique prime of K above 3. By computing resultants we see that A has good reduction away from 3. In particular χ has conductor a power of $\mathfrak{p}$, say $\mathfrak{p}^m$. The restriction of χ to $(\mathbb{Z}_K/\mathfrak{p}^m)^\times$ has finite order and takes values in K, and therefore has order dividing 18. By studying the 3-adic convergence of $(1+x)^{1/18}$ we see that $1+\mathfrak{p}^{16} \subset (K_\mathfrak{p}^\times)^{18}$ and in particular we have $m \leq 16$. Alternatively, we could bound m by using the reduction theory of Picard curves [2], but the above method works in cases where no reduction theory is available.

prime $\mathfrak{r}$	$\chi(\mathfrak{r}) \in \mathbb{C}$	$\chi(\mathfrak{r}) \in K$
3.1	$\langle \exp(\frac{i\pi}{9}) \rangle 1.73205\ldots i$	$\langle -\zeta_9 \rangle \sqrt{-3} = \langle -\zeta_9 \rangle (1 + 2\zeta_9^3)$
19.1	$4.34002\ldots + 0.40522\ldots i$	$2\zeta_9^5 + 2\zeta_9^4 + 2\zeta_9^3 + \zeta_9^2 - 2\zeta_9 + 2$
19.2	$-4.11721\ldots + 1.43128\ldots i$	$-\zeta_9^5 + 2\zeta_9^4 + 2\zeta_9^3 - 2\zeta_9^2 + 4\zeta_9 + 2$
19.3	$4.34002\ldots - 0.40522\ldots i$	$4\zeta_9^5 + \zeta_9^4 - 2\zeta_9^3 + 2\zeta_9^2 - \zeta_9$
19.4	$-4.11721\ldots - 1.43128\ldots i$	$-2\zeta_9^5 + \zeta_9^4 - 2\zeta_9^3 - 4\zeta_9^2 + 2\zeta_9$
19.5	$2.77718\ldots + 3.35964\ldots i$	$-\zeta_9^5 - 4\zeta_9^4 + 2\zeta_9^3 + \zeta_9^2 - 2\zeta_9 + 2$
19.6	$2.77718\ldots - 3.35964\ldots i$	$-2\zeta_9^5 - 2\zeta_9^4 - 2\zeta_9^3 + 2\zeta_9^2 - \zeta_9$
37.1	$4.34002\ldots - 4.26194\ldots i$	$4\zeta_9^5 + 4\zeta_9^4 - 2\zeta_9^3 + 5\zeta_9^2 + 2\zeta_9$
37.2	$2.77718\ldots - 5.41176\ldots i$	$-5\zeta_9^5 - 2\zeta_9^4 - 2\zeta_9^3 - \zeta_9^2 - 4\zeta_9$
37.3	$-4.11721\ldots - 4.47756\ldots i$	$-4\zeta_9^5 + 5\zeta_9^4 + 2\zeta_9^3 - 2\zeta_9^2 + 4\zeta_9 + 2$
37.4	$4.34002\ldots + 4.26194\ldots i$	$2\zeta_9^5 - \zeta_9^4 + 2\zeta_9^3 - 2\zeta_9^2 - 5\zeta_9 + 2$
37.5	$2.77718\ldots + 5.41176\ldots i$	$2\zeta_9^5 - 4\zeta_9^4 + 2\zeta_9^3 + 4\zeta_9^2 + \zeta_9 + 2$
37.6	$-4.11721\ldots + 4.47756\ldots i$	$\zeta_9^5 - 2\zeta_9^4 - 2\zeta_9^3 - 4\zeta_9^2 + 2\zeta_9$
64.1	-8	-8

Table 4: Values of the algebraic character χ attached to an abelian threefold

Using our implementation we compute the group of characters of modulus $\mathfrak{p}^{16}$. The subgroup of finite order characters is isomorphic to C_9^4. There exists an algebraic character of type Φ^*, unique up to multiplication by a finite order character. Out of these $9^4 = 6561$ candidate characters, checking that the value of a_{19} is sufficiently close to the value for A, namely $a_{19}(A) = 6$, eliminates all but 2 candidates. Checking that the value of a_{109} is sufficiently close to $a_{109}(A) = -21$ leaves only one remaining candidate, which must therefore be χ. The conductor of χ is $\mathfrak{p}^4$ and χ is in fact the unique algebraic character of type Φ^* and conductor $\mathfrak{p}^4$, and the restriction of χ to $(\mathbb{Z}_K/\mathfrak{p}^4)^\times$ has order 18. The values of χ at some prime ideals [2] are given in Table 4.

5.5 Density of gamma shifts

The spectral parameters of an L-function are the gamma shifts μ_j appearing in the gamma factor

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

[2]Labels are as in [6] but with respect to the cyclotomic polynomial Φ_9, which is not the `polredabs` polynomial.

of its normalized functional equation $\Lambda(s) = \epsilon\overline{\Lambda}(1-s)$. In this setting, the real parts $\mathrm{Re}(\mu_j)_{j\le r_1}$ and $\mathrm{Re}(2\mu_j)_{j>r_1}$ are expected to be integers, whereas the imaginary parts can be arbitrary transcendentals subject to $\sum_{j=1}^{r_1}\mu_j + \sum_{j=r_1+1}^{r_1+r_2} 2\mu_j \in \mathbb{R}$.

As a matter of fact, Hecke characters allow us to attain a dense subspace of these possible gamma shifts. The following statement must be well-known but we could not find a reference for it.

Proposition 44. *Let $r_1, r_2 \ge 0$ and $(\mu_j) \in (\{0,1\} + i\mathbb{R})^{r_1} \times (\frac{1}{2}\mathbb{Z} + i\mathbb{R})^{r_2}$ a family of spectral parameters such that $\sum_{j\le r_1}\mu_j + 2\sum_{j>r_1}\mu_j \in \mathbb{R}$.*

Then for every number field F of signature (r_1, r_2) and every $\epsilon > 0$, there exists a Hecke character χ of F whose L-function gamma shifts $\mu_j(\chi)$ satisfy

$$|\mu_j(\chi) - \mu_j| < \epsilon.$$

Proof. Let F be a number field of signature (r_1, r_2). For every modulus $\mathfrak{m}$, let $G_{\mathfrak{m}} \subset \widehat{F_{\mathbb{R}}^\times}$ be the image of the map $\widehat{C}_{\mathfrak{m}} \to \widehat{F_{\mathbb{R}}^\times}$, that is, the group of infinity-types of characters of modulus $\mathfrak{m}$. The group $G_{\mathfrak{m}}$ is the group of elements $\chi \in \widehat{F_{\mathbb{R}}^\times}$ such that $\chi(u) = 1$ for all $u \in \mathbb{Z}_F^\times(\mathfrak{m}) = \ker(\mathbb{Z}_F^\times \to (\mathbb{Z}_F/\mathfrak{m})^\times)$.

Let $M > 0$ be an integer. By the congruence subgroup property for unit groups of number fields [3, Théorème 1], there exists a modulus $\mathfrak{m}$ such that $\mathbb{Z}_F^\times(\mathfrak{m}) \subset (\mathbb{Z}_F^\times)^M$. In particular, we get that

$$\left\{\chi \in \widehat{F_{\mathbb{R}}^\times} \mid \chi^M \in G_1\right\} \subset G_{\mathfrak{m}}.$$

Since the image of G_1 in $\mathbb{R}^{r_1+r_2} \times \mathbb{Z}^{r_2}$ has full rank, this proves that $\bigcup_{\mathfrak{m}} G_{\mathfrak{m}}$ is dense in $\widehat{F_{\mathbb{R}}^\times}$, which implies the claim. $\square$

This makes Hecke characters good test cases for L-functions software, since their coefficients are relatively easy to compute, compared to other transcendental automorphic forms.

Example 45. We exhibit a character of conductor 2^{20} over the real cubic field $F = \mathbb{Q}[x]/(x^3 - 3x + 1)$ whose parameters φ_1 and φ_2 approximate the constants π and e to 5 digits.

```
> g=gcharinit(x^3-3*x+1,2^20); chi = [0,-2033118, 694865]~;
> gcharlocal(g,chi,1)
[0, 3.1415922385511383833775758885544915179]
> gcharlocal(g,chi,2)
[0, 2.7182831477529933175766620889117919084]
```

5.6 Partially algebraic Hecke characters

In view of the special role played by algebraic Hecke characters, it is natural to ask whether there exists partially algebraic Hecke characters, that is, characters such that $\varphi_\sigma = 0$ for some σ but not all [3]. We provide a construction of such characters.

Proposition 46. *Assume F is a quadratic extension of another number field F_0. Let R be the set of real places of F_0 that become complex in F, and let n_0 be the degree of F_0. Then for every modulus $\mathfrak{m}$ of F, there exists a subgroup H of $\widehat{C}_\mathfrak{m}$ of rank n_0 in which every character satisfies $\varphi_\sigma = 0$ for every $\sigma \in R$.*

Proof. It suffices to prove the statement for the modulus $\mathfrak{m} = 1$. Let g be the nontrivial element of $\mathrm{Gal}(F/F_0)$, which acts on $\widehat{C_1}$. Let H be the subgroup of $\chi \in \widehat{C_1}$ such that there exists a finite order $\xi \in \widehat{C_1}$ with $\chi^g = \xi\chi^{-1}$. We have $\mathrm{rk}(\widehat{C_1^1(F)}) = n - 1 = 2n_0 - 1$ and $\mathrm{rk}(\widehat{C_1(F_0)}) = n_0 - 1$ (as is well-known but also easily seen from Proposition 14), so the rank of H is exactly n_0. Moreover, for every infinite place σ of F, every element of H satisfies $\varphi_{\sigma\circ g} = -\varphi_\sigma$. In particular for $\sigma \in R$ this means that $\varphi_\sigma = 0$. □

Corollary 47. *Under the same hypotheses as Proposition 46, let $r = 0$ if F does not contain a CM subfield and r be the degree of the maximal real subfield of F otherwise. Then for every modulus $\mathfrak{m}$ of F, there exists a subgroup H of $\widehat{C}_\mathfrak{m}$ of rank $n_0 - r$ in which every character satisfies $\varphi_\sigma = 0$ for every $\sigma \in R$ and such that H contains no nonzero almost-algebraic character. In particular, if F is not CM then there exists a partially algebraic character over F.*

Proof. The integer r is the rank of the group of almost-algebraic characters. □

Example 48. 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]
```

[3] See https://mathoverflow.net/questions/310706/are-there-partially-algebraic-hecke-characters

The character χ satisfies

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

and is therefore an example of a partially algebraic character. Since $n_0 = 2$ there is another independent partially algebraic character (namely `[0,1,0]~`).

In a general number field F, if one fixes a set of infinite places Σ, a natural question is to determine the group of Σ-*algebraic* characters, i.e. characters such that $\varphi_\sigma = 0$ for every $\sigma \in \Sigma$. The field F contains a maximal subfield K_0 that is real at places below Σ, and may contain a quadratic extension K of K_0 in which all places below Σ are complex. When this is the case, one obtains a corresponding group of Σ-algebraic characters. Does this constuction account for all the possible infinity types? Unlike the algebraic case where Galois theory is sufficient to obtain a complete characterisation, the general case seems to involve transcendence problems.

By automorphic induction to GL_2, partially algebraic characters yield automorphic representations that are non-algebraic principal series at some infinite places and discrete series at other ones. Analogously to [21], one may ask to explicitly construct such "partial Maass forms" that do not come from Hecke characters. A possible way of doing this would be to compute Maass forms on a well-chosen quaternion algebra and to use the Jacquet–Langlands correspondence.

5.7 Twists and special values

Another interesting use of Hecke characters is to twist other L-functions to obtain new ones.

Let E/F an elliptic curve over an imaginary quadratic field F, and χ an algebraic Hecke character of type (a,b) and conductor $\mathfrak{f}$ over F.

Assume $\gcd(\mathfrak{f}, N_{E/F}) = 1$, then the twist

$$L(E \otimes \chi, s) = \sum_{(\mathfrak{n},\mathfrak{f})=1} a_{\mathfrak{n}}(E)\chi(\mathfrak{n})N(\mathfrak{n})^{-s}$$

satisfies

$$\Lambda(E \otimes \chi, s) = W\Lambda(E \otimes \overline{\chi}, 1 + a + b - s)$$

where

$$\Lambda(E\otimes\chi, s) = (N(\mathfrak{f})^2 N_{E/F})^{\frac{s}{2}}\Gamma_{\mathbb{C}}(s-\min(a,b))\Gamma_{\mathbb{C}}(s-\min(a,b)-\mathbb{1}_{a\neq b})L(E\otimes\chi, s).$$

Example 49. Let $F = \mathbb{Q}(\sqrt{-43})$, E/F the curve `43.1.a.1` of equation $y^2 + y = x^3 + x^2$, and χ the character of conductor 1 and type $(-2, 2)$.

We check numerically the equality of special value predicted by Deligne's period conjecture [7]

$$\begin{aligned} L(E\otimes\chi,1) &\approx 2.996120826544463\ldots \\ &\approx \frac{2\pi}{\sqrt{43}^5}\Omega_F^8, \text{ where } \Omega_F = \sqrt{\prod_{a=1}^{42}\Gamma(\frac{a}{43})^{(\frac{-43}{a})}}. \end{aligned}$$

References

[1] Andrew R. Booker and Holger Then. "Rapid computation of L-functions attached to Maass forms". In: *Int. J. Number Theory* 14.5 (2018), pp. 1459–1485. ISSN: 1793-0421. DOI: 10.1142/S1793042118500896. URL: https://doi.org/10.1142/S1793042118500896.

[2] Irene I. Bouw, Angelos Koutsianas, Jeroen Sijsling, and Stefan Wewers. "Conductor and discriminant of Picard curves". In: *J. Lond. Math. Soc. (2)* 102.1 (2020), pp. 368–404. ISSN: 0024-6107. DOI: 10.1112/jlms.12323. URL: https://doi.org/10.1112/jlms.12323.

[3] Claude Chevalley. "Deux théorèmes d'arithmétique". In: *J. Math. Soc. Japan* 3 (1951), pp. 36–44. ISSN: 0025-5645. DOI: 10.2969/jmsj/00310036. URL: https://doi.org/10.2969/jmsj/00310036.

[4] Henri Cohen. *Advanced topics in computational number theory.* Vol. 193. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. xvi+578. ISBN: 0-387-98727-4. DOI: 10.1007/978-1-4419-8489-0. URL: https://doi.org/10.1007/978-1-4419-8489-0.

[5] Henri Cohen and Fredrik Strömberg. *Modular forms.* Vol. 179. Graduate Studies in Mathematics. A classical approach. American Mathematical Society, Providence, RI, 2017, pp. xii+700. ISBN: 978-0-8218-4947-7. DOI: 10.1090/gsm/179. URL: https://doi.org/10.1090/gsm/179.

[6] John Cremona, Aurel Page, and Andrew V. Sutherland. *Sorting and labelling integral ideals in a number field.* 2020. arXiv: 2005.09491 [math.NT].

[7] Pierre Deligne. *Valeurs de fonctions L et périodes d'intégrales.* French. Automorphic forms, representations and L-functions, Proc. Symp. Pure Math. Am. Math. Soc., Corvallis/Oregon 1977, Proc. Symp. Pure Math. 33, No. 2, 313-346 (1979). 1979.

[8] Erich Hecke. *Mathematische Werke.* Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen. Vandenhoeck & Ruprecht, Göttingen, 1959, 955 pp. (1 plate).

[9] Mark van Hoeij, Jürgen Klüners, and Andrew Novocin. "Generating subfields". In: *J. Symbolic Comput.* 52 (2013), pp. 17–34. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2012.05.010. URL: https://doi.org/10.1016/j.jsc.2012.05.010.

[10] Serge Lang. *Algebraic number theory.* Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+357. ISBN: 0-387-94225-4. DOI: 10.1007/978-1-4612-0853-2. URL: https://doi.org/10.1007/978-1-4612-0853-2.

[11] Serge Lang. *Complex multiplication.* Vol. 255. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, New York, 1983, pp. viii+184. ISBN: 0-387-90786-6. DOI: 10.1007/978-1-4612-5485-0. URL: https://doi.org/10.1007/978-1-4612-5485-0.

[12] A. K. Lenstra. "Factoring polynomials over algebraic number fields". In: *Computer algebra (London, 1983).* Vol. 162. Lecture Notes in Comput. Sci. Springer, Berlin, 1983, pp. 245–254. DOI: 10.1007/3-540-12868-9_108. URL: https://doi.org/10.1007/3-540-12868-9_108.

[13] The LMFDB Collaboration. *The L-functions and modular forms database, Home page of classical modular forms.* https://www.lmfdb.org/ModularForm/GL2/Q/holomorphic/. [Online; accessed 21 February 2022]. 2022.

[14] The LMFDB Collaboration. *The L-functions and modular forms database, Home page of the genus 2 curve 28561.a.371293.1.* https://www.lmfdb.org/Genus2Curve/Q/28561/a/371293/1. [Online; accessed 21 February 2022]. 2022.

[15] The LMFDB Collaboration. *The L-functions and modular forms database, Home page of the genus 3 curve 3.9-1.0.3-9-9.6.* https://www.lmfdb.org/HigherGenus/C/Aut/3.9-1.0.3-9-9.6. [Online; accessed 21 February 2022]. 2022.

[16] J. S. Milne. *Complex multiplication.* https://www.jmilne.org/math/CourseNotes/cm.html. [Online; accessed 21 February 2022]. 2020.

[17] J. S. Milne. "On the arithmetic of abelian varieties". In: *Invent. Math.* 17 (1972), pp. 177–190. ISSN: 0020-9910. DOI: 10.1007/BF01425446. URL: https://doi.org/10.1007/BF01425446.

[18] Pascal Molin and Aurel Page. *Hecke Grossencharacters support.* Version 2.14.0. 2022. URL: https://pari.math.u-bordeaux.fr/dochtml/html/General_number_fields.html#gcharinit.

[19] Sidney A. Morris. "Duality and structure of locally compact abelian groups... for the layman". In: *Math. Chronicle* 8 (1979), pp. 39–56. ISSN: 0581-1155.

[20] Sidney A. Morris. *Pontryagin duality and the structure of locally compact abelian groups*. London Mathematical Society Lecture Note Series, No. 29. Cambridge University Press, Cambridge-New York-Melbourne, 1977, pp. viii+128.

[21] Richard A. Moy and Joel Specter. "There exist non-CM Hilbert modular forms of partial weight 1". In: *Int. Math. Res. Not. IMRN* 24 (2015), pp. 13047–13061. ISSN: 1073-7928. DOI: 10.1093/imrn/rnv089. URL: https://doi.org/10.1093/imrn/rnv089.

[22] *PARI/GP version 2.14.0*. available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2022.

[23] Stefan Patrikis. "Variations on a theorem of Tate". In: *Mem. Amer. Math. Soc.* 258.1238 (2019), pp. viii+156. ISSN: 0065-9266. DOI: 10.1090/memo/1238. URL: https://doi.org/10.1090/memo/1238.

[24] Kenneth A. Ribet. "Galois representations attached to eigenforms with Nebentypus". In: *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*. 1977, 17–51. Lecture Notes in Math., Vol. 601.

[25] Norbert Schappacher. *Periods of Hecke characters*. Vol. 1301. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1988, pp. xvi+160. ISBN: 3-540-18915-7. DOI: 10.1007/BFb0082094. URL: https://doi.org/10.1007/BFb0082094.

[26] Goro Shimura. "On the zeta-function of an abelian variety with complex multiplication". In: *Ann. of Math. (2)* 94 (1971), pp. 504–533. ISSN: 0003-486X. DOI: 10.2307/1970768. URL: https://doi.org/10.2307/1970768.

[27] Yutaka Taniyama. "L-functions of number fields and zeta functions of abelian varieties". In: *J. Math. Soc. Japan* 9 (1957), pp. 330–366. ISSN: 0025-5645. DOI: 10.2969/jmsj/00930330. URL: https://doi.org/10.2969/jmsj/00930330.

[28] J. T. Tate. "Fourier analysis in number fields, and Hecke's zeta-functions". In: *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*. Thompson, Washington, D.C., 1967, pp. 305–347.

[29] Michel Waldschmidt. "Sur certains caractères du groupe des classes d'idèles d'un corps de nombres". In: *Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981)*. Vol. 22. Progr. Math. Birkhäuser Boston, Boston, MA, 1982, pp. 323–335.

[30] Mark Watkins. "Computing with Hecke Grössencharacters". In: *Actes de la Conférence "Théorie des Nombres et Applications"*. Vol. 2011. Publ. Math. Besançon Algèbre Théorie Nr. Presses Univ. Franche-Comté, Besançon, 2011, pp. 119–135.

[31] André Weil. "On a certain type of characters of the idèle-class group of an algebraic number-field". In: *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*. Science Council of Japan, Tokyo, 1956, pp. 1–7.

[32] André Weil. "Sur la théorie du corps de classes". In: *J. Math. Soc. Japan* 3 (1951), pp. 1–35. ISSN: 0025-5645. DOI: 10.2969/jmsj/00310001. URL: https://doi.org/10.2969/jmsj/00310001.