CM-values of p-adic Theta-functions

Daas, M.A.

Citation

Daas, M. A. (2024, October 30). *CM-values of p-adic Theta-functions*. Retrieved from https://hdl.handle.net/1887/4106986

CM-values of p-adic Θ-functions

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr.ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op woensdag 30 oktober 2024
klokke 16:00 uur

door

Michael Alexander Daas
geboren te Zaandijk, Nederland
in 1997

Promotores:

Prof. dr. J. B. Vonk

Prof. dr. P. Stevenhagen

Promotiecommissie:

Prof. dr. ir. G. L. A. Derks	
Prof. dr. D. S. T. Holmes	
Prof. dr. P. Charollois	(Sorbonne Université)
Prof. dr. H. Darmon	(McGill University)
Dr. A. Pozzi	(University of Bristol)

Publications and preprints

Parts of this thesis are based on the following paper:

Michael A. Daas. CM-values of p-adic Θ-functions. *arXiv preprint arXiv:2309.17251*, 2023

Contents

A guide to notation

Keeping track of notation in a long text on mathematics can be a daunting task for a reader of any level of mathematical experience. Especially when proofs become increasingly technical with many moving parts and auxilliary variables, maps and objects, it is very easy to lose track of every little bit of notation that was introduced beforehand. Even though the author likes to convince himself that every reader will carefully go through their work from start to finish, reading every page with equal interest and energy, reality is often different, and skipping certain proofs, sections or chapters is a common cause for confusion about notation.

For this reason, this thesis aims to approach the problem of identifying missing pieces of notation in a very systematic manner that should, if executed without error by the author, in principle allow one to get a hold of notation after checking only a few easy to locate places in the thesis, without having to skim many pages of mathematics, tracking down the seemingly first instance of a certain symbol.

If in any instance while perusing this thesis, a certain piece of notation is used, you should find its meaning in a finite number of quick steps:

- It could be that the notation is introduced *earlier in the proof* you are reading; this happens for example with dummy variables used in some matrix manipulations.

- If not, then it is possible that this notation is either introduced or repeated from earlier sections *at the very start of the current section*; this happens for example when notation from a previous section is carried over to the next and is thus repeated for the reader's convenience.

- If not, then it is possible that this notation is either introduced or repeated from earlier chapters *at the very start of the current chapter*; this happens for example when specific objects from the main results from earlier chapters are used again in the present chapter.

- If not, then the notation is *introduced below*; this is the case for some of the most fundamental pieces of notation that will be used many times throughout the entire thesis.

If any instance of notation fails to be tracked down after following the steps outlined above, the author would be happy to receive their well-deserved reprimand through any medium of the reader's preference.

The relevant fields

As is standard, we let $\mathbb{Z}$ denote the integers and $\mathbb{N} := \mathbb{Z}_{\geq 1}$ the positive integers. Next, we let $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the fields of rationals, reals and complex numbers respectively. Furthermore, $\mathcal{H} \subset \mathbb{C}$ denotes the complex upper half plane $\mathcal{H} := \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}$. For any field M, we let $\overline{M}$ be an algebraic closure of M and we let $G_M := \mathrm{Gal}(\overline{M}/M)$ denote its absolute Galois group.

If M is a number field, then $\mathcal{O}_M$ denotes its ring of integers and $\mathrm{Pic}(M)$ the ideal class group of the maximal order $\mathcal{O}_M$. Furthermore, we let H_M denote the Hilbert class field of M, so that the Artin map yields an isomorphism $\mathrm{Pic}(M) \xrightarrow{\sim} \mathrm{Gal}(H_M/M)$.

For any rational prime p, by $\mathbb{Q}_p$ we will mean the field of p-adic numbers. Let $\mathbb{C}_p$ be a completion of $\overline{\mathbb{Q}}_p$. We may now define the *p-adic upper half plane* as

$$\mathcal{H}_p := \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p),$$

where $\mathbb{P}^1(-)$ denotes the projective line over the field considered. For any number field M and rational prime ℓ, we define $M_\ell := M \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

Throughout this thesis, we specify two *coprime* fundamental discriminants $D_1, D_2 < 0$. Write $K_i := \mathbb{Q}(\sqrt{D_i})$ for $i \in \{1, 2\}$ with rings of integers $\mathcal{O}_1$ and $\mathcal{O}_2$ and Hilbert class fields H_1 and H_2 respectively. We write $w_i := \#\mathcal{O}_i^\times$ for $i \in \{1, 2\}$ and let $D := D_1 D_2 > 0$. Next, we let $F := \mathbb{Q}(\sqrt{D})$ be the real quadratic field and $L := \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ be the biquadratic field completing the following field diagram:

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[d, dash, "\chi"] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & F \arrow[d, dash] & K_2 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Explicitly, we will denote the elements of these Galois groups by

$$\mathrm{Gal}(F/\mathbb{Q}) = \{1, \sigma\} \quad \text{and} \quad \mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_F\},$$

where σ_1, σ_2 and σ_F are all involutions with fixed fields K_1, K_2 and F respectively.

For any subset $S \subset F$, we let $S^+ \subset S$ denote the subset of totally positive elements of S. For $x \in F$, the notation $x \gg 0$ also denotes that x is totally positive and these are used interchangeably.

The Artin map induces an isomorphism

$$\mathrm{Pic}(F)^+ \xrightarrow{\sim} \mathrm{Gal}(H_F^+/F),$$

where H_F^+ denotes the narrow Hilbert class field of F. Because precisely those primes dividing the discriminant ramify, the field extension L/F is unramified at all finite places. Since L/F is also abelian, the field L must be contained in H_F^+ and as such, we obtain a natural quotient map by restriction

$$\chi : G_F \to \mathrm{Gal}(H_F^+/F) \to \mathrm{Gal}(L/F) \cong \{\pm 1\}.$$

The composition of the above two maps also defines a character on the narrow ideal class group of F, which we will, by slight abuse of notation, also denote by $\chi : \mathrm{Pic}(F)^+ \to \{\pm 1\}$.

We let $\mathcal{D}_F$ denote the different ideal of F and we define

$$\rho(I) := \#\left\{ J \subset \mathcal{O}_L \mid \mathrm{Nm}_F^L(J) = I \right\}$$

for any ideal $I \subset \mathcal{O}_F$.

We let N be a positive integer that is the product of two distinct prime numbers p and q, so we may write $N = pq$. But for the coprimality of D_1 and D_2, all the notation introduced above has so far been independent of one another. However, we must make the following crucial assumption about how the integer N interacts with the fields introduced above.

Throughout this thesis, we will make the assumption that both p and q are *inert* in both K_1 and K_2.

As a result, both p and q must split in F and we let $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathcal{O}_F$ denote the two primes above p respectively, and similarly $\mathfrak{q}_1, \mathfrak{q}_2 \subset \mathcal{O}_F$. Also, both p and q are in particular *unramified* in $L/\mathbb{Q}$.

Quaternion algebras

For any ring R, we let $R^\times$ denote the subgroup of units in R.

For any positive squarefree integer M, we let B_M denote the unique (up to isomorphism) quaternion algebra for which a finite prime is ramified if and only if it divides M. In particular, if M contains an even number of prime factors, B_M must be indefinite, and if M contains an odd number of prime factors, B_M must be definite.

For any such quaternion algebra B_M we let $R_M \subset B_M$ denote a maximal order; this choice need not be unique, even up to conjugation.

Because we assume the prime q to be inert in both K_1 and K_2, we can find embeddings $\alpha_1 : \mathcal{O}_1 \to B_q$ and $\alpha_2 : \mathcal{O}_2 \to B_q$, see [Voi21].

We assume throughout that R_q is the only maximal order of B_q up to conjugation. That is, we assume that $q \in \{2, 3, 5, 7, 13\}$.

Choose any splitting $B_q \hookrightarrow M_2(\mathbb{Q}_p)$. This matrix algebra acts on $\mathbb{C}_p$ through fractional linear transformations:

$$\text{if} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{then} \quad A \cdot z = \frac{az+b}{cz+d}.$$

We compute the fixed points for the action of A through

$$z = \frac{az+b}{cz+d} \iff cz^2 + (d-a)z - b = 0.$$

This also shows that every element in the ring $\mathbb{C}_p[A]$ shares the same fixed points. If $c \neq 0$, one checks that the two fixed points coincide if and only if $(2A - \operatorname{tr}(A))^2 = 0$, so the ring $\mathbb{C}_p[A]$ would not be reduced. If $c = 0$, then A satisfies the equation $(A-a)(A-d) = 0$ over $\mathbb{Q}_p$.

Through the embeddings $\alpha_i : \mathcal{O}_i \to R_q$ for $i \in \{1, 2\}$ and this splitting, the orders $\mathcal{O}_i$ act on $\mathbb{C}_p$ too. Clearly, their images in $M_2(\mathbb{Q}_p)$ must be reduced. In addition, any element from $K_i \setminus \mathbb{Q}$ for $i \in \{1, 2\}$ is quadratic over $\mathbb{Q}_p$, because p is inert in both fields. As such, their images under the splitting cannot be upper-triangular and so these images always have two conjugate fixed points in $\mathcal{H}_p$.

We will denote the common fixed points for the action of $\mathcal{O}_i$ on $\mathcal{H}_p$ through the embedding $\alpha_i : \mathcal{O}_i \to R_q$ with τ_i and τ_i', for $i \in \{1, 2\}$.