Fields of definition of finite hypergeometric functions

Frits Beukers

Abstract Finite hypergeometric functions are functions of a finite field $\mathbb{F}_q$ to $\mathbb{C}$. They arise as Fourier expansions of certain twisted exponential sums and were introduced independently by John Greene and Nick Katz in the 1980's. They have many properties in common with their analytic counterparts, the hypergeometric functions. One restriction in the definition of finite hypergeometric functions is that the hypergeometric parameters must be rational numbers whose denominators divide $q-1$. In this note we use the symmetry in the hypergeometric parameters and an extension of the exponential sums to circumvent this problem as much as posssible.

1 Introduction

In the 1980's John Greene [5] and Nick Katz [6] independently introduced functions from finite fields to the complex numbers which can be interpreted as finite sum analogues of the classical one variable hypergeometric functions. These functions, also known as Clausen-Thomae functions are determined by two multisets of d entries in $\mathbb{Q}$ each. We denote them by $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_d)$. Throughout we assume that these sets have empty intersection when considered modulo $\mathbb{Z}$. The Clausen-Thomae functions satisfy a linear differential equation of order d with rational function coefficients. See [2].

Let $\mathbb{F}_q$ be the finite field with q elements. Let ζ_p be a primitive p-th root of unity and define the additive character $\psi_q(x) = \zeta_p^{\mathrm{Tr}(x)}$ where Tr is trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. For any multiplicative character $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ we define the Gauss sum

$$g(\chi) = \sum_{x \in \mathbb{F}_q^\times} \chi(x) \psi_q(x) \,.$$

Let ω be a generator of the character group on $\mathbb{F}_q^\times$. We use the notation $g(m) = g(\omega^m)$ for any $m \in \mathbb{Z}$. Note that $g(m)$ is periodic in m with period $q-1$. Note that the dependence of $g(m)$ on ζ_p and ω is not made explicit. Very often we shall need characters on $\mathbb{F}_q^\times$ of a given order. For that we use the notation $\mathfrak{q} = q-1$ so that a character of order d can be given by $\omega^{\mathfrak{q}/d}$ for example, provided that d divides $\mathfrak{q}$ of course.

Now we define finite hypergeometric sums. Let again $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be multisets of d rational numbers each, and disjoint modulo $\mathbb{Z}$. We need the following crucial assumption.

Assumption 1.1 *Suppose that*

$$(q-1)\alpha_i, (q-1)\beta_j \in \mathbb{Z}$$

University of Utrecht, e-mail: f.beukers@uu.nl

for all i and j.

Definition 1.2 (Finite hypergeometric sum) *Keep the above notation and Assumption 1.1. We define for any $t \in \mathbb{F}_q$,*

$$H_q(\boldsymbol{\alpha},\boldsymbol{\beta}|t) = \frac{1}{1-q}\sum_{m=0}^{q-2}\prod_{i=1}^{d}\left(\frac{g(m+\alpha_i\mathrm{q})g(-m-\beta_i\mathrm{q})}{g(\alpha_i\mathrm{q})g(-\beta_i\mathrm{q})}\right)\,\omega((-1)^d t)^m\,.$$

It is an exercise to show that the values of $H_q(\boldsymbol{\alpha},\boldsymbol{\beta}|t)$ are independent of the choice of ζ_p. The hypergeometric sums above were considered without the normalizing factor $(\prod_{i=1}^d g(\alpha_i\mathrm{q})g(-\beta_i\mathrm{q}))^{-1}$ by Katz in [6, p258]. Greene, in [5], has a definition involving Jacobi sums which, after some elaboration, amounts to

$$\omega(-1)^{|\boldsymbol{\beta}|\mathrm{q}}q^{-d}\prod_{i=1}^{d}\frac{g(\alpha_i\mathrm{q})g(-\beta_i\mathrm{q})}{g(\alpha_i\mathrm{q}-\beta_i\mathrm{q})}\;H_q(\boldsymbol{\alpha},\boldsymbol{\beta}|t)\,,$$

where $|\boldsymbol{\beta}| = \beta_1+\cdots+\beta_d$. The normalization we adopt in this paper coincides with that of Dermot McCarthy, [7, Def 3.2].
Let

$$A(x) = \prod_{j=1}^{d}(x-e^{2\pi i\alpha_j}),\qquad B(x) = \prod_{j=1}^{d}(x-e^{2\pi i\beta_j}).$$

An important special case is when $A(x),B(x)\in\mathbb{Z}[x]$. In that case we say that the hypergeometric sum is defined over $\mathbb{Q}$. Another way of describing this case is that $k\boldsymbol{\alpha}\equiv\boldsymbol{\alpha}(\mathrm{mod}\ \mathbb{Z})$ and $k\boldsymbol{\beta}\equiv\boldsymbol{\beta}(\mathrm{mod}\ \mathbb{Z})$ for all integers k relatively prime to the common denominator of the α_i,β_j. In other words, multiplication by k of the $\alpha_i(\mathrm{mod}\ \mathbb{Z})$ simply permutes these elements. Similarly for the β_j. From work of Levelt [2, Thm 3.5] it follows that in such a case the monodromy group of the classical hypergeometric equation can be defined over $\mathbb{Z}$. It also turns out that hypergeometric sums defined over $\mathbb{Q}$ occur in point counts in $\mathbb{F}_q$ of certain algebraic varieties, see [1, Thm 1.5] and the references therein. It is an easy exercise to show that $H_q(\boldsymbol{\alpha},\boldsymbol{\beta}|t)$ is independent of the choice of ω (it is already independent of the choice of ψ_q).
One of the obstacles in the definition of finite hypergeometric sums over $\mathbb{Q}$ is Assumption 1.1 which has to be made on q, whereas one has the impression that such sums can be defined for any q relatively prime with the common denominator of the α_i,β_j. This is resolved in [1, Thm 1.3] by an extension of the definition of hypergeometric sum. The idea is to apply the theorem of Hasse-Davenport to the products of Gauss sums which occur in the coefficients of the hypergeometric sum. Another way of dealing with this problem is given by McCarthy, who uses the Gross-Koblitz theorem which expresses Gauss sums as values of the p-adic Γ-function.

Theorem 1.3 (Gross-Koblitz) *Let ω be the inverse of the Teichmüller character. Let $\pi^{p-1}=-p$ and ζ_p such that $\zeta_p\equiv 1+\pi(\mathrm{mod}\ \pi^2)$. Let Γ_p be the p-adic Morita Γ-function. Let $q=p^f$ and $g_q(m)$ denote the Gauss-sum over $\mathbb{F}_q$ with multiplicative character ω^m. Then, for any integer m we have*

$$g_q(m) = -\prod_{i=0}^{f-1}\pi^{(p-1)\left\{\frac{p^i m}{q-1}\right\}}\Gamma_p\left(\left\{\frac{p^i m}{q-1}\right\}\right).$$

Here $\{x\}=x-\lfloor x\rfloor$ is the fractional part of x. In particular, when $q=p$ we get

$$g_p(m) = -\pi^{(p-1)\left\{\frac{m}{p-1}\right\}}\Gamma_p\left(\left\{\frac{m}{p-1}\right\}\right).$$

See Henri Cohen's book [4] for a proof. When p does not divide the common denominator of the α_i, β_j one easily writes down a p-adic version of our hypergeometric sum for the case $q = p$.

Definition 1.4 *We define $G_p(\boldsymbol{\alpha}, \boldsymbol{\beta}|t)$ by the sum*

$$\frac{1}{1-p}\sum_{m=0}^{q-2}\omega((-1)^d t)^m(-p)^{\Lambda(m)}\prod_{i=1}^{d}\frac{\Gamma_p\left(\left\{\alpha_i+\frac{m}{p-1}\right\}\right)}{\Gamma_p(\{\alpha_i\})}\frac{\Gamma_p\left(\left\{-\beta_i-\frac{m}{p-1}\right\}\right)}{\Gamma_p(\{-\beta_i\})},$$

where

$$\Lambda(m)=\sum_{i=1}^{d}\left\{\alpha_i+\frac{m}{p-1}\right\}-\{\alpha_i\}+\left\{-\beta_i-\frac{m}{p-1}\right\}-\{-\beta_i\}.$$

Note that

$$\Lambda(m)=\sum_{i=1}^{d}-\left\lfloor\alpha_i+\frac{m}{p-1}\right\rfloor+\lfloor\alpha_i\rfloor-\left\lfloor-\beta_i-\frac{m}{p-1}\right\rfloor+\lfloor-\beta_i\rfloor.$$

In particular $\Lambda(m) \in \mathbb{Z}$. Definition 1.4 almost coincides with McCarthy's function ${}_dG_d$ from [7, Def 1.1] in the sense that our function coincides with ${}_dG_d(1/t)$. We prefer to adhere to the definition given above. The advantage of Definition 1.4 is that Assumption 1.1 is not required, it is well-defined for all parameters α_i, β_j as long as they are p-adic integers. Define

$$\delta=\delta(\boldsymbol{\alpha},\boldsymbol{\beta})=\max_{x\in[0,1]}\sum_{i=1}^{d}\lfloor x+\alpha_i\rfloor-\lfloor\alpha_i\rfloor+\lfloor -x-\beta_i\rfloor-\lfloor-\beta_i\rfloor.$$

Then, using Definition 1.4 and the fact that $-\Lambda(m) \le \delta$ one easily deduces that $p^{\delta}G_p(\boldsymbol{\alpha}, \boldsymbol{\beta}|t)$ is a p-adic integer. In [7, Prop 3.1] we find this in a slightly different formulation. However, it is not clear from the definition whether this value is algebraic or not over $\mathbb{Q}$. It is the purpose of the present note to be a bit more specific by proving the following theorem.

Theorem 1.5 *Let notations be as above and let K be the field extension of $\mathbb{Q}$ generated by the coefficients of $A(x)$ and $B(x)$. Suppose p splits in K, i.e. p factors into $[K:\mathbb{Q}]$ distinct prime ideals in the integers of K. Let $\Delta = \max_k \delta(k\boldsymbol{\alpha}, k\boldsymbol{\beta})$ over all integers k relatively prime with the common denominator of the α_i, β_j. Then $p^{\Delta}G_p(\boldsymbol{\alpha}, \boldsymbol{\beta}|t)$ is an algebraic integer in K.*

For the proof we construct in Section 2 a generalization of the hypergeometric function $H_q(A,B|t)$ involving two semisimple finite algebras A and B over $\mathbb{F}_q$. We show that it belongs to K and then, in Section 3 identify its p-adic evaluation with $G_p(\boldsymbol{\alpha}, \boldsymbol{\beta}|t)$.

2 Gauss sums on finite algebras

The main idea of the proof of Theorem 1.5 is to use Gauss sums on finite commutative algebras over $\mathbb{F}_q$ with 1. Let A be such an algebra. For any $x \in A$ we define the trace $\mathrm{Tr}(x)$ and norm $N(x)$ as the trace and norm of the $\mathbb{F}_p$-linear map given by multiplication with x on A.

Choose an additive character ψ on A which is *primitive*. That is, to any ideal $I \subset A, I \neq (0)$ there exists $x \in I$ such that $\psi(x) \neq 1$. Any other non-degenerate additive character is of the form $\psi(ax)$ with $a \in A^{\times}$. A multiplicative character χ is called *primitive* if its kernel does not contain any subgroup of the form $\{1+a|a \in I\}$ for some non-zero ideal I in A.

For any multiplicative character χ on $A^{\times}$ we can define a Gauss sum

$$g_A(\psi,\chi) = \sum_{x\in A^\times} \psi(x)\chi(x).$$

When A is not semisimple, the Gauss sum can be 0, as illustrated by the following example.

Example 2.1. Let $A = \mathbb{F}_p[x]/(x^2)$. Choose the additive character $\psi(a+bx) = \zeta_p^b$. It is easy to see that this is a primitive character. Note that $a+bx \in A^\times \iff a \in \mathbb{F}_p^\times$. Let χ be a nontrivial multiplicative character on $\mathbb{F}_p^\times$ and extend it to $A^\times$ by $\chi(a+bx) = \chi(a)$. Then

$$g_A(\psi,\chi) = \sum_{a\in\mathbb{F}_p^\times, b\in\mathbb{F}_p} \zeta_p^b \chi(a) = 0.$$

$\diamondsuit$

So we restrict ourselves to semisimple algebras. These are precisely the finite sums of finite field extensions of $\mathbb{F}_q$. In this case there is an obvious choice for the additive character.

Lemma 2.2 *Suppose A is a direct sum of finite field extensions of $\mathbb{F}_q$. Then $\psi(x) = \zeta_p^{\mathrm{Tr}(x)}$ is a primitive additive character.*

Proof : Let $A \cong \oplus_{i=1}^r F_i$ with F_i a finite field extension of $\mathbb{F}_q$ for all i. Then $\psi(x) = \zeta_p^{\mathrm{Tr}_1(x_1)+\cdots+\mathrm{Tr}_r(x_r)}$, where Tr_i stands for the trace function on F_i. If ψ were not primitive then there exists $a \in A, a \neq 0$ such that $\psi(ax) = 1$ for all $x \in A$. Suppose $a = (a_1,\ldots,a_r)$ and assume, without loss of generality, $a_1 \neq 0$. Then $\psi(x,0,\ldots,0) = \zeta_p^{\mathrm{Tr}(a_1 x)} = 1$ for all $x \in F_1$. By the properties of the trace of a field this is not possible.

$\square$

From now on we use the trace character on a semisimple algebra A as additive character and write $g_A(\chi)$ for the Gauss sum. So we dropped the dependence of the Gauss sum on the aditive character. The only amount of freedom in the additive character rests on the choice of ζ_p.

Proposition 2.3 *Let A be a direct sum of finite fields over $\mathbb{F}_q$ and $\psi(x) = \zeta_p^{\mathrm{Tr}(x)}$ the additive character. Let χ a multiplicative character. Then there exists a non-negative integer f such that*

$$|g_A(\chi)|^2 = q^f.$$

Proof : Again, write $A = \oplus_{i=1}^r F_i$. Then χ can be written as $\chi(x_1,\ldots,x_r) = \chi_1(x_1)\cdots\chi_r(x_r)$, where χ_i is a multplicative character on $F_i^\times$. This implies that

$$g_A(\psi,\chi) = \prod_{i=1}^r g(\chi_i),$$

where $g(\chi_i)$ is the usual Gauss sum on the field F_i. The additive character on F_i is $\zeta_p^{\mathrm{Tr}_i(x)}$ with the same choice of ζ_p for each i. Our assertion follows directly.

$\square$

Choose two finite semisimple algebras A, B over $\mathbb{F}_q$. Choose the trace characters on each of them with the same choice of ζ_p and call them ψ_A, ψ_B. Let χ_A, χ_B be multiplicative characters on $A^\times, B^\times$. Denote the norms on A, B by N_A, N_B.

Definition 2.4 *We define*

$$H_q(A,B|t) = \frac{-1}{g_A(\chi_A)g_B(\chi_B)} \sum_{x\in A^\times, y\in B^\times, tN_A(x)=N_B(y)} \psi_A(x)\psi_B(-y)\chi_A(x)\overline{\chi_B(y)},$$

for any $t \in \mathbb{F}_q$.

The following theorem gives its Fourier expansion in t.

Theorem 2.5 *Let ω be a generator of the multiplicative characters on $\mathbb{F}_q^\times$. When the context is clear we denote both functions $\omega(N_A(x))$ and $\omega(N_B(y))$ by ω_N. We then have,*

$$H_q(A,B|t) = \frac{1}{1-q}\sum_{m=0}^{q-2} \frac{g_A(\chi_A\omega_N^m)g_B(\overline{\chi_B}\omega_N^{-m})}{g_A(\chi_A)g_B(\chi_B)}\omega(N_B(-1)t)^m.$$

Proof : We compute the Fourier expansion $\sum_{m=0}^{q-2} c_m\omega(t)^m$ of $H_q(A,B|t)$. The coefficient c_m can be computed using

$$c_m = \frac{1}{q-1}\sum_{t\in\mathbb{F}_q^\times} H_q(A,B|t)\omega(t)^{-m}.$$

When we substitute the definition for $H_q(A,B|t)$ in the summation over t, we get a summation over $t\in\mathbb{F}_q^\times, x\in A^\times, y\in B^\times$ with the restriction $tN_A(x) = N_B(y)$. So we might as well substitute $t = N_B(y)/N_A(x)$ and sum over x,y. We get,

$$c_m = \frac{1}{1-q}\sum_{x\in A^\times, y\in B^\times} \frac{1}{g_A g_B}\psi_A(x)\psi_B(-y)\chi_A(x)\chi_B(y)^{-1}\omega(N_A(x))^m\omega(N_B(y))^{-m}.$$

The summation over x yields $g_A(\chi_A\omega_N^m)$. To sum over y we first replace y by $-y$ and then perform the summation. We get $\omega(N_B(-1))^m g_B(\overline{\chi_B}\omega_N^{-m})$. This proves our theorem.

□

Example 2.6. As in the previous section take two multisets of hypergeometric parameters $\boldsymbol{\alpha},\boldsymbol{\beta}$. Suppose that $(q-1)\alpha_i,(q-1)\beta_j$ are in $\mathbb{Z}$ for all i,j. Take $A = B = \mathbb{F}_q^d$, the direct sum of d copies of $\mathbb{F}_q$ with componentwise addition and multiplication. The norm on A,B is given by $N(x_1,\ldots,x_d) = x_1\cdots x_d$. In particular $N_B(-1) = (-1)^d$. For both A,B we take the additive character $\psi(x_1,\ldots,x_d) = \zeta_p^{\mathrm{Tr}(x_1+\cdots+x_d)}$, where Tr the trace function on $\mathbb{F}_q$. As multiplicative characters we take

$$\chi_A(x_1,\ldots,x_d) = \prod_{i=1}^d \omega(x_i)^{(q-1)\alpha_i}, \qquad \chi_B(x_1,\ldots,x_d) = \prod_{j=1}^d \omega(y_j)^{(q-1)\beta_j}.$$

An easy calculation shows that $g_A(\chi_A\omega_N^m) = \prod_{i=1}^d g(m+(q-1)\alpha_i)$ and similarly for g_B. So we see that we recover the finite hypergeometric sum of the previous section.

♢

Lemma 2.7 *Suppose $\dim_{\mathbb{F}_q}(A) = \dim_{\mathbb{F}_q}(B)$. Then $H_q(A,B|t)$ does not depend on the choice of ζ_p in the additive characters.*
As a corollary, in this equi-dimensional case the values of $H_q(A,B|t)$ are contained in the field generated by the charactervalues of χ_A,χ_B.

Proof : When we choose $\zeta_p^a, a\in\mathbb{F}_p^\times$ instead of ζ_p in the definition of the additive character it is easy to check that $g_A(\chi_A)$ gets replaced by $\chi_A(a)^{-1}g_A(\chi_A)$. And similarly for B. As a corollary any term in the sum in the hypergeometric sum in Theorem 2.4 is multiplied by $\omega(N_B(a)/N_A(a))^m$. Since $a\in\mathbb{F}_p$ is a scalar, $N_A(a) = N_B(a) = a^d$, where $d = \dim_{\mathbb{F}_q}(A) = \dim_{\mathbb{F}_q}(B)$. Hence, in the case of equal dimensions of A,B the multiplication factor is 1.
Let $\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be such that it fixes the values of χ_A,χ_B but sends ζ_p to ζ_p^a. According to the above calculation $H_q(A,B|t)$ is fixed under this substitution and hence under σ.

□

Let us return momentarily to Example 2.6 and suppose that the parameters $\boldsymbol{\alpha}$ have the property that $k\boldsymbol{\alpha} \equiv \boldsymbol{\alpha} (\text{mod } \mathbb{Z}), k\boldsymbol{\beta} \equiv \boldsymbol{\beta} (\text{mod } \mathbb{Z})$ for all k relative prime with the common denominator of the α_i, β_j. Then, for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ there exists a permutation ρ of the summands of $A = \oplus_{i=1}^d \mathbb{F}_p$ such that $\chi_A(\rho(x)) = \chi_A(x)^\sigma$ for all $x \in A^\times$. A similar permutation exists for B. Notice also that $\text{Tr}(\rho(x)) = \text{Tr}(x)$ and $N(\rho(x)) = N(x)$.
A similar situation arises in the case $A = \mathbb{F}_{p^r}$ as $\mathbb{F}_p$-algebra. Let χ_A be a character of order d dividing $p^r - 1$. Let ρ be the p-th power Frobenius on A, then $\chi_A(\rho(x)) = \chi_A(x)^p$, a conjugate of $\chi_A(x)$ for all $x \in A^\times$. Notice also that $\text{Tr}(\rho(x)) = x$ and $N(\rho(x)) = N(x)$.

Definition 2.8 *Let A be a finite dimensional $\mathbb{F}_q$-algebra. A ring automorphism $\rho : A \to A$ is called an $\mathbb{F}_q$-automorphism if it is $\mathbb{F}_q$-linear and it fixes both norm and trace of A.*

Proposition 2.9 *Let A, B be finite commutative semisimple $\mathbb{F}_q$-algebras. Let χ_A, χ_B be multiplicative characters. Consider the subgroup G of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of elements σ for which there exists an $\mathbb{F}_q$-automorphisms ρ_A of A and ρ_B of B with the property that $\chi_A(\rho_A(x)) = \chi_A(x)^\sigma$ and $\chi_B(\rho_B(x)) = \chi_B(x)^\sigma$ for every $\sigma \in G$. Then $H_q(A, B|t)$ lies in the fixed field of G for every $t \in \mathbb{F}_q^\times$.*

Proof : Let $\sigma \in G$. We first compute the action of σ on $g_A(\chi_A)$. Suppose that $\sigma(\zeta_p) = \zeta_p^a$.

$$\begin{aligned} g_A(\chi_A)^\sigma &= \sum_{x \in A^\times} \zeta_p^{a\text{Tr}(x)} \chi_A(x)^\sigma \\ &= \sum_{x \in A^\times} \zeta_p^{a\text{Tr}(x)} \chi_A(\rho(x)) \\ &= \sum_{x \in A^\times} \zeta_p^{\text{Tr}(\rho^{-1}(x))} \chi_A(a^{-1}x) \\ &= \chi_A(a)^{-1} g_A(\chi_A) \end{aligned}$$

A similar calculation holds for B. Now apply σ to the terms in the sum in Definition 2.4. A similar calculation as above shows that the sum gets multiplied with $\chi_A(a)^{-1}\chi_B(a)^{-1}$. This cancels the factor coming from $g_A(\chi_A)g_B(\chi_B)$. Hence $H_q(A, B|t)$ is fixed under all $\sigma \in G$.
□

3 Proof of Theorem 1.5

We use the notations from the introduction. In particular

$$A(x) = \prod_{j=1}^d (x - e^{2\pi i \alpha_j}), \quad B(x) = \prod_{j=1}^d (x - e^{2\pi i \beta_j})$$

and K is the field generated by the coefficients of $A(x)$ and $B(x)$. Let p be a prime which splits completely in K. Then we can consider $A(x)$ as element of $\mathbb{F}_p[x]$. Let $A(x) = A_1(x) \cdots A_r(x)$ be the irreducible factorization of $A(x)$ in $\mathbb{F}_p[x]$. For the $\mathbb{F}_p$-algebra we take $\oplus_{i=1}^r \mathbb{F}_p[x]/(A_i(x))$. The construction of a multiplicative character on A is as follows. First we choose a multiplicative character ω on $\overline{\mathbb{F}_p}$ such that its restriction to $\mathbb{F}_{p^r}$ has order $p^r - 1$ for all $r \geq 1$ and fix in the remainder of the proof.
Since p splits in K multiplication by p gives a permutation of the multiset $\boldsymbol{\alpha}$ modulo $\mathbb{Z}$. Under this action $\boldsymbol{\alpha} (\text{mod } \mathbb{Z})$ decomposes into a union of orbits, which we call p-orbits. Let O be such a p-orbit. Then $\prod_{\alpha \in O}(x - e^{2\pi i \alpha})$ is a polynomial and p splits in the field generated by its coefficients. So we can consider it modulo a prime ideal dividing p and hence as an element of $\mathbb{F}_p[x]$. It is one of the factors $A_i(x)$ of the mod p factorization

of $A(x)$. The orbit O will now be denoted by O_i. There are r orbits and we renumber the indices of the α_i such that $\alpha_i \in O_i$ for $i = 1,\dots,r$. On $\mathbb{F}_p[x]/(A_i)$ we define the multiplicative character $\chi_i = \omega^{\alpha_i(q_i-1)}$, where $q_i = p^{\deg(A_i)}$. If we would have chosen $p\alpha_i$ instead of α_i, the new character would simply consist of the Frobenius transform followed by χ_i. For the character χ_A on $A = \sum_{i=1}^r \mathbb{F}_p[x]/(A_i)$ we choose

$$\chi_A(x_1,\dots,x_r) = \prod_{i=1}^r \omega(x_i)^{\alpha_i(q_i-1)}.$$

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. It acts as $\omega(x) \mapsto \omega(x)^k$ for some integer k. Hence

$$\chi_A(x_1,\dots,x_r)^\sigma = \prod_{i=1}^r \omega(x_i)^{k\alpha_i(q_i-1)}.$$

This permutes the factors by a permutation $s \in S_r$ and we get

$$\chi_A(x_1,\dots,x_r)^\sigma = \prod_{i=1}^r \omega\left(x_{s^{-1}(i)}\right)^{p^{l_i}\alpha_i(q_i-1)},$$

where $0 \le l_i < \deg(A_i)$ for each i. We used $q_{s(i)} = q_i$. We finally get

$$\chi_A(x_1,\dots,x_r)^\sigma = \prod_{i=1}^r \omega\left(x_{s^{-1}(i)}^{p^{l_i}}\right)^{\alpha_i(q_i-1)} = \chi_A\left(x_{s^{-1}(1)}^{p^{l_i}},\dots,x_{s^{-1}(r)}^{p^{l_r}}\right).$$

In other words, $\chi_A(x)^\sigma = \chi_A(\rho(x))$ for a suitable $\mathbb{F}_p$-automorphism ρ of A. Notice that norm and trace of A are preserved by ρ. A similar construction can be performed for $B(x)$. According to Proposition 2.9 we get $H_p(A,B|t) \in K$ for all $t \in \mathbb{F}_q^\times$.
In order to connect to the p-adic function G_p we take the inverse of the Teichmüller character for ω and compute the terms given in Definition 2.4 p-adically. The Gauss sum $g_A(\chi_A\omega_N^m)$ is the product of ordinary Gauss sums of the form $g(\omega^{(q-1)\alpha+m(1+p+\cdots+p^{l-1})})$ over the field $\mathbb{F}_q$ with $q = p^l$. The occurrence of $m(1+p+\cdots+p^{l-1})$ is due to $\omega(N_{\mathbb{F}_q/\mathbb{F}_p}(x)^m) = \omega(x)^{m(1+\cdots+p^{l-1})}$. The Gross-Koblitz theorem for Gauss sums over $\mathbb{F}_q$ with $q = p^l$ gives us

$$g_q(\omega^a) = -\prod_{i=0}^{l-1} \pi^{\left\{\frac{p^i a}{q-1}\right\}} \Gamma_p\left(\left\{\frac{p^i a}{q-1}\right\}\right)$$

for every integer a. When applied to $a = (q-1)\alpha + m(q-1)/(p-1)$ this amounts to

$$-\prod_{i=0}^{l-1} \pi^{\left\{p^i\alpha+\frac{m}{p-1}\right\}} \Gamma_p\left(\left\{p^i\alpha + \frac{m}{p-1}\right\}\right).$$

Note that this is a product over the p-orbit containing α and each factor is precisely of the type that occur in the definition of the p-adic hypergeometric sum. A similar story goes for $B(x)$. As a result we get

$$\frac{g_A(\chi_A\omega_N^m)g_B(\overline{\chi_B}\omega_N^{-m})}{g_A(\chi_A)g_B(\overline{\chi_B})} = (-p)^{\Lambda(m)} \prod_{i=1}^d \frac{\Gamma_p\left(\left\{\alpha_i + \frac{m}{p-1}\right\}\right)\Gamma_p\left(\left\{-\beta_i - \frac{m}{p-1}\right\}\right)}{\Gamma_p(\{\alpha_i\})\Gamma_p(\{-\beta_i\})},$$

where $\Lambda(m)$ is as defined in the introduction. So we find that p-adically

$$H_p(A,B|t) = G_p(\boldsymbol{\alpha},\boldsymbol{\beta}|t).$$

Hence we conclude that the values of G_p are in K. It remains to give an estimate for the denominator. From Definition 2.4 it follows that $H_p(A,B|t)$ has the denominator $g_A g_B$. Hence, by Proposition 2.3 there exists a power p^r of p such $p^r H_p(A,B|t)$ is an integer in K. It remains to determine a value for r. The conjugates of $H_p(A,B|t)$ are obtained by taking χ_A^k, χ_B^k as multiplicative characters. The corresponding hypergeometric parameters are $k\boldsymbol{\alpha}, k\boldsymbol{\beta}$. From McCarthy's work it follows that $p^\Delta G_p(k\boldsymbol{\alpha}, k\boldsymbol{\beta}|t)$ is a p adic integer for all k relatively prime to the common denominator of α_i, β_j. This implies that $p^\Delta H_p(A,B|t)$ is an algebraic integer in K.

References

1. F. Beukers, H. Cohen, A. Mellit, Finite hypergeometric functions, Pure and Applied Mathematics Quarterly **11** (2015), 559–589, also at arXiv:1505.02900.
2. F. Beukers, G. Heckman, Monodromy for the hypergeometric function ${}_nF_{n-1}$. Invent. Math. **95** (1989), 325–354
3. H. Cohen, *Number Theory, Volume I: Tools and Diophantine Equations*, Graduate Texts in Math. **239**, Springer Verlag, 2007.
4. H. Cohen, *Number Theory, Volume II: Analytic and Modern Tools*, Graduate Texts in Math. **240**, Springer Verlag, 2007.
5. J. Greene, Hypergeometric functions over finite fields, Trans. Amer. Math. Soc. **301** (1987), 77–101.
6. N. M. Katz, *Exponential Sums and Differential Equations*, Annals of Math Studies **124**, Princeton 1990.
7. D. McCarthy, The trace of Frobenius of elliptic curves and the p-adic gamma function. Pacific J. Math., **261**(1) (2013), 219–236.