Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

FUNDAMENTAL THEOREM MODULO p^m

Raf Cluckers

Tome 135
Fascicule 4

2007

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique
pages 1-

Bull. Soc. math. France
135 (4), 2007, p. 475–

THE FUNDAMENTAL THEOREM OF PREHOMOGENEOUS VECTOR SPACES MODULO p^m (WITH AN APPENDIX BY F. SATO)

by Raf Cluckers & Adriaan Herremans

Abstract. — For a number field K with ring of integers $\mathcal{O}_K$, we prove an analogue over finite rings of the form $\mathcal{O}_K/\mathcal{P}^m$ of the fundamental theorem on the Fourier transform of a relative invariant of prehomogeneous vector spaces, where $\mathcal{P}$ is a big enough prime ideal of $\mathcal{O}_K$ and $m > 1$. In the appendix, F. Sato gives an application of the Theorems 1.1, 1.3 and the Theorems A, B, C in J. Denef and A. Gyoja [*Character sums associated to prehomogeneous vector spaces*, Compos. Math., **113** (1998), 237–346] to the functional equation of L-functions of Dirichlet type associated with prehomogeneous vector spaces.

Texte recu le 12 septembre 2006, révisé le 16 novembre 2006

Raf Cluckers, Katholieke Universiteit Leuven, Departement wiskunde, Celestijnenlaan 200B, B-3001 Leuven (Belgium). Current address: École Normale Supérieure, Département de mathématiques et applications, 45 rue d'Ulm, 75230 Pari Cedex 05 (France)
E-mail : `cluckers@ens.fr` • *Url :* `www.dma.ens.fr/~cluckers/`
Adriaan Herremans, Katholieke Universiteit Leuven, Departement wiskunde, Celestijnenlaan 200B, B-3001 Leuven (Belgium)
E-mail : `adriaan.herremans@wis.kuleuven.ac.be`

2000 Mathematics Subject Classification. — 11S90, 11L07, 11M41, 11T24, 11L05, 20G40.

Key words and phrases. — Prehomogeneous vector spaces, L-functions, Bernstein-Sato polynomial, fundamental theorem of prehomogeneous vector spaces, exponential sums.

During the preparation of the paper, the authors were postdoctoral fellows of the Fund for Scientific Research – Flanders (Belgium) (F.W.O.). The first author was partially supported by The European Commission - Marie Curie European Individual Fellowship with contract number HPMF CT 2005-007121.

Résumé (*Théorème fondamental des espaces vectoriels préhomogènes modulo p^m. Avec un appendice par F. Sato*)

Soit K un corps de nombres avec anneaux d'entiers $\mathcal{O}_K$; nous prouvons un analogue, sur des anneaux finis de la forme $\mathcal{O}_K/\mathcal{P}^m$, du théorème fondamental sur la transformation de Fourier de l'invariante relative d'un espace vectoriel préhomogène. Ici, $\mathcal{P}$ est un idéal premier assez grand de $\mathcal{O}_K$ et $m > 1$. Dans l'appendice, F. Sato donne une application des théorèmes 1.1, 1.3 et des théorèmes A, B, C de J. Denef et A. Gyoja [*Character sums associated to prehomogeneous vector spaces*, Compos. Math., **113** (1998), 237–346] à l'équation fonctionelle de L-fonctions de type Dirichlet associées aux espaces vectorielles préhomogènes.

1. Introduction

We prove an analogue over finite rings of the fundamental theorem on the Fourier transform of a relative invariant of prehomogeneous vector spaces. In general, this fundamental theorem expresses the Fourier transform of $\chi(f)$, with χ a multiplicative (quasi-)character and f a relative invariant, in terms of $\chi(f^\vee)^{-1}$, with $f^\vee$ the dual relative invariant. Roughly speaking, M. Sato [18] proved the fundamental theorem over archimedian local fields, J. Igusa [7] over p-adic number fields, and J. Denef and A. Gyoja [5] over finite fields of big enough characteristic. In [9], the regular finite field case is reproved. When the prehomogeneous vector space is regular and defined over a number field K we prove an analogue of the fundamental theorem over rings of the form $\mathcal{O}_K/\mathcal{P}^m$, where $\mathcal{P}$ is a big enough prime ideal of the ring of integers $\mathcal{O}_K$ of K and $m > 1$, see Theorem 1.1. This result is derived from the results of [5] by using explicit calculations of exponential sums over the rings $\mathcal{O}_K/\mathcal{P}^m$.

In [16], F. Sato introduces L-functions of Dirichlet type associated to regular prehomogeneous vector spaces. In the appendix by F. Sato to this paper, our results are used to obtain functional equations for these L-functions and, under extra conditions, their entireness.

To state the main results, we fix our notation on prehomogeneous vector spaces. Let (G, ρ, V) be a reductive prehomogeneous vector space, meaning that G is a connected complex linear reductive algebraic group, $\rho : G \to \mathrm{GL}(V)$ is a finite dimensional rational representation, and V has an open G-orbit which is denoted by Ω. Assume that (G, ρ, V) has a relative invariant $0 \neq f \in \mathbb{C}[V]$ with character $\phi \in \mathrm{Hom}(G, \mathbb{C}^\times)$, that is, $f(gv) = \phi(g)f(v)$ for all $g \in G$ and $v \in V$. We assume that f is a *regular* relative invariant, namely, $\Omega = V \setminus f^{-1}(0)$ is a single G-orbit. Writing $\rho^\vee : G \to \mathrm{GL}(V^\vee)$ for the dual of ρ, $(G, \rho^\vee, V^\vee)$ is also a prehomogeneous vector space, with an open G-orbit which is denoted by $\Omega^\vee$, and there exists a relative invariant $0 \neq f^\vee \in \mathbb{C}[V^\vee]$ whose character is ϕ^{-1}. Then $\Omega^\vee = V^\vee \setminus f^{\vee -1}(0)$. The map $F := \operatorname{grad} \log f$ is an isomorphism between Ω and $\Omega^\vee$ with inverse $F^\vee := \operatorname{grad}\log f^\vee$. One has $\dim V = \dim V^\vee =: n$ and $\deg f = \deg f^\vee =: d$.

Let K be a number field with ring of integers $\mathcal{O}_K$. Suppose that (G,ρ,V) is defined over K. We fix a basis of the K-vector space $V(K)$ and we suppose that f is in $K[V]$ and has coefficients in $\mathcal{O}_K$ (with respect to the fixed K-basis of $V(K)$). Similarly we suppose that $f^\vee$ is in $K[V^\vee]$ and has coefficients in $\mathcal{O}_K$ (with respect to the basis of $V^\vee$ dual to the fixed basis of V). Write $V(\mathcal{O}_K)$ for the points of $V(K)$ with coefficients in $\mathcal{O}_K$ (with respect to the fixed K-basis of $V(K)$), and similarly for $V^\vee(\mathcal{O}_K)$. For I an ideal of $\mathcal{O}$, write $V(\mathcal{O}_K/I)$ for the reduction modulo I of the lattice $V(\mathcal{O}_K)$.

The Bernstein-Sato polynomial $b(s)$ of f is defined by

$$f^\vee(\operatorname{grad}_x) f(x)^{s+1} = b(s) f(x)^s.$$

Write b_0 for the coefficient of the term of highest degree of $b(s)$; one has $b_0 \in K$.

The following theorem is an analogue of the fundamental theorem for prehomogeneous vector spaces.

THEOREM 1.1. — *Let $m \geq 2$ be an integer, $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$ above a big enough prime $p \in \mathbb{Z}$, χ be a primitive multiplicative character modulo $\mathcal{P}^m$ (extended by zero outside the multiplicative units), and let ψ be a primitive additive character modulo $\mathcal{P}^m$. Write $q := \#(\mathcal{O}_K/\mathcal{P})$. For $L \in V^\vee(\mathcal{O}_K/\mathcal{P}^m)$ write*

$$S(L) := \sum_{x \in V(\mathcal{O}_K/\mathcal{P}^m)} \chi\big(f(x)\big)\psi\big(L(x)\big).$$

Then the following hold:

1) *if $f^\vee(L) \not\equiv 0 \bmod \mathcal{P}$, then*

$$S(L) = q^{\frac{1}{2}mn}\Big(\frac{\sum_{y\in\mathcal{O}_K/\mathcal{P}^m}\chi^d(y)\psi(y)}{q^{\frac{1}{2}m}}\Big)\chi\Big(\frac{b_0 f^\vee(L)^{-1}}{d^d}\Big)\alpha(\chi,m)^{n-1}\kappa^\vee(L),$$

where $\kappa^\vee(L)$ and $\alpha(\chi,m)$ are 1 or -1;

2) *if $f^\vee(L) \equiv 0 \bmod \mathcal{P}$, then $S(L) = 0$.*

The essential (and typical) content of this fundamental theorem is that the discrete Fourier transform of the function $\chi(f)$ on $V(\mathcal{O}_K/\mathcal{P}^m)$ is equal to the function $\chi(f^\vee)^{-1}$ on $V^\vee(\mathcal{O}_K/\mathcal{P}^m)$ times some factors, and vice versa.

The first part of Theorem 1.1 is obtained by combining explicit calculations of character sums of quadratic functions (§2) and of discrete Fourier transforms (§4), a p-adic version of Morse's lemma (§3), and results of [5]. The second part of Theorem 1.1 is established by comparing the L_2-norms of $\chi(f)$ and of its discrete Fourier transform.

We also obtain explicit formulas for the constants $\kappa^\vee(L)$ and $\alpha(\chi,m)$ of Theorem 1.1, by using work in [5] and elementary calculations. To state these formulas we use the notion of the discriminant of a matrix, as in [5, 9.1.0].

Definition 1.2. — For a symmetric (n,n)-matrix A with entries in a field k, if ${}^tXAX = \mathrm{diag}\ (a_1,\ldots,a_m,0,\ldots,0)$ with $X \in \mathrm{GL}_n(k)$, ${}^tX$ its transposed, and $a_i \in k^\times$, put

$$\Delta(A) := \prod_{i=1}^{m} a_i \in k^\times/k^{\times 2},$$

with $k^{\times 2}$ the squares in $k^\times$, and call it the *discriminant* of A.

Write $k_\mathcal{P}$ for the finite field $\mathcal{O}_K/\mathcal{P}$ and $k_\mathcal{P}^{\times 2}$ for the squares in $k_\mathcal{P}^\times$. For $m>1$ and L in $V^\vee(\mathcal{O}_K/\mathcal{P}^m)$ with $f^\vee(L)\not\equiv 0 \bmod \mathcal{P}$, denote by $h^\vee(L)$ the image in $k_\mathcal{P}^\times/k_\mathcal{P}^{\times 2}$ of the discriminant of the matrix $(\partial^2 \log f^\vee(L)/\partial y_i \partial y_j)_{ij}$, where $\{y_1,\ldots,y_n\}$ is the previously fixed K-basis of $V^\vee(K)$. Write $\chi_{\frac12}$ for the Legendre symbol mod $\mathcal{P}$. We then obtain

Theorem 1.3. — *The following hold in case* 1) *of Theorem* 1.1:

1) $\kappa^\vee(L) = \chi_{\frac12}(-d\,2^{n-1}\,h^\vee(L))^m$;
2) $\alpha(\chi,m) = 1$ *for m even*;
3) $\alpha(\chi,m) = G(\chi_{\frac12},\psi')/\sqrt{q}$ *for m odd, with ψ' any additive character defined by* $y\mapsto \chi(1+\pi_\mathcal{P}^{m-1}y)$, $\pi_\mathcal{P}$ *any element in $\mathcal{P}$ of $\mathcal{P}$-adic order* 1, $\chi_{\frac12}$ *the Legendre symbol* mod $\mathcal{P}$, *and* $G(.,.)$ *the classical Gauss sum.*

Remark 1.4. — It is interesting to compare the formulas of Theorems 1.1 and 1.3 to the formulas for $m=1$ given in [5]; it seems that for $m=1$ the formulas depend more on subtle information of the Bernstein-Sato polynomial of f.

Acknowledgement. — The authors would like to express gratitude to Jan Denef and Akihiko Gyoja for many helpful comments during the preparation of this paper. We are indebted to Jan Denef for giving the essential outline of the proofs of the main results, and to Fumihiro Sato for agreeing on writing an appendix to this paper.

2. Preliminaries on character sums

Let χ be a multiplicative character mod $\mathcal{P}^m$, extended by zero for $a \equiv 0 \bmod \mathcal{P}$. Say that χ is induced by a character $\chi_1 \bmod \mathcal{P}^n$ for $n < m$ if $\chi_1(a \bmod \mathcal{P}^n) = \chi(a)$ for all $a \in \mathcal{O}_K/\mathcal{P}^m$. Call χ *primitive* mod $\mathcal{P}^m$ if there exists no such $n < m$ and $\chi_1 \bmod \mathcal{P}^n$ such that χ is induced by χ_1. Analogously, call an additive character ψ mod $\mathcal{P}^m$ on $\mathcal{O}_K$ *primitive* if it is not induced by a character $\psi_1 \bmod \mathcal{P}^n$ for $n < m$. Let f be a polynomial in n variables over $\mathcal{O}_K$. If we evaluate $\sum \chi(f(x)) \bmod \mathcal{P}^m$, with χ primitive mod $\mathcal{P}^m$ for some $m > 1$, it is well known that only the critical points mod $\mathcal{P}$ contribute to the sum, i.e. the elements $c \in \mathcal{O}_K/\mathcal{P}^m$ for which $\operatorname{grad}(f)_{|c} \equiv 0 \bmod \mathcal{P}$. The following is an extension of this result.

PROPOSITION 2.1. — *Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$, $m > 1$ an integer, χ a primitive multiplicative character* mod $\mathcal{P}^m$ *and $f \in \mathcal{O}_K[x]$ a polynomial in n variables. Define S_f as*

$$S_f = \sum_{x \in (\mathcal{O}_K/\mathcal{P}^m)^n} \chi\big(f(x)\big). \tag{2.1}$$

Then

$$S_f = \sum_{\substack{x \in (\mathcal{O}_K/\mathcal{P}^m)^n \\ v_{\mathcal{P}}(\operatorname{grad}(f)_{|x}) \geq \frac{1}{2}(m-1)}} \chi\big(f(x)\big),$$

where $v_{\mathcal{P}}(\operatorname{grad}(f)_{|x})$ is the minimum of the $\mathcal{P}$-valuations of $\partial f/\partial x_{j\,|x}$ for $j = 1, \ldots, n$. Moreover, the same formulas hold for an additive character ψ instead of χ.

Proof. — We treat the case that f is a function of one variable; the general case is completely analogous. It suffices to prove that

$$S_f(i,c) := \sum_{\substack{x \in \mathcal{O}_K/\mathcal{P}^m \\ v_{\mathcal{P}}(f'(x)) = i \\ x \equiv c \bmod \mathcal{P}^{m-i-1}}} \chi\big(f(x)\big)$$

is zero for every $i < \frac{1}{2}(m-1)$ and every $c \in \mathcal{O}_K/\mathcal{P}^{m-i-1}$. If $f(c) \equiv 0 \bmod \mathcal{P}$, then $S_f(i,c)$ is trivially zero. Suppose $f(c) \not\equiv 0 \bmod \mathcal{P}$. Let $\pi_{\mathcal{P}}$ be in $\mathcal{P}$ of $\mathcal{P}$-adic order 1. Writing $f(x)$ as a polynomial in $(x-c)$, we get the equalities

$$S_f(i,c) = \sum_{\substack{x \in \mathcal{O}_K/\mathcal{P}^m \\ v_{\mathcal{P}}(f'(x)) = i \\ x \equiv c \bmod \mathcal{P}^{m-i-1}}} \chi\big(f(c) + (x-c)f'(c) + \cdots\big) \tag{2.2}$$

$$= \chi\big(f(c)\big) \sum_{\substack{x\in \mathcal{O}_K/\mathcal{P}^m \\ v_{\mathcal{P}}(f'(x))=i \\ x\equiv c \bmod \mathcal{P}^{m-i-1}}} \chi\Big(1+(x-c)\frac{f'(c)}{f(c)}\Big) \tag{2.3}$$

$$= q^i\chi\big(f(c)\big) \sum_{z\in \mathcal{O}_K/\mathcal{P}} \chi(1+\pi_{\mathcal{P}}^{m-1}z\alpha) = 0, \tag{2.4}$$

with α a unit in $\mathcal{O}_K/\mathcal{P}$. Equality (2.3) comes from the fact that the $\mathcal{P}$-valuation of the terms of degree ≥ 2 in $x-c$ are at least m. Indeed $2m-2i-2\geq m$ if $i\leq \frac{1}{2}(m-2)$ or $i<\frac{1}{2}(m-1)$. Either there are no terms in (2.3) and then it is automatically zero, or, there are terms and then equality (2.4) follows immediately. We conclude that the sum (2.4) is zero since we sum a non-trivial additive character $\psi(z) := \chi(1+\pi_{\mathcal{P}}^{m-1}\alpha z)$ over $\mathcal{O}_K/\mathcal{P}$; ψ is indeed non-trivial since χ is primitive. □

Definition 2.2. — Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$ not containing 2 and let $m>1$ be an integer. Let χ, resp. ψ, be a primitive multiplicative, resp. primitive additive, character mod $\mathcal{P}^m$. Then, put

$$\widetilde{\alpha}(\chi,m) := \sum_{x\in \mathcal{O}_K/\mathcal{P}^m} \chi(1+x^2), \quad \widetilde{\alpha}(\psi,m) := \sum_{x\in \mathcal{O}_K/\mathcal{P}^m} \psi(x^2).$$

One can calculate the value of $\widetilde{\alpha}(\chi,m)$, using Proposition 2.1 in an elementary way, to obtain the following lemma.

Lemma 2.3. — *With the assumptions and notation of Definition 2.2, the following hold*

- $\widetilde{\alpha}(\chi,m) = q^{\frac{1}{2}m}$ *if m is even;*
- $\widetilde{\alpha}(\chi,m) = q^{\frac{1}{2}(m-1)}G(\chi_{\frac{1}{2}},\psi')$ *if m is odd. Herein, $\chi_{\frac{1}{2}}$ is the Legendre symbol* mod $\mathcal{P}$, *ψ' is any additive character defined by $y\mapsto \chi(1+\pi_{\mathcal{P}}^{m-1}y)$ with $\pi_{\mathcal{P}}$ any element in $\mathcal{P}$ of $\mathcal{P}$-adic order 1, and $G(.,.)$ is the classical Gauss sum.*

Similar formulas can be obtained for $\widetilde{\alpha}(\psi,m)$ with ψ a primitive additive character modulo $\mathcal{P}^m$. This lemma and an induction argument yield the following proposition.

Proposition 2.4. — *Use the assumptions and notation of Definition 2.2. Let f be a polynomial in n variables over $\mathcal{O}_K$ of the form*

$$f(x) = a_0 + a_1x_1^2 + \cdots + a_nx_n^2,$$

with $a_0,a_1,\ldots,a_n$ multiplicative units mod $\mathcal{P}^m$. *Then*

$$S_f = \chi(a_0)\chi_{\frac{1}{2}}(a_0^n a_1\cdots a_n)^m \widetilde{\alpha}(\chi,m)^n$$

with $\chi_{\frac{1}{2}}$ the Legendre symbol mod $\mathcal{P}$, *and S_f as in (2.1).*

3. A p-adic analogue of the lemma of Morse

We prove an analogue of the Morse's lemma (originally formulated for C^∞ functions on real manifolds), for p-adic analytic functions. This lemma is normally stated as a local property, but here we can work with fixed (large) neighborhoods. To deal with the fact that $\mathbb{Z}_p$ is totally disconnected, we will use a global notion of analycity for p-adic maps. Results in this section also hold for finite field extensions of $\mathbb{Q}_p$.

By a p-adic manifold we mean a p-adic manifold as defined in [2] or equivalently [20], Section 3.

DEFINITION 3.1. — Let $A \subset \mathbb{Z}_p^n$ be open.

— Call a function $f : A \to \mathbb{Z}_p$ *globally analytic* if there is a power series $\sum c_i x^i \in \mathbb{Z}_p[[x]]$ which converges on A such that $f(x) = \sum c_i x^i$ for each $x \in A$, with $x = (x_1, \ldots, x_n)$, $i = (i_1, \ldots, i_n)$ and $x^i = \prod_{j=1}^n x_j^{i_j}$.

— Call f *analytic* if there is a finite cover of A by opens U such that the restriction of f to each U is globally analytic. Similarly, call a map $f : A \subset \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ analytic if it is given by analytic functions on A. An analytic bijection with analytic inverse is called *bi-analytic.*

— For an analytic function $f : A \subset \mathbb{Z}_p^n \to \mathbb{Z}_p$, define the *gradient* of f in $a \in A$ as

$$\operatorname{grad}(f)_{|a} = \Big(\frac{\partial f}{\partial x_1}\Big|_a, \ldots, \frac{\partial f}{\partial x_n}\Big|_a\Big)$$

and the *Hessian* of f in a as

$$\operatorname{Hs}(f)_{|a} = \Big(\frac{\partial^2 f}{\partial x_i \partial x_j}\Big|_a\Big)_{ij}.$$

— Say that a is a *critical point* if $\operatorname{grad}(f)_{|a} = 0$ and call the critical point $a \in A$ *non-degenerate* if $\det(\operatorname{Hs}(f)_{|a}) \neq 0$. Call $a \in A$ a *non-degenerate critical point modulo* p if $\operatorname{grad}(f)_{|a} \equiv 0 \bmod p$ and $\det(\operatorname{Hs}(f)_{|a}) \not\equiv 0 \bmod p$.

Let $M \subset \mathbb{Z}_p^n$ be a compact p-adic manifold of pure dimension d and $f : M \to \mathbb{Z}_p$ an analytic function. Then there exists a finite disjoint cover of M by opens U_i and analytic isometries π_i from U_i to open balls in $\mathbb{Z}_p^d$ such that the maps $f \circ \pi_i^{-1}$ are globally analytic, see e.g. [20], Section 3.

— Call a point $a \in U_i \subset M$ a critical point of f if $\pi_i(a)$ is a *critical point* of $f \circ \pi_i^{-1}$ as defined above. Similarly we speak of *non-degenerate critical points* and *non-degenerate critical point modulo p.* This is independent of the choice of U_i and π_i.

The next lemma is a p-adic variant of the inverse function theorem.

LEMMA 3.2 (see [8, Cor. 2.2.1]). — *Suppose that* $g_1, \ldots, g_n \in \mathbb{Z}_p[[x_1, \ldots, x_n]]$ *satisfy* $\det(\partial g_i/\partial x_{j\,|0})_{ij} \not\equiv 0 \bmod p$ *and* $g_i(0) \equiv 0 \bmod p$ *for* $i = 1, \ldots, n$. *Then the map*

$$g : (p\mathbb{Z}_p)^n \longrightarrow (p\mathbb{Z}_p)^n, \quad x \longmapsto \big(g_1(x), \ldots, g_n(x)\big)$$

is (globally) bi-analytic.

The following is a p-adic analogue of the Morse's lemma. The proof goes along the same lines as in [10] and we refer to [10], Lemma 2.2 for the details.

LEMMA 3.3 (Morse). — *Let* $p \neq 2$ *and let* $f : (p\mathbb{Z}_p)^n \to p\mathbb{Z}_p$ *be a globally analytic map (thus* f *is given by a single power series in* $\mathbb{Z}_p[[x]]$*) such that* 0 *is a non-degenerate critical point modulo* p. *Then there is a unique critical point* c *of* f *and there is a (globally) bi-analytic map*

$$T : (p\mathbb{Z}_p)^n \longrightarrow (p\mathbb{Z}_p)^n, \quad x \longmapsto T(x) = u$$

such that

$$f(x) = f(c) + \sum_{i=1}^{n} a_i u_i^2, \quad \text{for all } x \in (p\mathbb{Z}_p)^n,$$

with a_i *in* $\mathbb{Z}_p^\times$. *Moreover,* $\chi_{\frac{1}{2}}(H) = \chi_{\frac{1}{2}}(\prod_i a_i)$ *with* $H = 2^{-n}\det(\mathrm{Hs}(f)_{|c})$.

Proof. — The uniqueness of the critical point c is proved in Lemma 3.4 below. We may suppose that $f(0) = 0$ and $c = 0$. We can write $f(x) = \sum_{i,j} x_i x_j h_{ij}(x)$ with $h_{ij}(x) \in \mathbb{Z}_p[[x]]$ and since $p \neq 2$ we can assume that $h_{ij} = h_{ji}$. Suppose by induction that we have a (globally) bi-analytic map $T_{r-1} : (p\mathbb{Z}_p)^n \to (p\mathbb{Z}_p)^n : x \mapsto u$ such that for each $x \in (p\mathbb{Z}_p)^n$

$$f(x) = \sum_{i=1}^{r-1} a_i u_i^2 + \sum_{i,j \geq r} u_i u_j H_{ij}(u),$$

with $H_{ij}(u) \in \mathbb{Z}_p[[u]]$, $H_{ij} = H_{ji}$ and $a_i \in \mathbb{Z}_p^\times$. We have

$$\det\big(\mathrm{Hs}(f)_{|0}\big) = \lambda \det\big(H_{ij}(0)\big)_{ij}$$

with λ a unit in $\mathbb{Z}_p$, so $\det(H_{ij}(0))_{ij} \not\equiv 0 \bmod p$ and after a linear change in the last $n - r + 1$ coordinates we may assume that $H_{rr}(0) \not\equiv 0 \bmod p$. Put $a_r = H_{rr}(0)$. Then $H_{rr}(u)/a_r \equiv 1 \bmod p$ for each $u \in (p\mathbb{Z}_p)^n$. There is a well-defined square root function $\sqrt{} : 1 + p\mathbb{Z}_p \to 1 + p\mathbb{Z}_p$ which is (globally) analytic. Put

$$g(u) = \sqrt{H_{rr}(u)/a_r}$$

for $u \in (p\mathbb{Z}_p)^n$. Then, g is (globally) analytic on $(p\mathbb{Z}_p)^n$. We can now define a (globally) analytic map $T'_{r-1} : (p\mathbb{Z}_p)^n \to (p\mathbb{Z}_p)^n : u \mapsto T'_{r-1}(u) = (v_i)$ by

$$v_i = u_i \;\text{ if }\; i \neq r \quad \text{and} \quad v_r = g(u)\Big(u_r + \sum_{i>r} u_i \frac{H_{ir}(u)}{H_{rr}(u)}\Big).$$

Clearly we have that $\det(\partial v_i/\partial u_{j\,|0}) = g(0) \not\equiv 0 \bmod p$, thus, the map T'_{r-1} is (globally) bi-analytic by Lemma 3.2. Put $T_r = T'_{r-1} \circ T_{r-1}$. We then obtain for all $x \in (p\mathbb{Z}_p)^n$ and $v = T_r(x)$

$$f(x) = \sum_{i=1}^{r} a_i v_i^2 + \sum_{i,j>r} v_i v_j H'_{ij}(v),$$

with $H'_{ij}(v) \in \mathbb{Z}_p[[v]]$. This finishes the induction argument.

The equality $\chi_{\frac{1}{2}}(\det(\mathrm{Hs}(f)_{|0}) = \chi_{\frac{1}{2}}(\prod_i 2a_i)$ follows by a classical argument as in [10]. To finish the proof we only have to prove the Lemma below. □

Lemma 3.4. — *Let $p \neq 2$ and let $f : (p\mathbb{Z}_p)^n \to p\mathbb{Z}_p$ be a globally analytic map (i.e., given by a power series in $\mathbb{Z}_p[[x]]$) such that 0 is a non-degenerate critical point modulo p. Then f has a unique critical point $c \in (p\mathbb{Z}_p)^n$ and this is a non-degenerate critical point.*

Proof. — We can write

$$f(x) = f(0) + \sum_i a_i x_i + g(x)$$

with $g(x) = \sum_{ij} x_i x_j h_{ij}(x)$ for some $h_{ij} \in \mathbb{Z}_p[[x]]$. Since 0 is a non-degenerate critical point of f modulo p, we see that $a_i \equiv 0 \bmod p$ and $\det(\mathrm{Hs}(g)_{|0}) \not\equiv 0 \bmod p$. By Lemma 3.2 the map

$$T : (p\mathbb{Z}_p)^n \longrightarrow (p\mathbb{Z}_p)^n, \quad x \longmapsto \mathrm{grad}(g)_{|x} = \Big(\frac{\partial g}{\partial x_1}(x), \dots, \frac{\partial g}{\partial x_n}(x)\Big)$$

is a bi-analytic bijection. A fortiori, there is a unique point $c \in (p\mathbb{Z}_p)^n$ such that $T(c) = (-a_1, \dots, -a_n)$. Since $\mathrm{grad}(f)_{|x} = \mathrm{grad}(g)_{|x} + (a_1, \dots, a_n)$, the condition $T(x) = (-a_1, \dots, -a_n)$ is equivalent with the condition $\mathrm{grad}(f)_{|x} = 0$ for $x \in (p\mathbb{Z}_p)^n$. Thus c is the unique critical point of f. Moreover, $\det(\mathrm{Hs}(f)_{|c}) \neq 0$ since $\det(\mathrm{Hs}(f)_{|c}) \equiv \det(\mathrm{Hs}(f)_{|0}) \not\equiv 0 \bmod p$. □

Finally, we give an application of Morse's lemma to calculate character sums of polynomials.

Proposition 3.5. — *Let $p \neq 2$, let $f \in \mathbb{Z}_p[x_1, \dots, x_n]$ be a polynomial, and let X be a smooth subvariety of $\mathbb{A}^n_{\mathbb{Z}_p}$ (smooth variety meaning a separated, reduced, irreducible scheme of finite type and smooth over $\mathbb{Z}_p$). Let M be the compact p-adic variety $X(\mathbb{Z}_p) \setminus f^{-1}(p\mathbb{Z}_p)$ and write d for the dimension of M. Let χ be a primitive multiplicative character* mod p^m, *$m > 1$. Let $c_1, \dots, c_\ell$ in M be the critical points of $f_{|M} : M \to \mathbb{Z}_p$ and suppose that the critical points $c_1, \dots, c_\ell$ are non-degenerate modulo p. Put*

$$S_f = \sum_{x \in X(\mathbb{Z}_p/p^m\mathbb{Z}_p)} \chi\big(f(x)\big).$$

Then the following holds

$$S_f = \sum_{i=1}^{\ell} \chi\big(f(c_i)\big)\chi_{\frac{1}{2}}\big(f(c_i)^d H_{c_i}\big)^m \widetilde{\alpha}(\chi, m)^d,$$

with $H_{c_i} = 2^{-d}\Delta(\mathrm{Hs}(f)_{|c_i})$, $\widetilde{\alpha}(\chi, m)$ *as in Section 2, and* Δ *the discriminant as defined in 1.2.*

Proof. — That M is a compact p-adic variety follows from Hensel's lemma, by using Taylor expansions for the equations defining X around points in $\mathbb{Z}_p^n$ with different residues mod p. Similarly, there is a cover of M by finitely many disjoint compact opens U such that for each U there is an analytic isometry $\pi : U \to (p\mathbb{Z}_p)^d$. For $i = 1, \ldots, r$, let U_i be the open in this cover containing c_i and we write π_i for the corresponding isometry. By Proposition 2.1 and Lemma 3.4 it follows that $S_f = \sum_{i=1}^{\ell} S_f(c_i)$ where

$$S_f(c_i) = \sum_{x \in (p\mathbb{Z}_p/p^m\mathbb{Z}_p)^d} \chi\big(f \circ \pi_i^{-1}(x)\big).$$

By Morse's lemma we can find for each critical point c_i a bi-analytic isometric transformation $T_i : (p\mathbb{Z}_p)^d \to (p\mathbb{Z}_p)^d$ such that

$$f(x) = f(c_i) + \sum_{j=1}^{d} a_j u_j^2 \quad \text{for all } x \in U_i \text{ and } u = T_i(\pi_i(x)),$$

with a_j in $\mathbb{Z}_p^\times$ and $\chi_{\frac{1}{2}}(H_{c_i}) = \chi_{\frac{1}{2}}(\prod_j a_j)$. We can now calculate

$$S_f(c_i) = \sum_{u \in (p\mathbb{Z}/p^m\mathbb{Z})^d} \chi\Big(f(c_i) + \sum_{j=1}^{d} a_j u_j^2\Big) \tag{3.1}$$

$$= \sum_{u \in (\mathbb{Z}/p^m\mathbb{Z})^d} \chi\Big(f(c_i) + \sum_{j=1}^{d} a_j u_j^2\Big) \tag{3.2}$$

$$= \chi\big(f(c_i)\big)\chi_{\frac{1}{2}}\Big(f(c_i)^d \prod_j a_j\Big)^m \widetilde{\alpha}(\chi, m)^d \tag{3.3}$$

$$= \chi\big(f(c_i)\big)\chi_{\frac{1}{2}}\big(f(c_i)^d H_{c_i}\big)^m \widetilde{\alpha}(\chi, m)^d.$$

Equality (3.1) is clear. Also equality (3.2) is easy and follows by similar arguments as in the proof of Proposition 2.1. Equality (3.3) comes from Proposition 2.4 and the last equality holds because $\chi_{\frac{1}{2}}(H_{c_i}) = \chi_{\frac{1}{2}}(\prod_j a_j)$. □

4. Discrete Fourier transforms of characters of homogeneous polynomials

Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$ and let $\pi_{\mathcal{P}} \in \mathcal{P}$ be of $\mathcal{P}$-adic order 1. Let $L(x) = \sum_{i=1}^n a_i x_i$ be a linear form on $(\mathcal{O}_K/\mathcal{P}^m)^n$, with $m > 1$ and $a_i \in \mathcal{O}_K/\mathcal{P}^m$. Let $f \in \mathcal{O}_K[x]$ be a homogeneous polynomial of degree d and let χ, resp. ψ, be a primitive multiplicative, resp. primitive additive, character $\bmod \mathcal{P}^m$.

We will calculate the discrete Fourier transform of $\chi(f)$, defined by

$$S(L) := \sum_{x\in(\mathcal{O}_K/\mathcal{P}^m)^n} \chi\big(f(x)\big)\psi\big(L(x)\big).$$

After a linear change of variables one can assume that the $\mathcal{P}$-valuation of a_1 is minimal among the $v_{\mathcal{P}}(a_i)$. Write

$$k := v_{\mathcal{P}}(a_1) \quad \text{and} \quad L(x) = \pi_{\mathcal{P}}^k(a_1'x_1 + a_2'x_2 + \cdots + a_n'x_n)$$

for some $a_i' \in \mathcal{O}_K/\mathcal{P}^m$. After applying the invertible linear transformation

$$(x_1,\ldots,x_n) \longmapsto (a_1'x_1 + \cdots + a_n'x_n, x_2, \ldots, x_n),$$

one reduces to the case that $L(x) = \pi_{\mathcal{P}}^k x_1$. This reduction is used in the proof of the following result.

Proposition 4.1. — *Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$ and let $\pi_{\mathcal{P}} \in \mathcal{P}$ be of $\mathcal{P}$-adic order* 1. *Let $L(x) = \sum_{i=1}^n a_i x_i$ be a linear form on $(\mathcal{O}_K/\mathcal{P}^m)^n$, with $m > 1$ and $a_i \in \mathcal{O}_K/\mathcal{P}^m$. Let $f \in \mathcal{O}_K[x]$ be a homogeneous polynomial of degree d and let χ, (resp. ψ), be a primitive multiplicative, (resp. primitive additive, character* $\bmod \mathcal{P}^m$). *Put $k := \min_{i=1,\ldots,n} v_{\mathcal{P}}(a_i)$ and*

$$S(L) = \sum_{x\in(\mathcal{O}_K/\mathcal{P}^m)^n} \chi\big(f(x)\big)\psi\big(L(x)\big).$$

If $\mathcal{P} \nmid d$, then $S(L) = 0$ if $k \neq 0$ and

$$S(L) = \Big(\sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(y)\psi(y)\Big)\Big(\sum_{\substack{x\in(\mathcal{O}_K/\mathcal{P}^m)^n \\ L(x)\equiv 1 \bmod \mathcal{P}^m}} \chi\big(f(x)\big)\Big) \quad \textit{if } k = 0.$$

Proof. — As explained in the previous discussion, we may assume that $L(x) = \pi_{\mathcal{P}}^k x_1$, with $\pi_{\mathcal{P}} \in \mathcal{P}$ of $\mathcal{P}$-adic order 1. We split up the sum depending on the $\mathcal{P}$-valuation of x_1. Let us denote by A_{jk} the subsum of $S(L)$ over the elements x with $v_{\mathcal{P}}(x_1) = j$. So, $S(L) = \sum_{j=0}^m A_{jk}$, with

$$A_{jk} := \sum_{\substack{y\in(\mathcal{O}_K/\mathcal{P}^{m-j})^\times \\ x_1 = y\pi_{\mathcal{P}}^j \\ \widehat{x}\in(\mathcal{O}_K/\mathcal{P}^m)^{n-1}}} \chi\big(f(y\pi_{\mathcal{P}}^j, \widehat{x})\big)\psi(\pi_{\mathcal{P}}^{j+k}y),$$

where $\widehat{x} := (x_2, \ldots, x_n)$. Rewrite $q^j A_{jk}$ as

$$\sum_{\substack{y\in(\mathcal{O}_K/\mathcal{P}^m)^\times\\ \widehat{x}\in(\mathcal{O}_K/\mathcal{P}^m)^{n-1}}} \chi\big(f(y\pi_{\mathcal{P}}^j, \widehat{x})\big)\psi(\pi_{\mathcal{P}}^{j+k} y) \tag{4.1}$$

$$= \sum_{\substack{y\in(\mathcal{O}_K/\mathcal{P}^m)^\times\\ \widehat{x}\in(\mathcal{O}_K/\mathcal{P}^m)^{n-1}}} \chi\big(f(y\pi_{\mathcal{P}}^j, y\hat{x})\big)\psi(\pi_{\mathcal{P}}^{j+k} y) \tag{4.2}$$

$$= \Bigg(\sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(y)\psi(\pi_{\mathcal{P}}^{j+k} y)\Bigg)\Bigg(\sum_{\widehat{x}\in(\mathcal{O}_K/\mathcal{P}^m)^{n-1}} \chi\big(f(\pi_{\mathcal{P}}^j, \widehat{x})\big)\Bigg). \tag{4.3}$$

Equality (4.1) holds because only the value of y mod $\mathcal{P}^{m-j}$ is relevant. Equality (4.2) is just substituting $\widehat{x} = (x_2, \ldots, x_n)$ by $y\widehat{x} = (yx_2, \ldots, yx_n)$; since y is a unit the set over which we sum does not change. The last equality uses that f is homogeneous of degree d and the fact that $\chi^d(y) = 0$ if $y \notin (\mathcal{O}_K/\mathcal{P}^m)^\times$.

We want to prove that all A_{jk} are zero except when $k = j = 0$. Since $\mathcal{P} \nmid d$, we have that χ^d is still a primitive character mod$\mathcal{P}^m$. Therefore, there exists an $a \in \mathcal{O}_K/\mathcal{P}^m$ such that $a \equiv 1 \bmod \mathcal{P}^{m-1}$ and $\chi^d(a) \neq 1$ (see Section 2). By a classical argument, we obtain

$$\begin{aligned}\sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(y)\psi(\pi_{\mathcal{P}}^{j+k} y) &= \sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(ay)\psi(a\pi_{\mathcal{P}}^{j+k} y)\\ &= \chi^d(a) \sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(y)\psi(\pi_{\mathcal{P}}^{j+k} y),\end{aligned}$$

if $j + k \geq 1$. Indeed, the first equation is just substituting y by ay, where a is a unit. The second uses the fact that χ^d is multiplicative and since $a \equiv 1$ mod $\mathcal{P}^{m-1}$, we have $ay \equiv y$ mod $\mathcal{P}^{m-k-j}$ if $j + k \geq 1$.

Since $\chi^d(a) \neq 1$, we conclude that

$$\sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(y)\psi(\pi_{\mathcal{P}}^{j+k} y) = 0.$$

Note that when $j + k \geq m$ this sum is just $\sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(y)$ which is directly seen to be zero. This proves the proposition since only A_{00} is non-zero by equality (4.3). This argument can also be found in [24], Chapter VII, Prop. 13. □

5. Applications to prehomogeneous vector spaces

We use the notation and the asumptions from the introduction.

Proof of Theorem 1.1. — For any $v^\vee \in V^\vee$ let $H(v^\vee)$ be the hyperplane in V defined by $v^\vee(x) - 1$. By [5, Lemma 9.1.2] and [5, Lemma 9.1.7], for any $v^\vee$ with $f^\vee(v^\vee) \neq 0$, the restriction $f_{|H(v^\vee)\cap\Omega}$ has the point $d^{-1}F^\vee(v^\vee)$ as its unique critical point and it is a non-degenerate critical point. The fact that this holds for all $v^\vee$ with $f^\vee(v^\vee) \neq 0$ is a first order statement (in the language of rings), and hence, the analogue statement is true over finite fields of big enough characteristic. That is, for all prime ideals $\mathcal{P}$ of $\mathcal{O}_K$ above big enough primes $p \in \mathbb{Z}$ with residue field $k_\mathcal{P}$, for all $v^\vee \in V^\vee(k_\mathcal{P})$ with $f^\vee(v^\vee) \neq 0$, the point $d^{-1}F^\vee(v^\vee)$ is the unique critical point of $f_{|H(v^\vee)\cap\Omega(k_\mathcal{P})}$ and it is a non-degenerate critical point.

Take a prime ideal $\mathcal{P}$ above a big enough prime p. Choose $L \in V^\vee(\mathcal{O}_K/\mathcal{P}^m)$ with $f^\vee(L) \not\equiv 0 \bmod \mathcal{P}$. Let $L_0 \in V^\vee(\mathcal{O}_K)$ lie above L. Let c be $d^{-1}F^\vee(L_0)$. Let R be the valuation ring of the $\mathcal{P}$-adic completion of K. Since $\mathcal{P}$ is supposed to lie above a big enough prime $p \in \mathbb{Z}$, we may suppose that d is invertible in R, and hence, c lies in $V(R)$. Make the plane $H(L_0)$ into a vector space by choosing a zero point in $H(L_0)(\mathcal{O}_K)$. Take a basis of the lattice $H(L_0)(\mathcal{O}_K)$ in $H(L_0)$ and take coordinates on $H(L_0)$ with respect to this basis. Let H_c be 2^{-n+1} times the determinant of the Hessian in c of $f_{|H(L_0)}$, expressed in these coordinates. Since $p \in \mathbb{Z}$ is big enough and by the above discussion, H_c lies in R and $H_c \bmod \mathcal{P}$ is nonzero in $\mathcal{O}_K/\mathcal{P}$, and this is so uniformly in $L \in V^\vee(\mathcal{O}_K/\mathcal{P}^m)$.

Then,

$$S(L) = \Big(\sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(y)\psi(y)\Big)\Big(\sum_{\substack{x\in V(\mathcal{O}_K/\mathcal{P}^m)\\ L(x)\equiv 1 \bmod \mathcal{P}^m}} \chi\big(f(x)\big)\Big) \tag{5.1}$$

$$= \Big(\sum_{y\in\mathcal{O}_K/\mathcal{P}^m} \chi^d(y)\psi(y)\Big)\chi\big(f(c)\big)\chi_{\frac12}\big(f(c)^{n-1}H_c\big)^m\widetilde{\alpha}(\chi,m)^{n-1} \tag{5.2}$$

$$= q^{\frac12 mn}\Big(\frac{\sum_{\mathcal{O}_K/\mathcal{P}^m}\chi^d(y)\psi(y)}{q^{\frac12 m}}\Big)\chi\Big(\frac{b_0 f^\vee(L)^{-1}}{d^d}\Big)\kappa^\vee(L)\frac{\widetilde{\alpha}(\chi,m)^{n-1}}{q^{\frac12(n-1)m}}, \tag{5.3}$$

with $\kappa^\vee(L) = \chi_{\frac12}(f(c)^{n-1}H_c)^m$. Equality (5.1) follows from Proposition 4.1. We obtain (5.2) from Proposition 3.5. If we now use the fact that $f(c) = d^{-d}f(F^\vee(L)) = d^{-d}b_0 f^\vee(L)^{-1}$ (see [5, Lemma 9.1.2] and [6, Lemma 1.8]), equation (5.3) and thus case 1) of the theorem follows with $\kappa^\vee(L) = \chi_{\frac12}(f(c)^{n-1}H_c)^m$ and $\alpha(\chi,m) = \widetilde{\alpha}(\chi,m)^{n-1}/q^{\frac12(n-1)m}$.

Now we prove case 2) of Theorem 1.1 with a technique of N. Kawanaka. The function $S : \mathrm{Hom}((\mathcal{O}_K/\mathcal{P}^m)^n, \mathcal{O}_K/\mathcal{P}^m) \to \mathbb{C}$, $L \mapsto S(L)$ is the discrete Fourier transform of $\chi(f) : (\mathcal{O}_K/\mathcal{P}^m)^n \to \mathbb{C}$, $x \mapsto \chi(f(x))$. By a classical result on

L_2-norms of Fourier transforms on finite abelian groups, it follows that

$$\|S\|_2^2 = q^{mn}\big\|\chi(f)\big\|_2^2 = q^{mn}N_1, \tag{5.4}$$

with $N_1 := \#A$ and $A := \{x \in V(\mathcal{O}_K/\mathcal{P}^m) \mid f(x) \not\equiv 0 \bmod \mathcal{P}\}$.

It follows from the formula in case 1), that $|S(L)|^2 = q^{mn}$ for $L \in A$. Writing $B := V(\mathcal{O}_K/\mathcal{P}^m) \setminus A$, one has

$$\|S\|_2^2 = \sum_A q^{mn} + \sum_B \big|S(L)\big|^2, \tag{5.5}$$

and hence, $S(L) = 0$ for $L \in B$. □

Proof of Theorem 1.3. — The statement about $\alpha(\chi, m)$ follows from equation (5.3) and Lemma 2.3. We recall that $h^\vee(L)$ is defined in the introduction, and that the number $\chi_{\frac{1}{2}}(h^\vee(L))$ is well-defined. We obtain the value of $\kappa^\vee(L)$ as an immediate corollary of [5, Lemma 9.1.7]. □

Appendix A

L-functions of prehomogeneous vector spaces (by Fumihiro Sato)

In this note, we give an application of Theorems 1.1 and 1.3 in [3] (and Theorems A, B, C in [5]) to the functional equation of L-functions of Dirichlet type associated with prehomogeneous vector spaces, which is a generalization of Theorem L in [16].

In the following we retain the notation in [3]. However, for simplicity, we assume that $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{P} = (p)$ with a rational prime p. Let χ be a primitive Dirichlet character with conductor $N > 1$. We extend χ to $\mathbb{Z}/N\mathbb{Z}$ by $\chi(a) = 0$ for $a \notin (\mathbb{Z}/N\mathbb{Z})^\times$. Put $m(p) = v_p(N)$, the p-order of N, for any rational prime p. Since $(\mathbb{Z}/N\mathbb{Z})^\times$ is isomorphic to $\prod_{p|N}(\mathbb{Z}/p^{m(p)}\mathbb{Z})^\times$, χ induces a primitive character $\chi^{(p)} : (\mathbb{Z}/p^{m(p)}\mathbb{Z})^\times \to \mathbb{C}^\times$ for each $p \mid N$.

Let (G, ρ, V) be a reductive prehomogeneous vector space defined over $\mathbb{Q}$. Let $P_1, \ldots, P_\ell$ be the fundamental relative invariants over $\mathbb{Q}$, namely, the $\mathbb{Q}$-irreducible relatively invariant polynomials on V. We denote by ϕ_i $(1 \le i \le \ell)$ the rational character of G corresponding to P_i. The fundamental relative invariants are determined uniquely up to a non-zero constant multiple in $\mathbb{Q}^\times$ and any relative invariant in $\mathbb{Q}[V]$ is a monomial of them.

We fix a basis of the $\mathbb{Q}$-vector space $V(\mathbb{Q})$ and take a relative invariant $f \in \mathbb{Q}[V]$ with coefficients in $\mathbb{Z}$ (with respect to the fixed $\mathbb{Q}$-basis of $V(\mathbb{Q})$). The character ϕ corresponding to f is defined over $\mathbb{Q}$.

In the following we assume that

A.1) f is a *regular* relative invariant, namely, $\Omega = V \backslash f^{-1}(0)$ is a single G-orbit;

A.2) for every $x \in \Omega(\mathbb{Q})$, the group of $\mathbb{Q}$-rational characters of the identity component of $G_x = \{g \in G \mid \rho(g)x = x\}$ is trivial.

We denote by G^+ the identity component of the real Lie group $G(\mathbb{R})$ and put $G_x^+ = G^+ \cap G_x$. Let $\Omega(\mathbb{R}) = \Omega_1 \cup \cdots \cup \Omega_\nu$ be the decomposition into the connected components (in the usual topology). By the assumption A.1), every Ω_i is a single G^+-orbit. Let Γ_N be an arithmetic subgroup of $G(\mathbb{Q})$ which stabilizes $V(\mathbb{Z})$ and induces the identity mapping on $V(\mathbb{Z})/NV(\mathbb{Z})$. Then the function $V(\mathbb{Z}) \ni x \mapsto \chi(f(x)) \in \mathbb{C}$ is Γ_N-invariant and factors through $V(\mathbb{Z}/N\mathbb{Z})$. The L-functions $L_i(\boldsymbol{s};\chi)$ $(1 \le i \le \nu)$ associated with (G,ρ,V) and χ are defined by

$$L_i(\boldsymbol{s};\chi) = \sum_{x \in \Gamma_N \backslash (V(\mathbb{Z}) \cap \Omega_i)} \mu(x)\chi\big(f(x)\big) \prod_{j=1}^{\ell} \big|P_j(x)\big|^{-s_j}, \quad \boldsymbol{s} = (s_1,\dots,s_\ell) \in \mathbb{C}^\ell,$$

where $\mu(x)$ is the volume of the fundamental domain $G_x^+/(\Gamma_N \cap G_x^+)$ with respect to the normalized Haar measure on G_x^+ (for the normalization of the Haar measure on G_x^+, see [15], §4). By the assumptions A.1), A.2) and [13, Theorem 1.1], the L-functions converge absolutely when the real parts of $s_1,\dots,s_\ell$ are sufficiently large.

We take a relative invariant $f^\vee$ of the dual prehomogeneous vector space $(G,\rho^\vee,V^\vee)$ with coefficients in $\mathbb{Z}$ (with respect to the basis of $V^\vee$ dual to the fixed basis of V) that corresponds to the character ϕ^{-1}. Then $f^\vee$ and $(G,\rho^\vee,V^\vee)$ satisfy the assumptions A.1) and A.2). Put $\Omega^\vee = V^\vee \setminus {f^\vee}^{-1}(0)$. We may order the fundamental relative invariants $P_1^\vee,\dots,P_\ell^\vee$ of $(G,\rho^\vee,V^\vee)$ such that the character corresponding to $P_i^\vee$ is ϕ_i^{-1}.

Our final assumption is the following:

A.3) for every prime factor p of N with $m(p) > 1$ (resp. $m(p) = 1$), Theorems 1.1 and 1.3 in [3] (resp. Theorems A, B, C in [5]) hold for $\chi^{(p)}$ and f.

Let $\psi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times$ be an additive primitive character. By the Chinese remainder theorem, ψ determines an additive primitive character $\psi^{(p)} : \mathbb{Z}/p^{m(p)}\mathbb{Z} \to \mathbb{C}^\times$ for each $p \mid N$. For $L \in V^\vee(\mathbb{Z})$, let us consider the character sum

$$S(\chi,f;L) = \sum_{x \in V(\mathbb{Z}/N\mathbb{Z})} \chi\big(f(x)\big)\psi\big(L(x)\big) = \prod_{p \mid N} \sum_{x \in V(\mathbb{Z}/p^{m(p)}\mathbb{Z})} \chi^{(p)}\big(f(x)\big)\psi^{(p)}\big(L(x)\big).$$

Then, by assumptions A.1) and A.3), we have

$$S(\chi,f;L) = \chi^{-1}(f^\vee(L)) \prod_{p \mid N} \kappa_p^\vee(L) g(\chi^{(p)},f), \tag{A.4}$$

with $L \bmod N \in \Omega^\vee(\mathbb{Z}/N\mathbb{Z})$ and where $\kappa_p^\vee(L)$ is the constant $\kappa^\vee(L) = \pm 1$ given for each (sufficiently large) p by Theorem 1.3 in [3] or Theorems B and C in [5], and $g(\chi^{(p)}, f)$ is a constant independent of L whose explicit value can be easily seen from Theorems 1.1 and 1.3 in [3] or Theorem A in [5] according as $m(p) > 1$ or $m(p) = 1$. Put

$$\kappa^\vee(L) = \prod_{p|N} \kappa_p^\vee(L) \quad \text{and} \quad g(\chi, f) = \prod_{p|N} g(\chi^{(p)}, f).$$

Now we define the L-functions associated with $(G, \rho^\vee, V^\vee)$ by

$$L_i^\vee(\boldsymbol{s}; \chi^{-1}) = \sum_{L \in \Gamma_N \backslash (V^\vee(\mathbb{Z}) \cap \Omega_i^\vee)} \mu^\vee(L)\kappa^\vee(L)\chi^{-1}\big(f^\vee(L)\big) \prod_{j=1}^{\ell} \left|P_j^\vee(L)\right|^{-s_j}.$$

Assumptions A.1), A.2) and [13, Thm. 1.1] again imply that these L-functions converge absolutely when the real parts of $s_1, \ldots, s_\ell$ are sufficiently large. The abscissa of absolute convergence is independent of χ and N.

To describe analytic properties of the L-functions, we need some more notational preliminaries. Let $b(\boldsymbol{s}) = b(s_1, \ldots, s_\ell)$ be the Bernstein-Sato polynomial defined by

$$\text{(A.5)} \qquad \Big(\prod_{i=1}^{\ell} P_i^\vee(\mathrm{grad}_x)\Big) \prod_{i=1}^{\ell} P_i(x)^{s_i} = b(\boldsymbol{s}) \prod_{i=1}^{\ell} P_i(x)^{s_i - 1}.$$

It is known that the function $b(\boldsymbol{s})$ is a product of inhomogeneous linear forms $s_1, \ldots, s_\ell$ of integral coefficients (see [18]). We also need the Bernstein-Sato polynomial $b_f(s)$ of f, which is defined by

$$f^\vee(\mathrm{grad}_x) f(x)^{s+1} = b_f(s) f(x)^s.$$

It is known that the roots of $b_f(s)$ are negative rational numbers.

Each of the assumptions A.1) and A.2) implies that there exists a $\delta = (\delta_1, \ldots, \delta_\ell) \in (\frac{1}{2}\mathbb{Z})^\ell$ such that the relative invariant $\prod_{i=1}^{\ell} P_i(x)^{2\delta_i}$ corresponds to the character $\det \rho(g)^2$ (see [19, Prop. 8] or [18, Prop. 11] for A.1) and [15, Lemma 4.1] for A.2)).

Finally we recall the fundamental theorem of the theory of prehomogeneous vector spaces over the real number field $\mathbb{R}$. For $i = 1, \ldots, \nu$ and $\boldsymbol{s}$ with $\mathrm{Re}(s_1), \ldots, \mathrm{Re}(s_\ell) > 0$, we define a continuous function $|P(x)|_{\Omega_i}^{\boldsymbol{s}}$ on $V(\mathbb{R})$ by

$$\left|P(x)\right|_{\Omega_i}^{\boldsymbol{s}} = \begin{cases} \prod_{j=1}^{\ell} |P_j(x)|^{s_j} & (x \in \Omega_i), \\ 0 & (x \notin \Omega_i). \end{cases}$$

The function $|P(x)|_{\Omega_i}^{\boldsymbol{s}}$ depends holomorphically on $\boldsymbol{s}$ and is extended to a tempered distribution on $V(\mathbb{R})$ depending meromorphically on $\boldsymbol{s} \in \mathbb{C}^\ell$. We denote the tempered distribution by the same symbol. We can also define the tempered distributions $|P^\vee(L)|^{\boldsymbol{s}}_{\Omega_i^\vee}$ on $V^\vee(\mathbb{R})$ quite similarly. Then the fundamental theorem reads

$$\int_{V(\mathbb{R})} \big|P(x)\big|^{\boldsymbol{s}-\delta}_{\Omega_i} \exp\big(2\pi i L(x)\big)\,\mathrm{d}x = \sum_{j=1}^{\nu} \gamma_{ij}(\boldsymbol{s})\big|P^\vee(L)\big|^{-\boldsymbol{s}}_{\Omega_j^\vee}, \tag{A.6}$$

where $\gamma_{ij}(\boldsymbol{s})$ $(i,j = 1,\dots,\nu)$ have elementary (but not explicit) expressions in terms of the gamma function and the exponential function (see [17], [15]).

Theorem A.1. — 1) *The L-functions $L_i(\boldsymbol{s};\chi)$ and $L_i^\vee(\boldsymbol{s};\chi^{-1})$ multiplied by $b(\boldsymbol{s}-\delta)$ have analytic continuations to holomorphic functions of $\boldsymbol{s}$ in $\mathbb{C}^\ell$ and satisfy the following functional equation*

$$g(\chi,f)\cdot L_j^\vee(\delta-\boldsymbol{s};\chi^{-1}) = N^{d_1 s_1+\cdots+d_\ell s_\ell}\sum_{i=1}^{\nu}\gamma_{ij}(\boldsymbol{s})L_i(\boldsymbol{s};\chi),$$

where d_i $(1\le i\le \ell)$ is the degree of the fundamental relative invariant P_i and $\gamma_{ij}(\boldsymbol{s})$ is the same as above.

2) *Assume that χ satisfies at least one of the following conditions:*

- *$m(p)\ge 2$ for some p dividing the conductor N of χ;*
- *the order of $\chi^{(p)}$ for some $p \mid N$ with $m(p)=1$ is different from the reduced denominators of the roots of the Bernstein-Sato polynomial $b_f(s)$.*

Then the L-functions $L_i(\boldsymbol{s};\chi)$ and $L_i^\vee(\boldsymbol{s};\chi^{-1})$ are entire functions of $\boldsymbol{s}$ in $\mathbb{C}^\ell$.

Since the proof of the theorem is almost the same as the one of Theorem 2 and Corollary 1 of [15], we shall give only an outline of the proof.

Denote by $\mathbb{A}$ the ring of adeles of $\mathbb{Q}$ and by $\mathbb{A}_0 = \prod'_{p<\infty}\mathbb{Q}_p$ the ring of finite adeles of $\mathbb{Q}$. Denote by $\Phi_p(x_p)$ the characteristic function of $V(\mathbb{Z}_p)$ and put $\Phi_0(x_0) = \prod_{p<\infty}\Phi_p(x_p)$ for $x_0 = (x_p)\in\mathbb{A}_0$. The function $\Phi_0(x_0)$ is the characteristic function of $\prod_{p<\infty}V(\mathbb{Z}_p)$. Let $\Phi_\infty(x_\infty)$ be a rapidly decreasing C^∞-function on $V(\mathbb{R})$ and define a function Φ_χ on $V(\mathbb{A})$ by

$$\Phi_\chi(x) = \Phi_\infty(x_\infty)\prod_{p\mid N}\chi^{(p)}\big(f(x_p)\big)\Phi_0(x_0)\quad\big(x=(x_\infty,x_0)\in V(\mathbb{A})\big).$$

The function Φ_χ is a Schwartz-Bruhat function on $V(\mathbb{A})$ and the Poisson summation formula implies the identity

$$\sum_{x\in V(\mathbb{Q})}\Phi_\chi\big(\rho(g)x\big) = \big|\det\rho(g)\big|^{-1}_{\mathbb{A}}\sum_{L\in V^\vee(\mathbb{Q})}\widehat{\Phi}_\chi\big(\rho^\vee(g)L\big)\quad\big(g\in G(\mathbb{A})\big), \tag{A.7}$$

where $\widehat{\Phi}_\chi$ is the Fourier transform of Φ_χ, which is defined by an additive character of $\mathbb{A}/\mathbb{Q}$ of conductor 1, more specifically, the additive character whose

p-component is of conductor 1 and coincides with $\psi^{(p)}(Nx)$ on $p^{-m(p)}\mathbb{Z}_p$ if p divides N. It is easy to see that

$$\widehat{\Phi}_\chi(L) = N^{-n}S(\chi, f; NL_0)\Phi_0(NL_0)\widehat{\Phi}_\infty(L_\infty), \tag{A.8}$$

with $L = (L_\infty, L_0) \in V^\vee(\mathbb{A})$ and $n = \dim V$. We note here that the function $S(\chi, f; L)$ originally defined on $V^\vee(\mathbb{Z})$ can naturally be extended to a function on $\prod_{p<\infty} V^\vee(\mathbb{Z}_p)$. By the usual technique of unfolding, we have

$$\begin{aligned}\int_{G^+/\Gamma_N} \prod_{j=1}^{\ell} |\phi_j(g_\infty)|^{s_j} \sum_{x\in\Omega(\mathbb{Q})} \Phi_\chi\big(\rho(g_\infty, 1)x\big)\,\mathrm{d}g_\infty \\ = \sum_{i=1}^{\nu} L_i(\boldsymbol{s};\chi)\big\langle |P(x)|_{\Omega_i}^{\boldsymbol{s}-\delta}, \Phi_\infty\big\rangle.\end{aligned} \tag{A.9}$$

By the identities (A.4) and (A.8), we also have

$$\begin{aligned}\int_{G^+/\Gamma_N} \prod_{j=1}^{\ell} |\phi_j(g_\infty)|^{-s_j} \sum_{L\in\Omega^\vee(\mathbb{Q})} \widehat{\Phi}_\chi\big(\rho^\vee(g_\infty, 1)L\big)\,\mathrm{d}g_\infty \\ = N^{\Sigma_{j=1}^{\ell} d_j s_j - n} g(\chi, f) \sum_{i=1}^{\nu} L_i^\vee(\boldsymbol{s};\chi^{-1})\big\langle |P^\vee(L)|_{\Omega_i^\vee}^{\boldsymbol{s}-\delta}, \widehat{\Phi}_\infty\big\rangle.\end{aligned}$$

Now Theorem A.1 can be proved in the same manner as in [15, §6] by using these integral representations of the L-functions, the Poisson summation formula (A.7), and the fundamental theorem (A.6) over $\mathbb{R}$. We note here that the Poisson summation formula (A.7) is used in the form

$$\sum_{x\in\Omega(\mathbb{Q})} \Phi_\chi\big(\rho(g)x\big) = \big|\det\rho(g)\big|_{\mathbb{A}}^{-1} \sum_{L\in\Omega^\vee(\mathbb{Q})} \widehat{\Phi}_\chi\big(\rho^\vee(g)L\big) + I(\Phi_\chi, g),$$

where

$$I(\Phi_\chi, g) = \big|\det\rho(g)\big|_{\mathbb{A}}^{-1} \sum_{L\notin\Omega^\vee(\mathbb{Q})} \widehat{\Phi}_\chi\big(\rho^\vee(g)L\big) - \sum_{x\notin\Omega(\mathbb{Q})} \Phi_\chi\big(\rho(g)x\big).$$

The contribution of $I(\Phi_\chi, g)$ to the integral representation contains the information on the poles of the L-functions and is in general very hard to calculate explicitly. However, if we take a test function of the form

$$\Phi_\infty(x_\infty) = \Big(\prod_{\ell=1}^{\ell} P_\ell^\vee(\mathrm{grad}_x)\Big)\Phi'_\infty(x_\infty)$$

for a C^∞-function Φ'_∞ with compact support in $\Omega(\mathbb{R})$, then $I(\Phi_\chi, g)$ vanishes and, by using (A.5), we can prove the first assertion of Theorem A.1. If the assumption of the second assertion of Theorem A.1 is fulfilled, then Theorem 1.1, 2) in [3] and Remark 5.2.3.3 in [5] imply the vanishing of $I(\Phi_\chi, (g_\infty, 1))$ for $g_\infty \in G^+$ and arbitrary Φ_∞ with compact support in $\Omega(\mathbb{R})$. The second assertion of Theorem A.1 follows immediately from this observation.

REMARK A.2. — The simplest example of the L-functions considered in this note is the Dirichlet L-function, which is the L-function associated with $(\mathrm{GL}_1, \rho, V(1))$, where ρ is the standard 1-dimensional representation of GL_1. Further examples of the L-functions associated with prehomogeneous vector spaces have been studied in [21], [4], [11], [12], [22] and [23]. It is noteworthy that, unlike the case of the Dirichlet L-functions, the L-functions $L_i(\mathbf{s};\chi)$ may have poles even for non-trivial χ, if χ does not satisfy any one of the conditions in Theorem A.1, 2) (for concrete examples, see [4, Thm. 6.2], [11, Thm. 4.2] and [12, Thm. 5]). It is an interesting problem to determine the conditions on χ under which $L_i(\mathbf{s};\chi)$ has actually poles.

BIBLIOGRAPHY

[1] Z. I. Borevitch & I. R. Chafarevitch – *Théorie des nombres*, Traduit par Myriam et Jean-Luc Verley. Traduction faite d'après l'édition originale russe. Monographies Internationales de Mathématiques Modernes, No. 8, Gauthier-Villars, 1967.

[2] N. Bourbaki – *Éléments de mathématique. Fasc. XXXIII. Variétés différentielles et analytiques. Fascicule de résultats (Paragraphes 1 à 7)*, Actualités Scientifiques et Industrielles, No. 1333, Hermann, 1967.

[3] R. Cluckers & A. Herremans – "The Fundamental Theorem of prehomogeneous vector spaces modulo p^m", main body of this article.

[4] B. Datskovsky & D. J. Wright – "The adelic zeta function associated to the space of binary cubic forms. II. Local theory", *J. Reine Angew. Math.* **367** (1986), p. 27–75.

[5] J. Denef & A. Gyoja – "Character sums associated to prehomogeneous vector spaces", *Compositio Math.* **113** (1998), p. 273–346.

[6] A. Gyoja – "Theory of prehomogeneous vector spaces without regularity condition", *Publ. Res. Inst. Math. Sci.* **27** (1991), p. 861–922.

[7] J.-i. Igusa – "Some results on p-adic complex powers", *Amer. J. Math.* **106** (1984), p. 1013–1032.

[8] ______, *An introduction to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics, vol. 14, American Mathematical Society, 2000.

[9] D. Kazhdan & A. Polishchuk – "Generalized character sums associated to regular prehomogeneous vector spaces", *Geom. Funct. Anal.* **10** (2000), p. 1487–1506.

[10] J. Milnor – *Morse theory*, Based on lecture notes by M. Spivak and R. Wells. Annals of Mathematics Studies, No. 51, vol. 51, Princeton University Press, 1963.

[11] H. Saito – "A generalization of Gauss sums and its applications to Siegel modular forms and L-functions associated with the vector space of quadratic forms", *J. Reine Angew. Math.* **416** (1991), p. 91–142.

[12] ______, "On L-functions associated with the vector space of binary quadratic forms", *Nagoya Math. J.* **130** (1993), p. 149–176.

[13] ______, "Convergence of the zeta functions of prehomogeneous vector spaces", *Nagoya Math. J.* **170** (2003), p. 1–31.

[14] F. Sato – "L-functions of prehomogeneous vector spaces", Appendix of this article.

[15] ______, "Zeta functions in several variables associated with prehomogeneous vector spaces. I. Functional equations", *Tōhoku Math. J. (2)* **34** (1982), p. 437–483.

[16] ______, "On functional equations of zeta distributions", *Adv. Stud. Pure Math.* **15** (1989), p. 465–508.

[17] M. Sato – "Theory of prehomogeneous vector spaces", *Sugaku no Ayumi* **15** (1970), p. 85–157, notes by T. Shintani.

[18] ______, "Theory of prehomogeneous vector spaces (algebraic part)—the English translation of Sato's lecture from Shintani's note", *Nagoya Math. J.* **120** (1990), p. 1–34, Notes by Takuro Shintani, Translated from the Japanese by Masakazu Muro.

[19] M. Sato & T. Kimura – "A classification of irreducible prehomogeneous vector spaces and their relative invariants", *Nagoya Math. J.* **65** (1977), p. 1–155.

[20] J-P. Serre – "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), p. 323–401.

[21] H. M. Stark – "L-functions and character sums for quadratic forms. I", *Acta Arith.* **14** (1967/1968), p. 35–50.

[22] T. Ueno – "Elliptic modular forms arising from zeta functions in two variables attached to the space of binary Hermitian forms", *J. Number Theory* **86** (2001), p. 302–329.

[23] ______, "Modular forms arising from zeta functions in two variables attached to prehomogeneous vector spaces related to quadratic forms", 2004, to appear in Nagoya Math. J., p. 1–37.

[24] A. Weil – *Basic number theory*, Die Grundlehren der mathematischen Wissenschaften, Band 144, Springer New York, Inc., New York, 1967.