数理解析研究所講究録
第 1715 巻 2010 年 32-36

Orbital Gauss sums associated with the space of binary cubic forms over a finite field

京都大学 理学部 数学教室　森 伸吾 (Shingo Mori)
Department of Mathematics, Kyoto University

§0 Introduction

We consider an orbital L-function associated with the space of binary cubic forms over rational integer ring. The orbital L-function satisfy a functional equation. The functional equation may be expressed in terms of an orbital Gauss sum. In this paper, we shall evaluate the orbital Gauss sum.

Notation. If K is a field, $K^\times$ is its group of units and $M_n(K)$ is the ring of $n\times n$ matrices over K. When K is commutative, $GL_n(K)$ is the group of $n\times n$ matrices over K which are invertible. We use the notation $B(K)$ and $N(K)$ for the subgroups of $GL_n(K)$ of matrices of the form

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \quad \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

respectively. Unless otherwise specified, $G_K = G(K) = GL_2(K)$.

Let χ be a Dirichlet character of conductor f. An usual Gauss sum is defined by

$$\tau(\chi) = \sum_{a=1}^{f} \chi(a) \exp\Big(\frac{2\pi\sqrt{-1}}{f}\Big).$$

§1 The space of binary cubic forms over a finite field.

First, a review of the basic theory is in order. Let K be a field. The space V_K of binary cubic forms with coefficients in the field K is of four dimensional, and we shall identify a 4-tuple $x=(x_1,x_2,x_3,x_4)\in K^4$ with the form given by:

$$F_x(u,v) = x_1u^3 + x_2u^2v + x_3uv^2 + x_4v^3.$$

We shall define an action of the group $G_K = GL_2(K)$ on V_K by the following functional equation:

$$F_{g\cdot x} = (\det g)^{-1} F_x((u,v)\begin{pmatrix} a & b \\ c & d \end{pmatrix})$$

where x is any element of V_K and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is any element of G_K. This is arranged so that $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot x = ax$. Let $P(x)$ denote the discriminant of the form F_x, explicitly given by

$$P(x) = x_2^2x_3^2 + 18x_1x_2x_3x_4 - 4x_2^3x_4 - 4x_1x_3^3 - 27x_1^2x_4^2.$$

The hypersurface $S_K = \{x \in V \mid P(x) = 0\}$ is invariant under G_K. Let V'_K denote the set of all nonsingular forms in V_K, $V'_K = \{x \in V_K \mid P(x) \neq 0\} = V_K - S_K$. A basic feature of this representation is that

$$P(g \cdot x) = (\det g)^2 P(x).$$

A non zero rational function $R(x)$ on V_K is called a relative G_K-invariant if there exists a character χ of G_K such that $R(g \cdot x) = \chi(g)R(x)$ for all $x \in V_K$ and $g \in G_K$. The discriminant generates the ring of relative invariants of this representation of $GL_2(K)$.

§2

Let p be a prime number. We shall assume that $p \neq 2, 3$. Let $\mathbb{F}_q$ be the finite field of prime power of order q. We put $K = \mathbb{F}_q$. The hypersurface S_K and nonsingular set V'_K decomposes into three G_K orbits.

Lemma 1. *We put $s_1 = (1,0,0,0)$ and $s_2 = (0,1,0,0)$. The G_K-orbits in S_K are preciously*

$$S_0 = \{0\};$$
$$S_1 = G_K \cdot s_1 = \{x \in V_K \mid F_x \text{ has a triple root}\};$$
$$S_2 = G_K \cdot s_2 = \{x \in V_K \mid F_x \text{ has a double root and a distinct simple root}\}.$$

For a form x in V'_K, let $K(x)$ denote the cubic ring of x over K. The degree of $K(x)$ is 3.

Lemma 2. *Two nonsingular binary cubic forms over $\mathbb{F}_q$ are G_K-equivalent if and only if their cubic ring are same. The G_K-orbits in V'_K are preciously*

$$V'_{K,1} = \{x \in V'_K \mid \mathbb{F}_q(x) = \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q\};$$
$$V'_{K,2} = \{x \in V'_K \mid \mathbb{F}_q(x) = \mathbb{F}_{q^2} \times \mathbb{F}_q\};$$
$$V'_{K,3} = \{x \in V'_K \mid \mathbb{F}_q(x) = \mathbb{F}_{q^3}\}.$$

The order of stabilizer in G_K of nonsingular binary cubic forms with cubic ring $\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q$, $\mathbb{F}_{q^2} \times \mathbb{F}_q$ and $\mathbb{F}_{q^3}$ is 6, 2 and 3, respectively. If $p \equiv 1 \bmod 3$, there are three nonsingular G_K-orbits with representatives:

$$x_I = (1, 0, -1, 0), \; x_{II} = (r, 0, -1, 0), \; x_{III} = (s, 0, 0, -1),$$

where r is any element of $\mathbb{F}_q^\times$ that is not a square and s is any element that is not a cube.

§3 The orbital Gauss sum.

For simplicity, we shall assume that $K = \mathbb{F}_p$. Let ψ be a character of multiplicative group of $\mathbb{F}_p^\times$ of nonzero elements of $\mathbb{F}_p$. Extend ψ to $\mathbb{F}_p$ by the convention $\psi(0) = 0$. The alternating form:

$$[x, y] = x_1y_4 - \frac{1}{3}x_2y_3 + \frac{1}{3}x_3y_2 - x_4y_1,$$

has the property that $[g \cdot x,\ \det(\mathrm{g})^{-1}g \cdot y] = [x, y]$ for all $x, y \in V_K$ and $g \in G_K$. For $x, y \in V_K$, we put

$$\langle x, y\rangle = \exp\Big(\frac{2\pi\sqrt{-1}}{p}[x, y]\Big).$$

We define the orbital Gauss sum.

Definition 1. *For $a, b \in V_K$, we define*

$$W(\psi, a, b) = \sum_{g \in G_K} \psi(\det(g))\langle x,\ g \cdot y\rangle$$

After basic calculation, we find that

$$W(\psi,\ g \cdot a,\ g' \cdot b) = \psi(\det g)^{-1}\psi(\det g')^{-1}W(\psi, a,\ b)$$

where $g, g' \in G(K)$. We can take the following set:

$$V(\mathbb{F}_p) = \{y_0|y_0 \in S_0\} \sqcup \{y_1|y_1 \in S_1\} \sqcup \{y_2|y_2 \in S_2\} \sqcup \{y_3|y_3 \in V'_{1,K}\} \sqcup \{y_4|y_4 \in V'_{1,K}\} \sqcup \{y_5|y_5 \in V'_{1,K}\}.$$

For positive integers $i,\ j,\ 0 \le i, j \le 5$, we define a matrix valued Gauss sum $W(\psi)$ as a 6×6 matrix whose (i, j) component is given by $\frac{1}{\sharp G(K)_{y_j}} W(\psi, y_i, y_j)$.

We shall assume that $\psi^3 = 1$. Our main result is as follows.

Theorem 1. *Let ψ be a trivial character. If $p \equiv 1 \bmod 3$, then*

$$W(1) = \begin{pmatrix} 1 & p^2-1 & p(p^2-1) & \frac{1}{6}p(p^2-1)(p-1) & \frac{1}{2}p(p-1)(p^2-1) & \frac{1}{3}p(p-1)(p^2-1) \\ 1 & -1 & p(p-1) & \frac{1}{6}p(p-1)(2p-1) & -\frac{1}{2}p(p-1) & -\frac{1}{3}p(p^2-1) \\ 1 & p-1 & p(p-2) & -\frac{1}{2}p(p-1) & -\frac{1}{2}p(p-1) & 0 \\ 1 & 2p-1 & -3p & \frac{1}{6}p(p+5) & -\frac{1}{2}p(p-1) & \frac{1}{3}p(p-1) \\ 1 & -1 & -p & -\frac{1}{6}p(p-1) & \frac{1}{2}p(p+1) & -\frac{1}{3}p(p-1) \\ 1 & -p-1 & 0 & \frac{1}{6}p(p-1) & -\frac{1}{2}p(p-1) & \frac{1}{3}p(p+2) \end{pmatrix}.$$

If $p \equiv 2 \bmod 3$, then

$$W(1) = \begin{pmatrix} 1 & p^2-1 & p(p^2-1) & \frac{1}{6}p(p^2-1)(p-1) & \frac{1}{2}p(p-1)(p^2-1) & \frac{1}{3}p(p-1)(p^2-1) \\ 1 & -1 & p(p-1) & \frac{1}{6}p(p-1)(2p-1) & -\frac{1}{2}p(p-1) & -\frac{1}{3}p(p^2-1) \\ 1 & p-1 & p(p-2) & -\frac{1}{2}p(p-1) & -\frac{1}{2}p(p-1) & 0 \\ 1 & 2p-1 & -3p & \frac{1}{6}p(-p+5) & \frac{1}{2}p(p+1) & -\frac{1}{3}p(p+1) \\ 1 & -1 & -p & \frac{1}{6}p(p+1) & \frac{1}{2}p(-p+1) & \frac{1}{3}p(p+1) \\ 1 & -p-1 & 0 & -\frac{1}{6}p(p+1) & \frac{1}{2}p(p+1) & \frac{1}{3}p(p-2) \end{pmatrix}.$$

Theorem 2. *Let ψ be a nontrivial cubic character. If $p \equiv 1 \bmod 3$, then*

$$W(\psi) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & p\tau(\bar{\psi}) & 0 & \frac{1}{6}p(p-1)\tau^2(\psi) & -\frac{1}{2}\psi(4r)p(p-1)\tau^2(\psi) & \frac{1}{3}\bar{\psi}(s)p(p-1)\tau^2(\psi) \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \tau^2(\psi) & 0 & \frac{1}{6}A & \frac{1}{2}X & \frac{1}{3}B \\ 0 & -\psi(4r)\tau^2(\psi) & 0 & \frac{1}{6}X & \frac{1}{2}Y & \frac{1}{3}D \\ 0 & \bar{\psi}(s)\tau^2(\psi) & 0 & \frac{1}{6}B & \frac{1}{2}D & \frac{1}{3}C \end{pmatrix}$$

where

$$A = \tau^4(\bar{\psi}) + 4\tau^2(\psi) - \frac{\tau^5(\psi)}{p}, \quad B = \bar{\psi}(s)\Big(\tau^4(\bar{\psi}) - 2\tau^2(\psi)p - \frac{\tau^5(\psi)}{p}\Big),$$
$$C = \psi(s)\Big(\tau^4(\bar{\psi}) + \tau^2(\psi)p - \frac{\tau^5(\psi)}{p}\Big), \quad D = \psi(4rs^2)\Big(\tau^4(\bar{\psi}) + \frac{\tau^5(\psi)}{p}\Big),$$
$$X = \psi(4r)\Big(\tau^4(\bar{\psi}) + \frac{\tau^5(\psi)}{p}\Big) \text{ and } Y = \tau^4(\bar{\psi}) - \frac{\tau^5(\psi)}{p}.$$

Proofs. For simplicity we assume $a = b = s_1$. We put $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Elementary methods of linear algebra give the Bruhat decomposition

$$G(K) = B(K) \sqcup B(K)wN(K)$$

where

$$B(K) = \Big\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} | a, c \in K^\times, n \in K \Big\}$$
$$\text{and } B(K)wN(K) = \Big\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} | a, c \in K^\times, n, m \in K \Big\}.$$

For $g_1 \in B(K)$ and $g_2 \in B(K)wN(K)$, we define

$$W_1(\psi, s_1, s_1) = \sum_{g_1 \in B(K)} \psi(\det g_1)\langle [s_1,\ g_1 \cdot s_1] \rangle$$

and

$$W_2(\psi, s_1, s_1) = \sum_{g_2 \in B(K)wN(K)} \psi(\det g_2)\langle [s_1,\ g_2 \cdot s_1] \rangle.$$

For $1 \le i \le 2$, the twisted action of g_i on the element s_1 is given by $g_1 \cdot s_1 = (a^2c^{-1}, 0, 0, 0)$, $g_2 \cdot s_1 = (a^2c^{-1}n^3, 3an^2, 3an, a^{-1}c^2)$. A straightforward calculation shows that

$$\begin{aligned} W_1(\psi, s_1, s_1) &= \sum_{g \in B(K)} \psi(\det g)\langle [s_1,\ g_i \cdot s_1] \rangle \\ &= \sum_{a,c \in K^\times,\ n \in K} \psi(ac)\langle 0 \rangle \\ &= \begin{cases} (p-1)^2 p & \text{if } \psi = 1, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

We deduce the analogous equality for $W_2(\psi, s_1, s_1)$

$$\begin{aligned} W_2(\psi, s_1, s_1) &= \sum_{g\in B(K)wN(K)} \psi(\det g)\langle [s_1,\ g_i \cdot s_1]\rangle \\ &= \sum_{a,c\in K^\times,\ n,m\in K} \psi(ac)\langle a^{-1}c^2\rangle \\ &= \sum_{a,c\in K^\times,\ n,m\in K} \psi(ac^3)\langle a^{-1}\rangle \\ &= \sum_{a,c\in K^\times,\ n,m\in K} \bar{\psi}(a)\langle a\rangle \\ &= p^2(p-1)\tau(\bar{\psi}). \end{aligned}$$

Combining all these equalities, we obtain

$$W(\psi, s_1, s_1) = W_1(\psi, s_1, s_1) + W_2(\psi, s_1, s_1) = \begin{cases} -p(p-1) & \text{if } \psi = 1, \\ p^2(p-1)\tau(\bar{\psi}) & \text{otherwise.} \end{cases}$$

More precious proof will be shown in [SM].

References

[B] M. Bhargava; Higher composition laws II: On cubic analogues of Gauss composition *Ann. of Math* **159** (2004), 865–886

[G] A. Gyoja; Character sums and intersection cohomology complexes associated to the space of square matrices, *Indag. Math. (N.S.)* **8** (1997), 371–385

[GGS] W.-T. Gan, B. H. Gross and G. Savin; Fourier coefficients of modular forms on G_2, *Duke. Math. J.* **115** (2002), no. 1, 105–169

[SH] 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), 91–142

[S-S] M. Sato and T. Shintani; On zeta functions associated with prehomogeneous vector spaces, *Ann. of Math. (2)* **100** (1974), 131–170

[SM] S. Mori; Orbital Gauss sum for the space of binary cubic forms over a finite field. in preparation.

[T] T. Taniguchi; Orbital L-functions for the space of binary cubic forms. in preparation.

[D1] D.J. Wright; The adelic zeta function associated to the space of binary cubic forms part I: Global theory, *Math. Ann* **270** (1985), 503–534

[D2] D.J. Wright; Cubic Character sums of cubic polynomial, *Amer. Math. Soc* **100** No. 3, (1987), 409–413

Department of Mathematics
Kyoto University
Kyoto 606-8502, Japan
sin-mori@math.kyoto-u.ac.jp