<table>
<thead>
<tr>
<th>Title</th>
<th>Orbital Gauss sums associated with the space of binary cubic forms over a finite field (Automorphic forms, automorphic representations and related topics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Mori, Shingo</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2010), 1715: 32-36</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2010-10</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/170304">http://hdl.handle.net/2433/170304</a></td>
</tr>
<tr>
<td>Right</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>
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, $K^*$ 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

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

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

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

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

§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:

$$
F_x(u, v) = x_1 u^3 + x_2 u^2 v + x_3 u v^2 + x_4 v^3.
$$

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 \(S_K = \{x \in V| P(x) = 0\}\) is invariant under \(G_K\). Let \(V_K'\) denote the set of all nonsingular forms in \(V_K\), \(V_K' = \{x \in V_K| P(x) \neq 0\} = V_K - S_K\). A basic feature of this representation is that
\[
P(g \cdot x) = (\det g)^2P(x).
\]
A non zero rational function \(R(x)\) on \(V_K\) is called a relative \(G_K\)-invariant if there exists a character \(\chi\) 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 \(GL_2(K)\).

\[\S 2\]

Let \(p\) be a prime number. We shall assume that \(p \neq 2,3\). Let \(F_q\) be the finite field of prime power of order \(q\). We put \(K = F_q\). 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 precisely

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

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 \(F_q\) are \(G_K\)-equivalent if and only if their cubic ring are same. The \(G_K\)-orbits in \(V_K'\) are precisely

\[
V_{K,1} = \{x \in V_{K}'| F_q(x) = F_q \times F_q \times F_q\}; \\
V_{K,2} = \{x \in V_{K}'| F_q(x) = F_{q^2} \times F_q\}; \\
V_{K,3} = \{x \in V_{K}'| F_q(x) = F_{q^3}\}.
\]

The order of stabilizer in \(G_K\) of nonsingular binary cubic forms with cubic ring \(F_q \times F_q \times F_q\), \(F_{q^2} \times F_q\) and \(F_{q^3}\) is 6, 2 and 3, respectively. If \(p \equiv 1 \mod 3\), 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 \(F_q^*\) that is not a square and \(s\) is any element that is not a cube.

\[\S 3\] The orbital Gauss sum.
For simplicity, we shall assume that $K = F_p$. Let $\psi$ be a character of multiplicative group of $F_p^\times$ of nonzero elements of $F_p$. Extend $\psi$ to $F_p$ 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 $[g \cdot x, \det(g)^{-1}g \cdot y] = [x, y]$ for all $x, y \in V_K$ and $g \in G_K$. For $x, y \in V_K$, we put

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

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:

$$V(F_p) = \{|y_0|y_0 \in S_0\} \cup \{|y_1|y_1 \in S_1\} \cup \{|y_2|y_2 \in S_2\} \cup \{|y_3|y_3 \in V_1^\prime\} \cup \{|y_4|y_4 \in V_1^\prime\} \cup \{|y_5|y_5 \in V_1^\prime\}.$$  

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

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

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

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

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

$$W(1) = \begin{pmatrix}
1 & p^2 - 1 & p(p^2 - 1) & \frac{1}{3}p(p - 1)(p^2 - 1) & \frac{1}{3}p(p - 1)(p^2 - 1) & \frac{1}{3}p(p - 1)(p^2 - 1)
1 & -1 & p(p - 1) & \frac{1}{6}p(p - 1)(2p - 1) & -\frac{1}{3}p(p - 1) & -\frac{1}{3}p(p^2 - 1)
1 & p - 1 & p(p - 2) & -\frac{1}{3}p(p - 1) & -\frac{1}{3}p(p - 1) & 0
1 & 2p - 1 & -3p & \frac{1}{3}p(p + 5) & -\frac{1}{3}p(p - 1) & \frac{1}{3}p(p - 1)
1 & -1 & -p & -\frac{1}{6}p(p - 1) & \frac{1}{3}p(p + 1) & -\frac{1}{3}p(p - 1)
1 & -p - 1 & 0 & \frac{1}{6}p(p - 1) & -\frac{1}{3}p(p - 1) & \frac{1}{3}p(p + 2)
\end{pmatrix}.$$
Theorem 2. Let \( \psi \) be a nontrivial cubic character. If \( p \equiv 1 \mod 3 \), then

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

where

\[
A = \tau^4(\overline{\psi}) + 4\tau^2(\psi) - \frac{\tau^5(\psi)}{p}, \quad B = \psi(s)\left(\tau^4(\overline{\psi}) - 2\tau^2(\psi)p - \frac{\tau^5(\psi)}{p}\right),
\]

\[
C = \psi(s)\left(\tau^4(\overline{\psi}) + \tau^2(\psi)p - \frac{\tau^5(\psi)}{p}\right), \quad D = \psi(4rs^2)\left(\tau^4(\overline{\psi}) + \frac{\tau^5(\psi)}{p}\right),
\]

\[
X = \psi(4r)\left(\tau^4(\overline{\psi}) + \frac{\tau^5(\psi)}{p}\right) \quad \text{and} \quad Y = \tau^4(\overline{\psi}) - \frac{\tau^5(\psi)}{p}.
\]

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

\[
B(K) = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} | a, c \in K^\times, n \in K \right\}
\]

and

\[
B(K)wN(K) = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} | a, c \in K^\times, n, m \in K \right\}.
\]

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 \( 1 \leq i \leq 2 \), 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

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

\[
= \sum_{a, c \in K^\times, n \in K} \psi(ac)\langle 0 \rangle
\]

\[
= \begin{cases} (p-1)^2p & \text{if } \psi = 1, \\ 0 & \text{otherwise}. \end{cases}
\]
We deduce the analogous equality for $W_2(\psi, s_1, s_1)$

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

$$= \sum_{a,c \in K^\times, n,m \in K} \psi(ac)(a^{-1}c^2)$$

$$= \sum_{a,c \in K^\times, n,m \in K} \psi(ac^3)(a^{-1})$$

$$= \sum_{a,c \in K^\times, n,m \in K} \overline{\psi}(a)(a)$$

$$= p^2(p - 1)\tau(\overline{\psi}).$$

Combining all these equalities, we obtain

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

More precious proof will be shown in [SM].

References


[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