J. Korean Math. Soc. **57** (2020), No. 3, pp. 571–583
https://doi.org/10.4134/JKMS.j190211
pISSN: 0304-9914 / eISSN: 2234-3008

THE JACOBI SUMS OVER GALOIS RINGS AND ITS ABSOLUTE VALUES

Young Ho Jang

Abstract. The Galois ring R of characteristic p^n having p^{mn} elements is a finite extension of the ring of integers modulo p^n, where p is a prime number and n, m are positive integers. In this paper, we develop the concepts of Jacobi sums over R and under the assumption that the generating additive character of R is trivial on maximal ideal of R, we obtain the basic relationship between Gauss sums and Jacobi sums, which allows us to determine the absolute value of the Jacobi sums.

1. Introduction

Throughout this paper, p will denote a fixed prime number and n, m positive integers. We set $q = p^m$. Let $\mathbb{Z}$, $\mathbb{C}$, $\mathbb{C}^1$, $\overline{a}$, $\mathbb{F}_q$, $\mathbb{Z}_{p^n}$ and $GR(p^n, m)$ be the ring of integers, the field of complex numbers, the unit circle in the complex plane, the complex conjugate of $a \in \mathbb{C}$, the finite field of order q, the ring of integers modulo p^n and the Galois ring of characteristic p^n having q^n elements, respectively.

Jacobi sums over finite fields and finite rings were introduced and studied by many mathematicians. For the detailed story and relative references see [1, 3, 7]. In particular, in [11, 12] Wang studied a general theory of Jacobi sums over residue class rings and finite commutative rings with identity. In [4], Ishibashi defined the Gauss sums and Jacobi sums over $GR(2^2, m)$ to find relations between the irreducible modules of the Terwilliger algebra and the Jacobi sums over the local ring. In [6], Jin et al. provided explicit description on the Gauss sums and Jacobi sums over $GR(p^2, m)$, and showed that the values of these sums can be reduced to the Gauss sums and Jacobi sums over $\mathbb{F}_q$ for all non-trivial cases. Also, in [5], Jang and Jun studied the Gauss sums over $GR(p^n, m)$ under the assumption that the generating additive character of $GR(p^n, m)$ is trivial on maximal ideal of $GR(p^n, m)$. As a follow-up to the previous work [5], we continue that line of research in this paper. The purpose of this paper is to develop the concepts of Jacobi sums over $GR(p^n, m)$ and

Received March 12, 2019; Accepted January 28, 2020.
2010 *Mathematics Subject Classification.* Primary 11L07, 11T23, 11T24.
Key words and phrases. Galois rings, characters, Gauss sums, Jacobi sums.

under the assumption that the generating additive character of $GR(p^n, m)$ is trivial on maximal ideal of $GR(p^n, m)$, we obtain the basic relationship between Gauss sums and Jacobi sums, which allows us to determine the absolute value of the Jacobi sums. Many of our results are exact analogues of those holding over $\mathbb{F}_q$. However, their proofs are complicated by the change in significance of the elements, which may be zero divisors in $GR(p^n, m)$.

We conclude this section by recalling some basic properties of the Galois ring $R = GR(p^n, m)$. These have been well documented in [8, 10]. R is a local ring having unique maximal ideal $M = pR$ and $|M| = q^{n-1}$. The group of units R^* of R contains a unique cyclic group of order $q-1$ (see [8, Theorem XVI.9]). If ξ is a generator of this group, then, by [8, Theorem XVIII.2], $R^* = \mathcal{T}^* \times (1+M)$ where $\mathcal{T}^* = \langle \xi \rangle$ is the cyclic group of order $q-1$ and $1+M$ is the multiplicative p-group of order q^{n-1}. The set $\mathcal{T} = \{0\} \cup \mathcal{T}^* = \{0, 1, \xi, \dots, \xi^{q-2}\}$ is called the Teichmüller set of R. Every element $z \in R$ has a unique p-adic representation:

$$z = z_0 + z_1 p + \cdots + z_{n-1} p^{n-1}, \text{ where } z_i \in \mathcal{T} \text{ for } 0 \le i \le n-1. \tag{1}$$

Moreover, $z \in R^*$ if and only if $z_0 \neq 0$ and $z \in M$ if and only if $z_0 = 0$. Any element of $R \backslash \{0\}$ is either a unit or a zero divisor. Since the zero divisors in R are those elements divisible by p, any element $z \in R \backslash \{0\}$ can be written as

$$z = p^k u, \ u \in R^*, \ 0 \le k \le n-1. \tag{2}$$

For any Galois ring R the trace mapping $\mathrm{Tr} : R \to \mathbb{Z}_{p^n}$ is defined by

$$\mathrm{Tr}\left(\sum_{i=0}^{n-1} z_i p^i\right) = \sum_{i=0}^{n-1} (z_i + z_i^p + \cdots + z_i^{p^{m-1}}) p^i. \tag{3}$$

Tr is an epimorphism of $\mathbb{Z}_{p^n}$-modules and Tr can be reduced by the mod-p reduction map to the trace mapping $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ of finite fields.

2. Characters of Galois rings and Gauss sums over Galois rings

An additive character of R is a homomorphism from the additive group of R to $\mathbb{C}^1$. Using (3), for any $x, y \in R$, the additive characters of R are given by

$$\psi_x(y) = e^{2\pi i \mathrm{Tr}(xy)/p^n}, \tag{4}$$

different x's affording different additive characters. In fact, $\{\psi_x\}_{x \in R}$ consists of all additive characters of R in [2, Lemma 6]. We see that ψ_0 is the trivial additive character of R, $\psi_x(y) = \psi_1(xy)$, $\overline{\psi_x(y)} = \psi_x(-y)$ and $\psi (= \psi_1)$ is called the generating additive character of R. Let $\widehat{R^+}$ denote the group of additive characters on R.

A multiplicative character χ of R^* is a homomorphism from the multiplicative group R^* to $\mathbb{C}^1$. We see that $\chi(1) = 1$, $\chi(x)$ is a $(q-1)q^{n-1}$-th root of unity and $\chi^{-1}(x) = \chi(x^{-1}) = \chi(x)^{-1} = \overline{\chi(x)} = \overline{\chi}(x)$. We extend χ as the character of R by defining $\chi(M) = 0$. We call this the multiplicative character of R. The trivial character χ_0 of R is defined by $\chi_0(R^*) = 1$. Let $\widehat{R^*}$ denote the group of multiplicative characters on R.

Remark 2.1. In [9], the authors extend χ as the character of $R = GR(2^2, m)$ by defining $\chi(M) = 1$ for $\chi = \chi_0$ and $\chi(M) = 0$ for $\chi \neq \chi_0$; this is different from the definition we have given here.

Remark 2.2. Since $R^* = \mathcal{T}^* \times (1 + M)$, we know that $\widehat{R^*} = \widehat{\mathcal{T}^*} \times \widehat{(1 + M)}$. In particular, the multiplicative characters χ of R that vanish on $\mathcal{T}^*$ (i.e., $\chi(\alpha) = 1$ for $\alpha \in \mathcal{T}^*$) are in one-to-one correspondence with the multiplicative characters of $1 + M$. Particularly, for $R = GR(p^2, m)$, from the p-adic representation (1)

$$z = z_0 + z_1 p \ (z_0, z_1 \in \mathcal{T}), \ M = p\mathcal{T}$$

and

$$(1 + M, \cdot) = (1 + p\mathcal{T}, \cdot) \cong (\mathbb{F}_q, +), \ 1 + px \longmapsto \overline{x} = x \bmod p \text{ for } x \in \mathcal{T}.$$

Hence multiplicative characters $\chi \in \widehat{R^*}$ that vanish on $\mathcal{T}^*$ are given by

$$\chi(1 + px) = \varphi_a(\overline{x}) \ (x \in \mathcal{T}, \ a, \overline{x} \in \mathbb{F}_q), \tag{5}$$

where φ_a is an additive character of $\mathbb{F}_q$ defined by

$$\varphi_a(\overline{x}) = e^{2\pi i \mathrm{tr}(a\overline{x})/p} \text{ for all } a, \overline{x} \in \mathbb{F}_q. \tag{6}$$

Remark 2.3. Let G be a finite abelian group with identity element 1_G and $\widehat{G}$ an abelian group of characters of G. It is well known in [7, Theorem 5.4] that if f is a nontrivial character of G, then

$$\sum_{g \in G} f(g) = 0. \tag{7}$$

Denote by $\mathbb{C}^R$ the vector space over $\mathbb{C}$ of all functions from R to $\mathbb{C}$. This is an inner product space with Hermitian inner product $\langle \ , \ \rangle$ defined for $f, g \in \mathbb{C}^R$ by

$$\langle f, g \rangle = \sum_{x \in R} f(x)\overline{g(x)}.$$

Then the set $\{\delta_x \,|\, x \in R\}$ of characteristic functions defined by

$$\delta_x(y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

forms an orthonormal basis for $\mathbb{C}^R$, with $\langle \delta_x, \delta_y \rangle = \delta_x(y)$. Hence $\mathbb{C}^R$ is a q^n-dimensional $\mathbb{C}$-vector space. Also, additive characters ψ_x of R defined by (4) are also orthogonal in this inner product space,

$$\langle \psi_x, \psi_y \rangle = \sum_{s \in R} \psi_x(s)\overline{\psi_y(s)} = \sum_{s \in R} \psi_{x-y}(s) = \begin{cases} q^n & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \quad \text{(by (7))} \tag{8}$$

and form an orthogonal basis for $\mathbb{C}^R$. Since $\chi \in \mathbb{C}^R$, hence χ is a linear combination of the additive characters of R. More precisely, for a nontrivial character $\chi \in \widehat{R^*}$, we have

$$\chi = \frac{1}{q^n} \sum_{x \in R} G(\chi, \psi_x) \overline{\psi_x}, \tag{9}$$

where

$$G(\chi, \psi_x) := \langle \chi, \overline{\psi_x} \rangle = \sum_{y \in R^*} \chi(y) \psi_x(y) = \sum_{y \in R^*} \chi(y) \psi(xy), \tag{10}$$

which is called the Gauss sum over R.

The elementary properties of Gauss sums over R in accordance with conditions of characters of R investigated in [5]. In particular, under the assumption that $\psi \in \widehat{R^+}$ is trivial on M, the authors computed the modulus of $G(\chi, \psi_x)$. The following two results has been proved in [5].

Proposition 2.4 ([5, Lemma 3.1]). *Let $\chi \in \widehat{R^*}$ be a nontrivial character. Then*

$$G(\chi, \psi_x) = \begin{cases} \overline{\chi}(x) G(\chi, \psi) & \text{if } x \in R^*, \\ 0 & \text{if } x \in M \text{ and } \psi \in \widehat{R^+} \text{ is trivial on } M. \end{cases} \tag{11}$$

Proposition 2.5 ([5, Theorem 3.3]). *Let $\chi \in \widehat{R^*}$ be a nontrivial character. If $\psi \in \widehat{R^+}$ is trivial on M, then*

$$|G(\chi, \psi_x)|^2 = \begin{cases} q^n & \text{if } x \in R^*, \\ 0 & \text{if } x \in M. \end{cases} \tag{12}$$

Proposition 2.6. *Let $\chi \in \widehat{R^*}$ be a nontrivial character. If $\psi \in \widehat{R^+}$ is trivial on M, then*

$$G(\chi, \psi) G(\overline{\chi}, \psi) = \chi(-1) q^n. \tag{13}$$

Proof. From (11) we have

$$\begin{aligned} \sum_{x \in R} G(\chi, \psi_x) G(\overline{\chi}, \psi_x) &= \sum_{x \in R^*} G(\chi, \psi_x) G(\overline{\chi}, \psi_x) = G(\chi, \psi) G(\overline{\chi}, \psi) \sum_{x \in R^*} 1 \\ &= (q-1) q^{n-1} G(\chi, \psi) G(\overline{\chi}, \psi). \end{aligned}$$

On the other hand, (10) yields that

$$\begin{aligned} \sum_{x \in R} G(\chi, \psi_x) G(\overline{\chi}, \psi_x) &= \sum_{x \in R} \sum_{y \in R^*} \chi(y) \psi_x(y) \sum_{z \in R^*} \overline{\chi(z)} \psi_x(z) \\ &= \sum_{y \in R^*} \sum_{z \in R^*} \chi(y) \overline{\chi(z)} \sum_{x \in R} \psi_x(y+z) \\ &= \chi(-1) \sum_{z \in R^*} \sum_{x \in R} 1 + \sum_{\substack{y, z \in R^* \\ y+z \neq 0}} \chi(yz^{-1}) \sum_{x \in R} \psi_x(y+z) \\ &= \chi(-1)(q-1) q^{n-1} q^n \text{ (by (7))}. \end{aligned}$$

By comparing above two formulas we have (13). □

Proposition 2.7. *Let $\chi \in \widehat{R^*}$ be a nontrivial character. If $\psi \in \widehat{R^+}$ is trivial on M, then*

$$\chi = \frac{1}{q^n} G(\chi, \psi) \sum_{x \in R^*} \chi(x^{-1}) \overline{\psi_x}. \tag{14}$$

Proof. From (9) and (11), it is obvious. □

3. Jacobi sums over Galois rings

Let $\chi_1, \ldots, \chi_l \in \widehat{R^*}$. For $\alpha \in R$, a sum of the form

$$J_\alpha(\chi_1, \ldots, \chi_l) = \sum_{\substack{s_1, \ldots, s_l \in R^* \\ s_1 + \cdots + s_l = \alpha}} \chi_1(s_1) \cdots \chi_l(s_l) \tag{15}$$

is called a Jacobi sum relative to $\chi_1, \ldots, \chi_l$. If $l-1$ of the terms in $s_1 + \cdots + s_l$ is chosen, the last term is uniquely determined by the requirement that whole sum equals α. Thus (15) contains $\big((q-1)q^{n-1}\big)^{l-1}$ terms. It is easy to show that if σ is a permutation of $\{1, \ldots, l\}$, then $J_\alpha(\chi_{\sigma(1)}, \ldots, \chi_{\sigma(l)}) = J_\alpha(\chi_1, \ldots, \chi_l)$.

We drop the subscript α from J_α when $\alpha = 1$. Then

$$\begin{aligned} J(\chi_1, \ldots, \chi_l) &= \sum_{\substack{s_1, \ldots, s_l \in R^* \\ s_1 + \cdots + s_l = 1}} \chi_1(s_1) \cdots \chi_l(s_l) \\ &= \chi_1 \cdots \chi_l(-1) \sum_{\substack{s_1, \ldots, s_l \in R^* \\ s_1 + \cdots + s_l + 1 = 0}} \chi_1(s_1) \cdots \chi_l(s_l). \end{aligned} \tag{16}$$

For $\alpha \in R \backslash \{0\}$, let $\alpha = p^k u,\ 0 \leq k \leq n-1,\ u \in R^*$ as in (2). Then

$$J_{p^k u}(\chi_1, \ldots, \chi_l) = \chi_1 \cdots \chi_l(u) J_{p^k}(\chi_1, \ldots, \chi_l)$$

and

$$J_u(\chi_1, \ldots, \chi_l) = \chi_1 \cdots \chi_l(u) J(\chi_1, \ldots, \chi_l).$$

In particular, $J(\chi_1) = \chi_1(1) = 1$ and for $l = 2$, we have

$$\begin{aligned} J(\chi_1, \chi_2) &= \sum_{\substack{s_1, s_2 \in R^* \\ s_1 + s_2 = 1}} \chi_1(s_1)\chi_2(s_2) = \chi_1\chi_2(-1) \sum_{\substack{s_1, s_2 \in R^* \\ s_1 + s_2 + 1 = 0}} \chi_1(s_1)\chi_2(s_2) \\ &= \sum_{x \in R^* \backslash (1+M)} \chi_1(x)\chi_2(1-x). \end{aligned} \tag{17}$$

The following two theorems are proved in [13, Theorem 4] for $GR(2^2, m)$ and in [6, Theorem 4.1] for $GR(p^2, m)$; the proofs of the more general results follow along precisely the same lines.

Theorem 3.1. *For $\chi_1, \chi_2 \in \widehat{R^*}$,*

$$J(\chi_1,\chi_2) = \begin{cases} (q-2)q^{n-1} & \text{if } \chi_1 = \chi_2 = \chi_0, \\ 0 & \text{if } \chi_2 = \chi_0 \text{ and } \chi_1(1+M) \neq 1, \\ -q^{n-1} & \text{if } \chi_2 = \chi_0,\ \chi_1 \neq \chi_0 \text{ and } \chi_1(1+M) = 1, \\ -\chi_1(-1)q^{n-1} & \text{if } \chi_1 \neq \chi_0,\ \chi_1\chi_2 = \chi_0 \text{ and } \chi_1(1+M) = 1, \\ 0 & \text{if } \chi_1 \neq \chi_0,\ \chi_1\chi_2 = \chi_0 \text{ and } \chi_1(1+M) \neq 1. \end{cases}$$

Proof. (i) From (17), if $\chi_1 = \chi_2 = \chi_0$, then $J(\chi_1,\chi_2) = (q-2)q^{n-1}$.

(ii) If $\chi_2 = \chi_0$ and $\chi_1(1+M) \neq 1$, then $\chi_1 \neq \chi_0$ and

$$J(\chi_1,\chi_2) = \sum_{x \in R^* \setminus (1+M)} \chi_1(x) = \sum_{x \in R^*} \chi_1(x) - \sum_{x \in 1+M} \chi_1(x) = 0 \text{ (by (7))}.$$

(iii) If $\chi_2 = \chi_0$, $\chi_1 \neq \chi_0$ and $\chi_1(1+M) = 1$, then

$$J(\chi_1,\chi_2) = \sum_{x \in R^* \setminus (1+M)} \chi_1(x) = \sum_{x \in R^*} \chi_1(x) - \sum_{x \in (1+M)} 1 = -q^{n-1} \text{ (by (7))}.$$

(iv) If $\chi_1 \neq \chi_0$ and $\chi_1\chi_2 = \chi_0$, then $\chi_2 = \chi_1^{-1} = \overline{\chi_1}$ and

$$\begin{aligned} J(\chi_1,\chi_2) &= \sum_{x \in R^* \setminus (1+M)} \chi_1(x)\overline{\chi_1(1-x)} \\ &= \chi_1(-1) \sum_{x \in R^* \setminus (1+M)} \chi_1(x(x-1)^{-1}) \text{ (let } z = x(x-1)^{-1}) \\ &= \chi_1(-1) \sum_{z \in R^* \setminus (1+M)} \chi_1(z) \\ &= -\chi_1(-1) \sum_{z \in (1+M)} \chi_1(z) \text{ (by (7))} \\ &= \begin{cases} -\chi_1(-1)q^{n-1} & \text{if } \chi_1(1+M) = 1, \\ 0 & \text{if } \chi_1(1+M) \neq 1 \text{ (by (7))}, \end{cases} \end{aligned}$$

where the third equality follows that for each $x \in R^* \setminus (1+M)$ multiplying x by $(x-1)^{-1}$ permutes $R^* \setminus (1+M)$. $\square$

Theorem 3.2. *For $k = 1, 2, \ldots, n-1$ and $\chi_1, \chi_2 \in \widehat{R^*}$,*

$$\begin{aligned} & J_{p^k}(\chi_1,\chi_2) \\ = & \sum_{x \in R^*} \chi_1(x)\chi_2(p^k - x) \\ = & \begin{cases} (q-1)q^{n-1} & \text{if } \chi_1 = \chi_2 = \chi_0, \\ 0 & \text{if } \chi_2 = \chi_0 \text{ and } \chi_1 \neq \chi_0, \\ \chi_1(-1)(q-1)q^{n-1} & \text{if } \chi_1 \neq \chi_0,\ \chi_1\chi_2 = \chi_0 \text{ and } \chi_1(1+M) = 1, \\ \chi_1(-1)q^k S(k) & \text{if } \chi_1 \neq \chi_0,\ \chi_1\chi_2 = \chi_0 \text{ and } \chi_1(1+M) \neq 1, \end{cases} \end{aligned}$$

where

$$S(k) = \sum_{\substack{z_0 \in \mathcal{T}^* \\ z_1,\ldots,z_{n-k-1} \in \mathcal{T}}} \chi_1\left(1 + p^k z_0 + p^{k+1} z_1 + \cdots + p^{n-k-1} z_{n-k-1}\right). \tag{18}$$

Proof. (i) If $\chi_1 = \chi_2 = \chi_0$, then $J_{p^k}(\chi_1, \chi_2) = \sum_{x \in R^*} 1 = (q-1)q^{n-1}$.

(ii) If $\chi_2 = \chi_0$ and $\chi_1 \neq \chi_0$, then, by (7), $J_{p^k}(\chi_1, \chi_2) = \sum_{x \in R^*} \chi_1(x) = 0$.

(iii) If $\chi_1 \neq \chi_0$ and $\chi_1\chi_2 = \chi_0$, then $\chi_2 = \chi_1^{-1} = \overline{\chi_1}$ and

$$\begin{aligned} J_{p^k}(\chi_1, \chi_2) &= \sum_{x \in R^*} \chi_1(x)\overline{\chi_1(p^k - x)} \\ &= \chi_1(-1) \sum_{x \in R^*} \chi_1(x(x - p^k)^{-1}) \text{ (since } x - p^k \in R^*) \\ &= \chi_1(-1) \sum_{x \in R^*} \chi_1(1 + p^k(x - p^k)^{-1}) \text{ (let } z = (x - p^k)^{-1}) \\ &= \chi_1(-1) \sum_{z \in R^*} \chi_1\left(1 + p^k z\right). \end{aligned}$$

Since $p^k z \in M$ for all $z \in R^*$, if $\chi_1(1 + M) = 1$, then

$$J_{p^k}(\chi_1, \chi_2) = \chi_1(-1)(q-1)q^{n-1}.$$

Assume $\chi_1(1+M) \neq 1$. Let $z = z_0 + z_1 p + \cdots + z_{n-1}p^{n-1}$, $z_0 \in \mathcal{T}^*$, $z_1, \ldots, z_{n-1} \in \mathcal{T}$ as in (1). Then we have

$$\begin{aligned} &J_{p^k}(\chi_1, \chi_2) \\ &= \chi_1(-1) \sum_{\substack{z_0 \in \mathcal{T}^* \\ z_1,\ldots,z_{n-1} \in \mathcal{T}}} \chi_1\left(1 + p^k(z_0 + pz_1 + \cdots + \cdots + p^{n-1}z_{n-1})\right) \\ &= \chi_1(-1)q^k \sum_{\substack{z_0 \in \mathcal{T}^* \\ z_1,\ldots,z_{n-k-1} \in \mathcal{T}}} \chi_1\left(1 + p^k z_0 + \cdots + p^{n-k-1} z_{n-k-1}\right). \end{aligned}$$

This completes the proof. □

Remark 3.3. Let $R = GR(p^2, m)$ and $\chi_1, \chi_2 \in \widehat{R^*}$. If $\chi_1 \neq \chi_0$, $\chi_1\chi_2 = \chi_0$ and $\chi_1(1 + M) \neq 1$, then from (18) we have

$$\begin{aligned} S(1) &= \sum_{z_0 \in \mathcal{T}^*} \chi_1(1 + pz_0) = \sum_{z_0 \in \mathcal{T}} \chi_1(1 + pz_0) - 1 \\ &= \sum_{\bar{z}_0 \in \mathbb{F}_q} \varphi_a(\bar{z}_0) - 1 \text{ (from (5) in Remark 2.2)} \\ &= -1 \text{ (by } \varphi_a \in \widehat{\mathbb{F}_q} \text{ is nontrivial and (7)).} \end{aligned}$$

Thus $J_p(\chi_1, \chi_2) = -\chi_1(-1)q$, which is given in [6, Theorem 4.1].

Proposition 3.4. *Let* $\chi_1, \ldots, \chi_l \in \widehat{R^*}$.

(i) *For $l \geq 3$,*

$$J(\chi_1, \dots, \chi_l) = \begin{cases} \big((q-1)q^{n-1}\big)^{l-1} & \text{if } \chi_1, \dots, \chi_l \text{ are all trivial,} \\ 0 & \text{if some but not all of } \chi_i \text{ are trivial.} \end{cases}$$

(ii) *For $l \geq 2$, if χ_l is nontrivial, then*

$$\begin{aligned} J_0(\chi_1, \dots, \chi_l) &= \sum_{\substack{s_1, \dots, s_l \in R^* \\ s_1 + \cdots + s_l = 0}} \chi_1(s_1) \cdots \chi_l(s_l) \\ &= \begin{cases} 0 & \text{if } \chi_1 \cdots \chi_l \neq \chi_0, \\ \chi_l(-1)(q-1)q^{n-1} J(\chi_1, \dots, \chi_{l-1}) & \text{if } \chi_1 \cdots \chi_l = \chi_0. \end{cases} \end{aligned}$$

Proof. For (i), if $l-1$ of the terms in $s_1 + \cdots + s_l = 1$ is chosen, the last term is uniquely determined. These $l-1$ terms can be chosen in $\big((q-1)q^{n-1}\big)^{l-1}$ ways, this proves part one. For the second part we have ordered the characters in such way that $\chi_1, \dots, \chi_j$ are nontrivial and $\chi_{j+1}, \dots, \chi_l$ are trivial, where $1 \leq j \leq l-1$. Then

$$\begin{aligned} J(\chi_1, \dots, \chi_l) &= \sum_{\substack{s_1, \dots, s_l \in R^* \\ s_1 + \cdots + s_l = 1}} \chi_1(s_1) \cdots \chi_l(s_l) = \sum_{\substack{s_1, \dots, s_l \in R^* \\ s_1 + \cdots + s_l = 1}} \chi_1(s_1) \cdots \chi_j(s_j) \\ &= \sum_{s_1, \dots, s_j \in R^*} \chi_1(s_1) \cdots \chi_j(s_j) \sum_{\substack{s_{j+1}, \dots, s_l \in R^* \\ s_{j+1} + \cdots + s_l = 1 - s_1 - \cdots - s_j}} 1 \\ &= \big((q-1)q^{n-1}\big)^{l-j-1} \sum_{s_1, \dots, s_j \in R^*} \chi_1(s_1) \cdots \chi_j(s_j) \\ &= \big((q-1)q^{n-1}\big)^{l-j-1} \left(\sum_{s_1 \in R^*} \chi_1(s_1) \right) \cdots \left(\sum_{s_j \in R^*} \chi_j(s_j) \right) \\ &= 0 \text{ (by (7)).} \end{aligned}$$

To prove (ii), we have

$$\begin{aligned} & J_0(\chi_1, \dots, \chi_l) \\ = & \sum_{\substack{s_1, \dots, s_l \in R^* \\ s_1 + \cdots + s_l = 0}} \chi_1(s_1) \cdots \chi_l(s_l) \\ = & \sum_{s_l \in R^*} \left(\sum_{\substack{s_1, \dots, s_{l-1} \in R^* \\ s_1 + \cdots + s_{l-1} = -s_l}} \chi_1(s_1) \cdots \chi_{l-1}(s_{l-1}) \right) \chi_l(s_l) \text{ (let } s_i = -s_l t_i) \\ = & \chi_1 \cdots \chi_{l-1}(-1) \left(\sum_{\substack{t_1, \dots, t_{l-1} \in R^* \\ t_1 + \cdots + t_{l-1} = 1}} \chi_1(t_1) \cdots \chi_{l-1}(t_{l-1}) \right) \left(\sum_{s_l \in R^*} \chi_1 \cdots \chi_l(s_l) \right) \end{aligned}$$

$$= \begin{cases} 0 & \text{if } \chi_1 \cdots \chi_l \neq \chi_0, \\ \chi_l(-1)(q-1)q^{n-1} J(\chi_1, \ldots, \chi_{l-1}) & \text{if } \chi_1 \cdots \chi_l = \chi_0, \end{cases}$$

where the last equality follows from (7). □

Theorem 3.5. *Let $\chi_1, \ldots, \chi_{l+1} \in \widehat{R^*}$ be nontrivial characters with $\chi_1 \cdots \chi_{l+1} = \chi_0$. If $\psi \in \widehat{R^+}$ is trivial on M, then*

$$J(\chi_1, \ldots, \chi_l) = \frac{1}{q^n} \chi_{l+1}(-1) G(\chi_1, \psi) \cdots G(\chi_{l+1}, \psi) \tag{19}$$

$$= \frac{G(\chi_1, \psi) \cdots G(\chi_l, \psi)}{G(\chi_1 \cdots \chi_l, \psi)} \tag{20}$$

and

$$|J(\chi_1, \ldots, \chi_l)|^2 = q^{n(l-1)}. \tag{21}$$

Proof. Since $\chi_1 \cdots \chi_{l+1} = \chi_0$, (16) implies that

$$\begin{aligned}
&J(\chi_1, \ldots, \chi_l) \\
&= \chi_1 \cdots \chi_l(-1) \sum_{\substack{s_1, \ldots, s_l \in R^* \\ s_1 + \cdots + s_l + 1 = 0}} \chi_1(s_1) \cdots \chi_l(s_l) \\
&= \frac{\chi_{l+1}(-1)}{(q-1)q^{n-1}} \sum_{s_{l+1} \in R^*} (\chi_1 \cdots \chi_{l+1})(s_{l+1}) \sum_{\substack{s_1, \ldots, s_l \in R^* \\ s_1 + \cdots + s_l + 1 = 0}} \chi_1(s_1) \cdots \chi_l(s_l) \\
&= \frac{\chi_{l+1}(-1)}{(q-1)q^{n-1}} \sum_{s_{l+1} \in R^*} \sum_{\substack{s_1, \ldots, s_l \in R^* \\ s_1 + \cdots + s_l + 1 = 0}} \chi_1(s_{l+1} s_1) \cdots \chi_l(s_{l+1} s_l) \chi_{l+1}(s_{l+1})
\end{aligned}$$

$$= \frac{\chi_{l+1}(-1)}{(q-1)q^{n-1}} \sum_{\substack{u_1, \ldots, u_{l+1} \in R^* \\ u_1 + \cdots + u_{l+1} = 0}} \chi_1(u_1) \cdots \chi_l(u_l) \chi_{l+1}(u_{l+1}). \tag{22}$$

From (22) and (14) in Proposition 2.8 we have

$$\begin{aligned}
&\chi_{l+1}(-1)(q-1)q^{n-1} J(\chi_1, \ldots, \chi_l) \\
&= \sum_{\substack{u_1, \ldots, u_{l+1} \in R^* \\ u_1 + \cdots + u_{l+1} = 0}} \left(\frac{1}{q^n} G(\chi_1, \psi) \sum_{t_1 \in R^*} \chi_1(t_1^{-1}) \overline{\psi_{t_1}(u_1)} \right) \\
&\quad \times \cdots \times \left(\frac{1}{q^n} G(\chi_{l+1}, \psi) \sum_{t_{l+1} \in R^*} \chi_{l+1}(t_{l+1}^{-1}) \overline{\psi_{t_{l+1}}(u_{l+1})} \right) \\
&= \frac{1}{q^{n(l+1)}} G(\chi_1, \psi) \cdots G(\chi_{l+1}, \psi) \sum_{t_1, \ldots, t_{l+1} \in R^*} \chi_1(t_1^{-1}) \cdots \chi_{l+1}(t_{l+1}^{-1})
\end{aligned}$$

$$\times \sum_{\substack{u_1,\ldots,u_{l+1}\in R^* \\ u_1+\cdots+u_{l+1}=0}} \overline{\psi(t_1u_1+\cdots+t_{l+1}u_{l+1})}.$$

On the other hand, we have

$$\begin{aligned} &\sum_{\substack{u_1,\ldots,u_{l+1}\in R^* \\ u_1+\cdots+u_{l+1}=0}} \overline{\psi(t_1u_1+\cdots+t_{l+1}u_{l+1})} \\ &= \sum_{\substack{u_1,\ldots,u_{l+1}\in R^* \\ u_1+\cdots+u_{l+1}=0}} \overline{\psi(u_1(t_1-t_{l+1})+\cdots+u_l(t_l-t_{l+1})+t_{l+1}(u_1+\cdots+u_{l+1}))} \\ &= \sum_{u_1,\ldots,u_l\in R^*} \overline{\psi(u_1(t_1-t_{l+1}))}\cdots\overline{\psi(u_l(t_l-t_{l+1}))}. \end{aligned}$$

Hence

$$\begin{aligned} &\chi_{l+1}(-1)(q-1)q^{n-1}J(\chi_1,\ldots,\chi_l) \\ &= \frac{1}{q^{n(l+1)}}G(\chi_1,\psi)\cdots G(\chi_{l+1},\psi) \sum_{t_1,\ldots,t_{l+1}\in R^*} \chi_1(t_1^{-1})\cdots\chi_{l+1}(t_{l+1}^{-1}) \\ &\quad\times \sum_{u_1,\ldots,u_l\in R^*} \overline{\psi(u_1(t_1-t_{l+1}))}\cdots\overline{\psi(u_l(t_l-t_{l+1}))} \\ &= \frac{1}{q^{n(l+1)}}G(\chi_1,\psi)\cdots G(\chi_{l+1},\psi) \\ &\quad\times \sum_{t_{l+1}\in R^*} \chi_{l+1}(t_{l+1}^{-1}) \prod_{i=1}^{l} \left\{ \sum_{t_i\in R^*} \chi_i(t_i^{-1}) \sum_{u_i\in R^*} \overline{\psi(u_i(t_i-t_{l+1}))} \right\}. \end{aligned}$$

Since for each $t_{l+1} \in R^*$

$$\begin{aligned} &\sum_{t_i\in R^*} \chi_i(t_i^{-1}) \sum_{u_i\in R^*} \overline{\psi(u_i(t_i-t_{l+1}))} \\ &= \chi_i(t_{l+1}^{-1}) \sum_{u_i\in R^*} 1 + \sum_{\substack{t_i\in R^* \\ t_i-t_{l+1}\neq 0}} \chi_i(t_i^{-1}) \sum_{u_i\in R^*} \overline{\psi(u_i(t_i-t_{l+1}))} \\ &= (q-1)q^{n-1}\chi_i(t_{l+1}^{-1}) + \sum_{\substack{t_i\in R^* \\ t_i-t_{l+1}\neq 0}} \chi_i(t_i^{-1}) \sum_{u_i\in R^*} \overline{\psi(u_i(t_i-t_{l+1}))} \\ &= (q-1)q^{n-1}\chi_i(t_{l+1}^{-1}) \\ &\quad + \sum_{\substack{t_i\in R^* \\ t_i-t_{l+1}\neq 0}} \chi_i(t_i^{-1}) \left\{ \sum_{u_i\in R} \overline{\psi_{t_i-t_{l+1}}(u_i)} - \sum_{u_i\in M} \overline{\psi(u_i(t_i-t_{l+1}))} \right\} \\ &= (q-1)q^{n-1}\chi_i(t_{l+1}^{-1}) - q^{n-1} \sum_{\substack{t_i\in R^* \\ t_i-t_{l+1}\neq 0}} \chi_i(t_i^{-1}) \end{aligned}$$

$$
\begin{aligned}
&= (q-1)q^{n-1}\chi_i(t_{l+1}^{-1}) - q^{n-1}\left(\sum_{t_i\in R^*}\chi_i(t_i^{-1}) - \chi_i(t_{l+1}^{-1})\right)\\
&= (q-1)q^{n-1}\chi_i(t_{l+1}^{-1}) + q^{n-1}\chi_i(t_{l+1}^{-1})\\
&= q^n\chi_i(t_{l+1}^{-1}),
\end{aligned}
$$

where the fourth equality follows from (7) and $\psi(u_i(t_i - t_{l+1})) = 1$ (since $t_i - t_{l+1} \neq 0$ and $u_i(t_i - t_{l+1}) \in M$ for all $u_i \in M$), and where the sixth equality follows from (7). Hence

$$
\begin{aligned}
&\chi_{l+1}(-1)(q-1)q^{n-1}J(\chi_1,\ldots,\chi_l)\\
&= \frac{1}{q^{n(l+1)}}G(\chi_1,\psi)\cdots G(\chi_{l+1},\psi)\left\{q^{nl}\sum_{t_{l+1}\in R^*}(\chi_1\cdots\chi_{l+1})(t_{l+1}^{-1})\right\}\\
&= \frac{1}{q^{n(l+1)}}G(\chi_1,\psi)\cdots G(\chi_{l+1},\psi)q^{nl}(q-1)q^{n-1}\\
&= \frac{q-1}{q}G(\chi_1,\psi)\cdots G(\chi_{l+1},\psi).
\end{aligned}
$$

Since $\chi_1\cdots\chi_l = \overline{\chi_{l+1}} \in \widehat{R^*}$ is nontrivial, by (12) in Proposition 2.6 we have $G(\chi_1\cdots\chi_l,\psi) \neq 0$. Thus we have

$$
\begin{aligned}
&J(\chi_1,\ldots,\chi_l)\\
&= \frac{1}{q^n}\chi_{l+1}(-1)G(\chi_1,\psi)\cdots G(\chi_{l+1},\psi)\\
&= \frac{1}{q^n}\chi_{l+1}(-1)G(\chi_1,\psi)\cdots G(\overline{\chi_1\cdots\chi_l},\psi)\\
&= \frac{1}{q^n}\overline{\chi_1\cdots\chi_l}(-1)G(\chi_1,\psi)\cdots G(\chi_l,\psi)\frac{\chi_1\cdots\chi_l(-1)q^n}{G(\chi_1\cdots\chi_l,\psi)} \text{ (by (11))}\\
&= \frac{G(\chi_1,\psi)\cdots G(\chi_l,\psi)}{G(\chi_1\cdots\chi_l,\psi)}.
\end{aligned}
$$

Again, by (12) in Proposition 2.6 we have $|J(\chi_1,\ldots,\chi_l)|^2 = q^{n(l-1)}$. □

Corollary 3.6. *Let $\chi_1,\ldots,\chi_{l+1} \in \widehat{R^*}$ be nontrivial characters with $\chi_1\cdots\chi_{l+1} = \chi_0$. If $\psi \in \widehat{R^+}$ is trivial on M, then*

$$J(\chi_1,\ldots,\chi_{l+1}) = -\chi_{l+1}(-1)J(\chi_1,\ldots,\chi_l) + (q-1)\sum_{k=1}^{n-1}J_{p^k}(\chi_1,\ldots,\chi_{l+1}).$$

Proof. From (10) and (15), we have

$$
\begin{aligned}
&G(\chi_1,\psi)\cdots G(\chi_{l+1},\psi)\\
&= \left(\sum_{s_1\in R^*}\chi_1(s_1)\psi(s_1)\right)\cdots\left(\sum_{s_{l+1}\in R^*}\chi_{l+1}(s_{l+1})\psi(s_{l+1})\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{s_1,\ldots,s_{l+1}\in R^*} \chi_1(s_1)\cdots\chi_{l+1}(s_{l+1})\psi(s_1+\cdots+s_{l+1}) \\
&= \sum_{s\in R}\left(\sum_{\substack{s_1,\ldots,s_{l+1}\in R^* \\ s_1+\cdots+s_{l+1}=s}} \chi_1(s_1)\cdots\chi_{l+1}(s_{l+1})\right)\psi(s) \\
&= J_0(\chi_1,\ldots,\chi_{l+1}) + \sum_{s\in R\setminus\{0\}} J_s(\chi_1,\ldots,\chi_{l+1})\psi(s) \text{ (let } s=p^k u \text{ as in (2))} \\
&= J_0(\chi_1,\ldots,\chi_{l+1}) + \sum_{k=0}^{n-1}\sum_{u\in R^*} \chi_1\cdots\chi_{l+1}(u) J_{p^k}(\chi_1,\ldots,\chi_{l+1})\psi(p^k u) \\
&= J_0(\chi_1,\ldots,\chi_{l+1}) + \sum_{k=0}^{n-1} J_{p^k}(\chi_1,\ldots,\chi_{l+1}) \sum_{u\in R^*}\psi(p^k u) \\
&= J_0(\chi_1,\ldots,\chi_{l+1}) + J(\chi_1,\ldots,\chi_{l+1})\left(\sum_{u\in R}\psi(u) - \sum_{u\in M}\psi(u)\right) \\
&\quad + \sum_{k=1}^{n-1} J_{p^k}(\chi_1,\ldots,\chi_{l+1}) \sum_{u\in R^*} 1 \text{ (since } \psi(p^k u)=1 \text{ for all } k=1,\ldots,n-1) \\
&= J_0(\chi_1,\ldots,\chi_{l+1}) - q^{n-1}J(\chi_1,\ldots,\chi_{l+1}) + (q-1)q^{n-1}\sum_{k=1}^{n-1} J_{p^k}(\chi_1,\ldots,\chi_{l+1}),
\end{aligned}
$$

where the last equality follows from (7). Hence from Proposition 3.4(ii) and (19) in Theorem 3.5 we have

$$
\begin{aligned}
&\chi_{l+1}(-1)q^n J(\chi_1,\ldots,\chi_l) \\
&= \chi_{l+1}(-1)(q-1)q^{n-1}J(\chi_1,\ldots,\chi_l) - q^{n-1}J(\chi_1,\ldots,\chi_{l+1}) \\
&\quad + (q-1)q^{n-1}\sum_{k=1}^{n-1} J_{p^k}(\chi_1,\ldots,\chi_{l+1}),
\end{aligned}
$$

which completes the proof. □

References

[1] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998.

[2] S. Fan and W. Han, *Character sums over Galois rings and primitive polynomials over finite fields*, Finite Fields Appl. **10** (2004), no. 1, 36–52. https://doi.org/10.1016/S1071-5797(03)00041-8

[3] K. F. Ireland and M. I. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, **84**, Springer-Verlag, New York, 1982.

[4] H. Ishibashi, *The Terwilliger algebras of certain association schemes over the Galois rings of characteristic* 4, Graphs Combin. **12** (1996), no. 1, 39–54. https://doi.org/10.1007/BF01858443

[5] Y. H. Jang and S. P. Jun, *The Gauss sums over Galois rings and its absolute values*, Korean J. Math. **26** (2018), no. 3, 519–535. https://doi.org/10.11568/kjm.2018.26.3.519

[6] J. Li, S. Zhu, and K. Feng, *The Gauss sums and Jacobi sums over Galois ring* $\mathrm{GR}(p^2, r)$, Sci. China Math. **56** (2013), no. 7, 1457–1465. https://doi.org/10.1007/s11425-013-4629-6

[7] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, London, 1997.

[8] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1974.

[9] Y. Oh and H. J. Oh, *Gauss sums over Galois rings of characteristic* 4, Kangweon-Kyungki Math. Jour. **9** (2001), no. 1, 1–7.

[10] Z.-X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing Co., Inc., River Edge, NJ, 2003. https://doi.org/10.1142/5350

[11] J. Wang, *On the Jacobi sums modulo* P^n, J. Number Theory **39** (1991), no. 1, 50–64. https://doi.org/10.1016/0022-314X(91)90033-8

[12] ———, *On the Jacobi sums for finite commutative rings with identity*, J. Number Theory **48** (1994), no. 3, 284–290. https://doi.org/10.1006/jnth.1994.1068

[13] M. Yamada, *Distance-regular digraphs of girth* 4 *over an extension ring of* $\mathbf{Z}/4\mathbf{Z}$, Graphs Combin. **6** (1990), no. 4, 381–394. https://doi.org/10.1007/BF01787706

Young Ho Jang
Department of Mathematics
Inha University
Incheon 22212, Korea
Email address: yjang6105@inha.ac.kr