Kangweon-Kyungki Math. Jour. **9** (2001), No. 1, pp. 1–7

GAUSS SUMS OVER GALOIS RINGS OF CHARACTERISTIC 4

Yunchang Oh and Heung-Joon Oh

Abstract. In this paper, we define and study Gauss sums over Galois rings of characteristic 4. In particular, we give the absolute value of Gauss sum over Galois rings of characteristic 4.

1. Introduction

Let $GF(2)$ be the prime field of characteristic 2 and $GF(2^r)$ an extension field of degree r. Then $GF(2^r)$ is a simple algebraic extension over $GF(2)$. That is, if Θ is a primitive element of $GF(2^r)$, then

$$GF(2^r) = GF(2)[\Theta] \cong GF(2)[x]/(F(x)) \tag{1.1}$$

where $F(x)$ is a monic irreducible polynomial in $GF(2)[x]$ of degree r having Θ as a root.

Let $\mathbb{Z}/4\mathbb{Z}$ denote the ring of integers modulo 4. It is a finite local commutative ring with the unique maximal ideal $m = 2(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Let $\mu_1 : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/4\mathbb{Z})/m \cong GF(2)$ denote reduction modulo 2. We can extend μ_1 to $(\mathbb{Z}/4\mathbb{Z})[x]$ in the natural way.

In (1.1), since Θ is a simple zero of $F(x)$, if $f \in (\mathbb{Z}/4\mathbb{Z})[x]$ is a preimage of F under the homomorphism μ_1, then by Theorem 1.1 below, there is precisely one element θ such that $\mu_1(\theta) = \Theta$ and $f(\theta) = 0$.

Theorem 1.1 [3, Lemma (XV.1)]. *Let $f \in (\mathbb{Z}/4\mathbb{Z})[x]$ be a regular polynomial (i.e., $\mu_1(f) \neq 0$) and suppose that $\mu_1(f)$ has a simple zero a in $GF(2^r)$. Then f has one and only one zero α such that $\mu_1(\alpha) = a$.*

The *Galois rings* $\mathcal{R}$ of characteristic 4 is defined to be the ring $(\mathbb{Z}/4\mathbb{Z})[\theta]$. Many papers have been studied concerning Gauss sums

Received October 10, 2000.
1991 Mathematics Subject Classification: 11Lxx, 11T23, 14M05, 13Hxx.
Key words and phrases: Galois rings; Gauss sums over Galois rings.

over finite fields (see [1]). In this paper, we define and study Gauss sums over Galois rings $\mathcal{R}$. In particular, we give the absolute value of Gauss sum over $\mathcal{R}$.

2. Characters on the Galois rings $\mathcal{R}$

It is well-known in [cf. 3] that

(GR1) $\mathcal{R}$ is a finitely generated free $\mathbb{Z}/4\mathbb{Z}$-module and $|\mathcal{R}| = 4^r$.

(GR2) $\mathcal{R}$ is a finite local commutative ring with the unique maximal ideal $M = 2\mathcal{R}$ and the residue field $K = \mathcal{R}/M \cong GF(2^r)$.

(GR3) $Gal(\mathcal{R}/(\mathbb{Z}/4\mathbb{Z})) \cong Gal(GF(2^r)/GF(2))$ and the Frobenius automorphism σ of $\mathcal{R}$ given by $\theta \mapsto \theta^2$ is a generator of $Gal(\mathcal{R}/(\mathbb{Z}/4\mathbb{Z}))$.

(GR4) Let $\mathcal{R}^*$ and K^* denote the unit group of $\mathcal{R}$ and K, respectively. Then

$$\mathcal{R}^* \cong K^* \times (1 + M) \quad \text{(direct product of groups)} \tag{2.1}$$

where K^* is a cyclic group of order $2^r - 1$ and $1 + M$ is a group of order 2^r such that $1 + M$ is a direct product of r cyclic groups each of order 2.

From (2.1), $\mathcal{R}^*$ contains a cyclic subgroup $\mathcal{T}_r^*$ of order $2^r - 1$. Let θ be a generator of $\mathcal{T}_r^*$ (such θ is called a *primitive element* of $\mathcal{R}$) and

$$\mathcal{T}_r = \mathcal{T}_r^* \cup \{0\} = \left\{\theta^i \mid 0 \le i \le 2^r - 2\right\} \cup \{0\},$$

which is called the *Teichmüller set* for $K(= \mathcal{R}/M)$ in $\mathcal{R}$. Then $\mathcal{T}_r$ is isomorphic to $GF(2^r)$ under the homomorphism obtained by reduction modulo 2. It can be shown that every element $s \in \mathcal{R}$ has the 2-adic expansion $s = \alpha + 2\beta \quad (\alpha, \beta \in \mathcal{T}_r)$. Thus $M = 2\mathcal{T}_r$, $M^2 = 0$ and every element of $\mathcal{R}^*$ has a unique representation in the form

$$\alpha(1 + 2\beta) \ (\alpha \in \mathcal{T}_r^*, \ \beta \in \mathcal{T}_r). \tag{2.2}$$

Also, from (GR3) the Frobenius automorphism σ on $\mathcal{R}$ is given by $\sigma(s) = \sigma(\alpha + 2\beta) = \alpha^2 + 2\beta^2$. In analogy with finite fields, the *trace function* $\mathrm{Tr} : \mathcal{R} \to \mathbb{Z}/4\mathbb{Z}$ is defined by

$$\mathrm{Tr}(s) = \sum_{\tau \in Gal(\mathcal{R}/(\mathbb{Z}/4\mathbb{Z}))} \tau(s) = \sum_{i=0}^{r-1} \sigma^i(s). \tag{2.3}$$

Also, the additive characters λ_t $(t \in \mathcal{R})$ on $\mathcal{R}$ are defined by

$$\lambda_t(s) = \sqrt{-1}^{\,\mathrm{Tr}(ts)} \quad \text{for} \quad s \in \mathcal{R}. \tag{2.4}$$

We see that λ_0 is the trivial character on $\mathcal{R}$, $\lambda_t(s) = \lambda_1(ts)$ and $\overline{\lambda_t(s)} = \lambda_t(-s)$. Also, if $t_1 \neq t_2$ $(t_1, t_2 \in \mathcal{R})$, then $\lambda_{t_1} \neq \lambda_{t_2}$.

Since $1 + M$ has the structure of a multiplicative group of order 2^r, $1 + M$ is isomorphic to the additive group of $GF(2^r)$ via the map

$$1 + 2\beta \mapsto y \quad (\beta \in \mathcal{T}_r \text{ with } \beta \equiv y \pmod{M},\ y \in GF(2^r)). \tag{2.5}$$

Hence there is a one-to-one correspondence between the set of all multiplicative characters on $1+M$ and the set of all additive characters on $GF(2^r)$. Thus, each multiplicative character χ on $\mathcal{R}^*$ can be written as

$$\chi(s) = \eta(\alpha)\psi_x(y) \tag{2.6}$$

for all $s = \alpha(1 + 2\beta)$ $(\alpha \in \mathcal{T}_r^*,\ \beta \in \mathcal{T}_r$ with $\beta \equiv y \pmod{M}$, $y \in GF(2^r))$, where η is a character on $\mathcal{T}_r^*$ and ψ_x is an additive character on $GF(2^r)^+$ $(x \in GF(2^r))$ which is given by

$$\psi_x(y) = (-1)^{\mathrm{tr}(xy)} \quad \text{for} \quad y \in GF(2^r) \tag{2.7}$$

where $\mathrm{tr}(x)$ is the trace of x from $GF(2^r)$ to $GF(2)$ given by $\mathrm{tr}(x) = \sum_{j=0}^{r-1} x^{2^j}$.

3. Gauss sums over Galois rings $\mathcal{R}$ and its absolute value

Let $\mathbb{C}[\mathcal{R}]$ denote the space of all $\mathbb{C}$-valued functions on $\mathcal{R}$. Then the set of characteristic functions $\{\delta_t \mid t \in \mathcal{R}\}$, where

$$\delta_t(s) = \begin{cases} 1 & \text{if} \quad s = t \\ 0 & \text{if} \quad s \neq t, \end{cases}$$

is a basis of $\mathbb{C}[\mathcal{R}]$. Hence $\mathbb{C}[\mathcal{R}]$ is a 4^r-dimensional $\mathbb{C}$-vector space. We define an inner product on $\mathbb{C}[\mathcal{R}]$ by

$$\langle f, g \rangle = \frac{1}{|\mathcal{R}|} \sum_{s \in \mathcal{R}} f(s)\overline{g(s)} = \frac{1}{4^r} \sum_{s \in \mathcal{R}} f(s)\overline{g(s)}.$$

Then $\{\delta_t \mid t \in \mathcal{R}\}$ is an orthonormal basis of $\mathbb{C}[\mathcal{R}]$ and the set of all additive characters on $\mathcal{R}^+$ is an orthonormal basis of $\mathbb{C}[\mathcal{R}]$ by the character orthogonality condition [2, Theorem 4.4]

$$\sum_{s\in\mathcal{R}} \lambda_t(s) = \begin{cases} 4^r & \text{if } \ \lambda_t \text{ is trivial} \\ 0 & \text{if } \ \lambda_t \text{ is nontrivial.} \end{cases} \tag{3.1}$$

It is convenient to extend the domain of definition of a character χ from $\mathcal{R}^*$ to $\mathcal{R}$ by setting

$$\chi(M) = \begin{cases} 1 & \text{if } \ \chi \text{ is trivial} \\ 0 & \text{if } \ \chi \text{ is nontrivial.} \end{cases} \tag{3.2}$$

With above definition we have

$$\sum_{s\in\mathcal{R}} \chi(s) = \begin{cases} 4^r & \text{if } \ \chi \text{ is trivial} \\ 0 & \text{if } \ \chi \text{ is nontrivial,} \end{cases} \tag{3.3}$$

and $\chi \in \mathbb{C}[\mathcal{R}]$. Thus

$$\chi = \sum_{\lambda_t} \langle \chi, \overline{\lambda_t} \rangle \overline{\lambda_t} = \sum_{t\in\mathcal{R}} \langle \chi, \overline{\lambda_t} \rangle \overline{\lambda_t} = \frac{1}{4^r} \sum_{t\in\mathcal{R}} g(\chi, \lambda_t) \overline{\lambda_t} \tag{3.4}$$

where

$$g(\chi, \lambda_t) = \sum_{s\in\mathcal{R}} \chi(s)\lambda_t(s). \tag{3.5}$$

We call each $g(\chi, \lambda_t)$ the *Gauss sum* over $\mathcal{R}$. From (3.2), (3.3) and (3.5) we have

$$g(\chi, \lambda_t) = \begin{cases} 4^r & \text{if } \ \chi \text{ and } \lambda_t \text{ are both trivial} \\ 0 & \text{if } \ \chi \text{ is nontrivial and } \lambda_t \text{ is trivial.} \end{cases}$$

Also, we have the following theorem.

THEOREM 3.1. *Let χ be a nontrivial character on $\mathcal{R}^*$. Then* (a) *If $t \in \mathcal{R}^*$, then $g(\chi, \lambda_t) = \chi(t^{-1})g(\chi, \lambda_1)$. In particular, $\overline{g(\chi, \lambda_1)} = \chi(-1)g(\overline{\chi}, \lambda_1)$.* (b) *If $t \in M$ and χ is nontrivial on $1 + M$, then $g(\chi, \lambda_t) = 0$.*

Proof. For (a). If $t \in \mathcal{R}^*$, then

$$g(\chi,\lambda_t) = \sum_{s\in\mathcal{R}^*} \chi(s)\lambda_1(ts) = \chi(t^{-1}) \sum_{s\in\mathcal{R}^*} \chi(ts)\lambda_1(ts) \quad (\text{setting } u = ts)$$
$$= \chi(t^{-1}) \sum_{u\in\mathcal{R}^*} \chi(u)\lambda_1(u) = \chi(t^{-1}) g(\chi,\lambda_1).$$

Also, we have

$$\overline{g(\chi,\lambda_1)} = \sum_{s\in\mathcal{R}^*} \chi(s^{-1})\lambda_1(-s) = \chi(-1) \sum_{s\in\mathcal{R}^*} \chi((-s)^{-1})\lambda_1(-s)$$
$$= \chi(-1) \sum_{s\in\mathcal{R}^*} \chi(s^{-1})\lambda_1(s) = \chi(-1) g(\overline{\chi},\lambda_1).$$

To prove (b), let $t \in M$. If χ is nontrivial on $1 + M$, then by (2.6) we have $\chi = \eta \cdot \psi_x$, where η is a character on $\mathcal{T}_r^*$ and ψ_x is a nontrivial character on $GF(2^r)^+$. Thus

$$g(\chi,\lambda_t) = \sum_{s\in\mathcal{R}^*} \chi(s)\lambda_t(s)$$
$$(s = \alpha(1+2\beta),\ \alpha \in \mathcal{T}_r^*,\ \beta \in \mathcal{T}_r \text{ with } \beta \equiv y \pmod M,\ y \in GF(2^r))$$
$$= \sum_{\alpha\in\mathcal{T}_r^*} \sum_{y\in GF(2^r)} \eta(\alpha)\psi_x(y)\lambda_t(\alpha(1+2y))$$
$$= \sum_{\alpha\in\mathcal{T}_r^*} \sum_{y\in GF(2^r)} \eta(\alpha)(-1)^{\mathrm{tr}(xy)}\sqrt{-1}^{\mathrm{Tr}(t\alpha(1+2y))}$$
$$(\text{by (2.4) and (2.7)})$$
$$= \sum_{\alpha\in\mathcal{T}_r^*} \eta(\alpha)\sqrt{-1}^{\mathrm{Tr}(t\alpha)} \sum_{y\in GF(2^r)} (-1)^{\mathrm{tr}(xy)}\sqrt{-1}^{\mathrm{Tr}(2t\alpha y)}.$$

Since $t\alpha \in M$, i.e., $t\alpha \equiv 0 \pmod M$, we get

$$2t\alpha y \equiv 0 \pmod 4.$$

Hence

$$g(\chi,\lambda_t) = \sum_{\alpha\in\mathcal{T}_r^*} \eta(\alpha)\lambda_t(\alpha) \sum_{y\in GF(2^r)} \psi_x(y) = 0$$

since $\sum_{y\in GF(2^r)} \psi_x(y) = 0$ for a nontrivial character ψ_x. □

Corollary 3.2. *Let χ be a nontrivial character on $\mathcal{R}^*$. If χ is nontrivial on $1+M$, then*

$$\chi = 4^{-r} g(\chi, \lambda_1) \sum_{t \in \mathcal{R}^*} \chi(t^{-1}) \overline{\lambda_t}.$$

Proof.

$$\begin{aligned} \chi &= 4^{-r} \sum_{t \in \mathcal{R}} g(\chi, \lambda_t) \overline{\lambda_t} \quad \text{(see (3.4))} \\ &= 4^{-r} \sum_{t \in \mathcal{R}^*} g(\chi, \lambda_t) \overline{\lambda_t} + 4^{-r} \sum_{t \in M} g(\chi, \lambda_t) \overline{\lambda_t} \\ &= 4^{-r} g(\chi, \lambda_1) \sum_{t \in \mathcal{R}^*} \chi(t^{-1}) \overline{\lambda_t} \quad \text{(by Theorem 3.1 (a) and (b)).} \end{aligned}$$

□

Theorem 3.3. *Let χ be a nontrivial character on $\mathcal{R}^*$. If χ is nontrivial on $1+M$, then*

$$g(\chi, \lambda_1) g(\overline{\chi}, \lambda_1) = 4^r \chi(-1) \quad \textit{and} \tag{3.6}$$

$$|g(\chi, \lambda_t)| = \begin{cases} 2^r & \textit{if} \quad t \in \mathcal{R}^* \\ 0 & \textit{if} \quad t \in M. \end{cases} \tag{3.7}$$

Proof. For (3.6). Theorem 3.1 (a) and (b) imply

$$\begin{aligned} \sum_{t \in \mathcal{R}} g(\chi, \lambda_t) g(\overline{\chi}, \lambda_t) &= \sum_{t \in \mathcal{R}^*} g(\chi, \lambda_t) g(\overline{\chi}, \lambda_t) + \sum_{t \in M} g(\chi, \lambda_t) g(\overline{\chi}, \lambda_t) \\ &= g(\chi, \lambda_1) g(\overline{\chi}, \lambda_1) \sum_{t \in \mathcal{R}^*} 1, \end{aligned}$$

and so

$$\sum_{t \in \mathcal{R}} g(\chi, \lambda_t) g(\overline{\chi}, \lambda_t) = (4^r - 2^r) g(\chi, \lambda_1) g(\overline{\chi}, \lambda_1). \tag{3.8}$$

On the other hand, (3.5) yields that

$$\begin{aligned}\sum_{t\in\mathcal{R}} g(\chi,\lambda_t)g(\overline{\chi},\lambda_t) &= \sum_{t\in\mathcal{R}}\sum_{s\in\mathcal{R}^*}\sum_{u\in\mathcal{R}^*}\chi(su^{-1})\lambda_{s+u}(t)\\ &= \chi(-1)\sum_{t\in\mathcal{R}}\sum_{u\in\mathcal{R}^*}1+\sum_{u\in\mathcal{R}^*}\sum_{\substack{s\in\mathcal{R}^*\\ s+u\neq 0}}\chi(su^{-1})\sum_{t\in\mathcal{R}}\lambda_{s+u}(t).\end{aligned}$$

Since $\sum_{t\in\mathcal{R}}\lambda_{s+u}(t)=0$ for $s,u\in\mathcal{R}^*$ with $s+u\neq 0$, we have

$$\sum_{t\in\mathcal{R}} g(\chi,\lambda_t)g(\overline{\chi},\lambda_t) = (4^r-2^r)4^r\chi(-1). \tag{3.9}$$

By comparing (3.8) and (3.9) we have (3.6). Next, for (3.7). If $t\in M$, it follows from Theorem 3.1 (b). Let $t\in\mathcal{R}^*$. Then

$$\begin{aligned}|g(\chi,\lambda_t)|^2 &= g(\chi,\lambda_t)\overline{g(\chi,\lambda_t)} = g(\chi,\lambda_1)\overline{g(\chi,\lambda_1)} \text{(by Theorem 3.1 (a))}\\ &= \chi(-1)g(\chi,\lambda_1)g(\overline{\chi},\lambda_1) \quad \text{(by Theorem 3.1 (a))}\\ &= 4^r \quad \text{(by (3.6))}.\end{aligned}$$

□

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi sums*, John Wiley and Sons, New York, 1998.

[2] R. Lidl, H. Niederreiter and P. M. Cohn, *Finite fields*, Cambridge University Press, 1997.

[3] B. R. McDonald, *Finite rings with identity*, Marcel Dekker, New York, 1974.

Department of Mathematics
Suwon University
Whasung-Gun, Kyungkido, 445-743, Korea
E-mail: yc-oh@hanmail.net

Department of General Education
Chodang University
Muahn-Gun, Chonnam, 534-701, Korea
E-mail: heungjoon5@korea.com