Korean J. Math. **17** (2009), No. 1, pp. 43–52

REMARKS ON GAUSS SUMS OVER GALOIS RINGS

Tae Ryong Kwon and Won Sok Yoo*

Abstract. The Galois ring is a finite extension of the ring of integers modulo a prime power. We consider characters on Galois rings. In analogy with finite fields, we investigate complete Gauss sums over Galois rings. In particular, we analyze [1, Proposition 3] and give some lemmas related to [1, Proposition 3].

1. Introduction

Throughout this paper, p will denote a fixed prime and e, k positive integers. We set $q = p^k$. Let $\mathbf{Z}$, $\mathbf{C}$, $\mathbf{C}^1$, $\mathbf{F}_q$ and $\overline{a}$ denote the ring of integers, the field of complex numbers, the unit circle in the complex plane, the finite field of order q and the complex conjugate of $a \in \mathbf{C}$, respectively.

The Galois ring of characteristic p^e having $q^e (= p^{ek})$ elements, denoted by $A = GR(p^e, k)$, is the unique Galois extension of degree k of the prime ring $\mathbf{Z}/p^e\mathbf{Z}$. Note that $GR(p^e, 1) = \mathbf{Z}/p^e\mathbf{Z}$ and $GR(p, k) = \mathbf{F}_q$. In particular, A is a finite local commutative ring with identity 1, maximal ideal $M = pA$ and residue field $K = A/M \cong \mathbf{F}_q$. The reader can find further details about Galois rings in [3].

A complete Gauss sum attached to A is defined to be an expression of the form

$$G_A(\chi, \psi) = \sum_{x \in A^\times} \chi(x)\psi(x), \tag{1.1}$$

where $A^\times$ is the multiplicative group of invertible elements of A, χ a character of $A^\times$, and ψ a character of the additive group A^+ of A. Let

Received January 18, 2009. Revised March 3, 2009.
2000 Mathematics Subject Classification: 11T24, 13B05.
Key words and phrases: characters on galois rings, gauss sums over galois rings.
This research was supported by Kumoh National Institute of Technology in 2008.
*Corresponding author.

χ_0 (resp., ψ_0) denote the trivial character of $A^\times$ (resp., A^+). Then it is well known in [2, Theorem 5.4] that

$$\sum_{x\in A}\psi(x)=0 \quad \text{for } \psi\neq\psi_0, \tag{1.2}$$

and we have

$$G_A(\chi,\psi)=\begin{cases}|A^\times| & \text{for } \chi=\chi_0,\ \psi=\psi_0,\\ -\sum_{x\in M}\psi(x) & \text{for } \chi=\chi_0,\ \psi\neq\psi_0,\\ 0 & \text{for } \chi\neq\chi_0,\ \psi=\psi_0.\end{cases} \tag{1.3}$$

In [1, Proposition 3], P. Langevin and P. Sole showed that for a finite quasi-Frobenius local commutative ring $\mathcal{A}$ with maximal ideal $\mathcal{M}$ and generating character ψ of $\mathcal{A}^+$, and for a character χ of $\mathcal{A}^\times$,

$$|G_{\mathcal{A}}(\chi,\psi)|^2=\begin{cases}|\mathcal{A}| & \text{if } \chi \text{ is nontrivial on } S=1+\operatorname{ann}(\mathcal{M})\\ 0 & \text{if } \chi \text{ is trivial on } S=1+\operatorname{ann}(\mathcal{M})\end{cases} \tag{1.4}$$

by showing that

$$|G_{\mathcal{A}}(\chi,\psi)|^2=|\mathcal{A}|-|\mathcal{M}|\sum_{z\in S}\chi(z), \tag{1.5}$$

where $\operatorname{ann}(\mathcal{M})=\{x\in\mathcal{A}\mid xy=0\ \forall y\in\mathcal{M}\}$ and a ring $\mathcal{A}$ is called quasi-Frobenius if there exists a generating character ψ of $\mathcal{A}^+$, i.e., for each character λ of $\mathcal{A}^+$ there exists $a\in\mathcal{A}$ satisfying $\lambda(x)=\psi(ax)$ for any $x\in\mathcal{A}$. In particular, finite fields and Galois rings are quasi-Frobenius local commutative rings.

The purpose of this paper is to investigate complete Gauss sums over Galois rings. In particular, we analyze Eq. (1.5) and give some results related to Eq. (1.4).

2. Characters over Galois rings

Let $A,\ K,\ M,\ \mathbf{F}_q$ be as in Section 1. It is well known in [3] that:

$$A^\times\cong K^\times\times U, \tag{2.1}$$

where $K^\times$ is a cyclic group of order $q-1$ and $U=1+M$ is a multiplicative p-group of order q^{e-1}, which is called the principal units.

Following (2.1), the Galois ring A always contains a multiplicative cyclic group $T^\times$ of order $q-1$. Let β be a fixed generator of $T^\times$ (in

analogy with finite fields, β is called a primitive element of A), the generating multiplicative character χ can be defined by

$$\chi(\beta^l) = e^{2\pi il/q-1}, \text{ for } 0 \le l \le q-2. \tag{2.2}$$

For $0 \le j \le q-2$, define $\chi_j(\beta^l) = \chi(\beta^{lj})$. Then χ_j's are all the multiplicative characters of $T^\times$ and form a cyclic group with $q-1$ elements. Note that the order of each character χ_j is a divisor of $q-1$.

Let $T = T^\times \cup \{0\} = \{0, 1, \beta, \cdots, \beta^{q-2}\}$. Since T is isomorphic to K under the natural homomorphism from A to K, each element $a \in A$ has a unique p-adic representation:

$$a = a_0 + pa_1 + \cdots + p^{e-1}a_{e-1}, \quad a_i \in T.$$

Define the canonical projective map from A to T by $\phi(a) = a_0$. Let $n > 0$ be an integer and τ the Frobenius map of A over $\mathbf{Z}/p^e\mathbf{Z}$ given by

$$\tau(a) = a_0^p + pa_1^p + \cdots + p^{e-1}a_{e-1}^p, \text{ for } a = \sum_{i=0}^{e-1} p^i a_i \in A, \ a_i \in T.$$

It is well known that τ is the generator of the Galois group of $A/(\mathbf{Z}/p^e\mathbf{Z})$ which is a cyclic group of order k. The trace mapping $Tr(\cdot) : A \to \mathbf{Z}/p^e\mathbf{Z}$ is defined by

$$Tr(a) = a + \tau(a) + \tau^2(a) + \cdots + \tau^{k-1}(a), \text{ for } a \in A.$$

An additive character of A is a homomorphism from A to $\mathbf{C}^1$. Define

$$\psi(a) = e^{2\pi i Tr(a)/p^e}, \text{ for } a \in A. \tag{2.3}$$

It is easily seen that ψ is an additive character of A which is called the generating additive character. For $b \in A$, define $\psi_b(a) = \psi(ba), \ a \in A$. ψ_b is also an additive character. In fact, we have that $\{\psi_a\}_{a\in A}$ consists of all the additive characters of A.

3. Galois rings and proof of lemma's

Let $a \in A$, ψ a generating character of A^+ and χ (resp., χ_0) a character (resp., the trivial character) of $A^\times$. It is well known in [2, Theorem 5.4] that

$$\sum_{b\in A} \psi_b(a) = \sum_{b\in A} \psi_a(b) = \begin{cases} |A| & \text{if } a = 0, \\ 0 & \text{if } a \ne 0, \end{cases} \tag{3.1}$$

and

$$\sum_{b\in A^\times}\chi(b)=\begin{cases}|A^\times| & \text{if } \chi=\chi_0,\\ 0 & \text{if } \chi\neq\chi_0.\end{cases} \tag{3.2}$$

Also, it is easy to see that

$$\overline{G_A(\chi,\psi_a)}=\chi(-1)G_A(\overline{\chi},\psi_a) \quad \text{for } a\in A. \tag{3.3}$$

PROPOSITION 3.1. *Let $u\in A^\times$, t a fixed integer with $0\le t\le e-1$, χ a nontrivial character of $A^\times$ and ψ a generating character of A^+. Then*

$$G_A(\chi,\psi_{p^tu})=\overline{\chi}(u)G_A(\chi,\psi_{p^t}). \tag{3.4}$$

Proof. Eq. (3.4) follows from that

$$\begin{aligned} G_A(\chi,\psi_{p^tu}) &= \sum_{b\in A^\times}\chi(b)\psi_{p^tu}(b)=\overline{\chi}(u)\sum_{b\in A^\times}\chi(ub)\psi_{p^t}(ub) \quad (c=ub)\\ &= \overline{\chi}(u)\sum_{c\in A^\times}\chi(c)\psi_{p^t}(c)=\overline{\chi}(u)G_A(\chi,\psi_{p^t}). \end{aligned}$$

□

PROPOSITION 3.2. *Let ψ be a generating character of A^+. Then*

$$\sum_{t\in T}\psi_t(p^{e-1}a)=\begin{cases}|T| & \text{if } a\in M,\\ 0 & \text{if } a\in A^\times.\end{cases} \tag{3.5}$$

Proof. If $a\in M=pA$, then $p^{e-1}a=0$ in A and so that $\sum_{t\in T}1=|T|$. Let $a\in A^\times$. From Eq. (3.1), we have

$$\begin{aligned} 0 &= \sum_{b\in A}\psi_b(p^{e-1}a)-\sum_{b\in A}\psi_b(a) \quad (b=b_0+pb_1+\cdots+p^{e-1}b_{e-1},\ b_i\in T)\\ &= \left(\sum_{b_0\in T}\psi_{b_0}(p^{e-1}a)\sum_{b_1\in T}1\cdots\sum_{b_{e-1}\in T}1\right)\\ &\quad -\left(\sum_{b_0\in T}\psi_{b_0}(a)\cdots\sum_{b_{e-1}\in T}\psi_{b_{e-1}}(p^{e-1}a)\right)\\ &= \sum_{t\in T}\psi_t(p^{e-1}a)\left(q^{e-1}-\sum_{b_0\in T}\psi_{b_0}(a)\cdots\sum_{b_{e-2}\in T}\psi_{b_{e-2}}(p^{e-2}a)\right). \end{aligned}$$

On the other hand, we get

$$0 = \sum_{b\in A} \psi_b(a) = \sum_{t\in T} \psi_t(p^{e-1}a) \left(\sum_{b_0\in T} \psi_{b_0}(a) \cdots \sum_{b_{e-2}\in T} \psi_{b_{e-2}}(p^{e-2}a) \right).$$

If $\sum_{t\in T} \psi_t(p^{e-1}a) \neq 0$, then $\left(\sum_{b_0\in T} \psi_{b_0}(a) \cdots \sum_{b_{e-2}\in T} \psi_{b_{e-2}}(p^{e-2}a)\right) = q^{e-1} = 0$, i.e., $q = 0$. It is a contradiction. Thus if $a \in A^\times$, then $\sum_{t\in T} \psi_t(p^{e-1}a) = 0$. □

Lemma 3.3. *Let k be a fixed integer with $1 \leq k \leq e$ and ψ a generating character of A^+. Then*

(3.6)

$$\sum_{b\in A^\times} \psi_b(p^{e-k}a) = \begin{cases} |A^\times| & \text{if } k = 1 \text{ and } a \in M, \\ -|M| & \text{if } k = 1 \text{ and } a \in A^\times, \\ 0 & \text{if } 2 \leq k \leq e \text{ and } a \in A^\times, \\ |T|^{e-k+1} S(b_0, b_1, \cdots, b_{k-2}) & \text{if } 2 \leq k \leq e \text{ and } a \in M, \end{cases}$$

where

$$S(b_0, b_1, \cdots, b_{k-2}) = \left(\sum_{b_0\in T^\times} \psi_{b_0}(p^{e-k}a) \right) \prod_{i=1}^{k-2} \left(\sum_{b_i\in T} \psi_{b_i}(p^{e-k+i}a) \right).$$

Proof. Since every element $b \in A^\times$ has a unique p-adic representation

$$b = b_0 + pb_1 + p^2b_2 + \cdots + p^{e-1}b_{e-1},\ b_0 \in T^\times,\ b_1, \cdots, b_{e-1} \in T,$$

we have

$$\begin{aligned}
&\sum_{b\in A^\times}\psi_b(p^{e-1}a)\\
=\;&\left(\sum_{b_0\in T^\times}\psi_{b_0}(p^{e-1}a)\right)\left(\sum_{b_1\in T}\psi_{b_1}(p^{e}a)\right)\cdots\left(\sum_{b_{e-1}\in T}\psi_{b_{e-1}}(p^{e}(p^{e-2}a))\right)\\
=\;&\left(\sum_{b_0\in T^\times}\psi_{b_0}(p^{e-1}a)\right)\left(\sum_{b_1\in T}1\right)\cdots\left(\sum_{b_{e-1}\in T}1\right)\\
=\;&|T|^{e-1}\left(\sum_{b_0\in T}\psi_{b_0}(p^{e-1}a)-1\right)\\
=\;&\begin{cases}|T|^{e-1}(|T|-1)=|A^\times| & \text{if } a\in M\\ -|T|^{e-1}=-|M| & \text{if } a\in A^\times\end{cases}\ \text{(by Eq. (3.5))}.
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
&\sum_{b\in A^\times}\psi_b(p^{e-2}a)\\
=\;&\left(\sum_{b_0\in T^\times}\psi_{b_0}(p^{e-2}a)\right)\left(\sum_{b_1\in T}\psi_{b_1}(p^{e-1}a)\right)\left(\sum_{b_2\in T}1\right)\cdots\left(\sum_{b_{e-1}\in T}1\right)\\
=\;&|T|^{e-2}\left(\sum_{b_0\in T^\times}\psi_{b_0}(p^{e-2}a)\right)\left(\sum_{b_1\in T}\psi_{b_1}(p^{e-1}a)\right)\\
=\;&\begin{cases}|T|^{e-1}\left(\sum_{b_0\in T^\times}\psi_{b_0}(p^{e-2}a)\right) & \text{if } a\in M\\ 0 & \text{if } a\in A^\times\end{cases}\ \text{(by Eq. (3.5))}.
\end{aligned}$$

Generally, using Eq. (3.5), we have for $2 \le k \le e$

$$\begin{aligned}\sum_{b\in A^\times}\psi_b(p^{e-k}a) &= |T|^{e-k}\left(\sum_{b_0\in T^\times}\psi_{b_0}(p^{e-k}a)\right)\times \\ &\qquad \left(\sum_{b_1\in T}\psi_{b_1}(p^{e-k+1}a)\right)\cdots\left(\sum_{b_{k-1}\in T}\psi_{b_{k-1}}(p^{e-1}a)\right) \\ &= \begin{cases}|T|^{e-k+1}S(b_0,b_1,\cdots,b_{k-2}) & \text{if } a\in M,\\ 0 & \text{if } a\in A^\times,\end{cases}\end{aligned}$$

where

$$S(b_0,b_1,\cdots,b_{k-2}) = \left(\sum_{b_0\in T^\times}\psi_{b_0}(p^{e-k}a)\right)\prod_{i=1}^{k-2}\left(\sum_{b_i\in T}\psi_{b_i}(p^{e-k+i}a)\right).$$

□

LEMMA 3.4. *Let $S = 1 + ann(M)$ be strong units, where $ann(M) = \{x \in A \mid xy = 0\ \forall y \in M\}$. Then the modulus of a complete Gauss sum $G_A(\chi,\psi)$ is completely determined as*

$$|G_A(\chi,\psi)|^2 = |A| - |M|\sum_{z\in S}\chi(z) - \sum_{z\in A^\times - S}\chi(z)\sum_{y\in M}\psi((z-1)y). \tag{3.7}$$

Proof. The set $S = 1 + \mathrm{ann}(M)$ is a subgroup of $A^\times$. Thus $1 \in S$ and using Eq. (3.1) we get

$$
\begin{aligned}
& |G_A(\chi,\psi)|^2 \\
= & \sum_{x\in A^\times}\sum_{y\in A^\times}\chi(xy^{-1})\psi(x-y) = \sum_{z\in A^\times}\chi(z)\sum_{y\in A^\times}\psi((z-1)y) \\
& \qquad (\text{put } z = xy^{-1}) \\
= & \sum_{z\in S}\chi(z)\left(\sum_{y\in A}\psi((z-1)y) - \sum_{y\in M}\psi((z-1)y)\right) \\
& + \sum_{z\in A^\times - S}\chi(z)\left(\sum_{y\in A}\psi((z-1)y) - \sum_{y\in M}\psi((z-1)y)\right) \\
= & \sum_{z\in S}\chi(z)\sum_{y\in A}\psi((z-1)y) - \sum_{z\in S}\chi(z)\sum_{y\in M}\psi((z-1)y) \\
& + \sum_{z\in A^\times - S}\chi(z)\left(\sum_{y\in A}\psi((z-1)y) - \sum_{y\in M}\psi((z-1)y)\right) \\
= & \chi(1)\sum_{y\in A}1 - \sum_{z\in S}\chi(z)\sum_{y\in M}1 - \sum_{z\in A^\times - S}\chi(z)\sum_{y\in M}\psi((z-1)y) \\
= & |A| - |M|\sum_{z\in S}\chi(z) - \sum_{z\in A^\times - S}\chi(z)\sum_{y\in M}\psi((z-1)y).
\end{aligned}
$$

□

THEOREM 3.5. *Let t be a fixed integer such that $0 \le t \le e-1$. Let χ be a character of $A^\times$ and ψ a generating character of A^+. If χ is nontrivial on S, then*

$$\sum_{c\in A^\times - S}\chi(c)\sum_{b\in A^\times}\psi_b(p^t(c-1)) = 0.$$

If χ is trivial on $A^\times$, then

$$
\begin{aligned}
& \sum_{c\in A^\times - S}\chi(c)\sum_{b\in A^\times}\psi_b(p^t(c-1)) \\
= & \begin{cases} |M|^2 - |A^\times||K| & \text{if } t = e-1, \\ |T|^{t+1}\left\{|M| - |K|\right\}S(b_0, b_1, \cdots, b_{e-2-t}) & \text{if } 0 \le t \le e-2. \end{cases}
\end{aligned}
$$

Proof. Let $t = e - k$ for a fixed integer k with $1 \le k \le e$. From Eq. (3.6) in Lemma 3.3, for a character χ of $A^\times$ and for a generating

character ψ of A^+, we have

$$\begin{aligned}
&\sum_{c\in A^\times - S}\chi(c)\sum_{b\in A^\times}\psi_b(p^t(c-1))\\
&= \begin{cases}
|A^\times|\sum_{c\in A^\times-S}\chi(c) & \text{if } t=e-1 \text{ and } c-1\in M,\\
-|M|\sum_{c\in A^\times-S}\chi(c) & \text{if } t=e-1 \text{ and } c-1\in A^\times,\\
0 & \text{if } 0\le t\le e-2 \text{ and } c-1\in A^\times,\\
|T|^{t+1}\sum_{c\in A^\times-S}\chi(c)\times & \\
\quad S(b_0,b_1,\cdots,b_{e-t-2}) & \text{if } 0\le t\le e-2 \text{ and } c-1\in M,
\end{cases}\\
&= \begin{cases}
|A^\times|\left\{\sum_{c\in U}\chi(c)-\sum_{c\in S}\chi(c)\right\} & \\
\qquad -|M|\left\{\sum_{c\in A^\times}\chi(c)-\sum_{c\in U}\chi(c)\right\} & \text{if } t=e-1,\\
|T|^{t+1}\left\{\sum_{c\in U}\chi(c)-\sum_{c\in S}\chi(c)\right\}\times & \\
\quad S(b_0,b_1,\cdots,b_{e-2-t}) & \text{if } 0\le t\le e-2.
\end{cases}
\end{aligned}$$

By [1, Proposition 2], $|S| = |1+\mathrm{ann}(M)| = |\mathrm{ann}(M)| = |K|$. Also $|U| = |1+M| = |M|$. If χ is trivial on $A^\times$, then χ is also trivial on U and S, and so that

$$\begin{aligned}
&\sum_{c\in A^\times - S}\chi(c)\sum_{b\in A^\times}\psi_b(p^t(c-1))\\
&= \begin{cases}
|A^\times|\{|U|-|S|\}-|M|\{|A^\times|-|U|\} & \\
\quad =|M|^2-|A^\times||\mathcal{K}| & \text{if } t=e-1,\\
|T|^{t+1}S(b_0,\cdots,b_{e-2-t})\{|M|-|\mathcal{K}|\} & \text{if } 0\le t\le e-2.
\end{cases}
\end{aligned}$$

If χ is nontrivial on S, then χ is also nontrivial on U and $A^\times$, and so that

$$\sum_{c\in A^\times - S}\chi(c)\sum_{b\in A^\times}\psi_b(p^t(c-1)) = 0.$$

□

Corollary 3.6. *Let t be a fixed integer with $0\le t\le e-1$ and χ a character of $A^\times$ and ψ a generating character of A^+. If χ is nontrivial on S, then*

$$|G_A(\chi,\psi_{p^t})| = \sqrt{|A|} \quad \textit{and} \quad G_A(\chi,\psi_{p^t})G_A(\overline{\chi},\psi_{p^t}) = \chi(-1)|A|.$$

References

[1] P. Langevin and P. Sole, *Gauss sums over quasi-Frobenius rings*, Finite Fields and Applications (Augsburg, 1999) (2001), 329-340.
[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 Applied Mathematics
Kum-oh National Institute of Technology
Kumi 730-701, Korea
E-mail: wsyoo@kumoh.ac.kr

Department of Mathematics
Inha University
Incheon 402-751, Korea
E-mail: idstudy@hanmail.net