COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 45, No. 1 1996

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

Abelian Fields Generated by a Jacobi Sum

by

Noboru AOKI

(Received May 20, 1995)

Introduction

Let $m>1$ be a natural number and $K=\boldsymbol{Q}(\zeta_m)$ the m-th cyclotomic field. Let p be a prime number which does not divide m, and $\mathfrak{p}$ a prime ideal in K lying above p. We denote by f the order of p in $(\boldsymbol{Z}/m\boldsymbol{Z})^*$ and put $q=p^f$. Following Weil [14], for each integer $n\geq 0$ and for each $(n+2)$-tuple $\alpha=(a_0, \cdots, a_{n+1})\in(\boldsymbol{Z}/m\boldsymbol{Z})^{n+2}$ such that $a_0+\cdots+a_{n+1}=0$, we define the Jacobi sum by

$$J_\alpha(\mathfrak{p})=\frac{1}{q-1}\sum_{\substack{x_0,\cdots,x_{n+1}\in F_q^* \\ x_0+\cdots+x_{n+1}=0}}\chi_\mathfrak{p}(x_0)^{a_0}\cdots\chi_\mathfrak{p}(x_{n+1})^{a_{n+1}},$$

where $\chi_\mathfrak{p}$ denotes the m-th power residue symbol. Obviously $J_\alpha(\mathfrak{p})$ is an element of K. If $a_i=0$ for some (but not all) i, then one can easily see that $J_\alpha(\mathfrak{p})=0$. In view of this fact, let us consider the following set

$$\mathfrak{A}_m^n=\{(a_0, a_1, \cdots, a_{n+1})\in(\boldsymbol{Z}/m\boldsymbol{Z}\setminus\{0\})^{n+2}\,|\,a_0+a_1+\cdots+a_{n+1}=0\}$$

(see [13]). Then it is known that $J_\alpha(\mathfrak{p})\neq 0$ for any $\alpha\in\mathfrak{A}_m^n$.

In some cases we can compute the Jacobi sum explicitly. For example, if α is of the form $(a_0, -a_0, \cdots, a_r, -a_r)$, then $J_\alpha(\mathfrak{p})=\pm q^r$ (see Proposition 2.5). More generally Hasse-Davenport's relations of Gauss sums enable us to get explicit formulae of $J_\alpha(\mathfrak{p})$ for "standard elements" α (see Proposition 4.2). However, it seems rather difficult to determine the exact value of $J_\alpha(\mathfrak{p})$ in general, so we consider an easier problem instead:

(0.1) Determine the field $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))$ generated over $\boldsymbol{Q}$ by the Jacobi sum $J_\alpha(\mathfrak{p})$.

In a series of papers [7], [4], [10], Ono, Kida and Gyoja treated this problem. Their principal idea is to bound the Galois group $G(J_\alpha(\mathfrak{p})):=Gal(K/\boldsymbol{Q}(J_\alpha(\mathfrak{p})))$ from both above and below:

$$G(p)\subseteq G(J_\alpha(\mathfrak{p}))\subseteq G^*(J_\alpha(\mathfrak{p})), \tag{0.2}$$

where $G(p)$ is the decomposition group of $\mathfrak{p}$ and $G^*(J_\alpha(\mathfrak{p}))$ is the stabilizer in $Gal(K/\boldsymbol{Q})$ of the ideal $(J_\alpha(\mathfrak{p}))$ in K. Therefore, if $G(p)=G^*(J_\alpha(\mathfrak{p}))$, then $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))$ coincides with the decomposition field of $\mathfrak{p}$. They showed that this equality holds for the elements

of the form $\alpha=(1, \cdots, 1, -n)\in\mathfrak{A}_m^{n-1}$ under certain conditions on m, n and p.

The purpose of this paper is to generalize their results in several directions. For that purpose we improve (0.2). To state our main results, we fix some notation. In what follows we identify $Gal(K/\boldsymbol{Q})$ with $G:=(\boldsymbol{Z}/m\boldsymbol{Z})^*$ in the standard manner; $t\in G\leftrightarrow\sigma_t:=(\zeta_m\mapsto\zeta_m^t)\in Gal(K/\boldsymbol{Q})$. Then $G(p)=\{1, p, \cdots, p^{f-1}\}\subseteq G$ under this identification. We let G act on $\mathfrak{A}_m^n$ by setting $t\cdot(a_0, \cdots, a_{n+1})=(ta_0, \cdots, ta_{n+1})$ for $t\in G$. For any two elements $\alpha, \beta\in\mathfrak{A}_m^n$, we write $\alpha\sim\beta$ if α equals β up to permutation of the components. If $n=2r$ is even, we denote by $\mathfrak{D}_m^n$ the set of elements $\alpha\in\mathfrak{A}_m^n$ such that $\alpha\sim(a_0, -a_0, \cdots, a_r, -a_r)$ for some a_i. Let

$$G_\alpha(p)=\begin{cases} G & \text{if } \ v_p\alpha\in\mathfrak{D}_m^{(n+2)f-2}, \\ \{t\in G \mid t\cdot v_p\alpha\sim v_p\alpha\} & \text{otherwise}, \end{cases} \tag{0.3}$$

where $v_p\alpha\in\mathfrak{A}_m^{(n+2)f-2}$ denotes the iteration of f elements $\alpha, p\cdot\alpha, \cdots, p^{f-1}\cdot\alpha$. (See Section 1 for the precise definition of the "product" $v_p\alpha$.) It is then easy to see that $G(p)\subseteq G_\alpha(p)$. Moreover let

$$G_\alpha^*(p)=\left\{t\in G \,\middle|\, \sum_{i=0}^{n+1}\sum_{j=0}^{f-1}\left\langle\frac{tp^ja_i}{m}\right\rangle=\sum_{i=0}^{n+1}\sum_{j=0}^{f-1}\left\langle\frac{p^ja_i}{m}\right\rangle\right\}, \tag{0.4}$$

where, for each $a\in\boldsymbol{Z}/m\boldsymbol{Z}\setminus 0$, $\left\langle\frac{a}{m}\right\rangle$ denotes the rational number such that $0<\left\langle\frac{a}{m}\right\rangle<1$ and $m\left\langle\frac{a}{m}\right\rangle\equiv a \pmod m$. Clearly $G_\alpha(p)$ is a subgroup of $G_\alpha^*(p)$. The following theorem then gives a refinement of (0.2).

THEOREM 0.1 (cf. Theorem 5.1). *Notation being as above, we have*

$$G_\alpha(p)\subseteq G(J_\alpha(\mathfrak{p}))\subseteq G_\alpha^*(p). \tag{0.5}$$

In particular, if $G_\alpha(p)=G_\alpha^*(p)$, *then* $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=K^{G_\alpha(p)}$.

We shall see that $G_\alpha^*(p)$ coincides with $G^*(J_\alpha(\mathfrak{p}))$ (see Remark 5.6). So, comparing (0.5) with (0.2), the new point is the left incusion. Using a result of [1], we can give a sufficient condition for the equality $G_\alpha(p)=G_\alpha^*(p)$.

THEOREM 0.2 (cf. Theorem 5.2). *Suppose that one of the following two conditions holds*:

(i) *m is either 4 or a prime number; or*

(ii) *every prime factor of m is greater than $2(n+2)f$.*

Then $G_\alpha(p)=G_\alpha^*(p)$ (*hence* $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=K^{G_\alpha(p)}$) *for any* $\alpha\in\mathfrak{A}_m^n$.

For $\alpha=(a_0, \cdots, a_{n+1})\in\mathfrak{A}_m^n$, we say that α is *non-degenerate* if

$$\sum_{t\in G}\sum_{i=0}^{n+1}\left(\left\langle\frac{ta_i}{m}\right\rangle-\frac{1}{2}\right)\chi(t)\neq 0$$

for all odd Dirichlet characters χ of G. We will show that $G_\alpha^*(p)$ coincides with $G(p)$

if α is non-degenerate (Lemma 6.2). This fact leads to the following theorem, which has been proved by H. Yanai when m is a prime number.

THEOREM 0.3 (cf. Theorem 6.1). *If* $-1 \notin G(p)$ *and* α *is non-degenerate, then* $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))$ *is the decomposition field of* $\mathfrak{p}$.

For example, if m is a prime number and n is prime to m, then $\alpha = (1, \cdots, 1, -n) \in \mathfrak{A}_m^{n-1}$ is always non-degenerate ([10]). (See also Remark 6.6.) Thus this theorem may be regarded as a generalization of [4], Theorem 2, and the proof is essentially the same as the argument in [10].

When m is a power of an odd prime, we can give a complete answer to (0.2)

THEOREM 0.4 (cf. Theorem 7.1). *Let* $m = l^e$ *be a power of an odd prime. Then* $\boldsymbol{Q}(J_\alpha(\mathfrak{p})) = L(\zeta)$, *where* $L = K^{G_\alpha^*(p)}$ *and* ζ *is an* l^{e-1}*-th root of unity which can be computed explicitly.*

When $n=1$ and $p \equiv 1 \pmod{m}$, we can also give an almost complete answer to (0.2). To state it we define a finite set of natural numbers by

$$\mathscr{E} = \begin{cases} \{12, 15, 20, 21, 24, 26, 28, 30, 36, 39, 40, 42, \\ 48, 54, 60, 66, 72, 78, 84, 90, 120, 156, 180\}\,. \end{cases} \tag{0.6}$$

An element $\alpha = (a_0, \cdots, a_{n+1}) \in \mathfrak{A}_m^n$ is said to be *primitive* if $GCD(m, \tilde{a}_0, \cdots, \tilde{a}_{n+1}) = 1$, where $\tilde{a}_i$'s are any integers such that $\tilde{a}_i \equiv a_i \pmod{m}$. For any divisor d of m we denote by K_d the d-th cyclotomic field $\boldsymbol{Q}(\zeta_m^{m/d})$.

THEOREM 0.5 (cf. Theorem 8.1). *Suppose* $m \notin \mathscr{E}$ *and* $p \equiv 1 \pmod{m}$. *Let* $\alpha \in \mathfrak{A}_m^1$ *be a primitive element. Then the following statements hold.*

(i) *Suppose* $4 \mid m$ *and* $\alpha = (a, a, -2a)$. *Then*

$$\boldsymbol{Q}(J_\alpha(\mathfrak{p})) = \begin{cases} K_{m/2} & \text{if } \chi_{\mathfrak{p}}(2)^2 = 1\,, \\ K_m & \text{otherwise}\,. \end{cases}$$

(ii) *Suppose* $8 \mid m$ *and* $\alpha = \left(a, \frac{m}{2}+a, \frac{m}{2}-2a\right)$. *Then*

$$\boldsymbol{Q}(J_\alpha(\mathfrak{p})) = \begin{cases} K_{m/4} & \text{if } \chi_{\mathfrak{p}}(2)^4 = 1\,, \\ K_{m/2} & \text{otherwise}\,. \end{cases}$$

(iii) *In the other cases, we have* $\boldsymbol{Q}(J_\alpha(\mathfrak{p})) = K^{G_\alpha(p)}$.

The contents of this paper is as follows. In Section 1 we define some basic notations, and is Section 2 we recall fundamental results about Gauss sums and Jacobi sums. Section 3 concerns with Stickelberger's theorem and some related results. In Section 4, after defining standard elements, we state a theorem of Yamamoto on the "gap group" in a different style from the original one. In Section 5 we give more precise definition of $G_\alpha(p)$ and $G_\alpha^*(p)$, and prove Theorem 0.1 and 0.2. In Section 6 we define non-degenerate elements, p-simple elements and simple elements, and discuss

their interrelations. The proof of Theorem 0.3 is given there. Section 7 and 8 are devoted to the proof of Theorem 0.4 and 0.5 respectively.

I would like to express my thanks to Professor Takashi Ono for his fascinating lectures in Japan which led me to this topic. I would also like to thank Professor Hiromichi Yanai whoe suggestion was very useful in writing Section 6.

1. Preliminaries

Let R_m be the free abelian group generated by the elements of $\boldsymbol{Z}/m\boldsymbol{Z}\setminus\{0\}$. An element of R_m will be written as

$$\sum_a c_a(a) \qquad (c_a \in \boldsymbol{Z}),$$

where a runs over $\boldsymbol{Z}/m\boldsymbol{Z}\setminus\{0\}$. For any $a, b \in \boldsymbol{Z}/m\boldsymbol{Z}\setminus\{0\}$, we define the product of (a) and (b) in R_m by the rule:

$$(a)(b)=\begin{cases}(ab) & \text{if } ab\neq 0,\\ 0 & \text{if } ab=0.\end{cases}$$

We can naturally extend this definition to the whole R_m to get a multiplication law in R_m. Thus R_m becomes a commutative ring with the unit (1). If we put $G=(\boldsymbol{Z}/m\boldsymbol{Z})^*$, then R_m admits a G-module structure by letting

$$t\cdot\sum c_a(a)=\sum c_a(ta)$$

for $t\in G$. For $n\geq 0$, we write $(a_0, \cdots, a_{n+1})$ for $\sum_{i=0}^{n+1}(a_i)\in R_m$, and denote by R_m^n the set of such elements. Let

$$R_m^+=\bigcup_{n\geq 0} R_m^n .$$

Now we consider the ring homomorphism $\varphi: R_m\to \boldsymbol{Z}/m\boldsymbol{Z}$ defined by

$$\varphi\left(\sum c_a(a)\right)=\sum c_a a , \tag{1.1}$$

which is obviously a G-homomorphism. Let $A_m=\ker\varphi$ be the kernel of φ:

$$A_m=\left\{\sum c_a(a)\in R_m \,\middle|\, \sum c_a a=0\right\} .$$

Furthermore we consider the following subsets of A_m:

$$A_m^n=A_m\cap R_m^n , \qquad A_m^+=A_m\cap R_m^+ .$$

Note that there is a natural identification $A_m^n=\mathfrak{A}_m^n/\sim$, where $\mathfrak{A}_m^n$ and $\sim$ are as in the introduction. Let $D_m=(1,-1)R_m$ be the ideal of R_m generated by $(1,-1)$ and put

$$D_m^n=D_m\cap A_m^n$$

for any $n\geq 0$. Thus, if $n=2r$ is even, then D_m^n consists of elements of the form

$(a_0, -a_0, \cdots, a_r, -a_r)$ (hence $D_m^n = \mathfrak{D}_m^n/\sim$). On the other hand, if n is odd, then D_m^n is empty.

2. Gauss sums and Jacobi sums

In this section we recall some basic results on Gauss sums and Jacobi sums which will be needed later. For details we refer to [6] or [9]. Let m, p, $\mathfrak{p}$ and q be as in the introduction. Let μ_m be the group of m-th roots of unity in K. Then the m-th power residue symbol is the homomorphism

$$\chi_{\mathfrak{p}}: \boldsymbol{F}_q^* \to \mu_m$$

characterized by the relation

$$\chi_{\mathfrak{p}}(x) \equiv x^{(q-1)/m} \pmod{\mathfrak{p}}.$$

Here we have identified $\boldsymbol{F}_q$ with the residue field of $\mathfrak{p}$. Let $\psi_{\mathfrak{p}}: \boldsymbol{F}_q \to \mu_p$ be the additive character defined by $\psi_{\mathfrak{p}}(x) = \exp^{2\pi i T(x)/p}$, where T denotes the trace map from $\boldsymbol{F}_q$ to $\boldsymbol{F}_p$. For $a \in \boldsymbol{Z}/m\boldsymbol{Z} \setminus \{0\}$, we define the Gauss sum by

$$g_a(\mathfrak{p}) = \sum_{x \in F_q^*} \chi_{\mathfrak{p}}(x)^a \psi_{\mathfrak{p}}(x) \quad (\in K(\mu_p)),$$

which is known to be non-zero. The following properties are fundamental.

$$g_a(\mathfrak{p}) g_{-a}(\mathfrak{p}) = \chi_{\mathfrak{p}}(-1)^a q \quad \text{and} \quad |g_a(\mathfrak{p})| = q^{1/2}. \tag{2.1}$$

Davenport and Hasse discovered a beautiful relation (Davenport-Hasse's relation) between Gauss sums.

THEOREM 2.1. *Let l and d be divisors of m such that $m = ld$. Then*

$$\prod_{i=0}^{l-1} g_{a+id}(\mathfrak{p}) = \chi_{\mathfrak{p}}(l^{-la}) \cdot g_{la}(\mathfrak{p}) \prod_{i=1}^{l-1} g_{id}(\mathfrak{p}). \tag{2.2}$$

Proof. See [9], Chap. 2, Theorem 10.1. □

Following Weil [14], for $\alpha = (a_0, \cdots, a_{n+1}) \in \mathfrak{A}_m^n$ we define the Jacobi sum by

$$J_\alpha(\mathfrak{p}) = \frac{1}{q-1} \sum_{\substack{x_0, \cdots, x_{n+1} \in F_q^* \\ x_0 + \cdots + x_{n+1} = 0}} \chi_{\mathfrak{p}}(x_0)^{a_0} \cdots \chi_{\mathfrak{p}}(x_{n+1})^{a_{n+1}}.$$

Obviously $J_\alpha(\mathfrak{p})$ is an element of K. Gauss sums and Jacobi sums are related by the formula (2.3) below.

THEOREM 2.2. *If $\alpha = (a_0, \cdots, a_{n+1}) \in \mathfrak{A}_m^n$, then*

$$J_\alpha(\mathfrak{p}) = \frac{1}{q} g_{a_0}(\mathfrak{p}) \cdots g_{a_{n+1}}(\mathfrak{p}). \tag{2.3}$$

Proof. See [6], Chap. 8, §5, Theorem 3. □

It is clear from the definition that $J_\alpha(\mathfrak{p})$ depends only on the class of α in A_m^+. In other words, if $\alpha\sim\beta$, then $J_\alpha(\mathfrak{p})=J_\beta(\mathfrak{p})$. From now on we suppose that $J_\alpha(\mathfrak{p})$ is defined for $\alpha\in A_m^+$.

For any $a\in \boldsymbol{Z}/m\boldsymbol{Z}\setminus\{0\}$, let

$$\varepsilon_a(\mathfrak{p})=\frac{g_a(\mathfrak{p})}{\sqrt{\chi_{\mathfrak{p}}(-1)^a q}},$$

where the sign of the square root in the denominator is chosen so that its imaginary part is positive if $\chi_{\mathfrak{p}}(-1)^a<0$. Furthermore, for $\alpha=\sum c_a(a)\in R_m$, let

$$\varepsilon_\alpha(\mathfrak{p})=\prod_a \varepsilon_a(\mathfrak{p})^{c_a}.$$

Then, for $\alpha\in A_m^n$, Theorem 2.2 is equivalent to the following formula.

$$\varepsilon_\alpha(\mathfrak{p})=J_\alpha(\mathfrak{p})q^{-n/2}. \tag{2.4}$$

Note that $\varepsilon_\alpha(\mathfrak{p})\in K(\mu_p)$ if $p\geq 3$ and $\varepsilon_\alpha(\mathfrak{p})\in K(\sqrt{2})$ if $p=2$. Since p is prime to m, we can make $Gal(K/\boldsymbol{Q})$ act on $\varepsilon_\alpha(\mathfrak{p})$ through the canonical isomorphism $Gal(K/\boldsymbol{Q})\cong Gal(K(\mu_p)/\boldsymbol{Q}(\mu_p))$ if $p\geq 3$ and $Gal(K/\boldsymbol{Q})\cong Gal(K(\sqrt{2})/\boldsymbol{Q}(\sqrt{2}))$ if $p=2$. This action is given by

$$\varepsilon_\alpha(\mathfrak{p})^{\sigma_t}=\varepsilon_{t\cdot\alpha}(\mathfrak{p}) \qquad (t\in G). \tag{2.5}$$

Since $g_{p\alpha}(\mathfrak{p})=g_\alpha(\mathfrak{p})$ (see [9]), $\varepsilon_\alpha(\mathfrak{p})^{\sigma_p}=\varepsilon_\alpha(\mathfrak{p})$ for any $\alpha\in R_m$. This fact will be useful in later sections.

Using (2.1) and (2.5) we can easily see that

$$\overline{\varepsilon_\alpha(\mathfrak{p})}=\varepsilon_{(-1)\alpha}(\mathfrak{p}) \quad \text{and} \quad |\varepsilon_\alpha(\mathfrak{p})|=1. \tag{2.6}$$

Therefore, if $\varepsilon_\alpha(\mathfrak{p})$ is a unit in K, then $\varepsilon_\alpha(\mathfrak{p})$ is a root of unity in K.

3. Stickelberger's theorem

For $\alpha=(a_0, a_1, \cdots, a_{n+1})\in A_m^n$, we put

$$\|\alpha\|=\sum_{i=0}^{n+1}\left\langle\frac{a_i}{m}\right\rangle-1.$$

Then $\|\alpha\|\in\boldsymbol{Z}$ and $0\leq\|t\cdot\alpha\|\leq n$ for any $t\in G$. Moreover we have a symmetry

$$\|\alpha\|+\|-\alpha\|=n. \tag{3.1}$$

Let us define a *Stickelberger element* as an element of the group ring $\boldsymbol{Z}[Gal(K/\boldsymbol{Q})]$ defined by

$$\omega(\alpha)=\sum_{t\in G}\|t\cdot\alpha\|\sigma_t^{-1}\in\boldsymbol{Z}[Gal(K/\boldsymbol{Q})].$$

The following theorem is due to Stickelberger.

THEOREM 3.1. *The prime ideal decomposition in K of the ideal* $(J_\alpha(\mathfrak{p}))$ *generated by the Jacobi sum* $J_\alpha(\mathfrak{p})$ *is given by*

$$(J_\alpha(\mathfrak{p}))=\mathfrak{p}^{\omega(\alpha)}.$$

Proof. See [6] or [9]. □

Let f be the order of p in G. Then the decomposition group of $\mathfrak{p}$ is the cyclic group generated by σ_p, and it corresponds, under the identification $Gal(K/\boldsymbol{Q})=G$ in the introduction, to the group

$$G(p):=\{1, p, \cdots, p^{f-1}\}\subseteq G. \tag{3.2}$$

Let $v_p=(1, p, p^2, \cdots, p^{f-1})\in R_m^{f-2}$. Then Stickelberger's theorem may be rewritten as

$$(J_\alpha(\mathfrak{p}))=\prod_{u\in G/G(p)}\mathfrak{p}^{\|u\cdot v_p\alpha\|\sigma_u^{-1}}, \tag{3.3}$$

where the product is taken over the representatives of $G/G(p)$. As an example, let us consider the case $\alpha\in D_m^n$. Then from (3.1) we have $\|t\cdot\alpha\|=\frac{n}{2}$ for all $t\in G$. Therefore Stickelberger's theorem implies that

$$(J_\alpha(\mathfrak{p}))=\mathfrak{p}^{n/2\sum_{t\in G}\sigma_t}=(N\mathfrak{p})^{n/2}=(q^{n/2}).$$

Actually we have $J_\alpha(\mathfrak{p})=\pm q^{n/2}$ (see Proposition 4.2).

Now, it is useful to consider the additive homomorphism

$$\theta\colon R_m\to\boldsymbol{Q}[Gal(K/\boldsymbol{Q})]$$

defined by

$$\theta\left(\sum_a c_a(a)\right)=\sum_{t\in G}\sum_a c_a\left(\left\langle\frac{ta}{m}\right\rangle-\frac{1}{2}\right)\sigma_{-t}^{-1}. \tag{3.4}$$

Then θ is a G-module homomorphism in the sense that we have

$$\theta((t)\alpha)=\sigma_t\theta(\alpha)$$

for all $t\in G$. For $\alpha\in A_m^n$ two elements $\omega(\alpha)$ and $\theta(\alpha)$ are related as

$$\theta(\alpha)=\omega(\alpha)-\frac{n}{2}\sum_{t\in G}\sigma_t.$$

Let $B_m=\ker\theta$ be the kernel of θ, and put

$$B_m^n=B_m\cap A_m^n \quad\text{and}\quad B_m^+=\bigcup_{n\geq 0}B_m^n.$$

We easily find that B_m^n is empty if n is odd, and that for $n=2r$

$$B_m^{2r}=\{\alpha\in A_m^{2r}\mid\|t\cdot\alpha\|=r(\forall t\in G)\}.$$

Furthermore we put

$$B_m^n(p)=\{\alpha\in A_m^n \mid v_p\alpha\in B_m^{(n+2)f-2}\}\ .$$

It is then clear from the definition that the following inclusions hold:

$$D_m^n\subseteq B_m^n\subseteq B_m^n(p)\subseteq A_m^n\ .$$

For any $\alpha\in A_m^n$, (3.3) shows that $(J_\alpha(\mathfrak{p}))=(q^{n/2})$ (i.e., $\varepsilon_\alpha(\mathfrak{p})$ is a unit of K) if and only if $\alpha\in B_m^n(p)$. But the following stronger result is well known.

PROPOSITION 3.2. *Let $\mu(K)$ be the set of roots of unity in K. Then, for $\alpha\in A_m^n$, we have $\varepsilon_\alpha(\mathfrak{p})\in\mu(K)$ if and only if $\alpha\in B_m^n(p)$.*

Proof. This can be proved by combining Theorem 3.1 and (2.6) with Kronecker's theorem on units in algebraic number fields. For more details, see [13], Lemma 3.1. □

If $-1\in G(p)$, then we can easily see that $B_m^n(p)=A_m^n$, and so this proposition implies that $\varepsilon_\alpha(\mathfrak{p})$ is a root of unity in K for any $\alpha\in A_m$. But we can say more in this case.

PROPOSITION 3.3. *If $-1\in G(p)$, then $\varepsilon_\alpha(\mathfrak{p})=\pm 1$, hence $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=\boldsymbol{Q}$ for any $\alpha\in A_m^+$.*

Proof. This follows from (2.4), (2.5) and (2.6). For details see [13]. □

REMARK 3.4. The subsets $\mathfrak{B}_m^n$ and $\mathfrak{B}_m^n(p)$ of $\mathfrak{A}_m^n$ defined in [13] correspond to our B_m^n and $B_m^n(p)$ respectively, namely $B_m^n=\mathfrak{B}_m^n/\sim$ and $B_m^n(p)=\mathfrak{B}_m^n(p)/\sim$.

4. Standard elements

Let l be a divisor of m and put $d=\dfrac{m}{l}$. For each $a\in\boldsymbol{Z}/m\boldsymbol{Z}$ with $la\neq 0$, we define the *standard element* by

$$\sigma_{l,a}=\begin{cases}(a,\ a+d,\ \cdots,\ a+(l-1)d,\ -la) & \text{if } l \text{ is odd},\\ \left(a,\ a+d,\ \cdots,\ a+(l-1)d,\ -la,\ \dfrac{m}{2}\right) & \text{if } l \text{ is even}.\end{cases}$$

Note that $\sigma_{1,a}=(a,\ -a)\in D_m^0$.

PROPOSITION 4.1. *Let $n=l-1$ or l according as l is odd or even. Then $\sigma_{l,a}\in B_m^n$.*

Proof. It is clear that $\sigma_{l,a}$ belongs to A_m^n. We consider only the case l is odd. (The proof for even l is quite similar.) Since $t\cdot\sigma_{l,a}=\sigma_{l,ta}$ for any $t\in(\boldsymbol{Z}/m\boldsymbol{Z})^*$, we have only to prove that $\|\sigma_{l,a}\|=\dfrac{n}{2}$ for all $a\in\boldsymbol{Z}$ with $0<a<d$. But in this case, we have

$$\|\sigma_{l,a}\|=\sum_{i=0}^{l-1}\frac{a+id}{m}+\frac{m-la}{m}-1=\frac{l-1}{2}=\frac{n}{2}\ .$$

Hence the proposition holds for odd l. □

Thanks to Hasse-Davenport's relation (2.2) we can calculate Jacobi sums explicitly for standard elements.

PROPOSITION 4.2. *Let $\alpha=\sigma_{l,a}$ be a standard element defined above, and let n be $l-1$ or l according as l is odd or even. Then*

$$J_\alpha(\mathfrak{p})=\chi_\mathfrak{p}(-l)^{-la}q^{n/2}\,.$$

In particular, $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=\boldsymbol{Q}(\chi_\mathfrak{p}(-l)^{la})$.

Proof. For $l=1$ we must show that $J_{(a,-a)}(\mathfrak{p})=\chi_\mathfrak{p}(-1)^a$. But this is an immediate consequence of (2.1) and (2.3). Next suppose $l>1$ is an odd divisor of m. (We prove the proposition only for odd l since the proof for even l is quite similar.) By Davenport-Hasse's relation and (2.3), we have

$$J_\alpha(\mathfrak{p})=\frac{1}{q}\left(\prod_{i=0}^{l-1}g_{a+id}(\mathfrak{p})\right)g_{-la}(\mathfrak{p})=\chi_\mathfrak{p}(-1)^{-la}\chi_\mathfrak{p}(l^{-la})\prod_{i=1}^{l-1}g_{id}(\mathfrak{p})\,.$$

Since $g_{id}(\mathfrak{p})g_{-id}(\mathfrak{p})=\chi_\mathfrak{p}(-1)^{id}q$ by (2.1), the last formula equals $\chi_\mathfrak{p}(-l)^{-la}q^{(l-1)/2}$. The proposition now follows. □

Let S_m be the submodule of B_m generated by standard elements. It is not hard to see that S_m is a G-submodule of R_m generated by $\sigma_{l,d}$'s, where l is either 1 or a prime factor of m and d is a divisor of m such that $ld\neq m$. Proposition 4.2 then enables us to compute $\varepsilon_\alpha(\mathfrak{p})$ for any $\alpha\in S_m$; if $\alpha=\sum_{l,d}\beta_{l,d}\sigma_{l,d}\in S_m$ with some $\beta_{l,d}\in\boldsymbol{Z}[G]\subseteq R_m$, then

$$\varepsilon_\alpha(\mathfrak{p})=\prod_{l,d}\chi_\mathfrak{p}(-l)^{-\varphi(\beta_{l,d})l}\,. \tag{4.1}$$

It is clear that $A_2^n=B_2^n=D_2^n$. The following theorem shows how B_m differs from S_m when $m>2$. The quotient group B_m/S_m is called the *gap group*.

THEOREM 4.3. *Suppose that $m>2$. Let r be the number of prime factors of m. Then $B_m/S_m\cong\boldsymbol{Z}/2\boldsymbol{Z}^{\oplus s}$, where $s=2^{r-1}-1$ (resp. $2^{r-2}-1$) if $\operatorname{ord}_2 m\neq 1$ (resp. $\operatorname{ord}_2 m=1$). In particular, if m is a power of a prime, then $B_m=S_m$, that is, every element of B_m is generated by standard elements.*

Proof. This is essentially equivalent to Theorem 3 of [15], although his notation differs from ours. (See also [11].) In this formulation this is implicitly proved in [1]. □

This theorem, together with Proposition 4.2, enable us to compute $\varepsilon_\alpha(\mathfrak{p})^2$ for any $\alpha\in B_m$, so we get the value of $\varepsilon_\alpha(\mathfrak{p})$ up to sign.

Let us illustrate the theorem above in the case where $m=l_1l_2$ is a product of two odd prime l_1 and l_2 both of which are congruent to 3 modulo 4. We may (and do) suppose $\left(\frac{l_2}{l_1}\right)=1$ without loss of generality. In this case we have $B_m/S_m\cong\boldsymbol{Z}/2\boldsymbol{Z}$ by

the above theorem. Therefore, if we take an element $\alpha \in B_m \setminus S_m$, then B_m is generated by S_m and α. Let g_1, g_2 be any generators of $(\boldsymbol{Z}/l_1\boldsymbol{Z})^*$ and $(\boldsymbol{Z}/l_2\boldsymbol{Z})^*$ respectively, and let a_1, a_2 be elements of $(\boldsymbol{Z}/m\boldsymbol{Z})^*$ such that

$$a_1 \equiv \begin{cases} g_1^2 & (\text{mod. } l_1) \\ 1 & (\text{mod. } l_2), \end{cases} \qquad a_2 \equiv \begin{cases} 1 & (\text{mod. } l_1) \\ g_2^2 & (\text{mod. } l_2). \end{cases}$$

Then the element defined by

$$\alpha = (1, a_1, \cdots, a_1^{(l_1-3)/2}, -l_1)(1, a_2, \cdots, a_2^{(l_2-3)/2}) \in A_m^{(l_1+1)/2\cdot(l_2-1)/2-2} \tag{4.2}$$

gives the generator of B_m/S_m. In order to see that $2\alpha \in S_m$, let ε_1, ε_2 be elements of $(\boldsymbol{Z}/m\boldsymbol{Z})^*$ such that

$$\varepsilon_1 \equiv \begin{cases} -1 & (\text{mod. } l_1) \\ 1 & (\text{mod. } l_2), \end{cases} \qquad \varepsilon_2 \equiv \begin{cases} 1 & (\text{mod. } l_1) \\ -1 & (\text{mod. } l_2). \end{cases}$$

Then $\varepsilon_1\varepsilon_2 = -1$, and so

$$2(1) \equiv (1, \varepsilon_1) + (-\varepsilon_1)(1, \varepsilon_2) \quad (\text{mod. } D_m). \tag{4.3}$$

Moreover we have

$$(1, \varepsilon_1)\alpha \equiv (1, a_2, \cdots, a_2^{(l_2-3)/2})\sigma_{l_1,1}$$

$$\text{and} \quad (1, \varepsilon_2)\alpha \equiv (1, a_1, \cdots, a_1^{(l_1-3)/2})\sigma_{l_2,1} \quad (\text{mod. } D_m).$$

Therefore the formula (4.2) implies that $2\alpha \in S_m$.

EXAMPLE 4.4. If $m = 21$ ($l_1 = 3$, $l_2 = 7$), then the element defined by (4.2) is

$$\alpha = (1, -3)(1, 4, 16) = (1, 4, 9, 15, 16, 18) \in A_{21}^4.$$

In this case we have

$$2\alpha \equiv \sigma_{7,1} + (1, 4, 16)\sigma_{3,1} \quad (\text{mod. } D_{21}).$$

It follows from Proposition 4.2 and (4.1) that

$$\varepsilon_\alpha(\mathfrak{p})^2 = \varepsilon_{2\alpha}(\mathfrak{p}) = \chi_\mathfrak{p}(7^{-7})\chi_\mathfrak{p}(3^{-3})^{1+4+16} = \chi_\mathfrak{p}(7^{-7}),$$

and so $\varepsilon_\alpha(\mathfrak{p}) = \pm\chi_\mathfrak{p}(7)^7$. Therefore $J_\alpha(\mathfrak{p}) = \pm\chi_\mathfrak{p}(7)^7 q^2$.

5. The groups $G_\alpha(p)$ and $G_\alpha^*(p)$

For each $\alpha \in R_m$ we consider two subsets G_α and G_α^* of G defined by

$$G_\alpha = \{t \in G \mid t \cdot \alpha \equiv \alpha \ (\text{mod. } D_m)\},$$

$$G_\alpha^* = \{t \in G \mid t \cdot \alpha \equiv \alpha \ (\text{mod. } B_m)\}.$$

Note that both G_α and G_α^* are subgroups of G since both D_m and B_m are G-modules. Moreover, since D_m is a submodule of B_m, G_α is a subgroup of G_α^*. Letting $v_p = (1, p, \cdots, p^{f-1})$ be as in Section 3, we define

$$G_\alpha(p)=G_{v_p\alpha}\,,\qquad G^*_\alpha(p)=G^*_{v_p\alpha}\,.$$

It is not hard to see that

$$G_\alpha(p)=\begin{cases} G\,, & \text{if } v_p\alpha\in D_m\,,\\ \{t\in G\,|\,t\cdot v_p\alpha=v_p\alpha\}\,, & \text{otherwise}\,.\end{cases} \tag{5.1}$$

In particular, $G_\alpha(p)$ coincides with G whenever $G(p)$ contains -1. The following inclusions are clear from the definition:

$$G(p)\subseteq G_{v_p\alpha}\subseteq G_\alpha(p)\subseteq G^*_\alpha(p)\,. \tag{5.2}$$

We say that α is *weakly p-simple* (resp. *weakly simple*) if the equality $G_\alpha(p)=G^*_\alpha(p)$ (resp. $G_\alpha=G^*_\alpha$) holds.

Following [10], we define two subgroups $G(J_\alpha(\mathfrak{p}))$ and $G^*(J_\alpha(\mathfrak{p}))$ of G by

$$\begin{aligned} G(J_\alpha(\mathfrak{p})) &=\{t\in G\,|\,J_\alpha(\mathfrak{p})^{\sigma_t}=J_\alpha(\mathfrak{p})\}\,,\\ G^*(J_\alpha(\mathfrak{p}))&=\{t\in G\,|\,(J_\alpha(\mathfrak{p}))^{\sigma_t}=(J_\alpha(\mathfrak{p}))\}\,.\end{aligned}$$

Then we can state one of our main results as follows.

THEOREM 5.1. *Let the notation be as above. Then*

$$G_\alpha(p)\subseteq G(J_\alpha(\mathfrak{p}))\subseteq G^*_\alpha(p)\,.$$

In particular, if α is weakly p-simple, then $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=K^{G_\alpha(p)}$.

The following theorem provides a sufficient condition for every element of A^n_m to be weakly p-simple.

THEOREM 5.2. *Suppose that one of the following two conditions holds:*

(i) *m is either 4 or a prime number; or*

(ii) *every prime factor of m is greater than $2(n+2)f$.*

Then every element A^n_m is weakly p-simple, hence $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=K^{G_\alpha(p)}$ for any $\alpha\in A^n_m$.

Proof. Let $\alpha\in A^n_m$. Then, by definition, $G_\alpha(p)$ (resp. $G^*_\alpha(p)$) consists of elements $t\in G$ such that $(t,-1)v_p\alpha\in D_m^{2(n+2)f-2}$ (resp. $(t,-1)v_p\alpha\in B_m^{2(n+2)f-2}$). Now we have the following result.

LEMMA 5.3 ([1], Theorem A). *In order that $B^n_m=D^n_m$, it is necessary and sufficient that one of the following conditions holds:*

(i) *m is either 4 or a prime number; or*

(ii) *every prime factor of m is greater than $n+2$.*

If one of the condition (i) or (ii) of Theorem 5.2 holds, then this lemma implies that $B_m^{2(n+2)f-2}=D_m^{2(n+2)f-2}$. Therefore $G_\alpha(p)=G^*_\alpha(p)$ as required. □

To prove Theorem 5.1 we need two lemmas.

LEMMA 5.4. *If $\alpha\in A^n_m$, then*

(5.3) $$G(J_\alpha(\mathfrak{p}))=\{t\in G_\alpha^*(p)\mid \varepsilon_{(t,-1)\alpha}(\mathfrak{p})=1\}\,.$$

Proof. The proof proceeds as follows: Let $t\in G$. Then

$t\in G(J_\alpha(\mathfrak{p}))$

$\Leftrightarrow \varepsilon_{t\cdot\alpha}(\mathfrak{p})=\varepsilon_\alpha(\mathfrak{p})$ (by (2.4) and (2.5))

$\Leftrightarrow \varepsilon_{(t,-1)\alpha}(\mathfrak{p})=1$ (by (2.6))

$\Leftrightarrow (t,-1)\alpha\in B_m^{2n+2}(p)$ and $\varepsilon_{(t,-1)\alpha}(\mathfrak{p})=1$ (by Proposition 3.2)

$\Leftrightarrow t\in G_\alpha^*(p)$ and $\varepsilon_{(t,-1)\alpha}(\mathfrak{p})=1$ (by the definition of $G_\alpha^*(P)$).

Thus (5.3) holds. □

LEMMA 5.5. $H^1(G(p), R_m)=0$.

Proof. We first note that R_m is isomorphic to a direct sum of some $G(p)$-modules of the from $\boldsymbol{Z}[G(p)/H]$ with some subgroups H of $G(p)$. But, using the inflation-restriction exact sequence, we can easily see that $H^1(G(p), \boldsymbol{Z}[G(p)/H])=0$ for any subgroup H of $G(p)$. This shows that $H^1(G(p), R_m)=0$ as required. □

Proof of Theorem 5.1. If $v_p\alpha\in D_m$, then the assertion holds since $G_\alpha(p)=G_\alpha^*(p)=G$ by (5.1). So we may assume that $v_p\alpha\notin D_m$. By Lemma 5.4 it suffices to show that the inclusion $G_\alpha(p)\subseteq G(J_\alpha(\mathfrak{p}))$ holds. Let $t\in G_\alpha(p)$. Then $t\cdot v_p\alpha=v_p\alpha$ by (5.1) again, and so $t\cdot\alpha-\alpha$ belongs to ${}_{v_p}R_m$, the kernel of the multiplication by v_p in R_m. Since $G(p)$ is a cyclic group generated by p. Lemma 5.5 shows that ${}_{v_p}A_m=((p)-(1))A_m$. Therefore we can choose an element $\beta\in A_m$ such that

$$t\cdot\alpha=\alpha+((p)-(1))\beta\,,$$

or equivalently

$$(t,-1)\alpha=(1,-1)\alpha+((p)-(1))\beta\,.$$

Since $\varepsilon_\alpha(\mathfrak{p})^{\sigma_p}=\varepsilon_\alpha(\mathfrak{p})$ and $\varepsilon_{(1,-1)\alpha}(\mathfrak{p})=1$ by (4.1), this shows that

$$\varepsilon_{(t,-1)\alpha}(\mathfrak{p})=1\,.$$

Hence $G_\alpha(p)\subseteq G(J_\alpha(\mathfrak{p}))$. □

REMARK 5.6. As we have mentioned in the introduction, the new point of Theorem 5.1 is the first inclusion. Indeed, the second inclusion follows from (0.2) since the equality

(5.4) $$G^*(J_\alpha(\mathfrak{p}))=G_\alpha^*(p)$$

holds. This can be proved as follows. Let $t\in G$. It then follows from (3.3) that $t\in G^*(J_\alpha(\mathfrak{p}))$ if and only if the equality

$$\|tu\cdot v_p\alpha\|=\|u\cdot v_p\alpha\|$$

holds for all $u\in G$. But this is equivalent to the condition that $\|u\cdot(t,-1)v_p\alpha\|$ should

be independent of $u \in G$. Therefore, $t \in G^*(J_\alpha(\mathfrak{p}))$ if and only if $(t, -1)\alpha \in B_m^{2(n+1)}(p)$, which proves (5.4).

6. p-simple elements and non-degenerate elements

For any $\alpha \in A_m$ we say that α is *p-simple* if $G_\alpha^*(p) = G_{v_p}$. By definition, we have $G_{v_p} = G_{(1)}(p)$, or more precisely

$$G_{v_p} = \begin{cases} G, & \text{if } -1 \in G(p), \\ G(p), & \text{otherwise}. \end{cases} \tag{6.1}$$

It is clear from (5.2) that a p-simple element is always weakly p-simple.

Let θ be the homomorphism defined in (3.4). An element $\alpha \in A_m$ is said to be *non-degenerate if* $\chi(\theta(\alpha)) \neq 0$ for any odd character χ of G, and *degenerate* otherwise (see [8], [16]). Here χ is called odd if $\chi(\sigma_{-1}) = -1$.

THEOREM 6.1. *If $-1 \notin G(p)$ and α is non-degenerate, then $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))$ coincides with the decomposition field of* $\mathfrak{p}$.

Note that the condition of $G(p)$ is necessary. Indeed, as we have seen in Proposition 3.3, we have $\boldsymbol{Q}(J_\alpha(\mathfrak{p})) = \boldsymbol{Q}$ if $-1 \in G(p)$.

LEMMA 6.2. *Every non-degenerate element is p-simple.*

Proof. It follows from the definition that the necessary and sufficient condition for $t \in G$ to belong to $G_\alpha^*(p)$ is $\theta((t, -1)v_p\alpha) = 0$. It is easy to see that this is equivalent to $(\sigma_t - 1)v_p\theta(\alpha) = 0$, where v_p is identified with the element $\sum_{t \in G(p)} \sigma_t \in \boldsymbol{Z}[Gal(K/\boldsymbol{Q})]$. If α is non-degenerate, then $\chi((\sigma_t - 1)v_p) = 0$ for all odd character χ of G. It then follows that

$$(\sigma_t - 1)v_p \in \boldsymbol{Z}[Gal(K/\boldsymbol{Q})]^+ := (\sigma_{-1} + 1)\boldsymbol{Z}[Gal(K/\boldsymbol{Q})] .$$

But it is not hard to see that this occurs only when $t \in G_{v_p}$. Therefore $t \in G_\alpha^*(p)$ if and only if $t \in G_{v_p}$. Thus $G_\alpha^*(p) = G_{v_p}$ as required. □

Proof of Theorem 6.1. Theorem 6.1 is immediately follows from (6.1) and Lemma 6.2. □

In what follows we discuss the interrelations of non-degenerate elements, p-simple elements and weakly p-simple elements. Note that we have proved the following implications:

$$\text{non-degenerate} \Rightarrow p\text{-simple} \Rightarrow \text{weakly } p\text{-simple} . \tag{6.2}$$

But the converse implications do not always hold. First we give an example of a weakly p-simple element which is not p-simple. Suppose $m(>3)$ is a prime and f is odd (hence $-1 \notin G(p)$). Then every element of A_m^+ is weakly p-simple by Theorem 5.2, and α is p-simple if and only if $G_\alpha(p) = G(p)$. Take an element $a \in (\boldsymbol{Z}/m\boldsymbol{Z})^*$ whose

order s is greater than 2. Then $1+a+a^2+\cdots+a^{s-1}=0$, so we can define an element $\alpha\in A_m^{s-2}$ by

$$\alpha=(1, a, a^2, \cdots, a^{s-1}) . \tag{6.3}$$

In this case G_α is the cyclic group generated by a and $G_\alpha(p)=G(p)G_\alpha$. Thus α is not p-simple if s does not divide f.

Next we give an example of degenerate, p-simple elements. We continue to assume that $m>3$ is a prime. Consider the following congruence relation:

$$p^i+p^j+p^k\equiv 3 \pmod{m} , \tag{6.4}$$

with $(i, j, k)\in\mathfrak{A}_f^1$. (For the definition of $\mathfrak{A}_f^1$, see the introduction.)

PROPOSITION 6.3. *Suppose m (>3) is a prime. Let $(i, j, k)\in\mathfrak{A}_f^1$ be a solution of* (6.4) *and put*

$$\alpha=(p^i-1, p^{i+j}-p^i, 1-p^{i+j})\in A_m^1 .$$

Then $G_\alpha=\{1\}$. Moreover the element $u\in G$ such that $(p^i-1)u\equiv p^j-1 \pmod{m}$ belongs to $G_\alpha(p)$. Therefore, if $u\notin G(p)$, then α is not p-simple (hence degenerate).

Proof. First we note that $\alpha=(p^i-1)(1, up^i, -1-up^i)$. A simple calculation shows that

$$(up^i)^2\equiv -(1+up^i)p^i , \qquad u^3\equiv p^j \pmod{m} . \tag{6.5}$$

If $G_\alpha\neq\{1\}$, then $(up^i)^2\equiv -(1+up^i) \pmod{m}$. It follows from the first formula of (6.5) that $p^i\equiv 1 \pmod{m}$. But this contradicts the assumption that $i\not\equiv 0 \pmod{f}$. Thus $G_\alpha=\{1\}$, which proves the first statement. Note that the second formula of (6.5) shows that $u\in G_\alpha(p)$, hence α is not a p-simple if $u\notin G(p)$. This proves the second statement. □

EXAMPLE 6.4. Let us consider the case where $m=67$ and $p\equiv 9 \pmod{67}$ (see [3]). In this case we have $f=11$ and the equation (6.3) has essentially the unique solution

$$9^2+9^3+9^6\equiv 3 \pmod{67} .$$

If we take $(i, j, k)=(2, 6, 3)\in\mathfrak{A}_{11}^1$ in Proposition 6.3, then $\alpha=(13)(1, 6, 60)$. In this case we have $|G_\alpha(p)|=33$ and $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=K^{G_\alpha(p)}=\boldsymbol{Q}(\sqrt{-67})$.

Recall that $\alpha\in A_m$ is called weakly simple if $G_\alpha^*=G_\alpha$. We say that $\alpha\in A_m$ is *simple* if $G_\alpha^*=\{1\}$. Note that the following implications hold:

$$\text{non-degenerate} \Rightarrow \text{simple} \Rightarrow \text{weakly simple} \tag{6.6}$$

The proof of the first implication is essentially the same as that of Lemma 6.2, and the second one is clear from the definition. If m is a prime, then α is simple if and only if $G_\alpha=\{1\}$ by Theorem 5.2. If $p\equiv 1 \pmod{m}$, then there is no difference between two notions, p-simple elements and simple elements. However, if $p\not\equiv 1 \pmod{m}$, then this is not the case in general. For example the element (6.3) is p-simple but not

simple whenever $1<s|f$. Thus Proposition 6.3 provides an example of a simple element which is not p-simple.

REMARK 6.5. Let m be a prime number. For $\alpha=(a, b, c)\in A_m^1$, let

$$H_\alpha=\{t\in G \mid \|\alpha\|=0\}\,.$$

Then H_α is the CM type of the jacobian variety J_α of the curve $y^m=x^a(1-x)^b$ defined over the complex number field. It is known that J_α is simple if and only if α is simple in the above sense (for example see [12] or [2]). Moreover, one can easily see that α is non-degenerate if and only if the CM-type H_α is non-degenerate in the sense of [8], [5], [16].

REMARK 6.6. When m is a prime number, $\alpha=(a_0, \cdots, a_{n+1})\in A_m^n$ is non-degenerate if and only if

$$\chi(\alpha):=\sum_{i=0}^{n+1}\chi(a_i)\neq 0$$

for all odd Dirichlet character χ of $\boldsymbol{Z}/m\boldsymbol{Z}$. Indeed, we have

$$\begin{aligned}\chi(\theta(\alpha))&=-\sum_{i=0}^{n+1}\left(\sum_{t\in G}\left(\left\langle\frac{ta_i}{m}\right\rangle-\frac{1}{2}\right)\bar{\chi}(t)\right)\\&=-\chi(\alpha)B_{1,\bar{\chi}}\,,\end{aligned}$$

where $B_{1,\chi}$ denotes the generalized Bernoulli number. Since $B_{1,\chi}\neq 0$ for all odd character χ of $\boldsymbol{Z}/m\boldsymbol{Z}$, the above formula shows that $\chi(\theta(\alpha))\neq 0$ if and only if $\chi(\alpha)\neq 0$. Thus α is non-degenerate if and only if $\chi(\alpha)\neq 0$ for all odd character χ of $\boldsymbol{Z}/m\boldsymbol{Z}$. For example, if $n\geq 2$ is prime to m and $\alpha=(1, \cdots, 1, -n)\in A_m^{n-1}$, then $\chi(\alpha)=n-\chi(n)$ cannot be zero for any χ, hence α is non-degenerate. This example is intensively studied in [7], [4], [10]. We remark that, if m is not a prime and n is not prime to m, then α is not always non-degenerate. For example, if $\mathrm{ord}_2 m\geq 2$, then $(1, 1, -2)\in A_m^1$ is degenerate. Indded, we can shown that $\frac{m}{2}-1$ belongs to $G_\alpha^*(p)$ (see Lemma 8.2).

Therefore $G_\alpha^*(p)$ does not coincide with $G(p)$ whenever $\frac{m}{2}-1\notin G(p)$.

7. The case of prime powers

Throughout this section we assume that $m=l^e$ is a power of an odd prime l. Then every element $\alpha\in R_m$ has the following unique expansion:

$$\alpha=\sum_{i=0}^{e-1}(l^i)\alpha_i\,, \tag{7.1}$$

with $\alpha_i\in R_m\backslash(l)R_m$. Let $\varphi: R_m\to\boldsymbol{Z}/m\boldsymbol{Z}$ be the G-homomorphism defined by (1.1). If $\alpha\in R_m$ is expressed as (7.1), then

$$\varphi(\alpha)=\sum_{i=0}^{e-1} l^i\varphi(\alpha_i)\,.$$

We define another ring homomorphism $\psi: R_m\to \boldsymbol{Z}/m\boldsymbol{Z}$ by the formula

$$\psi(\alpha)=\sum_{i=1}^{e-1} il^i\varphi(\alpha_i)\,,$$

which is also a G-homomorphism. By definition ψ takes values in $l\boldsymbol{Z}/m\boldsymbol{Z}$, and $\psi(\delta)=0$ for any $\delta\in D_m$. Then the precise statement of Theorem 0.4 is given as follows.

THEOREM 7.1. *Let $m=l^e$ be a power of an odd prime l. For $\alpha\in A_m^+$, let $L=K^{G_\alpha^*(p)}$ and $\zeta=\chi_{\mathfrak{p}}(l)^{\psi(\alpha)}\in\mu_{m/l}$. Then $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=L(\zeta)$.*

LEMMA 7.2. *If $\alpha\in B_m$, then $\varepsilon_\alpha(\mathfrak{p})=\chi_{\mathfrak{p}}(l)^{\psi(\alpha)}$.*

Proof. As a G-module, B_m is generated by standard elements by Theorem 4.3, so we can choose $\beta,\gamma\in R_m$ such that

$$\alpha=\beta\sigma_{l,1}+\gamma(1,-1)\,.$$

It then follows from (4.1) that

$$\begin{aligned}\varepsilon_\alpha(\mathfrak{p})&=\chi_{\mathfrak{p}}(-l)^{-l\varphi(\beta)}\chi_{\mathfrak{p}}(-1)^{-\varphi(\gamma)}\\&=\chi_{\mathfrak{p}}(l)^{-l\varphi(\beta)}\,.\end{aligned}$$

The second equality holds since we are assuming that m is odd. Therefore in order to prove the lemma it suffices to show the formula

$$\psi(\alpha)=-l\varphi(\beta)\,. \tag{7.2}$$

Note that $\psi(\alpha)=\psi(\beta\sigma_{l,1})$ since $\psi(\gamma(1,-1))=0$, hence (7.2) is equivalent to

$$\psi(\beta\sigma_{l,1})=-l\varphi(\beta)\,. \tag{7.3}$$

Since both φ and ψ are G-homomorphisms, it suffices to show (7.3) for $\beta=(l^i)$ with $i=0,\cdots,e-1$. But, if $\beta=(l^i)$, then

$$\begin{aligned}\varphi(\beta\sigma_{l,1})&=\varphi\left((l^i)\sum_{k=0}^{l-1}(1+kl^{e-1})+(-l^{i+1})\right)\\&=\sum_{k=0}^{l-1} il^i(1+kl^{e-1})-(i+1)l^{i+1}\\&=-il^{i+1}\\&=-l\varphi(\beta)\,.\end{aligned}$$

Thus (7.3) holds. □

If H is a subgroup of G, we let

$$v_H=\sum_{t\in H}(t)\in R_m^+ .$$

In this notation $v_{G(p)}$ is nothing but v_p.

LEMMA 7.3. *If H is contained in the l-Sylow subgroup of G, then*

$$v_H\equiv(l^s) \quad (\mathrm{mod}.\ B_m)\ , \tag{7.4}$$

where $l^s=|H|$.

Proof. We prove this by induction on s. If $s=0$, then (7.4) is trivial. Let $s>0$ and suppose (7.4) holds for the subgroup H' of H with $|H'|=l^{s-1}$, that is,

$$v_{H'}\equiv(l^{s-1}) \quad (\mathrm{mod}.B_m)\ . \tag{7.5}$$

Since H (resp. H') is generated by $1+l^{e-s}$ (resp. $1+l^{e-s+1}$), we have

$$v_H=v_{H'}\sum_{k=0}^{l-1}(1+kl^{e-s})\ .$$

By the inductive hypothesis (7.5) this shows that

$$\begin{aligned} v_H &\equiv \sum_{k=0}^{e-1}(l^{s-1}+kl^{e-1}) \quad (\mathrm{mod}.\ B_m)\\ &=\sigma_{l,l^{s-1}}-(-l^s)\\ &\equiv(l^s) \qquad\qquad (\mathrm{mod}.\ B_m)\end{aligned}$$

Thus the lemma holds true for H. □

Proof of Theorem 7.1. Let Γ be the l-Sylow subgroup of $G(p)$ and let

$$\Delta=\{t\in G(p)\,|\,t^{l-1}=1\}\ .$$

Then the order d of Δ is not divisible by l, and $G(p)=\Gamma\times\Delta$, hence $v_p=v_\Gamma v_\Delta$. If d is even, then $-1\in G(p)$. In this case the assertion follows from Proposition 3.3. Indeed, we have $L=\boldsymbol{Q}$ since $G_\alpha^*(p)=G$, and $\zeta=1$ since $\chi_p(l)=1$.

In the following we assume that d is odd. Let $t\in G_\alpha^*(p)$. By definition this says that $(t,-1)v_p\alpha\in B_m$, which is equivalent to requiring that the class of $(t,-1)\alpha$ in A_m/B_m should be killed by the multiplication by v_p. But Lemma 7.3 shows that $v_\Gamma\equiv(l^s)$ (mod. B_m), where $l^s=|\Gamma|$. Therefore $(l^s)(t,-1)v_\Delta\alpha\in B_m$. Since $((l^s)A_m^+)\cap B_m=((l^s)B_m^+)\cap B_m$, we conclude that there exists an element $\beta\in(l^s)B_m^+$ such that

$$(l^s)(t,-1)v_\Delta\alpha=(l^s)\beta\ .$$

We claim that there exists an element $\gamma\in R_m$ such that

$$(t,-1)v_\Delta\alpha-\beta=\{(u)-(1)\}\gamma\ , \tag{7.6}$$

where u is a generator of Γ. To see this let $(t,-1)v_\Delta\alpha=(a_1,\cdots,a_r)$. Then β may be written as $(b_1,\cdots,b_r)$ with b_i's such that $l^sa_i=l^sb_i$ for all $i=1,\cdots,r$. Therefore $a_i\equiv b_i$

(mod. l^{e-s}). Consequently we have $a_i = u^{c_i} b_i$ with some integers c_i, and so

$$(t, -1)v_{\Delta}\alpha - \beta = \sum_{i=1}^{r} \{(u)^{c_i} - (1)\}(b_i)$$

$$= \{(u) - (1)\} \sum_{i=1}^{r} (u^{c_i - 1}, \cdots, u, 1)(b_i) .$$

This proves (7.6).

Now, since $G(p)$ acts trivially on $\varepsilon_{\alpha}(\mathfrak{p})$, we have $\varepsilon_{\alpha}(\mathfrak{p})^d = \varepsilon_{v_{\Delta}\alpha}(\mathfrak{p})$. Therefore

$$(\varepsilon_{\alpha}(\mathfrak{p})^{\sigma_t - 1})^d = \varepsilon_{(t, -1)v_{\Delta}\alpha}(\mathfrak{p}) .$$

The right hand side equals $\varepsilon_{\beta}(\mathfrak{p})$ by (7.6) since $\varepsilon_{\alpha}(\mathfrak{p})^{\sigma_u} = \varepsilon_{\alpha}(\mathfrak{p})$ (see Section 2). On the other hand, it follows from Lemma 7.2 and (7.6) that

$$\varepsilon_{\beta}(\mathfrak{p}) = \chi_{\mathfrak{p}}(l)^{\psi((t, -1)v_{\Delta}\alpha)}$$

$$= (\chi_{\mathfrak{p}}(l)^{\psi((t, -1)\alpha)})^d .$$

Consequently we find that

$$(\varepsilon_{\alpha}(\mathfrak{p})^{\sigma_t - 1})^d = (\zeta^{\sigma_t - 1})^d ,$$

where we have put $\zeta = \chi_{\mathfrak{p}}(l)^{\psi(\alpha)}$. Since $(d, 2m) = 1$, there is no d-th root of unity in K other than 1, hence

$$\varepsilon_{\alpha}(\mathfrak{p})^{\sigma_t - 1} = \zeta^{\sigma_t - 1} . \tag{7.7}$$

It then follows from Lemma 5.4 that

$$G(J_{\alpha}(\mathfrak{p})) = \{t \in G_{\alpha}^{*}(p) \mid \zeta^{\sigma_t} = \zeta\} ,$$

or equivalently

$$\boldsymbol{Q}(J_{\alpha}(\mathfrak{p})) = L(\zeta) .$$

This is what we wanted to prove. □

As a corollary to the proof of Theorem 7.1, we obtain the following result which is a generalization of Lemma 7.2.

PROPOSITION 7.4. *Suppose m is a power of an odd prime l and $\alpha \in B_m^n(p)$. Then*

$$J_{\alpha}(\mathfrak{p}) = \chi_{\mathfrak{p}}(l)^{\psi(\alpha)} q^{n/2} .$$

Proof. If $\alpha \in B_m^n(p)$, then $G_{\alpha}^{*}(p) = G$. Furthermore both $\varepsilon_{\alpha}(\mathfrak{p})$ and $\chi_{\mathfrak{p}}(-l)^{\psi(\alpha)}$ in the formula (7.7) are roots of unity in K. Therefore, putting $t = -1$ in the formula and taking the square root of the both sides, we find that

$$\varepsilon_{\alpha}(\mathfrak{p}) = \pm \chi_{\mathfrak{p}}(-l)^{\psi(\alpha)} . \tag{7.8}$$

Let λ be the prime ideal in K lying above l. Then the congruence relation

$$J_\alpha(\mathfrak{p}) \equiv 1 \pmod{\lambda}$$

shows that $\varepsilon_\alpha(\mathfrak{p}) \equiv 1 \pmod{\lambda}$, hence the sign of the right hand side of (7.8) is $+1$. Thus the proposition holds. □

8. The case of $n=1$ and $p \equiv 1 \pmod{m}$

In this section we prove Theorem 0.3 after giving the precise statement. To do this we classify primitive elements of A_m^1 into five types as follows. A primitives element $\alpha \in A_m^1$ is called

of type II-1 if $\alpha=(a, aw, -a(1+w))$ with $w^2=1$, $w \neq \pm 1$, and, in addition, $w \neq \frac{m}{2}+1$ if $\mathrm{ord}_2 m \geq 3$,

of type II-2 if $\alpha=(a, a, -2a)$ and $\mathrm{ord}_2 m \geq 2$,

of type II-3 if $a=\left(a, \frac{m}{2}+a, \frac{m}{2}-2a\right)$ and $\mathrm{ord}_2 m \geq 3$,

of type III if $\alpha=(a, aw, aw^2)$ with $1+w+w^2=0$

and *of type I* otherwise.

Let $\mathscr{E}$ be the finite set of natural numbers defined by (0.6). Then the precise statement of Theorem 0.3 is as follows.

THEOREM 8.1. *Suppose $m \notin \mathscr{E}$ and $p \equiv 1 \pmod{m}$. Let α be a primitive element of A_m^1.*

(i) *If α is of type I, then $\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=K$.*

(ii) *If $\alpha=(a, aw, -a(1+w))$ is of type II-1, then*

$$\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=\begin{cases} K_{m/4} & \text{if } \mathrm{ord}_2 m=2 \text{ and } w=\frac{m}{2}+1, \\ \boldsymbol{Q}(\zeta+\zeta^w) & \text{otherwise}. \end{cases}$$

(iii) *If $\alpha=(a, a, -2a)$ is of type II-2, then*

$$\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=\begin{cases} K_{m/2} & \text{if } \chi_{\mathfrak{p}}(2)^2=1, \\ K_m & \text{otherwise}. \end{cases}$$

(iv) *If $\alpha=\left(a, \frac{m}{2}+a, \frac{m}{2}-2a\right)$ is of type II-3, then*

$$\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=\begin{cases} K_{m/4} & \text{if } \chi_{\mathfrak{p}}(2)^4=1, \\ K_{m/2} & \text{otherwise}. \end{cases}$$

(v) *If $\alpha=(a, aw, aw^2)$ is of type III, then*

$$\boldsymbol{Q}(J_\alpha(\mathfrak{p}))=\begin{cases} K_{m/3} & \text{if } \mathrm{ord}_3 m>1, \text{ and } w \equiv 1 \left(\mathrm{mod.}\ \frac{m}{3}\right), \\ \boldsymbol{Q}(\zeta+\zeta^w+\zeta^{w^2}) & \text{otherwise}. \end{cases}$$

In order to prove this theorem we need the following result which is proved in [2], Theorem 0.2, where the group G_α is written as W_α. (The corresponding result for the group G_α^* is not stated explicitly there, but easy to prove.)

LEMMA 8.2. *Suppose $m \notin \mathscr{E}$. Let α be a primitive element of A_m^1.*

(i) *If α is of type I, then $G_\alpha^* = G_\alpha = \{1\}$.*

(ii) *If $\alpha = (a, aw, -a(1+w))$ is of type II-1, then $G_\alpha^* = G_\alpha = \{1, w\}$.*

(iii) *If $\alpha = (a, a, -2a)$ is of type II-2, then $G_\alpha^* = \left\{1, \frac{m}{2}-1\right\}$ and $G_\alpha = \{1\}$.*

(iv) *If $\alpha = \left(a, \frac{m}{2}+a, \frac{m}{2}-2a\right)$ is of type II-3, then $G_\alpha^* = \left\{1, \frac{m}{4}-1, \frac{m}{2}+1, \frac{3m}{4}-1\right\}$ and $G_\alpha = \left\{1, \frac{m}{2}+1\right\}$.*

(v) *If $\alpha = (a, aw, aw^2)$ is of type III, then $G_\alpha^* = G_\alpha = \{1, w, w^2\}$.*

In particular, α is weakly simple except for the case where α is of type II-2 or II-3.

REMARK 8.3. The finite set $\mathscr{E}$ of the excluded integers is smaller than that of [2]. As for the missing integers one can directly check the above lemma.

Proof of Theorem 8.1. Since we are assuming that $p \equiv 1 \pmod{m}$, we have $G_\alpha(p) = G_\alpha$ and $G_\alpha^*(p) = G_\alpha^*$. If α is of type I, II-1 or III, then α is weakly p-simple by Lemma 8.2. Therefore it follows from Theorem 5.1 that $\boldsymbol{Q}(J_\alpha(\mathfrak{p})) = K^{G_\alpha}$. To deduce the statements (i), (ii) and (v) from (i), (ii) and (v) of Lemma 8.2 respectively is an easy exercise of Galois theory.

If $\alpha = (a, a, -2a)$ is of type II-2, then $G^*(J_\alpha(\mathfrak{p})) = \left\{1, \frac{m}{2}-1\right\}$ by Lemma 8.2. Since

$$\left(1, \frac{m}{2}+1\right)\alpha + \left(\frac{m}{2}, \frac{m}{2}\right) = \left(a, a, \frac{m}{2}+a, \frac{m}{2}+a, -2a, -2a, \frac{m}{2}, \frac{m}{2}\right)$$
$$= 2\sigma_{2,a},$$

we have

$$\varepsilon_{(1,(m/2)+1)\alpha}(\mathfrak{p}) = \chi_{\mathfrak{p}}(2^{-2a})^2 = \chi_{\mathfrak{p}}(2)^{-2a}.$$

Therefore, by (5.3), $\frac{m}{2}-1 \in G(J_\alpha(\mathfrak{p}))$ if and only if $\chi_{\mathfrak{p}}(2)^2 = 1$. This proves (iii). The proof of (iv) is quite similar and we omit it. □

EXAMPLE 8.4. For $m \in \mathscr{E}$, the assertion of the theorem does not always hold. For example, let us consider the case where $m = 21$ and $p \equiv 1 \pmod{21}$. Let $\alpha = (1, 8, 12) \in A_m^1$. Then α is of type II-1. Direct calculations show that $G_\alpha = \{1\}$ and $G_\alpha^* = \{1, 2, 4, 8, 11, 16\}$. Note that

$$(1, -2)\alpha + (6, -6) = (1, 5, 6, 8, 12, 15, 18, 19) = \sigma_{3,1} + \sigma_{3,5},$$

and

$$(1, -2^i) \equiv (1, -2)(1, 2, \cdots, 2^{i-1}) \pmod{D_{21}}.$$

Therefore, by Proposition 4.2, we can easily see that

$$\varepsilon_{(1, -2^i)\alpha}(\mathfrak{p}) = \chi_{\mathfrak{p}}(3)^{3\cdot(2i-1)} \qquad (i=0, 1, \cdots, 5).$$

This shows that $G(J_\alpha(\mathfrak{p}))$ contains 2^i if and only if $3^{((p-1)/7)(2^i-1)} \equiv 1 \pmod{p}$, and so

$$G(J_\alpha(\mathfrak{p})) = \begin{cases} \{1, 2, 4, ,8, 11, 16\} & \text{if } 3^{(p-1)/7} \equiv 1 \pmod{p}, \\ \{1, 8\} & \text{otherwise}. \end{cases}$$

Thus we have

$$\boldsymbol{Q}(J_\alpha(\mathfrak{p})) = \begin{cases} \boldsymbol{Q}(\sqrt{-7}) & \text{if } 3^{(p-1)/7} \equiv 1 \pmod{p}, \\ K_7 & \text{otherwise}. \end{cases}$$

References

[1] Aoki, N.; On some arithmetic problems related to the Hodge cycles on the Fermat varieties, *Math. Ann.*, **266** (1983), 23–54. (Erratum: *Math. Ann.*, **267** (1984), p. 572.)

[2] Aoki, N.; Simple factors of the jacobian of a Fermat curve and the Picard number of a product of Fermat curves, *Amer. J. Math.*, **113** (1991), 779–833.

[3] Greenberg, R.; On the jacobian variety of some algebraic curves, *Comp. Math.*, **42** (1981), 345–359.

[4] Gyoja, A. and Ono, T.; A note on Jacobi sums II, *Proc. Japan Acad.*, **69** (1993), 91–93.

[5] Hazama, F.; Holdge cycles on abelian varieties of CM-type, *Res. Act. Fac. Sci. Engrg. Tokyo Denki Univ.*, **5** (1983), 31–33.

[6] Ireland, K. and Rosen, M.; A Classical Introduction to Modern Number Theory, Springer-Verlag 1993.

[7] Kida, M. and Ono, T.; A note on Jacobi sums, *Proc. Japan Acad.*, **69** (1993), 32–34.

[8] Kubota, T.; On the field extension by complex multiplication type, *Trans. AMS*, **118** (1965), 113–122.

[9] Lang, S.; Cyclotomic fields, Springer-Verlag 1978.

[10] Ono, T.; A note on Jacobi sums III, *Proc. Japan Acad.*, **69** (1993), 272–274.

[11] Schmidt, C.-G.; Die Relationenfaktorgruppen von Stickelberger-Elementen und Kreiszahlen, *J. reine angew. Math.*, **292** (1980), 60–72.

[12] Shimura, G. and Taniyama, Y., Complex multiplication of abelian varieties and its applications to number theory, Math. Soc. Japan, 1961.

[13] Shioda, T. and Katsura, T.; On Fermat varieties, *Tôhoku Math. J.*, **31** (1979), 97–115.

[14] Weil, A.; Number of solutions of equations in finite fields, *Bull. Amer. Math. Soc.*, **55** (1949), 497–508.

[15] Yamamoto, K.; The gap group of multiplicative relationship of Gauss sums, *Symp. Math.*, **XV** (1975), 427–440.

[16] Yanai, H.; On degenerate CM-types, *J. of Number Theory*, **49** (1994), 295–303.

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Toshima-ku
Tokyo 117, Japan