TOKYO J. MATH.
VOL. 31, NO. 1, 2008

A Remark on the Breuer's Conjecture Related to the Maillet's Matrix

Izumi KURIBAYASHI

Hamamatsu University

(Communicated by F. Momose)

Introduction

We are concerned with a question asked by F. Momose whether the $\phi(n)/2$ real numbers $\cot(u\pi/n)$ $(0 < u < n/2, (u, n) = 1)$ are independent over $\mathbf{Q}$ or not. Here $\phi(n)$ denotes Euler's phi function. In his book [1], T. Breuer settled the equivalent problem (cf. Proposition 1.3 and Proposition 3.2 below) in the case where n is a prime power with $n > 2$, and conjectured the $\mathbf{Q}$-independence for any n with $n > 2$ (cf. Conjecture C.12 in [1]). In this note, reducing to the nonvanishing of $L(1, \chi)$, we prove the following, which implies the $\mathbf{Q}$-independence of $\cot(u\pi/n)$'s (cf. §2).

PROPOSITION. *Let n be an integer with $n > 2$. Then the rank of the matrix $\left(\frac{1}{2} - \left\langle \frac{au_b^*}{n} \right\rangle\right)$ is equal to $\phi(n)/2$, where a, b range over the set $\{1, \ldots, n-1\}$ and $\{1, \ldots, \phi(n)/2\}$ respectively.*

As for notations such as $\langle\ \rangle$, u_b, u_b^*, see Notation below.

The Maillet's determinant, that is the determinant of the matrix in Proposition above in the case where a ranges over the set $\{u_1, \ldots, u_{\phi(n)/2}\}$, has been studied in various way (e.g., [2], [7], [6]). It is equal to the first factor of the class number, up to non-zero factor in the case where n is a prime power (cf. §3).

In this note, we deduce this Proposition by proving the following

THEOREM. *Let n be an integer with $n > 2$. Then the following holds*:

$$\begin{aligned}&\Delta(\zeta_n^{u_1}/(1-\zeta_n^{u_1}), \ldots, \zeta_n^{u_{\phi(n)/2}}/(1-\zeta_n^{u_{\phi(n)/2}}), 1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)/2-1})\\ &\quad = \pm\frac{2}{Qw}(n\sqrt{-1})^{\phi(n)/2} \cdot h_n^- \cdot d \cdot \prod_{\chi:odd} L_\chi\,,\end{aligned}$$

where as for the notation $\Delta(t_1, \ldots, t_{\phi(n)})$ see Notation below and the other symbols denote

Received June 6, 2005; revised September 14, 2007

as follows:

h_n^- *denotes the first factor of the class number of the n-th cyclotomic field* $\mathbf{Q}(\zeta_n)$ *where* $\zeta_n = \exp(2\pi\sqrt{-1}/n)$,
Q *is equal to* 1 (*resp.* 2) *if n is a prime power* (*resp. otherwise*),
w *denotes the number of roots of unity in* $\mathbf{Q}(\zeta_n)$,
d *is equal to 1/2* (*resp.* $1/\sqrt{p}$, 1) *if n is a* 2*-power* (*resp. a p-power with p prime* ($\neq 2$) , *otherwise*), *and*
$L_\chi = \prod_{p|n, p\not| f_\chi}(1 - \chi_*(p)/p)$ *where* f_χ *denotes the conductor of* χ *and* χ_* *denotes the primitive character belonging to* χ.

Here we note that our Theorem implies that the elements

$$\zeta_n^{u_a}/(1-\zeta_n^{u_a})(a = 1, \ldots, \phi(n)/2), 1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)/2-1}$$

form a $\mathbf{Q}$-basis of the field $\mathbf{Q}(\zeta_n)$ (cf. Corollary 2.2 below).

In §1, we consider the equivalent conditions related to the $\mathbf{Q}$-independence. In the proof we use a certain type of virtual characters of the additive group $\mathbf{Z}/n\mathbf{Z}$ as a basic tool. In §2, we give a proof of Theorem. Then, roughly speaking, our determinant equals, up to a nonzero factor, to the product of Det $(\cot(u_a u_b \pi/n))$ and Det $(\cos(2\, u_a(b-1)\pi/n))$, where a, b range over the set $\{1, \ldots, \phi(n)/2\}$ (cf. Lemma 2.3). In §3, we give some remarks in the case where n is a prime power. In fact, we give an another proof of Theorem C.2 in [1] using the method in the proof of Proposition 1.3.

NOTATION

$\mathbf{Q}$	the field of rational numbers.
$\mathbf{Z}$	the ring of rational integers.
n	an integer.
ζ_n	$\exp(2\pi\sqrt{-1}/n)$.
$\mathbf{Z}/n\mathbf{Z}$	the additive group of integers mod n.
$u_1, \ldots, u_{\phi(n)}$	the integers u with $0 < u \leq n$ such that $(u, n) = 1$ in the increasing order. Moreover put $I(n) = \{u_1, \ldots, u_{\phi(n)}\}$.
u^*	the integer such that $0 < u^* \leq n$ with $u^* u \equiv 1 \bmod n$, if exists.
(w_{ab})	the matrix of which (a, b)-component is w_{ab}.
$\langle r \rangle$	$r - [r]$, the fractional part of the real number r.
$\Delta(t_1, \ldots, t_{\phi(n)})$	=Det $(t_b^{\sigma_{u_a}})$ for $t_1, \ldots, t_{\phi(n)} \in \mathbf{Q}(\zeta_n)$, where a, b range over the set $\{1, \ldots, \phi(n)\}$ and σ_u denotes the $\mathbf{Q}$-automorphism of $\mathbf{Q}(\zeta_n)$ defined by $\zeta_n \longmapsto \zeta_n^u$ for u with $(u, n) = 1$.

1. Equivalent conditions

1.1. Statement. First, to state our proposition on the equivalent conditions, we mention some notations and notion.

NOTATION 1.1. In this note, for $n > 2$ we denote by MA_n the matrix $\left(\frac{1}{2}-\left\langle\frac{u_a u_b^*}{n}\right\rangle\right)$ where a, b range over the set $\{1, \ldots, \phi(n)/2\}$, by $MA_n^{'}$ the matrix $\left(\frac{1}{2}-\left\langle\frac{au_b^*}{n}\right\rangle\right)$ where a, b range over the sets $\{1, \ldots, [(n-1)/2]\}$ and $\{1, \ldots, \phi(n)/2\}$ respectively, and by $MA_n^{''}$ the matrix $\left(\frac{1}{2}-\left\langle\frac{a\, u_b^*}{n}\right\rangle\right)$ where $a,\ b$ range over the sets $\{1, \ldots, n-1\}$ and $\{1, \ldots, \phi(n)/2\}$ respectively.

Here we note that $\phi(n)$ is even for our n.

DEFINITION 1.2 [1, Definition C.1]. A subset I of $I(n) = \{u_1, \ldots, u_{\phi(n)}\}$ is called complementary if for each $u \in I(n)$, exactly one of u and $n-u$ is contained in I. We say that n has property (LI) if there is a complementary subset I of $I(n)$ such that the set $\{1\} \cup \{\zeta_n^u/(1-\zeta_n^u) \mid u \in I\}$ is $\mathbf{Q}$-independent.

Here, by observing the following equality, we note that (LI) implies the $\mathbf{Q}$-independence for any complementary subset I:

$$\zeta_n^u/(1-\zeta_n^u) + \zeta_n^{-u}/(1-\zeta_n^{-u}) = -1\,. \tag{1}$$

We prove the following in the subsection 1.3.

PROPOSITION 1.3. *For $n > 2$, the following conditions are equivalent.*

(i) *The rank of $MA_n^{''}$ is $\phi(n)/2$.*

(i$'$) *The rank of $MA_n^{'}$ is $\phi(n)/2$.*

(ii) *The elements* $1\,,\ \zeta_n^{u_1}/(1-\zeta_n^{u_1})\,, \ldots,$ and $\zeta_n^{u_{\phi(n)/2}}/(1-\zeta_n^{u_{\phi(n)/2}})$ *are $\mathbf{Q}$-independent, i.e., n has property* (LI).

(iii) *The elements* $\cot(u_1\,\pi/n)\,, \ldots,$ and $\cot(u_{\phi(n)/2}\,\pi/n)$ *are $\mathbf{Q}$-independent.*

1.2. Preliminaries. Here, for later use in the proof we state the notions and lemmas on virtual characters and the field-theoretic trace maps.

NOTATION 1.4. $\theta_n : \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Q}(\zeta_n)$ the character defined by $(1 \bmod n\mathbf{Z}) \mapsto \zeta_n$.

$$\Delta_n^{(u)} = \sum_{k=1}^{n}\left(\frac{k}{n}-\frac{1}{2}\right)\theta_n^{ku} \quad \text{for } u \text{ with } (u,n)=1\,.$$

Denoting by $\mathbf{Q} \otimes \mathrm{R}(\mathbf{Z}/n\mathbf{Z})$ the $\mathbf{Q}$-extension of the group of virtual characters of $\mathbf{Z}/n\mathbf{Z}$, we note that

(2) the n characters $\theta_n^0, \ldots, \theta_n^{n-1}$ form an orthogonal basis of $\mathbf{Q} \otimes \mathrm{R}(\mathbf{Z}/n\mathbf{Z})$ with respect to the scalar product defined by

$$\langle \psi_1 , \psi_2 \rangle = \frac{1}{n} \sum_{j=1}^{n} \psi_1(j \mod n\mathbf{Z})\psi_2(-j \bmod n\mathbf{Z}) .$$

The virtual characters $\Delta_n^{(u)}$ become essential tools in our proof. The following two lemmas are especially basic.

LEMMA 1.5. *Assume* $(u, n) = 1$.
(i) *For* $f|n$, put $m = n/f$. *Then*
$\Delta_n^{(u)}(f \bmod n\mathbf{Z}) = -\zeta_m^u/(1 - \zeta_m^u)$ if $f \neq n$ $(i.e.\ m \neq 1)$,
$\Delta_n^{(u)}(0 \bmod n\mathbf{Z}) = 1/2$.
(ii) $\langle \Delta_n^{(u)}, \theta_n^{-a} \rangle = \dfrac{1}{2} - \left\langle \dfrac{au^*}{n} \right\rangle$.

PROOF. (i) The situation is trivial when $n = 1$ or $f = n$. So, we assume that $n > 1$ and $f \neq n$.

In the case where $n > 1$, we see that

$$\frac{\zeta_n^\alpha}{1 - \zeta_n^\alpha} = \frac{1}{n} \sum_{k=1}^{n-1} k \zeta_n^{-k\alpha} = -\frac{1}{n} \sum_{k'=1}^{n} k' \zeta_n^{-k'\alpha} \tag{3}$$

for $\alpha \in \mathbf{Z}$ with $\alpha \not\equiv 0 \bmod n$.
From (3) it follows that

$$\begin{aligned} \Delta_n^{(u)}(f \bmod n\mathbf{Z}) &= \sum_{k=1}^{n} \left(\frac{k}{n} - \frac{1}{2} \right) \zeta_n^{kuf} \\ &= \frac{1}{n} \sum_{k=1}^{n} k \zeta_{n/f}^{ku} - \frac{1}{2} \sum_{k=1}^{n} \left(\zeta_{n/f}^{u} \right)^k \\ &= -\frac{\zeta_m^u}{1 - \zeta_m^u} , \end{aligned}$$

as asserted.
(ii) Using (3) we obtain (ii) by

$$\begin{aligned} \langle \Delta_n^{(u)}, \theta_n^{-a} \rangle &= \frac{1}{n} \sum_{j=1}^{n} \zeta_n^{aj} \sum_{k=1}^{n} \left(\frac{k}{n} - \frac{1}{2} \right) \zeta_n^{kuj} \\ &= \frac{1}{n} \sum_{k=1}^{n} \frac{k}{n} \sum_{j=1}^{n} \left(\zeta_n^{a+ku} \right)^j - \frac{1}{2n} \sum_{k=1}^{n} \sum_{j=1}^{n} \left(\zeta_n^{a+ku} \right)^j \\ &= \left(1 - \left\langle \frac{au^*}{n} \right\rangle \right) - \frac{1}{2} . \end{aligned}$$

□

LEMMA 1.6. *Assume $n = fm$ and $(u, n) = 1$. Embedding $\mathbf{Z}/f\mathbf{Z}$ into $\mathbf{Z}/n\mathbf{Z}$ by sending* $(1 \bmod m\mathbf{Z}) \mapsto (f \bmod n\mathbf{Z})$*, we have*

$$\Delta_n^{(u)}|_{\mathbf{Z}/f\mathbf{Z}} = \sum_{k'=1}^{m}\left(\frac{k'}{m} - \frac{1}{2}\right)\theta_m^{k'u}, \text{ i.e.}, = \Delta_m^{(u)},$$

where $\Delta_n^{(u)}|_{\mathbf{Z}/f\mathbf{Z}}$ denotes the restriction to $\mathbf{Z}/f\mathbf{Z}$ of $\Delta_n^{(u)}$.

PROOF. This is a consequence of Lemma 1.5 (i).

Here we show it directly. Since $\theta_n^u|_{\mathbf{Z}/f\mathbf{Z}} = \theta_m^u$, it suffices to show

$$\left\langle \sum_{k=1}^{n}\left(\frac{k}{n} - \frac{1}{2}\right)\theta_n^{ku}, \theta_n^{-a}\right\rangle = \left\langle \sum_{k'=1}^{m}\left(\frac{k'}{m} - \frac{1}{2}\right)\theta_m^{k'u}, \theta_m^{-a}\right\rangle. \tag{4}$$

In fact, we may obtain (4) using (2). □

For $m|n$, we denote by $\mathrm{Tr}_{n,m} : \mathbf{Q}(\zeta_n) \longrightarrow \mathbf{Q}(\zeta_m)$ the field-theoretic trace map. Here we prepare the following

LEMMA 1.7. *Assume $n = pm$ with p prime, and $(u, n) = 1$.*

(i) *The case $m \neq 1$. Taking α_p* with $0 < \alpha_p \leq m$ *such that $p\alpha_p \equiv 1 \bmod m$ in the case where $p \nmid m$, we have*

$$\mathrm{Tr}_{n,m}\,(\zeta_n^u/(1-\zeta_n^u)) = \begin{cases} p \cdot \zeta_m^u/(1-\zeta_m^u) & \text{if } p|m\,, \\ p \cdot \zeta_m^u/(1-\zeta_m^u) - \zeta_m^{\alpha_p u}/(1-\zeta_m^{\alpha_p u}) & \text{otherwise}\,. \end{cases}$$

(ii) $\mathrm{Tr}_{n,1}(\zeta_n^u/(1-\zeta_n^u)) = -\phi(n)/2$.

PROOF. (i) First, we note that such α_p exists uniquely up to modulo m and $(\alpha_p, m) \equiv 1 \bmod m$.

Next, we assert that

$$\sum_{i=0}^{p-1}\frac{\zeta_n^{1+im}}{1-\zeta_n^{1+im}} = p \cdot \frac{\zeta_m}{1-\zeta_m}.$$

In fact, using (3) we see that

$$\begin{aligned}\sum_{i=0}^{p-1}\frac{\zeta_n^{1+im}}{1-\zeta_n^{1+im}} &= \frac{1}{n}\sum_{k=1}^{n-1} k\,\zeta_n^{-k}\left(\sum_{i=0}^{p-1}\zeta_n^{-mki}\right) \\ &= p \cdot \frac{1}{n}\sum_{k'=1}^{m-1} k' p \zeta_n^{-k'p} \\ &= p \cdot \frac{1}{m}\sum_{k'=1}^{m-1} k' \zeta_m^{-k'},\end{aligned}$$

which is by (3) equal to $p \cdot \zeta_m/(1-\zeta_m)$ as asserted.

The case $p|m$. Since $(1+i\,m, n) = 1$ for $i = 0, \dots, p-1$, we have that

$$\mathrm{Aut}(\mathbf{Q}(\zeta_n)/\mathbf{Q}(\zeta_m)) = \{\sigma_{1+im} \mid i = 0, \dots, p-1\}$$

and hence by the definition of $\mathrm{Tr}_{n,m}$ that

$$\mathrm{Tr}_{n,m}(\zeta_n/(1-\zeta_n)) = \sum_{i=0}^{p-1} \left(\frac{\zeta_n}{1-\zeta_n}\right)^{\sigma_{1+im}} = \sum_{i=0}^{p-1} \frac{\zeta_n^{1+im}}{1-\zeta_n^{1+im}}\,.$$

The case $p \nmid m$. Since $(1+i\,m, n) = 1$ for $i = 0, \dots, p-1$ with omitting i such that $1 + i\,m = p\,\alpha_p$, we have that

$$\mathrm{Tr}_{n,m}(\zeta_n/(1-\zeta_n)) = \sum_{i=0}^{p-1} \frac{\zeta_n^{1+im}}{1-\zeta_n^{1+im}} - \frac{\zeta_n^{p\alpha_p}}{1-\zeta_n^{p\alpha_p}}\,.$$

Together with these we obtain (i), considering the automorphism σ_u.

(ii) Assume temporarily that $n = p$. By the definition and (3), we have that

$$\begin{aligned}\mathrm{Tr}_{n,1}(\zeta_n/(1-\zeta_n)) &= \frac{1}{n}\sum_{k=1}^{n-1} k \sum_{j=1}^{n-1} \left(\zeta_n^{-k}\right)^j \\ &= \frac{1}{n}\{-1 - \cdots - (n-1)\} \\ &= -(n-1)/2\,,\end{aligned}$$

which implies (ii) in this case, because then $\phi(n) = n-1$.

To prove the general case, we use an induction on n. If n is a prime (i.e., $m = 1$) then (ii) holds by the above consideration. Assume now $m \neq 1$. Then

$$\begin{aligned}&\mathrm{Tr}_{n,1}(\zeta_n/(1-\zeta_n)) \\ &\quad = \mathrm{Tr}_{m,1}\left(\mathrm{Tr}_{n,m}(\zeta_n/(1-\zeta_n))\right) \\ &\quad = \begin{cases}\mathrm{Tr}_{m,1}(p \cdot \zeta_m/(1-\zeta_m)) & \text{if } p|m\,, \\ \mathrm{Tr}_{m,1}(p \cdot \zeta_m/(1-\zeta_m) - \zeta_m^{\alpha_p}/(1-\zeta_m^{\alpha_p})) & \text{if } p \nmid m\,.\end{cases}\end{aligned}$$

On the other hand, we have

$$\phi(n) = \begin{cases} p\,\phi(m) & \text{if } p|m\,, \\ (p-1)\,\phi(m) & \text{if } p\nmid m\,.\end{cases}$$

By our induction hypothesis, these yield (ii). □

1.3. Proof of Proposition 1.3. The equivalence between (i) and (i') is deduced from the relation

(5) $$\left\langle \frac{au_b^*}{n} \right\rangle + \left\langle \frac{-au_b^*}{n} \right\rangle = 1\,,$$

for $a = 1, \dots, n-1$ and $b = 1, \dots, \phi(n)$.
To prove the equivalence between (ii) and (iii), we note that

$$\mathrm{Re}(\zeta_n^u/(1-\zeta_n^u)) = -\frac{1}{2}, \quad \mathrm{Im}\,(\zeta_n^u/(1-\zeta_n^u)) = \frac{1}{2}\cot(u\pi/n)\,, \tag{6}$$

for $u \in \mathbf{Z}$ with $u \not\equiv 0 \bmod n$.
Using (6), we see the equivalence by taking the real- and imaginary- parts of $\mathbf{Q}$-linear relations between the numbers in (ii) resp. (iii).

Now we show the implication (ii) $\Rightarrow$ (i). Assume (ii). To see (i), let $l_{u_1^*}, \dots, l_{u^*_{\phi(n)/2}}$ be elements of $\mathbf{Q}$ such that

$$MA_n^{''}\begin{pmatrix} l_{u_1^*} \\ \vdots \\ l_{u^*_{\phi(n)/2}} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \tag{7}$$

Put $\chi = \sum_{b=1}^{\phi(n)/2} l_{u_b^*}\,\Delta_n^{(u_b)}$. Then, from Lemma 1.5 (ii) it follows that

$$MA_n^{''}\begin{pmatrix} l_{u_1^*} \\ \vdots \\ l_{u^*_{\phi(n)/2}} \end{pmatrix} = \begin{pmatrix} \langle\chi, \theta^{-1}\rangle \\ \vdots \\ \langle\chi, \theta^{-(n-1)}\rangle \end{pmatrix}.$$

Hence we have by (7) that $\langle\chi, \theta^{-a}\rangle = 0$ for $a = 1, \dots, n-1$. From this, considering (2) we see that

$$\chi = \sum_{a=1}^{n-1}\langle\chi, \theta^{-a}\rangle\theta^{-a} + \langle\chi, \theta^0\rangle\theta^0 = \langle\chi, \theta^0\rangle\theta^0\,.$$

By Lemma 1.5 (i), this yields that

$$\chi(1 \bmod n\mathbf{Z}) = -\sum_{b=1}^{\phi(n)/2} l_{u_b^*}\zeta_n^{u_b}/(1-\zeta_n^{u_b}) = \langle\chi, \theta^0\rangle\,,$$

which is an element of $\mathbf{Q}$. Applying the assumption (ii), we have $l_{u_1*} = \cdots = l_{u^*_{\phi(n)/2}} = 0$, as desired.

Finally we show the implication (i) $\Rightarrow$ (ii). Here we prepare the following

LEMMA 1.8. *Assume $n > 1$ and $l_u \in \mathbf{Q}(u \in I(n))$. Put $\chi = \sum_{u\in I(n)} l_{u*}\,\Delta_n^{(u)}$. If $\chi(1 \bmod n\mathbf{Z}) \in \mathbf{Q}$ then χ is a constant map.*

PROOF. First, we note by Lemma 1.5 (i) and Lemma 1.7 that

$$\chi(\alpha \bmod n\mathbf{Z}) = -\sum l_{u*}\left(\zeta_n^u/(1-\zeta_n^u)\right)^{\sigma_\alpha} = \chi(1 \bmod n\mathbf{Z})^{\sigma_\alpha} \tag{8}$$

for $(\alpha, n) = 1$, and

$$\chi(0 \bmod n\mathbf{Z}) = \frac{1}{2}\sum l_{u*} = \frac{1}{\phi(n)}\mathrm{Tr}_{n,1}(\chi(1 \bmod n\mathbf{Z}))\,.$$

Next, assume $n = pm$ with p prime, and $m \neq 1$. Here we assert

$$\chi(p\alpha \bmod n\mathbf{Z}) = \chi(1 \bmod n\mathbf{Z})^{\sigma_\alpha} \quad \text{for } (\alpha, n) = 1\,. \tag{9}$$

To see (9), it suffices to show it in the case $\alpha = 1$, since we consider σ_α as above. In this case by Lemma 1.5 (i) we first note that

$$\begin{aligned}\chi(p \bmod n\mathbf{Z}) &= -\sum l_{u*}\,\zeta_m^u/(1-\zeta_m^u)\\ &= -\sum_{u'\in I(m)}\left(\sum_{u\in I(n),u\equiv u' \bmod m} l_{u*}\right)\zeta_m^{u'}/(1-\zeta_m^{u'})\,.\end{aligned} \tag{10}$$

In the case $p|m$, from (10) it follows that

$$\begin{aligned}\chi(p \bmod n\mathbf{Z}) &= -\frac{1}{p}\sum_{u'}\sum_{u} l_{u*}\mathrm{Tr}_{n,m}(\zeta_n^u/(1-\zeta_n^u))\\ &= -\frac{1}{p}\sum_{u} l_{u*}\mathrm{Tr}_{n,m}(\zeta_n^u/(1-\zeta_n^u))\\ &= -\frac{1}{p}\mathrm{Tr}_{n,m}\left(\sum_{u} l_{u*}\zeta_n^u/(1-\zeta_n^u)\right)\\ &= \frac{1}{p}\mathrm{Tr}_{n,m}(\chi(1 \bmod n\mathbf{Z}))\\ &= \chi(1 \bmod n\mathbf{Z})\,,\end{aligned}$$

as asserted.

In the case $p \nmid m$, assume $\tilde{\alpha}_p \in \mathbf{Z}$ be such that $(\tilde{\alpha}_p, n) = 1$ with $\tilde{\alpha}_p \equiv \alpha_p \bmod m$. From (10) it follows that

$$\begin{aligned}&\chi(p \bmod n\mathbf{Z})\\ &= -\frac{1}{p}\sum_{u'}\sum_{u} l_{u*}\{\mathrm{Tr}_{n,m}(\zeta_n^u/(1-\zeta_n^u)) + \zeta_m^{\alpha_p u}/(1-\zeta_m^{\alpha_p u})\}\\ &= \frac{1}{p}\left\{\mathrm{Tr}_{n,m}(\chi(1 \bmod n\mathbf{Z})) - \left(\sum_{u} l_{u*}\Delta^{(u)}(p \bmod n\mathbf{Z})\right)^{\sigma_{\tilde{\alpha}_p}}\right\}\\ &= \frac{1}{p}\left\{\mathrm{Tr}_{n,m}(\chi(1 \bmod n\mathbf{Z})) + \chi(p \bmod n\mathbf{Z})^{\sigma_{\tilde{\alpha}_p}}\right\}\,.\end{aligned}$$

Thus we have

$$\begin{aligned}\chi(p \bmod n\mathbf{Z})^{\sigma_{\tilde{\alpha}_p}} &- \frac{1}{p-1}\mathrm{Tr}_{n,m}(\chi(1 \bmod n\mathbf{Z})) \\ &= p\{\chi(p \bmod n\mathbf{Z}) - \frac{1}{p-1}\mathrm{Tr}_{n,m}(\chi(1 \bmod n\mathbf{Z}))\}\,.\end{aligned}$$

Since $\sigma_{\tilde{\alpha}_p}$ is of finite order and $\chi(1 \bmod n\mathbf{Z})$ is a rational number by our assumption, this means

$$\begin{aligned}\chi(p \bmod n\mathbf{Z}) &= \frac{1}{p-1}\mathrm{Tr}_{n,m}(\chi(1 \bmod n\mathbf{Z})) \\ &= \chi(1 \bmod n\mathbf{Z})\,,\end{aligned}$$

as asserted.
Finally, to prove Lemma 1.8 we apply an induction on n. In fact, putting

$$\chi_m = \sum_{u'\in I(m)}\left(\sum_{u\in I(m),u\equiv u' \bmod m} l_{u*}\right)\Delta_m^{(u')}\,,$$

where $\Delta_m^{(u')} = \sum_{k'=1}^{m}\left(\frac{k'}{m}-\frac{1}{2}\right)\theta_m^{k'u'}$ by the definition (cf. Lemma 1.6), we have by Lemma 1.6 and (9) that $\chi|_{\mathbf{Z}/f\mathbf{Z}} = \chi_m$, and hence $\chi_m(1 \bmod m\mathbf{Z}) = \chi(p \bmod n\mathbf{Z}) = \chi(1 \bmod n\mathbf{Z})$. Thus, applying an induction on n, we see that χ_m is a constant map, and hence by (9) that χ is a constant map. This completes the proof of Lemma 1.8. □

PROOF OF PROPOSITION 1.3 (continued). Assume (i). To see (ii), let $l_{u_1^*}, \dots, l_{u^*_{\phi(n)/2}}, c$ be elements of $\mathbf{Q}$ such that $\sum_{b=1}^{\phi(n)/2} l_{u_b*}\zeta_n^{u_b}/(1-\zeta_n^{u_b}) = c$. Put $\chi = \sum_{b=1}^{\phi(n)/2} l_{u_b^*}\Delta_n^{(u_b)}$. Then, by Lemma 1.5 (i) we see that $\chi(1 \bmod n\mathbf{Z}) = c$, which is a rational number. Hence by Lemma 1.8, χ is a constant map i.e., $\chi = \chi(0 \bmod n\mathbf{Z})\theta^0$. By (2) this means that $\langle\chi, \theta^{-a}\rangle = 0$ for $a = 1, \dots, n-1$. On the other hand, by Lemma 1.5 (ii) we have that

$$MA_n'' \begin{pmatrix} l_{u_1^*} \\ \vdots \\ l_{u^*_{\phi(n)/2}} \end{pmatrix} = \begin{pmatrix} \langle\chi, \theta^{-1}\rangle \\ \vdots \\ \langle\chi, \theta^{-(n-1)}\rangle \end{pmatrix}.$$

By our assumption on the rank of MA_n'', this means that $l_{u_1^*} = \cdots = l_{u^*_{\phi(n)/2}} = 0$ and hence $c = 0$, as desired. This completes the proof of Proposition 1.3. □

2. Q-basis

In this section, we give a proof of our Theorem.

2.1. Remarks. Before giving a proof we remark some consequences of our main theorem. First, noting (5) in §1 and Proposition 1.3, we see the following

COROLLARY 2.1 *Assume $n > 2$. Then, we have the following*:

(i) *The rank of MA_n' is $\phi(n)/2$.*

(ii) *n has property* (LI).

Next, applying σ_{-1} (i.e. the complex conjugation) and considering (1) in the subsection 1.1, we obtain other types of $\mathbf{Q}$-bases.

COROLLARY 2.2. *Assume $n > 2$. Then, we have the following*:

(i) *The elements $\zeta_n^{u_a}/(1-\zeta_n^{u_a})$ and $\zeta_n^{1-a}(a = 1, \dots, \phi(n)/2)$ form* a *$\mathbf{Q}$-basis of $\mathbf{Q}(\zeta_n)$.*

(ii) *The elements $\zeta_n^{u_a}/(1-\zeta_n^{u_a})$ and $\zeta_n^{1-a}/(1-\zeta_n)(a = 1, \dots, \phi(n)/2)$ form* a *$\mathbf{Q}$-basis of $\mathbf{Q}(\zeta_n)$.* □

2.2. Decomposition. To prove our Theorem, first we see the following

LEMMA 2.3. *Assume $n > 2$. Then we have*

$$\begin{aligned}&\Delta\,(\zeta_n^{u_1}/(1-\zeta_n^{u_1}), \dots, \zeta_n^{u_{\phi(n)/2}}/(1-\zeta_n^{u_{\phi(n)/2}}), 1,\ \zeta_n,\ \zeta_n^2, \dots, \zeta_n^{\phi(n)/2-1})\\ &\quad = \pm\left(\frac{\sqrt{-1}}{2}\right)^{\phi(n)/2} \operatorname{Det}\,(\cot(u_a u_b\,\pi/n))\operatorname{Det}\,(2\ \cos(2\,u_a(b-1)\,\pi/n))\ ,\end{aligned}$$

where a, b range over the set $\{1, \dots, \phi(n)/2\}$.

PROOF. First we put

$$\begin{aligned}\Delta &= \Delta(\zeta_n^{u_1}/(1-\zeta_n^{u_1}), \dots,\ 1,\ \zeta_n, \dots, \zeta_n^{\phi(n)/2-1})\\ &= \operatorname{Det}\begin{pmatrix} & 1 & \\ \frac{\zeta_n^{u_a u_b}}{1-\zeta_n^{u_a u_b}} & \vdots & \zeta_n^{u_a(b-1-\phi(n)/2)} \\ & 1 & \\ & 1 & \\ \frac{\zeta_n^{u_a u_b}}{1-\zeta_n^{u_a u_b}} & \vdots & \zeta_n^{u_a(b-1-\phi(n)/2)} \\ & 1 & \end{pmatrix},\end{aligned}$$

where a, b range over the set $\{1, \dots, \phi(n)\}$.

Next, observing that $u_{\phi(n)+1-i} = n - u_i$, we have by (1) in the subsection 1.1 that

$$\Delta = \mathrm{Det}\begin{pmatrix} & & & 1 & \\ & \frac{\zeta_n^{u_a u_b}}{1-\zeta_n^{u_a u_b}} & & \vdots & \zeta_n^{u_a(\tilde{b}-1)} \\ & & & 1 & \\ -1 & \dots & -1 & 2 & \\ \vdots & & \vdots & \vdots & \zeta_n^{u_a(\tilde{b}-1)} + \zeta_n^{-u_a(\tilde{b}-1)} \\ -1 & \dots & -1 & 2 & \end{pmatrix}$$

$$= \left(\frac{1}{2}\right)^{\phi(n)/2} \mathrm{Det}\begin{pmatrix} & & & 1 & \\ & 2\,\frac{\zeta_n^{u_a u_b}}{1-\zeta_n^{u_a u_b}} + 1 & & \vdots & \zeta_n^{u_a(\tilde{b}-1)} \\ & & & 1 & \\ 0 & \dots & 0 & 2 & \\ \vdots & & \vdots & \vdots & \zeta_n^{u_a(\tilde{b}-1)} + \zeta_n^{-u_a(\tilde{b}-1)} \\ 0 & \dots & 0 & 2 & \end{pmatrix}$$

$$= 2\left(\frac{1}{2}\right)^{\phi(n)/2} \mathrm{Det}\left(\, 2\,\frac{\zeta_n^{u_a u_a}}{1-\zeta_n^{u_a u_b}} + 1 \,\right) \mathrm{Det}\left(\, \zeta_n^{\breve{u}_a(b-1)} + \zeta_n^{-\breve{u}_a(b-1)} \,\right),$$

where we put $\breve{u}_a = u_{\phi(n)/2+1-a}$ and $\tilde{b} = b - \phi(n)/2$.

We consider these determinants separately.

As for the former, from

$$2\frac{\zeta_n^{u_a u_b}}{1-\zeta_n^{u_a u_b}} + 1 = \frac{\zeta_n^{u_a u_b}}{1-\zeta_n^{u_a u_b}} - \frac{\zeta_n^{-u_a u_b}}{1-\zeta_n^{-u_a u_b}} = \sqrt{-1}\,\cot(u_a u_b\,\pi/n)\,, \tag{11}$$

it follows that

$$\mathrm{Det}\left(2\frac{\zeta_n^{u_a u_b}}{1-\zeta_n^{u_a u_b}} + 1\right) = \sqrt{-1}^{\phi(n)/2}\mathrm{Det}\left(\cot(u_a u_b \pi/n)\right) .$$

As for the latter, exchanging rows and noting that $u_{\phi(n)+1-a} = n - u_a$, we see that

$$\begin{aligned}\mathrm{Det}\left(\zeta_n^{\breve{u}_a(b-1)} + \zeta_n^{-\breve{u}_a(b-1)}\right) &= \pm\mathrm{Det}\left(\zeta_n^{u_a(b-1)} + \zeta_n^{-u_a(b-1)}\right) \\ &= \pm\mathrm{Det}\left(2\cos(2u_a(b-1)\,\pi/n)\right) .\end{aligned}$$

Thus, together with these, we obtain the equality in Lemma 2.3. □

2.3. $\mathrm{Det}\,(2\cos(2u_a(b-1)\pi/n))$**.** In this subsection we calculate $\mathrm{Det}\,(2\cos(2u_a(b-1)\pi/n))$ in terms of the discriminants. For an algebraic number field K we denote by $d(K)$ the discriminant of K. In fact, we prove the following

PROPOSITION 2.4. *Assume $n > 2$. Then*

$$\mathrm{Det}\,(2\cos(2u_a(b-1)\pi/n)) = \pm 2\sqrt{d(\mathbf{Q}(\zeta_n + \zeta_n^{-1}))}\,,$$

where a, b range over the set $\{1, \ldots, \phi(n)/2\}$.

PROOF. First we note that $\mathbf{Z}[\zeta_n + \zeta_n^{-1}]$ is the ring of algebraic integers of $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ (cf. e.g., [11, Proposition 2.16]). On the other hand, it is easy to see that the elements $1,\ \zeta_n + \zeta_n^{-1},\ \zeta_n^2 + \zeta_n^{-2}, \ldots, \zeta_n^{\phi(n)/2-1} + \zeta_n^{-(\phi(n)/2-1)}$ forms an integral basis of $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$. Thus, by the definition of the discriminant

$$\begin{aligned} d(\mathbf{Q}(\zeta_n + \zeta_n^{-1})) &= \Delta(1,\ \zeta_n + \zeta_n^{-1}, \ldots, \zeta_n^{\phi(n)/2-1} + \zeta_n^{-(\phi(n)/2-1)})^2 \\ &= \frac{1}{4}\mathrm{Det}\left(\zeta_n^{u_a(b-1)} + \zeta_n^{-u_a(b-1)}\right)^2 . \end{aligned}$$

Since $d(\mathbf{Q}(\zeta_n + \zeta_n^{-1})) > 0$ (e.g., [11, Lemma 2.2]), this implies the desired equality of our proposition. □

2.4. $\mathrm{Det}\,(\cot(u_a u_b^* \pi/n))$**.** In this subsection we calculate $\mathrm{Det}\,(\cot(u_a u_b^* \pi/n))$ in terms of the values $L(1, \chi)$ at 1 of L-functions attached to Dirichlet characters χ mod n. Note that the matrix $(\cot(u_a u_b \pi/n))$ is obtained by exchanging columns of the matrix $(\cot(u_a u_b^* \pi/n))$.

PROPOSITION 2.5. *Assume $n > 2$. Then*

$$\mathrm{Det}\left(\cot(u_a u_b^* \pi/n)\right) = \left(\frac{n}{\pi}\right)^{\phi(n)/2} \prod_{\chi:\,\mathrm{odd}} L(1, \chi)\,,$$

where a, b range over the set $\{1, \ldots, \phi(n)/2\}$.

PROOF We use the Dedekind determinants such as

LEMMA 2.6 (cf. e.g., [9, Lemma], [8]). *Assume $n > 2$. Let G be the group $(\mathbf{Z}/n\mathbf{Z})^\times$. Then, for a complex-valued odd function $f : G \longrightarrow \mathbf{C}$, we have*

$$\mathrm{Det}\,(f(\bar{u_a}\bar{u_b}^{-1})) = \prod_{\chi:\,\mathrm{odd}} \left(\frac{1}{2}\sum_{\bar{u}\in G} \chi(\bar{u}) f(\bar{u}^{-1})\right),$$

where a, b range over the set $\{1, \dots, \phi(n)/2\}$, and $\bar{u}$ denotes the corresponding class in G for $u \in \mathbf{Z}$ with $(u, n) = 1$. □

Put $G = (\mathbf{Z}/n\mathbf{Z})^{\times}$, and $f(\bar{u}) = \cot(u\pi/n)$ for $\bar{u} \in G$ with $u \in \mathbf{Z}$ its representative. Noting that $f : G \longrightarrow \mathbf{C}$ is odd, we have by Lemma 2.6 that

$$\mathrm{Det}\,\left(\cot(u_a u_b^* \pi/n)\right) = \prod_{\chi:\,\mathrm{odd}} \left(\frac{1}{2} \sum_{\bar{u} \in G} \bar{\chi}(\bar{u})\, f(\bar{u})\right).$$

Next, we put $h_1(t) = \dfrac{1+t}{2\,(1-t)}$. To prove our Proposition, we need the following:

PROPOSITION 2.7 (cf. [4, Theorem 3.4]). *Assume $n > 1$. Then*

$$L(1, \chi) = \left(-\frac{2\pi\sqrt{-1}}{n}\right) \frac{1}{2} \sum_{u \in I(n)} \chi(\bar{u}) h_1(\zeta_n^u)\,. \qquad \square$$

Here we note that the equality in Proposition 2.7 is deduced from the equation

$$h_1(t) = -\frac{1}{2}\, \frac{1}{2\pi\sqrt{-1}} \sum_{k \in \mathbf{Z}} \left(\frac{1}{x+k} + \frac{1}{x-k}\right)$$

for $x \in \mathbf{C}$ with $x \notin \mathbf{Z}$ and $t = \exp(2\pi\sqrt{-1}x)$,
which is a consequence of the Euler's product for the sin −function

$$\sin(\pi x)/\pi x = \prod_{k=1}^{\infty} (1 - x^2/k^2)\,.$$

Returning to the proof, we see by (11) that

$$f(\bar{u}) = -2\sqrt{-1}h_1(\zeta_n^u)\,.$$

Hence, from Proposition 2.7 it follows that

$$\begin{aligned} \frac{1}{2} \sum_{u \in I(n)} \bar{\chi}(\bar{u}) f(\bar{u}) &= \frac{1}{2}(-2\sqrt{-1}) \sum_{u \in I(n)} \bar{\chi}(\bar{u}) h_1(\zeta_n^u) \\ &= \frac{n}{\pi} L(1, \bar{\chi})\,. \end{aligned}$$

Together with these, we obtain

$$\mathrm{Det}\,(\cot(u_a u_b^* \pi/n)) = \left(\frac{n}{\pi}\right)^{\phi(n)/2} \prod_{\chi:\,\mathrm{odd}} L(1, \chi)\,,$$

as asserted. □

2.5. Proof of Theorem. First we settle the part including L_χ in the following:

PROPOSITION 2.8. *Assume $n > 2$ with $n = fm$. Let χ be a Dirichlet character* $\bmod n$ *such that $\chi \neq 1$. Assume χ_f be a Dirichlet character* $\bmod f$ *such that χ_f induces χ. Then,*

$$L(1, \chi) = L(1, \chi_f) \prod_{p|n,\, p\nmid f_\chi} (1 - \chi_f(p)/p)\,.$$

PROOF. This follows from the Euler's product of $L(s, \chi)$ (e.g., [10, Proposition 12 in 3.3]). □

As for the parts of the class numbers and the discriminants, we quote the following:

PROPOSITION 2.9 [11, P. 42]. *Assume $n > 2$. Then,*

$$\prod_{\chi:\,\mathrm{odd}} L(1, \chi_*) = \frac{1}{Qw}\,(2\pi)^{\phi(n)/2} \cdot h_n^- \cdot \frac{1}{\sqrt{\frac{|d(\mathbf{Q}(\zeta_n))|}{d(\mathbf{Q}(\zeta_n+\zeta_n^{-1}))}}}\,,$$

where χ_* denotes the primitive character belonging to χ. □

PROPOSITION 2.10 [11, P. 44]. *Assume $n > 2$. Then*

$$\frac{d(\mathbf{Q}(\zeta_n + \zeta_n^{-1}))}{\sqrt{|d(\mathbf{Q}(\zeta_n))|}} = \begin{cases} 1/2 & \text{if } n \text{ is a 2-power}\,, \\ 1/\sqrt{p} & \text{if } n \text{ is a } p\text{-power with } p \text{ prime } (\neq 2)\,, \\ 1 & \text{otherwise}\,. \end{cases}$$ □

Together with these, we complete the proof of our Theorem. In fact, we obtain the equation in Theorem by Lemma 2.3, Proposition 2.4 and Proposition 2.5, substituting by Proposition 2.8, Proposition 2.9 and Proposition 2.10. □

3. Remarks in the case n is a prime power

In the case n is a prime power, the situations are somewhat simple (cf. e.g., Remark 3.1 below). In this section, also we provide an alternative proof of a theorem in [1, Theorem C.2] (cf. Proposition 3.3 below) in the line given in Proposition 1.3.

3.1. Statement As for our main theorem, considering that $L_\chi = 1$ in the case n is a prime power, we have

REMARK 3.1. Let n be a prime power with $n > 2$. Then, we have

$$\Delta\,(\zeta_n^{u_1}/(1-\zeta_n^{u_1}), \ldots, \zeta_n^{u_{\phi(n)/2}}/(1-\zeta_n^{u_{\phi(n)/2}})\,, 1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)/2-1})$$

$$= \begin{cases} \pm\dfrac{1}{n}\,(n\sqrt{-1})^{\phi(n)/2}\cdot h_n^- & \text{if } n \text{ is a 2-power}\,, \\ \pm\dfrac{1}{n\sqrt{p}}\,(n\sqrt{-1})^{\phi(n)/2}\cdot h_n^- & \text{if } n \text{ is a } p\text{-power with } p\neq 2\,, \end{cases}$$

where we use the notations as in Theorem. □

As for the Maillet's determinants, we have

PROPOSITION 3.2 [7]. *Let n be a prime power with $n > 2$. Then we have*

$$\mathrm{Det}\,(MA_n) = \begin{cases} \dfrac{1}{n}\,h_n^- & \textit{if } n \textit{ is a 2-power}\,, \\ \dfrac{1}{2n}h_n^- & \textit{if } n \textit{ is a } p\textit{-power with } p \textit{ prime } (\neq 2)\,. \end{cases}$$ □

Thus, applying the implication (i) ⇒ (ii) in Proposition 1.3 we also have

PROPOSITION 3.3 [1, Theorem C.2]. *Let n be a prime power with $n > 2$. Then the elements* $1\,,\ \zeta_n^{u_1}/(1-\zeta_n^{u_1})\,,\ldots,\ \zeta_n^{u_{\phi(n)/2}}/(1-\zeta_n^{u_{\phi(n)/2}})$ *are* $\mathbf{Q}$*-independent.* □

3.2. A remark on the alternative proof. Seeing the proof of the implication (i) ⇒ (ii) in Proposition 1.3, we moreover have the following:

PROPOSITION 3.4. *Let n be a prime power with $n > 2$ and assume $n = fm$. Put* $\chi = \sum_{u\in I(n)} l_{u^*}\,\Delta_n^{(u)}$ with $l_{u^*} \in \mathbf{Q}(u \in I(n))$. *Then*

$$\chi(f \bmod n\mathbf{Z}) = \frac{\phi(m)}{\phi(n)}\mathrm{Tr}_{n,m}\,(\chi(1 \bmod n\mathbf{Z}))$$ □

This means that the virtual character $\sum_{u\in I(n)} l_{u*}\,\Delta_n^{(u)}$ is completely determined by the value at 1 mod $n\mathbf{Z}$ in our case.

References

[1] T. BREUER, *Characters and Automorphism Groups of Compact Riemann Surfaces*, London Math. Soc. Lecture Note Series 280, Cambridge Univ.Press, 2000.

[2] L. CARLITZ and F. R. OLSON, Maillet's determinant, Proc. Amer. Math. Soc. 6(1955), 265–269.

[3] H. HASSE, *Number Theory* (3rd ed.), Grundlehren 229, Springer-Verlag, 1980.

[4] K. KATOU, N. KUROKAWA and T. SAITOU, *Number Theory* 1 (in Japanese), Iwanami, 1996.

[5] I. KURIBAYASHI, A remark on the numbers $\cot(u\pi/n)$ as a $\mathbf{Q}$-linear basis, J. of Fac. of Administration and Informatics (Tokoha-Gakuen Hamamatsu Univ.) 9(1996), 173–180.

[6] R. KUČERA, On Bases of the Stickelberger Ideal and of the Group of Circular Units of a Cyclotomic Field, J. Number Theory **40**(1992), 264–283.

[7] J. KÜHNOVÁ, Maillet's Determinant $D_{p^{n+1}}$, Arch. Math. **15**(1979), 209–212.

[8] S. LANG, *Cyclotomic Fields I and II* (3rd ed.), G.T.M.121, Springer-Verlag, 1990.

[9] S. OKADA, Generalized Maillet determinant, Nagoya Math. J. **94**(1984), 165–170.

[10] J.P. SERRE, *A Course in Arithmetic*, Springer-Verlag, G.T.M.7, 1973.

[11] L.C. WASHINGTON, *Introduction to Cyclotomic Fields* (2nd ed.), Springer-Verlag, G.T.M.83, 1997.

Present Address:
FACULTY OF ADMINISTRATION AND INFORMATICS,
HAMAMATSU UNIVERSITY,
HAMAMATSU, 431–2102 JAPAN.