A formula which connects the determinant of the Demjanenko matrix with the relative class number of the cyclotomic field is given. A close relation between this matrix and the Hodge group of some Abelian variety is also revealed.

In [2], Folz and Zimmer investigate the rank of the Demjanenko matrix $D_p$ for a prime $p$ (see [2] for the definition) in connection with the problem of giving an explicit bound for the order of torsion points on some elliptic curves. They call a prime $p$ exceptional or nonexceptional according to whether the mod 2 rank of $D_p$ drops or not. And they explain "the significance of the distinction between exceptional and non-exceptional primes." In the present article we prove that $p$ is nonexceptional if the relative class number $h_p^-$ of the cyclotomic field $\mathbb{Q}(\zeta_p)$ is odd. (This also explains the occurrence of asterisks in the Table 1 of [2].) Moreover we show that this matrix is essentially the same as the one which appears as a matrix representation of the character group of the Hodge group of some abelian variety of CM-type. This shows another significance of the Demjanenko matrix. A similar kind of matrix was used in [1] to obtain a bound for $h_p^-$; therefore our result may be of use for this purpose as well as for actual calculation of $h_p^-$ for small values of $p$.

I thank the referee for his kind advice.

Notation

Throughout this paper, we fix an odd prime $p$ and put $g = (p - 1)/2$. We denote by $F_p$ the finite field with $p$ elements. Let $f$ denote the multiplicative
order of 2 in $F_p^* = F_p - \{0\}$. We put $e = (p - 1)/f$. We denote by $S$ the set \{1, ..., $g$\}, which is considered as a subset of $F_p$, and denote by $\chi(S)$ the sum $\sum_{x \in S} \chi(x)$. For a positive integer $n$, we denote by $\zeta_n$ the primitive root of unity, $\exp(2\pi i/n)$, and denote by $h_p^-$ the relative class number of the cyclotomic field $Q(\zeta_p)$. Finally, for a real number $x$, we denote by $\{x\}$ (resp. $\lfloor x \rfloor$) the distance of $x$ to the nearest integer in $Z$ (resp. in $pZ$) and by $\lfloor x \rfloor$ the integral part of $x$.

2. Hodge Group and Demjanenko Matrix

Let $A$ be an abelian variety defined over $C$. The Hodge group $Hg(A)$ of $A$ is a reducible algebraic group over $Q$ (see [4, 7] for the definition and its fundamental property). When $A$ is of CM-type, $Hg(A)$ is an algebraic torus and its character group can be given in terms of the embeddings of the corresponding CM-field into $C$ (see [8, 33]). In particular, when $A$ has complex multiplication by $Q(\zeta_p)$ and its "type" is given by the embeddings defined by $\zeta_p \rightarrow \zeta_p^i (i = 1, ..., g)$, the character group of $Hg(A)$ is isomorphic to $Q[\text{Gal}(Q(\zeta_p)/Q) \cdot \sum_{i \in S} (i - (-i))]$, where we identify the Galois group $\text{Gal}(Q(\zeta_p)/Q)$ with $F_p^*$ naturally.

Now we introduce the following three $g$ by $g$ matrices:

$A = (a_{ij})$, where $a_{ij} = 1$ if $i \cdot j \in S$ and $= -1$ otherwise;

$H = (h_{ij})$, where $h_{ij} = 1$ if $i \cdot j \in S$ and $= 0$ otherwise;

$D = (d_{ij})$, where $d_{ij} = 1$ if $\{(i+1)j\}_p - \{(i-1)j\}_p > 0$

and $= 0$ otherwise.

Since the matrix $D$ is obtained by an elementary row operation from the modified Demjanenko matrix $D'_p$ (cf. [2]), their rank (over $Z$ or $F_p$) coincide. Recall that $D'_p$ is defined to be a submatrix of the original Demjanenko matrix $D_p$, and that $D_p$ is of full rank if $D'_p$ is. Moreover the matrix $H$ can be transformed into $A$ by a number of elementary row operations, so it is easy to see that $2^{g-1} \det H = \det A$ (it is known that $H$ is nondegenerate [5, 8]). Now we observe the following:

**Proposition 2.1.** $D = H$.

**Proof.** Since $\{(i+1)j\}_p - \{(i-1)j\}_p = \{ij + j\}_p - \{ij - j\}_p$ holds, we are reduced to showing the following: for any $r \in (0, 1/2)$ and $a \in (0, 1/2)$, $\{(a+r)j\}_p + \{a-r\} > 0$ if and only if $a \in (0, 1/2)$. Assume that $a \in (0, 1/2)$. When $r$ is smaller than or equal to $a$, we have

\[
\{a+r\} - \{a-r\} = \begin{cases} (a+r) - (a-r) = 2r > 0 & \text{if } a + r \leq \frac{1}{2} \\
(1-(a+r)) - (a-r) = 1 - 2a > 0 & \text{if } a + r > \frac{1}{2}.
\end{cases}
\]
On the other hand, when \( r \) is greater than \( a \), we have
\[
\{a + r\} - \{a - r\} = \begin{cases} (a + r) - (r - a) = 2a > 0 & \text{if } a + r \leq \frac{1}{2} \\ (1 - (a + r)) - (r - a) = 1 - 2r > 0 & \text{if } a + r > \frac{1}{2}. \end{cases}
\]
The converse is proved similarly.

3. Determinant of Demjanenko Matrix

In [9], Wang gives an argument to obtain a formula for the Maillet determinant. A similar argument enables us to obtain the following (see [8] for a formula expressed by the character sums \( \chi(F_p^*) \)):

**Proposition 3.1.** \( \det H = (-1)^{[g/2]} \cdot 2^{1-g} \prod_{\chi \text{ odd}} \chi(S). \)

On the other hand, we have the following formula due to Kubota [5] which relates the "half sum" \( \chi(S) \) with the Bernoulli number \( B_{1, \chi} \):

**Proposition 3.2.** \( \chi(S) = (1 - 2 \cdot \chi(2)) \cdot B_{1, \chi}/\chi(2). \)

(Note that Kubota used \( \Theta_\chi = \sum_{a=1}^{p-1} \chi(a)a \) instead of \( B_{1, \chi} = \sum_{a=1}^{p-1} \chi(a)a/p = \Theta_\chi/p. \))

Moreover we have the following well known formula:

**Theorem 3.3** (see [6], for example). \( h_p^- = 2p \cdot (1 - \chi(2)) \cdot B_{1, \chi}/\chi(2). \)

Combining these three equalities, we prove the main theorem:

**Theorem 3.4.** We have
\[
\det D = \det H = (-1)^{[g/2]} \cdot 2^{1-g} \prod_{\chi \text{ odd}} \chi(S) \quad \text{and} \quad (2f - 1)^{e/2} \quad \text{if } f \text{ is even}
\]
\[
(2f - 1)^{e/2} \quad \text{if } f \text{ is odd}
\]
(see Section 1 for the meaning of \( e \) and \( f \)).

**Corollary 3.5.** A prime \( p \) is nonexceptional if \( h_p^- \) is odd.

**Proof.** We have the following equalities:
\[
\det H = (-1)^{[g/2]} \cdot 2^{1-g} \prod_{\chi \text{ odd}} \chi(S) \quad \text{(by Prop. 3.1)}
\]
\[
= (-1)^{[g/2]} \cdot 2^{1-g} \prod_{\chi \text{ odd}} \left( (1 - 2\chi(2)) \cdot B_{1, \chi}/\chi(2) \right) \quad \text{(by Prop. 3.2)}
\]
\[
= (-1)^{g + [g/2]} \cdot h_p^- \cdot p^{-1} \prod_{\chi \text{ odd}} \left( (1 - 2\chi(2))/\chi(2) \right) \quad \text{(by Th. 3.3)}
\]
\[
= (-1)^{g + [g/2]} \cdot h_p^- \cdot p^{-1} \prod_{\chi \text{ odd}} (\chi(2) - 2)
\]
The last factor on the rightmost side is computed as follows. Since $f$ is the order of 2 in $\mathbb{F}_p^*$ and $e = (p - 1)/f$, the values $\chi(2)$ for odd $\chi$ are given by (*) $\zeta_f, \zeta_f^3, \ldots, \zeta_f^{p-2}$.

Case 1. $f$ is even: The $(f/2)$th roots of $-1$ are given by $\zeta_f, \zeta_f^3, \ldots, \zeta_f^{f/2}$, hence we have

$$\prod_{\chi: \text{odd}} (X - \chi(2)) = (X^{f/2} + 1)^e$$

which implies

$$\det H = (-1)^{\left\lfloor \frac{f}{2} \right\rfloor} \cdot h_p^{-1} \cdot (2^{f/2} + 1)^e \cdot (-1)^g$$

$$= (-1)^{\left\lfloor \frac{f}{2} \right\rfloor} \cdot h_p^{-1} \cdot (2^{f/2} + 1)^e.$$ 

Case 2. $f$ is odd: Since the first $f$ numbers in (*) are the $f$th roots of 1, we have

$$\prod_{\chi: \text{odd}} (X - \chi(2)) = (X^f - 1)^{e/2}$$

which implies

$$\det H = (-1)^{\left\lfloor \frac{f}{2} \right\rfloor} \cdot h_p^{-1} \cdot (2^f - 1)^{e/2}.$$ 

This completes the proof of the theorem.

**REFERENCES**