Another proof of Iwasawa's class number formula

by

LADISLAV SKULA (BÝRO)

1. Introduction. K. Iwasawa ([3]) has proved that the first class number factor of the $p^{n+1}$th cyclotomic field $F_n(p)$ is equal to the group index $[\mathbb{Z}^r : \mathbb{Z}^s]$, where $\mathbb{Z}^r$ and $\mathbb{Z}^s$ are certain subgroups of the additive group of the group ring $\mathbb{Z}[G_n]$ of the group $G_n$ over the ring of rational integers $\mathbb{Z}$. The group $G_n$ denotes the Galois group of $F_n$ over the rational field $\mathbb{Q}$.

Iwasawa's proof is based on the representations of a semi-simple algebra. In the present paper, we shall give another proof of this Iwasawa's formula based on the presentation of a special basis of $\mathbb{Z}^r$. By the calculation of the determinant of the transition matrix from a certain basis of $\mathbb{R}^r$ to this basis of $\mathbb{Z}^r$ we obtain Iwasawa's class number formula or the $p^{n+1}$th cyclotomic field.

2. Notation. In this paper the following symbols are used:

- $p$ an odd prime,
- $n$ a non-negative integer,
- $h_n$ the first factor of the class number of the cyclotomic field generated by $p^{n+1}$th roots of unity over the rational field,
- $Z$ the ring of integers,
- $q = p^{n+1}$,
- $M = p^n(p-1)$,
- $N = M/2$,
- $\epsilon$ a primitive root modulo $q$,
- $r_j$ the integer $(j \in \mathbb{Z})$, $0 < r_j < q$,
- $r_j = r^j \mod q$ for $j \geqslant 0$,
- $r_j = r^{-j} \mod q$ for $j < 0$,
- $h_j = M^{-1} \sum_{j}^{M-1} \epsilon^{\delta_j}$ for suitable symbols $\delta_j$,
- $F(X)$ polynomial over the complex field.
\( \theta \) a primitive \( M \)th root of unity, 
\( G \) a cyclic group of order \( M \) (written multiplicatively), 
\( \sigma \) a generator of \( G \); thus \( G = \{1, \sigma, \sigma^2, \ldots, \sigma^{M-1}\} \), 
\( \mathbb{R} = \mathbb{Z}[G] \) the group ring of \( G \) over \( \mathbb{Z} \); thus
\[ \mathbb{R} = \left\{ \sum_j a_j \sigma^j : a_j \in \mathbb{Z} \right\}, \]
\[ a_0 = \sum \sigma^{-j} a_j, \]
\[ \mathbb{S} = \left\{ a \in \mathbb{R} : \exists q \in \mathbb{R}, q \cdot a_0 = qa \right\}, \]
\[ \mathbb{S}^- = \{ a \in \mathbb{R} : (1 + \sigma^0) a = 0 \}, \]
\[ \mathbb{S}^- = \mathbb{S} \cap \mathbb{S}^- \).

3. The expressing of \( \kappa_\infty^+ \) as a determinant. From [2] we obtain the following formula:

\[ \kappa_\infty^+ = \frac{1}{(2q)^{N-1}} |E(\theta) E(\theta^2) \ldots E(\theta^{M-1})|. \]

For odd \( \ell \) we get
\[ E(\theta^\ell) = \sum \sigma^j = \sum_{j=0}^{N-1} \sigma^j = \sum_{j=0}^{N-1} \sigma^j \cdot \theta^j, \]
therefore
\[ E(\theta^\ell) = \sum_{j=0}^{N-1} (\sigma^j - \sigma^{j + \ell}) \theta^j, \]
for each \( 0 \leq j \leq N-1 \).

Put
\[ C = (\theta^{(j+1)})(0 \leq j \leq N-1), \quad A = (\sigma^j - \sigma^{j + \ell})(0 \leq j \leq N-1), \]
\[ D = C \cdot A = (a_{ij})(0 \leq i, j \leq N-1). \]

Then
\[ a_{ij} = -\sum_{j=0}^{N-1} (\sigma^j - \sigma^{j + \ell}) \theta^{(j+1) \cdot (j+1)} \theta^{(j+1) \cdot j} = -\theta^{(j+1) \cdot (j+1)} E(\theta^{j+1}), \]

\[ |\det D| = |E(\theta) E(\theta^2) \ldots E(\theta^{M-1})| \cdot |\det C| = |\det C| \cdot |\det A|. \]

It follows from (1)
\[ (2) \quad \kappa_\infty^+ = \frac{1}{2q^{N-1}} |\det (\sigma^j - \sigma^{j + \ell})(0 \leq j, \ell \leq N-1)|. \]

For \( n = 0 \) this formula is given in the exercise 3, § 5, Chapter V of [1].

Let us put as for \( n = 0 \) in [4]
\[ b_{0}\ell = q - 2, \]
\[ b_{ji} = 1 - r_{ij}, \quad 1 \leq j \leq N - 1, \]
\[ b_{ii} = 1 - r_{ii}, \quad 1 \leq i \leq N - 1, \]
\[ b_{ji} = \frac{1}{q} (r_{ij} - r_{ji}), \quad 1 \leq i, j \leq N - 1, \]
\[ B = (b_{ij})(0 \leq i, j \leq N - 1). \]

By the same way as for \( n = 0 \) in [4] \((A = (q - 2r_{ij})(0 \leq i, j \leq N - 1), \)
subtraction of the row 0 of \( A \) from every other row, removing of the factor 2 from the last \( N - 1 \) rows, subtraction of \( r_{ij} \) times the column 0 from the column \( j \) \((1 \leq j \leq N - 1) \) and removing of the factor \( q \) from the last \( N - 1 \) columns) we obtain from (2)
\[ (3) \quad \kappa_\infty^+ = |\det B|. \]

4. The basis \( \{a_j : i \in \mathbb{S}\} \) of \( \mathbb{S}^- \). If \( a = \sum_{j} a_j \sigma^j \in \mathbb{S} \), then there exists
\[ q = \sum_{j} a_j \sigma^j \in \mathbb{R} \] such that \( q \cdot a_0 = qa \). Hence \( qa = \sum_{j} r_{ij} \sigma^j \sum_{j} a_j \sigma^j \)
\[ = \sum_{j} \sigma^j \sum_{j} a_j r_{ij} \sigma^j \]
and it follows \( a_j = \frac{1}{q} \sum_{j} a_j r_{ij} \sigma^j \) for each \( 0 \leq j \leq M - 1 \).

Let conversely \( a_j \in \mathbb{Z} \) \((0 \leq j \leq M - 1)\), \( \sum_{j} a_j r_{ij} = 0 \) \((\mod q)\) and \( a_j \)
\[ = \frac{1}{q} \sum_{j} a_j r_{ij} \sigma^j \]
\((0 \leq j \leq M - 1)\). Then \( a_j \in \mathbb{Z} \) and \( a = \sum_{j} a_j \sigma^j \in \mathbb{S} \). Put
\[ e = \sum_{j} a_j \sigma^j. \]

\[ q \in \mathbb{R} \text{ and } q \cdot a_0 = \sum_{j} a_j \sigma^j \sum_{j} r_{ij} \sigma^j = \sum_{j} \sigma^j \sum_{j} a_j r_{ij} = qa, \]

Therefore we have
\[ (4) \quad \mathbb{S}^- = \left\{ a = \sum_{j} a_j \sigma^j : a_j = \frac{1}{q} \sum_{j} a_j r_{ij} \sigma^j, a_j \in \mathbb{Z}, \sum_{j} a_j r_{ij} = 0 \} \). \]

It is easy to see that it holds
\[ \mathbb{S}^- = \left\{ a = \sum_{j} a_j \sigma^j : a_j \in \mathbb{Z}, a_j + a_{j+N} = 0, 0 \leq j \leq N - 1 \right\}. \]

5. \( \mathbb{S}^- = \left\{ a = \sum_{j} a_j \sigma^j : a_j = \frac{1}{q} \sum_{j} a_j r_{ij} \sigma^j, a_j \in \mathbb{Z}, \sum_{j} a_j r_{ij} = 0 \} \).
It follows that
\[ \beta = -\sum_{i \in \mathcal{E}} y_i a_i + da, \]
therefore
\[ (9) \quad \{a_i; \ i \in \mathcal{E}\} \text{ is a system of generators of the additive group } \mathbb{Z}. \]

The additive group \( \mathbb{R}^+ \) has a basis \( s(1 - sN), \ 0 \leq j < N. \) The determinant \( \Delta \) of the transition matrix from this basis to the system of generators \( \{a_i; \ i \in \mathcal{E}\} \) is equal to \( \det(a_{ij}; 0 \leq j \leq N - 1). \)

If we subtract the column 0 from every other column, we obtain
\[
\begin{vmatrix}
2 - q & 2(r_{j-1}) & \cdots & q - 2 & 1 - r_j & \cdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\
\end{vmatrix}
\]
\[
\Delta = \begin{vmatrix}
1 - r_i & 2 & \cdots & q - 2 & 1 - r_j & \cdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\
\end{vmatrix}
\]

Since \( r_j = r_{M-j} \) we have
\[
|\Delta| = \begin{vmatrix}
q - 2 & \cdots & 1 - r_{j+N} & \cdots \\
\vdots & \ddots & \vdots & \ddots \\
\end{vmatrix}
\]
\[
\Delta = \begin{vmatrix}
1 - r_i & 2 & \cdots & q - 2 & 1 - r_j & \cdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\
\end{vmatrix}
\]

If we add the column 0 to every other column, we obtain, according to \( r_{j+N} = q - r_j \)
\[
|\Delta| = \begin{vmatrix}
q - 2 & \cdots & 1 - r_j & \cdots \\
\vdots & \ddots & \vdots & \ddots \\
\end{vmatrix}
\]

If we add the row 0 to the \( i \)th row for each \( i \geq N, \) we get, according to \( r_i + r_{j-N} = q \) and (3),
\[
h_n = |\Delta|.
\]

From the results we obtain the following theorem.

\textbf{Theorem.} The system \( \{a_i; \ i \in \mathcal{E}\} \) is a basis of the additive group \( \mathbb{Z} \) and for the determinant \( \Delta \) of the transition matrix from the basis \( s(1 - sN), \ 0 \leq j < N. \) of the additive group \( \mathbb{R}^+ \) to the basis \( \{a_i; \ i \in \mathcal{E}\} \) of the additive group \( \mathbb{Z} \), there holds
\[
h_n = |\Delta|.
\]

Therefore \( h_n = [\mathbb{R}^+: \mathbb{Z}]. \)
The primality of certain integers of the form $2A\tau^n - 1$

by

H. C. WILLIAMS (Winnipeg)

1. Introduction. In [6] Lucas presented conditions which are sufficient for integers of the form $Br^n - 1$ ($B < r^a$) $r = 2, 3, 5$, to be prime. Lehmer [4], Riesel [7] and Stechkin [8] have given criteria which are both necessary and sufficient for the primality of $A2^n - 1$ ($A < 2^n$) and Williams [10], [12] has given necessary and sufficient criteria for the primality of $2A3^n - 1$ ($A < 3^n$) and $A2^n3^m - 1$ ($A < 2^{s+1}3^m$). All of these tests make use of Lucas functions or functions similar to the Lucas functions. In this paper we present, using the Lucas functions together with the generalized Lehmer functions of [11], a necessary and sufficient criterion for the primality of certain numbers of the form $N = 2A\tau^n - 1$ ($A < r^a$) when $r$ and $s$ are odd primes, $r = 2s + 1$, and $2A - 1$ is a primitive root of $s$.

We define the Lucas functions

$$V_n(P, Q) = a^n + \beta^n, \quad U_n(P, Q) = (a^n - \beta^n)/(a - \beta),$$

where $a, \beta$ are the roots of the auxiliary quadratic

$$a^2 - P_ay + Q = 0$$

and $P, Q$ are coprime integers. (While it is usual to insist that $(P, Q) = 1$, it is sufficient in dealing with the functions modulo $N$ to have $(N, Q) = 1$.) The usual test for the primality of $N = Br^n - 1$ ($B < r^a$) (see, for example, Brillhart, Lehmer, Selfridge [1]) involves attempting to find $P, Q$ such that $(Q, N) = 1$ and

$$N|U_{N+1}(P, Q),$$

$$[N, U_{(N+1)/r}(P, Q)] = 1. \tag{1.1}$$

If such a pair $P, Q$ can be found, $N$ is a prime. The determination of this pair is done by trial, subject to the constraint that the Jacobi symbol $(P^2 - 4Q|N) = -1$. Under this constraint, if (1.1) is not satisfied, $N$ is composite.