On the units of cyclotomic fields

by

K. Ramachandra (Bombay)

§ 1. Let \( f \geq 1 \) be a natural number with \( \varphi(f) > 2 \), \( \varphi \) being the Euler totient function. Let \( a \) be a primitive \( f \)th root of unity and \( Q(a) \) the cyclotomic field generated by \( a \) over the rational number field \( Q \). It is clear that for \( (s, f) = 1, 1 < s < f/2 \), the numbers

\[
 u_s = \frac{a^s - 1}{a - 1}
\]

are units of \( Q(a) \). Some time back Professor J. Milnor(1) asked the following question: Do the units \( u_s \) together with \( \pm a \) form a basis for the units of \( Q(a) \)?

In this note we prove the following two theorems.

**Theorem 1.** Let \( f = \prod_{i=1}^{k} p_i^{a_i} \) be the prime factor decomposition of \( f \) and for \( 1 < s < f/2, (s, f) = 1 \) let

\[
 v_s = \prod_{i=1}^{k} \left( \frac{1-a_{p_i^{a_i}}}{1-a} \right)
\]

where the product is extended over all \( a_i = 0 \) or 1, \( i = 1, 2, \ldots, k \), except \( a_1 = a_2 = \ldots = a_k = 1 \). Then the \( \frac{1}{2} \varphi(f) - 1 \) units \( v_s \) of \( Q(a) \) generate a subgroup of finite index in the group of units of \( Q(a) \).

**Theorem 2.** Let \( p \) and \( q \) be two odd primes dividing \( f \), \( q \) having the property that the residue class group \( \mathbb{Z} / q \mathbb{Z} \) has a nonprincipal character \( x \) with \( x(-1) = 1 \), and \( p \equiv 1 \pmod{q} \). Then the units \( u_s \) defined in (1) are multiplicatively dependent.

Theorem 1 shows that if, in particular, \( f \) is a power of a prime, then the units \( u_s \) in (1) are multiplicatively independent, and hence generate

---

(1) In a letter to Professor K. G. Ramanathan dated 6th February 1964.
a subgroup of finite index in the unit group of $Q(a)$. Theorem 2, in addition shows that if $f$ is composite and divisible by at least two distinct odd primes the units $u_i$ need not be independent. In the case of the units $v_i$ of Theorem 1, the index of the subgroup generated by $v_i$ in the group of all units of $Q(a)$, is intimately connected with the class number of the cyclotomic field $Q(a)$. These results in a more general setting will appear elsewhere.

After this paper was written we came to know from Professor Hyman Bass that he had proved some theorems which gave a system of units generating a subgroup of finite index in the group of all units of $Q(a)$, this system being in general bigger than the maximal set. He has also a fairly simple proof of Theorem 2. However, our point of view is different and Theorem 1 appears to be new.

We should also mention that in the case where $f = p$ is an odd prime greater than 3, Theorem 1 is proved in Siegel's [7] lectures.

§ 2. In this section we set our notations and terminology and prove three lemmas which lead to the theorems stated in § 1. We denote by $\mathfrak{A}$, the multiplicative group of residue classes prime to $f$ modulo the subgroup generated by the classes 1 and $-1$. Let $\chi$ be a nonprincipal character of $\mathfrak{A}$. Now if $f_1 > 1$ is a divisor of $f$ then we have a map from $\mathfrak{A}$ to $\mathfrak{A}_{f_1}$ which takes a class $E$ of $\mathfrak{A}$ to the class of $\mathfrak{A}_{f_1}$ represented by a representative of $E$. This map is well defined and onto. It may happen that for some divisor $f_1$ of $f$, $\chi$ will pass to a character of $\mathfrak{A}_{f_1}$ if it passes to a character of $\mathfrak{A}$, it also passes to a character of $\mathfrak{A}_{f_1}$ where $f_1 = (f_1, f_2)$ is the g.c.d. of $f_1$ and $f_2$. In this way we arrive at the least divisor $f_1$ of $f$ such that $\chi$ will not pass to a character of $\mathfrak{A}_{f_1}$ for a divisor $f_1$ of $f_1$, $f_1 \neq f_2$. The character of $\mathfrak{A}_{f_1}$ derived from $\chi$ will be denoted by $\chi_{f_1}$.

Let $g$ be a divisor of $f$, $1 \leq g < f$, and write

$$q_{f_1}(R) = \log(1 - e^{\pi \sqrt{f_1}})$$

where $r$ is a representative of the class $R$ of $\mathfrak{A}_{f_1}$.

**Lemma 1.**

$$V_{f_1}(\chi) = \sum_{R \in \mathfrak{A}_{f_1}} \overline{\chi}(R)q_{f_1}(R)$$

where $T(f_1)$ is a certain gaussian sum of absolute value $\sqrt{f_1}$ and $\overline{\chi}$ is the complex conjugate character of $\chi$.

**Proof.** If $r$ is a representative of $R$ we write $\chi(R) = \chi(r)$ and $\overline{\chi}(r) = 0$ if $(r, f_1) > 1$. Now

$$V_{f_1} = \sum_{R \in \mathfrak{A}_{f_1}} \overline{\chi}(R) \log(1 - e^{\pi \sqrt{f_1}}) + \log(1 - e^{-\pi \sqrt{f_1}})$$

$$= \frac{1}{2} \sum_{r \in \mathfrak{A}} \overline{\chi}(r) \log(1 - e^{\pi \sqrt{f_1}})$$

$$= \frac{1}{2} \sum_{r \in \mathfrak{A}_{f_1}} \overline{\chi}(r) \log(1 - e^{\pi \sqrt{f_1}})$$

such rearrangements being permissible since we could have started with the series in (5) with $e^{\pi \sqrt{f_1}} (\sigma > 1)$ in place of $e^{-\pi \sqrt{f_1}}$ and then passed to the limit $\sigma \to 1$.

Let

$$f = \prod_{i=1}^{k} \prod_{j=1}^{n_i} \prod_{l=1}^{m_i} \prod_{s=1}^{p_{ij}} p_i^{a_i} \quad (i,j,l,k,n_i,m_i,s \geq 1, a_i > 0, j = 1, \ldots, k),$$

$$f_s = \prod_{i=1}^{k_s} \prod_{j=1}^{n_s} \prod_{l=1}^{m_s} \prod_{s=1}^{p_{ij}} p_i^{a_i} \quad (1 \leq s \leq k, 0 < r_i \leq n_i, j = 1, \ldots, k),$$

$$h = \prod_{i=1}^{k_h} \prod_{j=1}^{n_h} \prod_{l=1}^{m_h} \prod_{s=1}^{p_{ij}} p_i^{a_i} \quad (1 \leq h \leq k, 0 < r_i \leq n_i, j = 1, \ldots, k).$$

Now as $a$ runs through a complete system of coprime residues $b \mod f$ and $\beta$ through a complete system of coprime residues $\mod h$, the numbers

$$r = f \cdot a + \frac{f_s}{h} \quad \beta$$

run through a complete system of coprime residues $\mod f$ each only once. Thus we have

$$T_{f_1}(\chi) = \sum_{r \in \mathfrak{A}_{f_1}} \overline{\chi}(r) e^{\pi \sqrt{f_1}} = \sum_{r \in \mathfrak{A}_{f_1}} \overline{\chi}(r) \sum_{a \in \mathfrak{A}_{f_1}} e^{\pi \sqrt{f_1} \log(1 + \frac{f_s}{h})}$$

$$= \sum_{a \in \mathfrak{A}_{f_1}} \overline{\chi}(a) \sum_{r \in \mathfrak{A}_{f_1}} e^{\pi \sqrt{f_1} \log(1 + \frac{f_s}{h})}$$

$$= \sum_{a \in \mathfrak{A}_{f_1}} \overline{\chi}(a) \sum_{r \in \mathfrak{A}_{f_1}} e^{\pi \sqrt{f_1} \log(1 + \frac{f_s}{h})}$$

$$= \sum_{a \in \mathfrak{A}_{f_1}} \overline{\chi}(a) e^{\pi \sqrt{f_1} \log(1 + \frac{f_s}{h})}$$

$$= \sum_{a \in \mathfrak{A}_{f_1}} \overline{\chi}(a) e^{\pi \sqrt{f_1} \log(1 + \frac{f_s}{h})}$$

$$= \sum_{a \in \mathfrak{A}_{f_1}} \overline{\chi}(a) e^{\pi \sqrt{f_1} \log(1 + \frac{f_s}{h})}.$$
The sum in the second bracket vanishes unless \( h f_x \mid ng \). In this case the sum is \( h f_x \), and further since \( ng/h \) will have an exact denominator which divides \( f_x \), the sum in the first bracket will vanish unless \( ng/h \) will have exact denominator \( f_x \). The sum in the third bracket is the Ramanujan sum \( C_{\alpha}(ng) \) (properties necessary will be stated below and are not hard to prove). Thus

\[
T_{f_x}(\chi) = \frac{1}{f_x} \left( \frac{h}{f_x} \right) C_{\alpha}(ng) \sum_{\alpha \mod f_x} \frac{\chi(\beta)}{\beta} e^{2\pi i ng/\alpha} \quad \text{if} \quad (h, ng) = \frac{1}{f_x}.
\]

It is a standard result that the sum

\[
\sum_{\alpha \mod f_x} \frac{1}{\alpha} \left( \frac{\delta, \eta \mod f_x}{\alpha} \right) e^{2\pi i \delta \eta/\alpha} = T(f_x)
\]

is independent of \( \delta, \eta \) and is of absolute value \( f_x \). Hence

\[
T_{f_x}(\chi) = \frac{1}{f_x} \left( \frac{h}{f_x} \right) C_{\alpha}(ng) \sum_{\alpha \mod f_x} \frac{\chi(\beta)}{\beta} e^{2\pi i ng/\alpha} = T(f_x)
\]

if \( (h, ng) = \frac{1}{f_x} \).

Also

\[
C_{\alpha}(ng) = \frac{1}{f_x} \left( \frac{h}{f_x} \right) C_{\alpha}(ng)
\]

by the multiplicative property of the Ramanujan sum and

\[
C_{p^3}(ng) = \begin{cases} 0 & \text{if} \quad (ng, p^2) \neq 1, \\ -p^2 & \text{if} \quad (ng, p^2) = 1, \\ p^2 & \text{if} \quad (ng, p^2) = p^2.
\end{cases}
\]

We now go back to the series (5) for \( V_{f_x} \). If \( f_x \mid f/g \), i.e. \( g \not\mid f/f_x \), then (8) vanishes identically by (8) or directly from the definition of \( f_x \), since the series in the curly brackets in (5) is an invariant of the classes of the quotient of \( \mathscr{A} \) modulo \( \mathscr{A} f_{f_x} \). As for the series (6), we write

\[
g_x = \prod_{j=1}^{k} p_{\alpha_j}^{l_j} \quad (0 < l_j < a_j; j = 1, \ldots, k),
\]

\[
g_x = \prod_{j=1}^{k} p_{\alpha_j}^{l_j} \quad (0 < l_j < a_j; j = i+1, \ldots, k),
\]

\[
g_x = \prod_{j=1}^{k} p_{\alpha_j}^{l_j}, \quad g_x = \prod_{j=1}^{k} p_{\alpha_j}^{l_j}, \quad g_x = \prod_{j=1}^{k} p_{\alpha_j}^{l_j}
\]

\[
h_x = \prod_{j=1}^{k} p_{\alpha_j}^{l_j} \quad \left( \frac{f}{h_x} \right)
\]

The condition \((ng, h) = h f_x \) for \( n \) now reads

\[
\left( \prod_{j=1}^{k} p_{\alpha_j}^{l_j} \right) n = \frac{1}{f_x} \prod_{j=1}^{k} p_{\alpha_j}^{l_j} n,
\]

and so all such \( n \) are given by

\[
u = \left( \prod_{j=1}^{k} p_{\alpha_j}^{l_j} \right) m_x = \frac{h m_x}{f_x g_x}
\]

where \( m_x \) runs through integers prime to \( h \), i.e. to \( f_x \). Inserting (12) into (6) and using (8) we get

\[
V_{f_x} = \frac{1}{f_x} \left( \frac{h}{f_x} \right) T(f_x) \sum_{n=1}^{\infty} \frac{1}{n} \left( \frac{C_{\alpha}(ng) n}{f_x} \right) \text{ if } g \not\mid f_x,
\]

where \( \sum_{n=1}^{\infty} \) denotes the sum over integers given by (12). We have

\[
X_x \left( \frac{ng}{f_x} \right) = X_x(m_x) X_x \left( \frac{h y}{g f_x} \right)
\]

By (9) and (10) we may restrict the sum only to those \( n \) for which

\[
\left( \frac{ng}{f_x} \right) = \left( \frac{f}{f_x} \right) = \prod_{j=1}^{k} p_{\alpha_j}^{l_j} \quad (\alpha_j = 0 \text{ or } 1, j = i+1, \ldots, k).
\]

Observing further that for those \( f \) for which \( p_j / g, \eta_j \) has necessarily to be zero, the summation may further be restricted only to those \( n \) for which

\[
\nu = \left( \prod_{j=1}^{k} p_{\alpha_j}^{l_j-\eta_j} \right) m_x \frac{h}{f_x g_x}
\]

where \( m_x \) is coprime to \( f_x \prod_{j=1}^{k} p_{\alpha_j}^{l_j} = f_x k_1 \), say. Hence the summation may be split up into \( 2^{-l+\infty} \) parts (where \( \mu \) is the total number of prime factors of \( g_x \) each with a different choice of the numbers \( \eta_j \) \( j \geq l+1, \eta_j < n_j \)). With a particular choice of the numbers \( \eta_j \) we have in case \( g \mid f_x \) the contribution

\[
\sum_{n=1}^{\infty} X_x \left( \frac{ng}{f_x} \right) C_{\alpha}(ng) n^{-1}
\]
to the sum over $n$ in (13); here the sum is over all numbers $n$ of the form (15). We have

$$
X_{\alpha} \left( \frac{mgf_{m}}{f} \right) = X_{\alpha}(m) X_{\alpha} \left( \frac{gh_{k}}{f_{k}} \right) X_{\alpha} \left( \frac{h_{k}}{g_{k}} \right) \prod_{p|\alpha, n^{2}} X_{\alpha}(p^{n} p^{'-1}),
$$

(17)

$$
\sigma \left( \frac{g, h}{b, a} \right) X_{\alpha}(a) = \prod_{p|\alpha, n^{2}} \left( \frac{\sigma(p \cdot p')}{\sigma(p)} \right) \prod_{p|\alpha, n^{2}} \left[ \left( \frac{\sigma(p \cdot p')}{\sigma(p)} \right)^{-1} - \left( \frac{\sigma(p \cdot p')}{\sigma(p)} \right) \right] = \sigma \left( \frac{f}{h} \right) \prod_{p|\alpha, n^{2}} \left( 1 - \frac{1}{p} \right) ^{-1} \times \prod_{p|\alpha, n^{2}} \frac{X_{\alpha}(p)}{m},
$$

Hence if $g[f]/f$, we have, for $V_{\alpha}$ from (13), the expression

$$
-\frac{1}{2} \frac{X_{\alpha}(h_{k})}{g_{k}} \prod_{p|\alpha, n^{2}} \left[ -X_{\alpha}(p) \right] \prod_{p|\alpha, n^{2}} \left( 1 - \frac{1}{p} \right) ^{-1} \times \prod_{p|\alpha, n^{2}} \frac{X_{\alpha}(p)}{m}.
$$

(18)

$$
\Psi_{\alpha}(R) = \Psi_{\alpha}(E) = \sum_{\sigma \in \sigma_{\alpha}} \sigma^{\alpha_{1} + \cdots + \alpha_{n}} \chi_{(\sigma \cdot (a + b)) \cdot c} = \sum_{\sigma \in \sigma_{\alpha}} \sigma^{\alpha_{1} + \cdots + \alpha_{n}} \chi_{(\sigma \cdot (a + b)) \cdot c} \times \prod_{p|\alpha, n^{2}} \left( 1 - \frac{1}{p} \right) ^{-1} \times \prod_{p|\alpha, n^{2}} \frac{X_{\alpha}(p)}{m},
$$

the sum extended over all $(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)$. We then have

(19) $U = \sum_{\sigma \in \sigma_{\alpha}} \psi_{\sigma}(R) = -\frac{1}{2} T(f_{k}) L(1, \alpha) \prod_{p|\alpha, n^{2}} \left( 1 - \frac{\sigma(p \cdot p')}{\sigma(p)} \right) = \prod_{p|\alpha, n^{2}} \left( 1 - \frac{\sigma(p \cdot p')}{\sigma(p)} \right) = \prod_{p|\alpha, n^{2}} \left( 1 - \frac{\sigma(p \cdot p')}{\sigma(p)} \right).$

We now define the function (constructed from (3))

$$
U = \sum_{\sigma \in \sigma_{\alpha}} \psi_{\sigma}(R) = -\frac{1}{2} T(f_{k}) L(1, \alpha) \prod_{p|\alpha, n^{2}} \left( 1 - \frac{\sigma(p \cdot p')}{\sigma(p)} \right) \prod_{p|\alpha, n^{2}} \left( 1 - \frac{\sigma(p \cdot p')}{\sigma(p)} \right)
$$

(20) $\sum_{(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)} \chi_{(\sigma \cdot (a + b)) \cdot c} = \sum_{(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)} \chi_{(\sigma \cdot (a + b)) \cdot c} = \sum_{(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)} \chi_{(\sigma \cdot (a + b)) \cdot c}$

because all our calculations fail when all the $e$'s are equal to 1 (and to avoid this trouble) we could have taken continuous invariants

$$
\psi_{\sigma}(R, \alpha) = \frac{1}{2} \sum_{\sigma \in \sigma_{\alpha}} \sigma^{\alpha_{1} + \cdots + \alpha_{n}} \chi_{(\sigma \cdot (a + b)) \cdot c} = \frac{1}{2} \sum_{\sigma \in \sigma_{\alpha}} \sigma^{\alpha_{1} + \cdots + \alpha_{n}} \chi_{(\sigma \cdot (a + b)) \cdot c}
$$

and come to the conclusion that the term for which $f = g$ is zero.

Next we prove

Lemma 3. Let $\alpha$ be a primitive $f$-th root of unity and $w_{\alpha}$ as defined in (1). Then for a non-principal character $\chi$ of $\mathbb{R}_{F}$,

$$
\sum_{(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)} \psi_{\sigma}(R) = \frac{1}{2} \sum_{(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)} \psi_{\sigma}(R) = \frac{1}{2} \sum_{(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)} \psi_{\sigma}(R)
$$

where $\phi_{\alpha}$ is a certain root of unity depending on $\alpha$ and $\chi$.

Proof. Let $\alpha = \sigma^{\alpha_{1} \alpha_{2} \cdots \alpha_{n}} \cdot (b, f) = 1$. Then $\log \left| 1 - \frac{\sigma^{\alpha_{1} \alpha_{2} \cdots \alpha_{n}} \cdot (b, f)}{\sigma^{\alpha_{1} \alpha_{2} \cdots \alpha_{n}} \cdot (b, f)} \right| = \psi_{\chi}(R_{\alpha})$ where $R_{\alpha}$ is the class of $b$. Hence

$$
\sum_{(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)} \psi_{\sigma}(R) = \sum_{(a_{1}, a_{2}, \ldots, a_{n}) \neq (1, 1, \ldots, 1)} \psi_{\sigma}(R) = \chi_{(\sigma \cdot (a + b)) \cdot c} \psi_{\chi}(R_{\alpha}) = \chi(R_{\alpha}) V_{R_{\alpha}}
$$

and this proves Lemma 3.
§ 3. We now prove Theorems 1 and 2 stated in § 1.

Proof of Theorem 2. Let \( \psi \) be the real nonprincipal character mod \( q \) for which \( \psi(-1) = 1 \). We extend it to a character \( \chi \) of \( \mathbb{Z}_q \) in a natural way (since \( \mathbb{Z}_q \) is a quotient of \( \mathbb{Z} \)). For this character \( \chi \), Lemma 3 at once gives

\[
\prod_{(a) = 1, 1 \leq a < q} \psi \left( \frac{a^\theta}{a^\eta} \right) = 1
\]

whenever be the primitive root \( a \) with which we start. Hence the unit

\[
\prod_{(a) = 1, 1 \leq a < q} a^{\psi(r_{a})^{\eta}}
\]

is a root of unity.

Proof of Theorem 1. Denote the elements of \( \mathbb{Z}_q \) by \( E_1, E_2, E_3, \ldots \), \( E_q \) being the unit element. Let \( \psi(E) = \prod_{t \leq q} (1 - \alpha_t^{E_{t1}^{E_{t2} \cdots E_{tn}^{E_{tn+1}}}}) \), the product being extended over all \( k \)-tuples except \((1, 1, \ldots, 1)\), and \( r \) being a representative of \( E \). Now we have \( \psi = \psi(E_1) = \psi(E) \) and if the units \( \psi \) are dependent, say \( \prod_{(a) = 1, 1 \leq a < q} a^{\psi(a)} = 1 \), on applying the isomorphisms \( E \mapsto E^{-1} \) we have

\[
\prod_{(a) = 1, 1 \leq a < q} a^{\psi(E_{a}^{E^{-1}})} = 1 \quad (j = 0, 1, 2, \ldots)
\]

i.e.

\[
\sum_{a \neq 0} b_i \log \frac{\theta(E_i E^{-1})}{\theta(E_{-i})} = 0 \quad (j = 0, 1, 2, \ldots)
\]

where we have changed \( a \) to \( i \) and replaced the expression for \( \psi \) in terms of \( \psi(E) \). Since \( b_i \) are not all zero, we have

\[
\text{determinant} \left| \psi(E_i E^{-1}) \right| = 0.
\]

But by Dedekind-Frobenius group determinant formula the determinant on the left is nothing but \( \sum_{E} x(E) \log(\theta(E)) = \sum_{E} x(E) \psi(E) \) by (19) and this contradicts (22). Hence Theorem 1 is proved.

References