A NOTE ON UNITS IN SUPER-CYCLIC FIELDS

BY H. S. VANDIVER

1. Comparison of Two Known Results Concerning Cyclotomic Units. Kummer* first showed that if

\[ \xi = e^{2i\pi / l} \]

with \( l \) an odd prime, and if \( \eta \) is a unit in \( k(\xi) \) such that

\[ \eta \equiv a \pmod{\mathfrak{l}}, \]

where \( a \) is a rational integer, then

\[ \eta = \rho^l, \]

where \( \rho \) is in \( k(\xi) \), provided none of the Bernoulli numbers

\[ B_1, B_2, \ldots, B_d, \quad (d = (l - 3)/2), \]

is divisible by \( l \). Kummer's proof of this depended on the fact that under the assumptions mentioned there exists an integer \( c \) prime to \( l \) such that

\[ \eta^c = E_1^{a_1}E_2^{a_2} \cdots E_d^{a_d}. \]

Here

\[ E_n = \prod_{r=0}^{d} \epsilon(\xi^r)^{-2in}, \]

\[ \epsilon = \left( \frac{(1 - \xi^r)(1 - \xi^{-r})}{(1 - \xi)(1 - \xi^{-1})} \right)^{1/2}. \]

From this we obtain an identity in an indeterminate \( x \) by adding a certain multiple of

\[ \frac{x^l - 1}{x - 1}. \]

Setting \( x = e^r \), taking logarithms and differentiating \( 2n \) times, \((n = 1, 2, \ldots, d)\), we find, using relations in another paper,†

† Transactions of this Society, vol. 31 (1929), pp. 619–620, relations (4) and (5).
which is the result.

By using a quite different method, Hilbert\* gave proof that if
\[ \eta \equiv 1 \pmod{\lambda}, \quad \lambda = 1 - \zeta \]
and \( k(\zeta) \) is a regular field, then \( \eta = p^\ell \).

A field \( k(\zeta) \) is said to be regular if and only if \( l \) is prime to its class number. It is known that this condition is equivalent to the statement that the set \( (1) \) contains no numbers divisible by \( l \).

Comparing the different forms of \( \eta \) in the two statements of Kummer and Hilbert, we note that if \( \eta = a + \theta l \), where \( \theta \) is in \( k(\zeta) \), we may write \( \theta = b + \lambda \theta_1 \) where \( b \) is rational, and obtain \( \eta = a + lb + \lambda \omega \). Now \( (a + lb) \) is not necessarily equal to 1, so the two forms are not the same.

Hilbert's proof of the result as stated by him depended on his theory of class-fields. It was reproduced by Landau\† who commented on the great length of the proof and the complexity of one of the lemmas involved, that is, the existence of a system of relative fundamental units in a Kummer field.

In the present paper I shall consider further the principles involved in the demonstration of this theorem and give an extension of it involving super-cyclic fields. I shall also consider analogous questions in connection with the cyclotomic field which is not regular. The proofs, in the main, will be merely sketched.

2. A Theorem Concerning Primary Units in Super-Cyclic Fields. Furtwängler\‡ gave the result that if \( K \) contains the field \( k(\zeta) \) and if the class number of \( K \) be \( H = \ell h q, \) \( q \not\equiv 0 \pmod{l} \), and a basis for the Abelian group formed by the \( q \)th powers of the ideal classes of \( K \) be \( C_1, C_2, \cdots, C_e \), then there exists a basis for the singular primary numbers in \( K, \omega_1, \omega_2, \cdots, \omega_e \), such that any singular primary number in \( K \) may be written in the form \( \omega_1^\alpha \omega_2^\alpha \cdots \omega_e^\alpha \). Also, corresponding to any singular primary number belonging to the basis, there is an ideal class \( C \) belonging to the basis of the so-called irregular class group.

\* Werke, vol. 1, p. 287.
The above shows that if we have the primary units in $K$, that is, a unit $\eta$ such that

$$
\eta \equiv \gamma^l \pmod{\lambda^l},
$$

it follows that if the field $K$ has a class number which is prime to $l$, then no $C$ exists and therefore no singular primary number. Hence $\eta$ is an $l$th power in $K$.

The above argument can be put in somewhat different form by employing the law of reciprocity

$$
\left\{ \frac{\alpha}{\beta} \right\} = \left\{ \frac{\beta}{\alpha} \right\},
$$

where each member denotes an $l$th power character in $K$ and $\alpha$ is a primary integer in $K$. As a special case of this we have*

$$
\left\{ \frac{\omega}{\beta} \right\} = 1,
$$

where $\omega$ is a singular primary number in $K$. Let $\beta = p^h$, where $p$ is a prime ideal in $K$ and $h$ is the class number of $K$; then the above relation gives

$$
\left\{ \frac{\omega}{p} \right\} = 1
$$

for any $p$ in $K$ prime to $l$. From this it follows† that $\omega$ is the $l$th power of the number in $K$; whence $\eta$ is also an $l$th power. We may then state the following theorem.


If an algebraic field $K$ contains a cyclotomic field $k(\xi)$, $\xi = e^{2\pi i/l}$, and $\eta$ is a primary unit in the former field, then $\eta$ is the $l$th power of a unit in $K$ provided the class number of $K$ is prime to $l$.

We now observe that super-cyclic fields exist in which the class number is prime to $l$. Such a field is a Kummer field defined by $\xi$ and $(\sigma)^{1/l}$, where $\sigma$ is a unit in $k(\xi)$ which is not primary. The class number of such a field is prime to $l$, provided‡ the class number of $k(\xi)$ is prime to $l$. 
3. The Unit $E_n$ not an $l$th Power. We now consider the units in $k(\zeta)$ when the class number of this field is not prime to $l$. In this case the integer $c$ in (2) might be divisible by $l$; in particular one of the $E$'s may be the $l$th power of the unit in $k(\zeta)$.

We shall now show that if
\[ r^{l-1} \not\equiv 1 \pmod{l^2}, \]
then
\[ E_n \not\equiv \rho^n, \]
where $\rho$ is in $k(\zeta)$. Assuming an equality of this type, and using the same method by which, in a previous paper by the writer, the relations (3) and (3a) were handled,* we obtain the following identity in $e^v$:
\[ E_n^{l-1}(e^v) = (\rho(e^v))^\mu(l-1) + X(e^v)(e^{vl} - 1) + lj \frac{e^{vl} - 1}{e^v - 1}, \]

where $j$ is a rational integer and $X(e^v)$ is a polynomial in $e^v$ with rational integral coefficients. In this expression, taking logarithms and differentiating $2l$ times, we obtain, using relations (4) and (4a) of the paper last mentioned (p. 620) for $n \neq 1$,
\[ \frac{r^{(l-1)(l^n)} - 1}{r^{2l-2n} - 1} \frac{B_l}{2l} (r^{2l} - 1) \equiv 0 \pmod{l^2}. \]

Now, since
\[ r^{l-1} \not\equiv 1 \pmod{l^2}, \]
then
\[ r^{(l-1)(l^n)} - 1 \]
is divisible by $l$ but not by $l^2$, which gives a contradiction since $(r^{2l} - 1)$ and $B_l/l$ are prime to $l$.

THE UNIVERSITY OF TEXAS