Cyclotomic units and Hilbert's Satz 90

by

Morris Newman (Santa Barbara, Calif.)

Introduction. The purpose of this paper is to derive a formula for any unit of \( K_n = \mathbb{Q}(\zeta_n) \), where \( \zeta_n \) is a primitive \( n \)th root of unity, whenever the Galois group of \( K_n \) over \( \mathbb{Q} \) is cyclic. The formula is in the spirit of Hilbert's Satz 90 ([1], pp. 149-150), which states that such a unit \( \alpha \) is of the form \( \beta'/\beta \), where \( \beta, \beta' \) are conjugate integers, and supplies an answer to the question of when \( \beta \) itself may be taken to be a unit. For simplicity, the details will be presented only for the case when \( n = p \), a prime > 3. Only trivial modifications are required for the more general case.

Accordingly, let \( p \) be a prime > 3. Let \( \zeta = \zeta_p \) be a primitive \( p \)th root of unity. Let \( g \) be a fixed primitive root modulo \( p \). If \( a = a(\zeta) \) is any integer of \( K_p \), then \( a(1) \) is well-defined modulo \( p \), since \( \Phi_p(1) = p \), where \( \Phi_p(x) = (x^p - 1)/(x - 1) \) is the cyclotomic polynomial of level \( p \). The integer \( 1 - \zeta \) is a prime of norm \( p \), and \( p \) is the only rational prime with ramification.

The Theorem and its proof. The theorem we wish to prove is the following:

Theorem. Let \( a \) be any unit of \( K_p \). Then

\[
(1) \quad \alpha = \left( \frac{1 - \zeta^r}{1 - \zeta} \right) \frac{\beta(\zeta^p)}{\beta(\zeta)},
\]

where the rational integer \( r \) satisfies \( 0 \leq r \leq p - 2 \), \( \beta \) is again a unit of \( K_p \), and the representation is unique, apart from the fact that \( \beta \) may be replaced by \( -\beta \).

We first prove two lemmas.

Lemma 1. Let \( a \) be an integer of \( K_p \), normalized so that the polynomial \( a(x) \) is of degree \( \leq p - 2 \), and such that

* The preparation of this paper was supported by NSF Grant MCS76-8293.
(2) \( a(t^i) = e \alpha(t) \), where \( e \) is a unit of \( K_p \) and \( t \) is a primitive root modulo \( p \),

(3) \( (\alpha(1), \eta) = 1 \),

(4) the content of the polynomial \( \alpha(x) \) is \( 1 \).

Then \( \alpha \) is a unit of \( K_p \).

Proof. Suppose the contrary. Let \( P \) be a prime ideal divisor of \( \alpha(t) \). Then the conjugate ideal \( P^{\sigma(x)} \) (obtained by applying the automorphism \( \zeta \to \zeta^p \)) is also a prime ideal, and must be a divisor of \( \alpha(t^i) \), and so also of \( \alpha(t) \), because of (3). It follows that \( \alpha(t) \) is divisible by every conjugate of \( P \), since \( t \) is a primitive root modulo \( p \), and \( \zeta \to \zeta^p \) is therefore a generating automorphism of the Galois group.

Now \( (\alpha(t), 1-\zeta) = (\alpha(1), 1-\zeta) = 1 \), since \( 1-\zeta \) divides \( \eta \) and (3) holds. Thus \( P \neq (1-\zeta) \).

We have that \( N(P') = q^s \), where \( N(P) \) is the norm of \( P \), \( q \) is a prime, and \( s \) is the degree of \( P \). Then \( q \neq \eta \), and the principal ideal \( (\eta) \) must be the product of the distinct conjugates of \( P \). But this implies that \( q \) divides \( \alpha(t) \), which is in contradiction with (4). This completes the proof.

For the second lemma, we define the special units

(5) \[ \eta_h = \eta(\zeta^h) = \frac{1-t^{\sigma^h}}{1-t^{\zeta^{h-1}}} \]

Then

(6) \[ \eta_{h-1}(\zeta^p) = \eta_h(\zeta) \]

We have

**Lemma 2. Let \( r \) be any positive integer. Then**

(7) \[ \frac{1-t^{\sigma^r}}{1-t^{\zeta}} = \tau(\zeta)^r \frac{1-t^{\zeta^r}}{1-t^{\zeta}} \]

where

\[ \tau(\zeta) = \prod_{i=2}^{r} \prod_{k=2}^{r} \frac{\eta_k}{\eta_{k-1}} = \prod_{i=2}^{r} \prod_{k=2}^{r} \frac{\eta_{k-1}(\zeta^p)}{\eta_{k-1}(\zeta)} \]

is clearly of the form \( \beta(\zeta^r)/\beta(\zeta) \), \( \beta \) a unit of \( K_p \). Furthermore

\[ \left( \frac{1-t^{\sigma^r}}{1-t^{\zeta}} \right)^{r-1} = \tau(\zeta)^{-1} \]

is also of this form.


**Proof.** We have

\[ \prod_{i=2}^{r} \frac{\eta_h}{\eta_{h-1}} = \frac{1-t^{\sigma^r}}{1-t^{\eta_h}} \]

\[ \tau(\zeta) = \prod_{i=2}^{r} \frac{1-t^{\eta_i}}{1-t^{\zeta}} \frac{1-t^{\zeta^r}}{1-t^{\zeta}} \]

from which formula (7) follows. Formula (6) and the fact that \( \frac{1-t^{\sigma^r}}{1-t^{\zeta}} = 1 \) now imply the remainder of the lemma, and the proof is concluded.

We are now prepared to prove the theorem. Let \( \alpha \) be any unit of \( K_p \). Then \( (\alpha(1), \eta) = 1 \) (since otherwise \( 1-\zeta \) would divide \( \alpha \). Thus \( \alpha(1) \equiv g^r \mod p \), for some \( r \) with \( 0 \leq r < p-2 \). Write

\[ \alpha = \left( \frac{1-t^{\sigma^r}}{1-t^{\zeta}} \right)^{r-1} \beta \]

where \( \beta \) is also a unit of \( K_p \), and \( \beta(1) \) must satisfy

\[ \beta(1) = g \mod p \]

By Hilbert's Satz 90, we may write

\[ \beta(z) = \gamma(\zeta^r)/\gamma(\zeta) \]

where \( \gamma(\zeta) \) is an integer of \( K_p \). The theorem also tells us that \( t \) may be taken as a primitive root modulo \( p \), but we do not assume this, since it develops naturally in the proof.

We may write

\[ \gamma(\zeta) = (1-\zeta)^s \delta(\zeta) \]

where \( s \) is a nonnegative integer and \( \delta(\zeta) = 1 \), so that \( \delta(1, \eta) = 1 \). Furthermore, we may assume that \( \deg \delta(z) \leq p-2 \), and that the content of \( \delta(z) \) is \( 1 \), since

(8) \[ \beta(\zeta) = \left( \frac{1-t^{\sigma^r}}{1-t^{\zeta}} \right)^{r-1} \frac{\delta(\zeta^r)}{\delta(\zeta)} \]

and the greatest common divisor of the coefficients of \( \delta(z) \) may be cancelled out in (8). Now (8) implies that

\[ \beta(1) \equiv t^r \mod p \]

Since \( \beta(1) \equiv g \mod p \), \( t \) must itself be a primitive root modulo \( p \). Thus Lemma 1 implies that \( \delta(\zeta) \) is a unit of \( K_p \).
Since $\ell$ is a primitive root modulo $p$, we may write $\ell \equiv g^a \mod p$, where $1 \leq a \leq p-2$ (in fact, $(a, p-1) = 1$). Then
\[
\frac{\delta(\ell^a)}{\delta(\ell)} = \frac{\delta(\ell^a) \delta(\ell^a \ell^a) \ldots \delta(\ell^{a(a-1)})}{\delta(\ell) \delta(\ell^2) \ldots \delta(\ell^{a-1})}.
\]
Put
\[s(\ell) = \delta(\ell) \delta(\ell^2) \ldots \delta(\ell^{a-1}).\]
Then $s(\ell)$ is also a unit of $K_p$, and
\[(9)\quad \frac{\delta(\ell)}{\delta(\ell)} = \frac{s(\ell^a)}{s(\ell)}.
\]
Thus we have that
\[(10)\quad a = \left(\frac{1-\ell^2}{1-\ell}\right)^{-1} \left(\frac{1-\ell^{a^2}}{1-\ell}\right) \frac{s(\ell^a)}{s(\ell)}.
\]
Now Lemma 2 implies that
\[(11)\quad \frac{1-\ell^a}{1-\ell} = \frac{\ell(\ell^a)}{s(\ell)} \left(\frac{1-\ell^a}{1-\ell}\right),
\]
where $\ell(\ell^a)$ is a unit of $K_p$. Thus (10) and (11) together imply that
\[a = \left(\frac{1-\ell^2}{1-\ell}\right)^{-1+as} \frac{\ell(\ell^a)}{\ell(\ell^a)} \frac{s(\ell^a)}{s(\ell)}.
\]
so that $a$ is in the form required, except possibly for the exponent $r-1+sa$. But Lemma 2 implies that this may be reduced modulo $p-1$. This completes the proof of the first part of the theorem. To establish the uniqueness, suppose that there are two representations
\[a = \left(\frac{1-\ell^2}{1-\ell}\right)^{r_1} \beta_1(\ell), \quad b = \left(\frac{1-\ell^2}{1-\ell}\right)^{r_2} \beta_2(\ell),
\]
where $0 \leq r_1, r_2 < p-2$ and $\beta_1, \beta_2$ are units of $K_p.$ Modulo $1-\ell$ we get
\[g^{r_1} \equiv g^{r_2} \mod 1-\ell,
\]
so that
\[g^{r_1} \equiv g^{r_2} \mod p.
\]
This implies that $r_1 \equiv r_2 \mod p-1$, so that $r_1 = r_2$. Thus
\[\frac{\beta_1(\ell^a)}{\beta_1(\ell)} = \frac{\beta_2(\ell^a)}{\beta_2(\ell)}, \quad \frac{\beta_1(\ell)}{\beta_1(\ell)} = \frac{\beta_2(\ell)}{\beta_2(\ell)}.
\]
The unit $\beta_1/\beta_2$ is thus invariant with respect to the generating automorphism $\ell \rightarrow \ell^a$, and so must be rational, and hence can only be $\pm 1$. This completes the proof of the second part of the theorem.

Conclusions. A nice group-theoretic interpretation can be given to these results. For a fixed primitive root $g$ modulo $p$, the set of units of the form $\beta(\ell^a)/\beta(\ell)$, $\beta$ a unit, clearly forms a multiplicative subgroup $E_\beta$ of the full group of units $E$. What has been shown is that $E_\beta$ is of index $p-1$ in $E$, and that the quotient group $E/E_\beta$ is cyclic, with generator $\frac{1-\ell^a}{1-\ell} E_\beta$.

An interesting corollary which follows directly supplies an answer to the question of when a unit of $K_p$ may be written as the quotient of conjugate units:

**Corollary.** The unit $a = a(\ell)$ of $K_p$ may be written as the quotient of conjugate units if and only if $a(1) \equiv 1 \mod p$.

It is only necessary to note that if $a$ is a unit and $t$ any integer, then another unit $e$ exists such that
\[\frac{\delta(\ell^a)}{\delta(\ell)} = \frac{s(\ell^a)}{s(\ell)},
\]
the argument being identical with the one leading to formula (9).

References