ACTA ARITHMETICA
XLI (1982)

Cyclotomic units and Hilbert's Satz 90*

by

MORIS NEWMAN (Santa Barbara, Calif.)

Introduction. The purpose of this paper is to derive a formula for any unit of $K_n = Q(\zeta_n)$, where ζ_n is a primitive nth root of unity, whenever the Galois group of K_n over Q is cyclic. The formula is in the spirit of Hilbert's Satz 90 ([1], pp. 149–150), which states that such a unit α is of the form β'/β, where β, β' are conjugate integers, and supplies an answer to the question of when β 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 pth root of unity. Let g be a fixed primitive root modulo p. If $\alpha = \alpha(\zeta)$ is any integer of K_p, then $\alpha(1)$ 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 α be any unit of K_p. Then*

$$\alpha = \left(\frac{1-\zeta^g}{1-\zeta}\right)^r \frac{\beta(\zeta^g)}{\beta(\zeta)}, \tag{1}$$

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

We first prove two lemmas.

LEMMA 1. *Let α be an integer of K_p, normalized so that the polynomial $\alpha(x)$ is of degree $\leqslant p-2$, and such that*

* The preparation of this paper was supported by NSF Grant MCS76-8293.

(2) $\alpha(\zeta^t) = \varepsilon\alpha(\zeta)$, *where ε is a unit of K_p and t is a primitive root modulo p,*

(3) $$\big(\alpha(1), p\big) = 1,$$

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

Then α is a unit of K_p.

Proof. Suppose the contrary. Let P be a prime ideal divisor of $\alpha(\zeta)$. Then the conjugate ideal $P^{(t)}$ (obtained by applying the automorphism $\zeta \to \zeta^t$) is also a prime ideal, and must be a divisor of $\alpha(\zeta^t)$, and so also of $\alpha(\zeta)$, because of (2). It follows that $\alpha(\zeta)$ is divisible by every conjugate of P, since t is a primitive root modulo p, and $\zeta \to \zeta^t$ is therefore a generating automorphism of the Galois group.

Now $\big(\alpha(\zeta), 1-\zeta\big) = \big(\alpha(1), 1-\zeta\big) = (1)$, since $1-\zeta$ divides p 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 $q \neq p$, and the principal ideal (q) must be the product of the distinct conjugates of P. But this implies that q divides $\alpha(\zeta)$, which is in contradiction with (4). This completes the proof.

For the second lemma, we define the special units

(5) $$\eta_k = \eta\ (\zeta) = \frac{1-\zeta^{g^k}}{1-\zeta^{g^{k-1}}}.$$

Then

(6) $$\eta_{k-1}(\zeta^g) = \eta_k(\zeta).$$

We have

LEMMA 2. *Let r be any positive integer. Then*

(7) $$\frac{1-\zeta^{g^r}}{1-\zeta} = \tau(\zeta)\left(\frac{1-\zeta^g}{1-\zeta}\right)^r,$$

where

$$\tau(\zeta) = \prod_{l=2}^{r}\prod_{k=2}^{l}\frac{\eta_k}{\eta_{k-1}} = \prod_{l=2}^{r}\prod_{k=2}^{l}\frac{\eta_{k-1}(\zeta^g)}{\eta_{k-1}(\zeta)}$$

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

$$\left(\frac{1-\zeta^g}{1-\zeta}\right)^{p-1} = \tau(\zeta)^{-1}$$

is also of this form.

Proof. We have

$$\prod_{k=2}^{l}\frac{\eta_k}{\eta_{k-1}} = \frac{\eta_l}{\eta_1} = \frac{1-\zeta^{g^l}}{1-\zeta^{g^{l-1}}}\cdot\frac{1-\zeta}{1-\zeta^g},$$

$$\tau(\zeta) = \prod_{l=2}^{r}\frac{\eta_l}{\eta_1} = \frac{1-\zeta^{g^r}}{1-\zeta}\left(\frac{1-\zeta}{1-\zeta^g}\right)^r,$$

from which formula (7) follows. Formula (6) and the fact that $\dfrac{1-\zeta^{g^{p-1}}}{1-\zeta} = 1$ now imply the remainder of the lemma, and the proof is concluded.

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

$$\alpha = \left(\frac{1-\zeta^g}{1-\zeta}\right)^{r-1}\beta,$$

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

$$\beta(1) \equiv g \bmod p.$$

By Hilbert's Satz 90, we may write

$$\beta(\zeta) = \gamma(\zeta^t)/\gamma(\zeta),$$

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 $\big(\delta(\zeta), 1-\zeta\big) = 1$, so that $\big(\delta(1), p\big) = 1$. Furthermore, we may assume that $\deg\delta(x) \leqslant p-2$, and that the content of $\delta(x)$ is 1, since

(8) $$\beta(\zeta) = \left(\frac{1-\zeta^t}{1-\zeta}\right)^s\frac{\delta(\zeta^t)}{\delta(\zeta)},$$

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

$$\beta(1) \equiv t^s \bmod p.$$

Since $\beta(1) \equiv g \bmod p$, t must itself be a primitive root modulo p. Thus Lemma 1 implies that $\delta(\zeta)$ is a unit of K_p.

Since t is a primitive root modulo p, we may write $t \equiv g^a \bmod p$, where $1 \leqslant a \leqslant p-2$ (in fact, $(a, p-1) = 1$). Then

$$\frac{\delta(\zeta^t)}{\delta(\zeta)} = \frac{\delta(\zeta^{g^a})}{\delta(\zeta)} = \frac{\delta(\zeta^g)\delta(\zeta^{g^2})\ldots\delta(\zeta^{g^a})}{\delta(\zeta)\delta(\zeta^g)\ldots\delta(\zeta^{g^{a-1}})}.$$

Put

$$\varepsilon(\zeta) = \delta(\zeta)\delta(\zeta^g)\ldots\delta(\zeta^{g^{a-1}}).$$

Then $\varepsilon(\zeta)$ is also a unit of K_p, and

$$\frac{\delta(\zeta^t)}{\delta(\zeta)} = \frac{\varepsilon(\zeta^g)}{\varepsilon(\zeta)}. \tag{9}$$

Thus we have that

$$\alpha = \left(\frac{1-\zeta^g}{1-\zeta}\right)^{r-1}\left(\frac{1-\zeta^{g^a}}{1-\zeta}\right)^{s}\frac{\varepsilon(\zeta^g)}{\varepsilon(\zeta)}. \tag{10}$$

Now Lemma 2 implies that

$$\frac{1-\zeta^{g^a}}{1-\zeta} = \frac{\xi(\zeta^g)}{\xi(\zeta)}\left(\frac{1-\zeta^g}{1-\zeta}\right)^a, \tag{11}$$

where $\xi(\zeta)$ is a unit of K_p. Thus (10) and (11) together imply that

$$\alpha = \left(\frac{1-\zeta^g}{1-\zeta}\right)^{r-1+sa}\frac{\xi(\zeta^g)^s\varepsilon(\zeta^g)}{\xi(\zeta)^s\varepsilon(\zeta)},$$

so that α 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 extablish the uniqueness, suppose that there are two representations

$$\alpha = \left(\frac{1-\zeta^g}{1-\zeta}\right)^{r_1}\frac{\beta_1(\zeta^g)}{\beta_1(\zeta)} = \left(\frac{1-\zeta^g}{1-\zeta}\right)^{r_2}\frac{\beta_2(\zeta^g)}{\beta_2(\zeta)},$$

where $0 \leqslant r_1, r_2 \leqslant p-2$ and β_1, β_2 are units of K_p. Modulo $1-\zeta$ we get

$$g^{r_1} \equiv g^{r_2} \bmod 1-\zeta,$$

so that

$$g^{r_1} \equiv g^{r_2} \bmod p.$$

This implies that $r_1 \equiv r_2 \bmod p-1$, so that $r_1 = r_2$. Thus

$$\frac{\beta_1(\zeta^g)}{\beta_1(\zeta)} = \frac{\beta_2(\zeta^g)}{\beta_2(\zeta)}, \quad \frac{\beta_2(\zeta^g)}{\beta_1(\zeta^g)} = \frac{\beta_2(\zeta)}{\beta_1(\zeta)}.$$

The unit β_2/β_1 is thus invariant with respect to the generating automorphism $\zeta \to \zeta^g$, and so must be rational, and hence can only be ± 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 $\beta(\zeta^g)/\beta(\zeta)$, β a unit, clearly forms a multiplicative subgroup E_g of the full group of units E. What has been shown is that E_g is of index $p-1$ in E, and that the quotient group E/E_g is cyclic, with generator $\frac{1-\zeta^g}{1-\zeta}E_g$.

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 $\alpha = \alpha(\zeta)$ of K_p may be written as the quotient of conjugate units if and only if*

$$\alpha(1) \equiv 1 \bmod p.$$

It is only necessary to note that if δ is a unit and t any integer, then another unit ε exists such that

$$\frac{\delta(\zeta^t)}{\delta(\zeta)} = \frac{\varepsilon(\zeta^g)}{\varepsilon(\zeta)},$$

the argument being identical with the one leading to formula (9).

References

[1] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jber. Deutsch. Math.-Verein. 4 (1897), pp. 175–546. Reprinted in the first volume of Hilbert's collected works, Springer 1932.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA
Santa Barbara, California, USA

Received on 21. 10. 1980 (1227)