Pusan Kyŏngnam Math. J. 10(1994), No. 1, pp. 203-209

ON A CONVRETE EXAMPLE OF HILBERT THEOREM 90

EUNG SEOP HAN

§1. Introduction

Let p be an odd prime and d be a positive integer with $d \not\equiv 2 \pmod 4$ and $p \equiv 1 \pmod d$. For each $n \geq 0$, let $K_n = \mathbb{Q}(\zeta_{p^{n+1}d})$ is a primitive $p^{n+1}d$-th root of 1. We assume that $\zeta_{p^{n+1}d}$ has been chosen so that $\zeta_{p^{n+1}d}^{p^{m-n}} = \zeta_{p^{n+1}d}$ for each $m \geq n$. Let $G_n = \mathrm{Gal}(K_n/K_0)$. Thus G_n is a cyclic group of order p^n and we fix a generator σ of G_n. Most of our work will be done in those fields.

The Hilbert theorem 90 states as follows : Let K/k be a cyclic extension of degree n with Galois group G. Let σ be a generator of G. Let $\alpha \in K$. Then the norm $N_{K/k}(\alpha)$ is equal to 1 if and only if there exists an element $\beta \in K^\times$ such that $\beta = \alpha^{\sigma-1}$. In the cohomological language, this statement can be put into $H^{-1}(G, K^\times) = 0$.

In this paper, we take a particular element ξ_n in K_n which will be shown to be of norm 1 to K_0 (Theorem 3.1). Thus by Hilbert theorem 90, $\xi_n = \alpha_n^{\sigma-1}$ for some α_n in K_n. The aim of this paper is to examine the nature of this element α_n. Not any of the proofs of Hilbert theorem 90, even though some proofs are constructive, tells what α_n would look like. But since our choice of ξ_n will be very special, we will have additional information on α_n. To be precise, in theorem 3.5, we show that α_n can be chosen to be a p-unit, which means that in the factorzation of the principal ideal (α_n) into a product of prime ideals, only those primes of K_n above p appear. This, hopefully, could provide certain relations among prime ideals of K_n just as the factorization of the Gauss sum into a product of prime ideals is used to prove the Stickelberger theorem.

Received May 6, 1994.

The next section is preliminary. We review cohomology theory very briefly and explain Hilbert Theorem 90 in terms of cohomological language. Structure theorems of the group of units in number fields are also included in the next section. Especially, we put some emphasis on cyclotomic units since they are the ones that we use to find an explicit example of the Hilbert theorem 90 as the title of this paper indicates. The last section deals with our main results. As was already mentioned, we will choose a particular cyclotomic unit ξ_n in K_n whose norm from K_n to K_0 equals 1 and show that $\xi_n = \beta_n^{\sigma-1}$ for some p-unit β_n in K_n.

§2. Preliminary

1. Group Cohomology and Hilbert Theorem 90

Let G be a finite group and A be an abelian group on which G acts. Cohomology theory deals with $H^n(G,A)$ for all integers n and any G-module A. However, since we will use only H^{-1} and H^1, we accept the following formula for H^{-1} and H^1 as definitions. Let ${}_NA = \{a \in A | Na = 0\}$ where $N = \sum_{\sigma\in G}\sigma$. And let IA be the subgroup of A generated by the elements of the from $(\sigma - 1)a$ for $a \in A$ and $\sigma \in G$. Then we define $H^{-1}(G,A) = {}_NA/IA$. For H^1, we need to explain more terminologies. By a crossed homomorphism, we means a map $f : G \to A$ satisfying

$$f(\sigma\tau) = \sigma f(\tau) + f(\sigma), \quad \forall\sigma,\tau \in G.$$

And by a trivial crossed homomorphism, we mean a map $f : G \to A$ satisfying

$$f(\sigma) = (\sigma - 1)a \text{ for some } a \in A.$$

Then clearly any trivial crossed homomorphism is a crossed homomorphism. We define $H^1(G,A)$ be the quotient group of the group of all crossed homomorphisms by the subgroup of all trivial crossed homomorphisms. Namely,

$$\begin{aligned} H^1(G,A) &= \frac{\{\text{crossed homomorphism}\}}{\{\text{trivial crossed homomorphism}\}} \\ &= \frac{\{\text{maps} G \xrightarrow{f} A | f(\sigma\tau) = \sigma f(\tau) + f(\tau) \forall\sigma,\tau \in G\}}{\{\text{maps} G \xrightarrow{f} A | f(\sigma) = (\sigma - 1)a \text{ for some } a \in A\}} \end{aligned}$$

Note that if G is a cylic group and σ is generator of G, then IA is generated by elements of the form $(\sigma^k - 1)a$. But we can write

$$(\sigma^k - 1)a = (\sigma - 1)((\sigma^{k-1} + \cdots + \sigma + 1)a) \in (\sigma - 1)A.$$

Thus we have $IA = (\sigma - 1)A$ and $H^{-1}(G, A) = {}_N A/(\sigma - 1)A$. Below we list some theorems and examples on cohomology groups that we use later.

Theorem 2.1. If G is a finite cyclic group, then $H^i(G, A) = H^{i+2}(G, A)\ \forall i$.
In particular, $H^1(G, A) = H^{-1}(G, A) = {}_N A/(\sigma - 1)A$.

Proof. See Serre [5].

Let H be a normal subgroup of G.Then the canonical projection $G \to G/H$ induces a map $H^i(G/H, A^H) \to H^i(G, A), i \geq 1$, where $A^H = \{a \in A | ha = a \forall h \in H\}$. This induced map is called the inflation map.

Theorem 2.2. The inflation map $H^1(G/H, A^H) \to H^1(G, A)$ is injective.

Proof. See Serre [5].

Example 1(Hilbert Theorem 90). Let K be a Galois extension of a field k and $G = Gal(K/k)$. Then $H^1(G, K^\times) = 0$.

Proof. See Lang[4].

Example 2(Classical version of Hilbert Theorem 90). Let K be a cylic extension of k. Then $H^{-1}(G, K^\times) = 0$. This means that if $\alpha \in K$ satisfies $N_{K/k}(\alpha) = 1$, then $\alpha = \beta^{\sigma-1}$ for some $\beta \in K$,where σ is a generator of G.

Proof. See Lang[4].

2. Units and Cyclotomic Units

Let K be a number field, $\mathcal{O}_K$ be the ring of integers of K, and E_K be the unit group of $\mathcal{O}_K$. We describe the well-known structure theorem of E_K :

Theorem 2.3. E_K is a finitely generated abelian group, which is isomorphic to $W \times \mathbb{Z}^{r_1+r_2-1}$, where W is the group of roots of 1 in K and r_1, r_2 are the number of real and complex embeddings of K into $\mathbb{C}$, respectively. More generally, let S be a finite set of prime ideals of K, and $E_{K,S}$ be the group of S-units in K, then $E_{K,S} = W \times \mathbb{Z}^{r_1+r_2-1+\#S}$.

Proof. See Lang[4].

Now we introduce cyclotomic units. Let $K = \mathbb{Q}(\zeta_n)$, where $n \not\equiv 2(\text{mod } 4)$, and ζ_n is a primitive n-th root of 1. Let V be the multiplicative subgroup of $K^\times$ generated by

$$\{\pm\zeta_n^a\}_{a\in\mathbb{Z}} \text{ and } \{1-\zeta_n^a\}_{a\not\equiv 0(\text{mod } n)}$$

and define $C_K = V \cap E_K$.

C_k is called the group of cyclotomic units of K.

Theorem 2.4(W. Sinnott). $[E_K : C_K] = 2^b h_K^+$, where h_K^+ is the class number of $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, which is maximal real subfield of K, $b = 0$ if $g = 1$, $b = 2^{g-2} + 1 - g$ if $g \geq 2$, and g is the number of distinct prime factors of n.

Proof. See Sinnott [3].

§3. Main Theorems

Let d be a positive integers with $d \not\equiv 2$ (mod 4), and p be an odd prime such that $p \equiv 1$ (mod d), so that the ideal (p) in $\mathbb{Z}$ splits completely in $\mathbb{Q}(\zeta_d)$.

Let $K_n = \mathbb{Q}(\zeta_{p^{n+1}d})$ for $n \geq 0$ and $K_\infty = \cup_{n\geq 0} K_n$. Let $\mathbb{Q}_n$ be the unique subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree p^n over $\mathbb{Q}$ and $\Delta = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. We use the same letter Δ for those Galois groups isomorphic to Gal-$(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. For instance, $\Delta \approx Gal(K_n/\mathbb{Q}_n(\zeta_d))$. Let

$$\zeta_n = \prod_{\gamma\in\Delta} (\zeta_{p^{n+1}}^\gamma - \zeta_d).$$

One can easily check that ζ_n is a cyclotomic unit in K_n. In theorem 3.5, we will show that ξ_n can be expressed as $\xi_n = \beta_n^{\sigma-1}$ for some p-unit β_n in K_n, where σ is a generator of $G_n = Gal(K_n/K_0)$.

But first, in theorem 3.1, we show that $\xi_n = \alpha_n^{\sigma-1}$ for some element α_n in K_n which is not necessarily a p-unit. By a p-unit we mean an element whose prime factors are above p.

Theorem 3.1. There exists $\alpha_n \in K_n$ such that $\xi_n = \alpha_n^{\sigma-1}$.

Proof.

$$\begin{aligned} N_{K_n/K_0}(\xi_n) &= N_{K_n/K_0}(\prod_{\gamma\in\Delta} \zeta_{p^{n+1}}^{\gamma} - \zeta_d) \\ &= \prod_{\gamma\in\Delta} N_{K_n/K_0}(\zeta_{p^{n+1}}^{\gamma} - \zeta_d) \\ &= \prod_{\gamma\in\Delta} (\zeta_{p^{n+1}}^{\gamma} - \zeta_d). \end{aligned}$$

Put $X = \zeta_d$ in the equation $\frac{1-X^p}{1-X} = \prod_{1\leq i\leq p-1}(\zeta_p^i - X) = \prod_{\gamma\in\Delta}(\zeta_p^{\gamma} - X)$. Then we get

$$\frac{1-\zeta_d^p}{1-\zeta_d} = \prod_{\gamma\in\Delta}(\zeta_p^{\gamma} - \zeta_d).$$

Since $p \equiv 1 \pmod{d}$, we have $\zeta_d^p = \zeta_d$. Therefore

$$N_{K_n/K_0}(\xi_n) = \prod_{\gamma\in\Delta}(\zeta_{p^{n+1}}^{\gamma} - \zeta_d) = \frac{1-\zeta_d^p}{1-\zeta_d} = \frac{1-\zeta_d}{1-\zeta_d} = 1.$$

Hence by the Hilbert Theorem 90, there exists $\alpha_n \in K_n$ such taht $\xi_n = \alpha_n^{\sigma-1}$. □

Theorme 3.2(Iwasawa). Let E_n' be the group of p-units in $K_n^{\times}$, where p-unit means a unit at all finite primes except those above p as before. Let $E' = \cup_{n\geq 0} E_n'$. Then $H^1(\Gamma, E') = \varinjlim H^1(G_n, E_n')$ is a finite group, where $\Gamma = Gal(K_\infty/K_0)$, and the direct limit $\varinjlim$ is taken over the inflation maps.

Proof. See Iwasawa [1].

Theorem 3.3(Kim). Let C_n be the group of cyclotomic units in K_n and $C = \cup_{n \geq 0} C_n$. Then $H^1(\Gamma, C) = (\mathbb{Q}_p/\mathbb{Z}_p)^l$, where $l = \frac{1}{2}\varphi(d)$ and φ is the Euler phifunction.

Proof. See Kim [2].

Lemma 3.4. The induced homomorphiam $H^1(\Gamma, C) \to H^1(\Gamma, E')$ by the natural inclusion $C \to E'$ is a zero map.

Proof. Let $f : H^1(\Gamma, C) \to H^1(\Gamma, E')$ be the induced map. By Theorem 3.3, $H^1(\Gamma, C)$ is a p-divisible group. Hence it has no nontrivial finite quotient group. But since the image of f is finite by theorem 3.2, f must be a zero map. □

Theorem 3.5. $\xi_n = \beta_n^{\sigma - 1}$ for some p-unit β_n in K_n.

Proof. Let $g : H^1(G_n, C_n) \to H^1(G_n, E'_n)$ be the induced homomorphism by the natural inclusion $C_n \to E'_n$. Note that we have the following commutative diagram :

$$\begin{array}{ccc} H^1(G_n, C_n) & \xrightarrow{g} & H^1(G_n, E'_n) \\ \mathrm{inf}\downarrow & & \mathrm{inf}\downarrow \\ H^1(\Gamma, C) & \xrightarrow{f} & H^1(\Gamma, E') \end{array}$$

Take x in $H^1(G_n, C_n)$ Since f is a zero map, $f \circ \mathrm{inf}(x) = 0$. By the commutativity of the diagram, $\mathrm{inf} \circ g(x) = 0$. But inflation map is injective as was mentioned in the introduction. Therefore $g(x) = 0$ and thus g is a zero map. Since G_n is cyclic, $\hat{H}^{-1}(G_n, C_n) \cong H^1(G_n, C_n)$ and $\hat{H}^{-1}(G_n, E'_n) \cong H^1(G_n, E'_n)$. Hence $\hat{H}^{-1}(G_n, C_n) \to \hat{H}^{-1}(G_n, E'_n)$ is also a zero map, which means that $\xi_n = \beta_n^{\sigma-1}$ for some $\beta_n \in E'_n$. □

References

[1] K. Iwasawa, On Cohomology groups of units for $\mathbb{Z}_p$-extensions, Amer. J. Math. 105, No.1 (1983), 189-200.

[2] J. M. Kim, Cohomology groups of cyclotomic units, J. Number Theory, Vol. 152, No.2 (1992), 514-519.
[3] S. Lang, Algebra, Addison-Wealey Publishing Company, INC., New York, 1965.
[4] S. Lang, Algebraic Number Theory, Addison-Wealey Publishing Company, INC., New York, 1970.
[5] J. P. Serre, Local fields, G.T.M. 67, Springer-Verlag, 1979.
[6] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. of Math., (2) 108 (1978), 107-134.
[7] L. Washington, Introduction to cyclotomic fields, G.T.M., Springer-Verlag, New York, 1980.

Department of Mathematics
Kyungsung University
Pusan, Korea