A NEW PROOF OF A THEOREM OF KUMMER

WILLIAM J. LEAHEY

Let p be an odd prime and denote by K the field obtained by adjoining the pth roots of unity to Q, the rational numbers. Let ζ be a fixed primitive pth root of unity and set $\pi = 1-\zeta$. The following theorem, due to Kummer, is of importance in proving the nonsolvability of $x^p+y^p=z^p$ in nonzero rational integers for regular primes p.

THEOREM. *Let ϵ be a unit in K and suppose that $\epsilon \equiv a \pmod{\pi^p}$, where a is a rational integer. Then if p is regular there exists $\epsilon_1 \in K$ such that $\epsilon_1^p = \epsilon$.*

The object of this note is to give a new proof of this theorem. The newness lies in the proof of the following theorem, from which Kummer's theorem is easily derived. In the statement of the theorem and throughout the cohomology groups in question are the Tate cohomology groups (see [**3**, Chapter VIII]).

THEOREM. *Let E be a number field and L a cyclic extension of E of odd prime degree. Denote by U the group of units in L and by G the Galois group of L/E. Then $H^{-1}(U, G) \neq 0$.*

PROOF. Let $(E/Q) = r+2s$ where r is the number of real infinite primes of E and s is the number of complex infinite primes. Thus if V is the group of units of E, V is of rank $t=r+s-1$.

Let ϕ be an isomorphism of E into the complex numbers. Then ϕ can be extended in exactly $p=(L/E)$ ways to L. If $\phi(E)$ is real then any extension of ϕ to L must also be real since p is odd. (If not, then the image of L would be of degree 2 over its maximal real subfield implying that p is even.) Thus $(L/Q) = pr+2ps$ and L has pr real infinite primes and ps complex infinite primes. Therefore U is of rank $u=pr+ps-1=pt+p-1$.

According to [**1**, Theorem 10.3] the Herbrand quotient of U is

$$p^{(pt-u)/(p-1)} = \frac{1}{p}.$$

It follows that order $(H^{-1}(U, G)) = p\cdot[\text{order}(H^0(U, G))] > 1$. This completes the proof of the theorem.

The derivation of Kummer's theorem from this theorem is well-

Received by the editors May 21, 1965.

known (e.g. see [2, Theorems 965–969]). It is given here for the sake of completeness.

Proof of Kummer's Theorem. Assume first that $a=1$ and that ϵ is not a pth power in K. Choose θ such that $\theta^p=\epsilon$ and let $L=K(\theta)$. Then L/K is cyclic of degree p. Let σ be a generator of G, the Galois group of L/K. Denote by U the group of units of L.

According to the above theorem $H^{-1}(U, G)\neq 0$ and thus there exists $\eta\in U$ such that $N_{L/K}(\eta)=1$, but η is not of the form $\xi/\sigma(\xi)$ for any $\xi\in U$. By Hilbert's Theorem 90, however, η is of the form $\alpha/\sigma(\alpha)$ for some integer $\alpha\in L$. Choose such an α.

Let $A_L=[\alpha]$, the principal ideal generated by α. Since α and $\sigma(\alpha)$ differ by a unit $\sigma^i(A_L)=A_L$ for $i=0, 1, \cdots, p-1$. Hence

$$A_L^p = \prod_{i=0}^{p-1} \sigma^i(A_L) = [\beta]$$

for some $\beta\in K$.

On the other hand since $\epsilon\equiv 1 \pmod{\pi^p}$ it is easy to check that $(1-\theta)/\pi$ is an integer and that the different of this element is a unit. Hence L/K is unramified and therefore since A_L is invariant under G, A_L arises from an ideal A_K of K.

A_K could not be principal. For if $A_K=[\gamma]$, $\gamma\in K$, then $\alpha=\lambda\cdot\gamma$ for some $\lambda\in U$ and then $\eta=\alpha/\sigma(\alpha)=\lambda/\sigma(\lambda)$, contradicting the choice of η. However, $A_L^p=[\beta]$ with $\beta\in K$. Therefore $A_K^p=[\beta]$. But p was assumed to be regular, i.e., p does not divide the class number of K, and therefore A_K is principal. This contradiction establishes the fact that ϵ must be a pth power in K in the case where $\epsilon\equiv 1 \pmod{\pi^p}$.

Now suppose $\epsilon\equiv a \pmod{\pi^p}$ where a is an arbitrary rational integer. Then if τ is a generator for the Galois group of K/Q, $\tau(\epsilon)\equiv a\equiv\epsilon \pmod{\pi^p}$. Therefore

$$1 = N_{K/Q}(\epsilon) = \prod_{i=0}^{p-2} \tau^i(\epsilon) \equiv \epsilon^{p-1} \pmod{\pi^p}.$$

By the above ϵ^{p-1} is a pth power, say $\epsilon^{p-1}=\epsilon_1^p$. Then $\epsilon =(\epsilon/\epsilon_1)^p$.

References

1. C. Chevalley, *Class field theory*, Nagoya University, Japan, 1953–1954.
2. E. Landau, *Vorlesungen über Zahlentheorie*, Vol. 3, S. Hirzel, Leipzig, 1927.
3. J-P. Serre, *Corps locaux*, Actualités Sci. Indust. No. 1296, Herman, Paris, 1962.

University of Illinois