TOKYO J. MATH.
VOL. 14, NO. 2, 1991

# Kummer's Criterion for Totally Real Number Fields

Masanari KIDA

*Waseda University*

(Communicated by Y. Shimizu)

## 1. Statement of the results.

The classical Kummer's criterion is one of the most interesting results in algebraic number theory, which connects the special values of the Dedekind zeta function with some algebraic objects: the class number and the existence of certain algebraic extensions of cyclotomic fields.

In this paper we prove the complete generalization of Kummer's criterion for totally real fields. Note that a recent work of Wiles on the Iwasawa main conjecture [Wil] gives a "piece-by-piece" description of the criterion.

To state our theorems we have to introduce some notations used in this paper. Let $p$ be an odd prime number and $\mu_{p^n}$ the group of $p^n$-th roots of unity. For a number field $M$, we denote by $S(M)$ the set of primes of $M$ lying above $p$. By a $p$-ramified extension of $M$ we mean an extension of $M$ which is unramified outside $S(M)$ and by a $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of $M$ a cyclic extension of degree $p$. We denote by $\zeta(s, M)$ the Dedekind zeta function of $M$ and by $A(M)$ the $p$-primary part of the ideal class group of $M$. And we define $E_p(s, M)=\prod_{\wp\in S(M)}(1-(N\wp)^{-s})$ where $N$ is the absolute norm. Moreover, if $M$ is a CM-field, then we denote by $M^+$ the maximal real subfield of $M$, and decompose $A(M)$ by the action of the complex conjugation $J$:

$$A(M)^+=\{a\in A(M)\ ;\ a^J=a\}\ ,\qquad A(M)^-=\{a\in A(M)\ ;\ a^J=-a\}\ .$$

Then we have $A=A^+\oplus A^-$ because $p$ is an odd prime. We fix a totally real field $k$ with the degree $r=[k:\boldsymbol{Q}]$, and put $K=k(\mu_p)$ and $d=[K:k]$. Now we can state our theorems.

THEOREM 1. *Let the fields $k$ and $K$ be as above. We assume that no element in $S(K^+)$ splits in $K$. Then the following four conditions are equivalent.*

1. $A(K)^-\neq 0$.
2. *There is an unramified $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of $K$.*
3. *$p$ divides one of the numerators of the following rational numbers.*[1]

Received October 25, 1990
Revised April 25, 1991

[1] The following numbers are rational by the results of Siegel [Sie].