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 μ_{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].

$$\zeta(1-i, k)\ (2 \leq i \leq d-2, \textit{even}), \qquad p^{\nu}\zeta(1-d, k),$$

where p^{ν} is the number of p-power roots of unity contained in K.

4. *There is a p-ramified $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of K^{+} other than the first layer of the cyclotomic $\boldsymbol{Z}_p$-extension of K^{+}.*

The equivalence $1 \Leftrightarrow 2$ is a simple consequence of class field theory and the reflection theorem of Leopoldt [Leo]. And the equivalence $1 \Leftrightarrow 3$ is essentially due to Greenberg [Gre1]. When the ground field k is a real quadratic field, Kudo also obtained this form of the result ([Kud] Theorem 2) by using the work of Coates and Sinnott [Co-Si]. Hence we only must show the equivalence $3 \Leftrightarrow 4$. But we also show $1 \Leftrightarrow 3$ in a slightly generalized form. We shall prove the following theorem.

THEOREM 2. *Let L be a CM-subfield of K containing k. Put $[K : L] = e$ and $[L : k] = f$. Moreover we assume no element in $S(L^{+})$ splits in L. Then $A(L)^{-} \neq 0$ if and only if*

(1) *in the case $e = 1$: p divides one of the numerators of the following rational numbers:*

$$\zeta(1-i, k)\ (2 \leq i \leq d-2, \textit{even}), \qquad p^{\nu}\zeta(1-d, k),$$

where p^{ν} is the number of p-power roots of unity contained in K.

(2) *in the case $e \neq 1$: p divides one of the numerators of the following rational numbers:*

$$\zeta(1-(ei+1), k)\ (1 \leq i \leq f, \textit{odd}).$$

We must make a number of remarks concerning our theorems.

If we take the field of rational numbers $\boldsymbol{Q}$ as k in Theorem 1 and use the fact $\zeta(1-i, \boldsymbol{Q}) = -B_i/i$ and von Staudt-Clausen's theorem (Theorem 5.10 [Was]), then we obtain the classical criterion of Kummer. And the case $k = \boldsymbol{Q}$ of Theorem 2 was previously obtained by Adachi [Ada].

By the work of Leopoldt [Leo], we know $A(K)^{+} \neq 0$ implies $A(K)^{-} \neq 0$. Hence we may replace the first condition with "$A(K) \neq 0$". On the other hand, in Theorem 2, we cannot replace the condition $A(L)^{-} \neq 0$ with $A(L) \neq 0$ whenever $e \neq 1$. (See Adachi [Ada]).

In proving the equivalence between the fourth condition and the others we must assume that the Leopoldt conjecture holds for K^{+}. But we can show that the negation of the first condition implies the conjecture (see the next section). Hence when we derive the other conditions from the fourth, we need not assume it.

For a fixed totally real field k, if p satisfies one of the conditions in Theorem 1, then we call the prime p a *k-irregular prime*. It is natural to ask whether there exist infinitely many k-irregular primes. The answer is "Yes". In fact, if p is irregular in the classical sense ($\boldsymbol{Q}$-irregular in our terminology) and does not divide the degree $[k : \boldsymbol{Q}]$, then p is obviously k-irregular. Therefore the infinitude of irregular primes (Theorem 5.17 [Was]) implies that of k-irregular primes.

An elliptic analogue of Kummer's criterion is also proved by Coates and Wiles [Co-Wi]. Our proof is inspired by their work.

2. A simple remark on the Leopoldt conjecture.

In this section we prove the result mentioned in the above remark. We first recall the Leopoldt conjecture for totally real fields.

THE LEOPOLDT CONJECTURE. *For any totally real field F, the p-adic regulator $R_p(F)$ of F does not vanish. Equivalently, there is no $\boldsymbol{Z}_p$-extension of F other than the cyclotomic one.* ■

We show the following.

PROPOSITION 1. *Let k, K, K^+, $A(K)^-$ be the same as Theorem 1. (We still assume that no element in $S(K^+)$ splits in K.) If $A(K)^-=0$, then the Leopoldt conjecture is valid for K^+ and p.*

This proposition is an immediate consequence of the following lemma.

LEMMA 1 (Candiotti, Proposition 5 [Can]). *Let F be a totally real field such that $A(F)=0$. And for each $\wp \in S(F)$, we assume that the completion $F_\wp$ of F at $\wp$ does not contain μ_p. Further we assume that the fundamental units of F are linearly independent in $U_p/(U_p)^p$ where U_p is defined as the product of the unit groups $U_\wp$'s of $F_\wp$ ranging over $\wp \in S(F)$; $U_p=\prod_{\wp \in S(F)} U_\wp$. Under these assumptions, the maximal abelian p-ramified p-extension of F agrees with the cyclotomic $\boldsymbol{Z}_p$-extension of F.* ■

M. Yamagishi kindly pointed out to the author that Candiotti's lemma follows from a general theorem due to Shafarevich [Sha].

We now give a proof of the proposition. Let $F=K^+$. Then the conditions in the lemma are satisfied. In fact, by the assumption $A(K)^-=0$ and the remark in the previous section, we have $A(K)=0$. And since none of the elements in $S(K^+)$ split in K, we have $\mu_p \notin K_\wp^+$ for all $\wp \in S(K^+)$. Finally if the fundamental units $\{\varepsilon_1, \cdots, \varepsilon_{rd/2-1}\}$ of K^+ are not linearly independent in $U_p/(U_p)^p$, then we have $\beta=\prod_{i=1}^{rd/2-1} \varepsilon_i^{m_i} \in (U_p)^p$ for some $m_i \in \boldsymbol{Z}_p$ which are not all in $p\boldsymbol{Z}_p$. By the ramification theory of Kummer extensions, we find the extension $K(\sqrt[p]{\beta})/K$ is an unramified extension of degree p. This contradicts $A(K)=0$. Hence we can apply the lemma to K^+. Since any $\boldsymbol{Z}_p$-extension is a p-ramified p-extension, K^+ has only one $\boldsymbol{Z}_p$-extension, i.e., the cyclotomic one by Lemma 1. ■

This proposition is known when $k=\boldsymbol{Q}$ ([Was] p. 71). Of course in this case a more general theorem was proved by Brumer [Bru]. And Lemma 1 also shows that the fourth condition implies the first in Theorem 1. But the converse part cannot be shown by this argument. The author would like to express his thanks to the referee for informing that the equivalence follows from a standard argument on the reflection principle. But

we give instead an analytic proof of the equivalence $3 \Leftrightarrow 4$ using p-adic L-functions.

REMARK. If L is an intermediate CM-field of K/k, then, as mentioned in the previous section, $A(L)^- = 0$ does not imply $A(L) = 0$ so far as $e \neq 1$. Thus we cannot derive the validity of the Leopoldt conjecture for L^+ in this way.

3. p-adic L-functions for totally real fields.

We need some preliminaries on p-adic L-functions for the proof of our theorems. (See, for example, [Coa] and [De-Ri] for more details.) From now on, we fix an embedding of the algebraic numbers into $\boldsymbol{C}_p$, the completion of the algebraic closure of $\boldsymbol{Q}_p$ and we may consider the algebraic numbers to be contained in $\boldsymbol{C}_p$ by this embedding. For an algebraic number field F, we put

$$\zeta^*(s, F) = E_p(s, F)\zeta(s, F) . \tag{1}$$

We consider, in particular, the case that F is totally real. Let ω be the p-adic Teichmüller character. We can then define the p-adic Hecke character associated with $F(\mu_p)/F$ as $\omega_F = \omega \circ N$. Now we put

$$L^*(s, \omega_F^i) = \sum_{(A,p)=1} \frac{\omega_F^i(A)}{(NA)^s} = \prod_{\wp \in \mathrm{Spec}(F) \setminus S(F)} \left(1 - \frac{\omega_F^i(\wp)}{(N\wp)^s}\right)^{-1} .$$

And let $d = [F(\mu_p) : F]$. If $i \equiv 0 \pmod{d}$, then we have

$$L^*(s, \omega_F^i) = \zeta^*(s, F) . \tag{2}$$

Let L be the CM-intermediate field of $F(\mu_p)/F$ and X the group of the characters associated with the extension L/F. Then it is easy to obtain the following two equalities:

$$\zeta^*(s, L) = \prod_{\chi \in X} L^*(s, \chi) , \tag{3}$$

$$\zeta^*(s, L^+) = \prod_{\chi \in X^+} L^*(s, \chi) . \tag{4}$$

Here we denote by X^+ the subset of X consisting of the even characters.

Under these settings, it is shown that, for each ω_F^i, there exists a continuous function $L_p(s, \omega_F^i)$ from $\boldsymbol{Z}_p$ (from $\boldsymbol{Z}_p \setminus \{1\}$ if $i \equiv 0 \pmod{d}$) to $\boldsymbol{C}_p$ such that

$$L_p(1-n, \omega_F^i) = L^*(1-n, \omega_F^{i-n}) , \qquad (n \geq 1) . \tag{5}$$

In particular, if $n \equiv i \pmod{d}$, we have

$$L_p(1-n, \omega_F^i) = \zeta^*(1-n, F) \tag{6}$$

by (2) and (5).

Now we fix a topological generator γ of the Galois group $\mathrm{Gal}(F(\bigcup_{n \geq 1} \mu_{p^n})/F(\mu_p))$

and define u by the element in $1+p\boldsymbol{Z}_p$ which satisfies $\zeta_{p^n}^{\gamma}=\zeta_{p^n}^{u}$ $(n\geq 1)$, where ζ_{p^n} is a generator of the group μ_{p^n}. Then it is also shown that there exists an element $G(T, \omega_F^{1-i})$ of the quotient field of the Iwasawa algebra $\Lambda=\boldsymbol{Z}_p[[T]]$ such that

$$L_p(s, \omega_F^i)=G(u^s-1, \omega_F^{1-i})\,. \tag{7}$$

Moreover, if we put

$$H(T, \omega_F^i)=\begin{cases} G(T, \omega_F^i) & (i\not\equiv 1 \pmod d) \\ (1+T-u)G(T, \omega_F^i) & (i\equiv 1 \pmod d)\,, \end{cases} \tag{8}$$

then we have

$$H(T, \omega_F^i)\in\Lambda\,, \tag{9}$$

that is, as far as $i\not\equiv 0 \pmod d$, $L_p(s, \omega_F^i)$ is an Iwasawa function.

4. Proof of Theorem 1.

Let M be the maximal abelian p-ramified p-extension and K_∞^+ the cyclotomic $\boldsymbol{Z}_p$-extension of K^+ respectively. Then the negation of the fourth condition of the theorem is equivalent to $M=K_\infty^+$. Therefore it is equivalent to $\mathrm{Gal}(M/K_\infty^+)=1$. We need a lemma.

LEMMA 2 (Coates [Coa] Appendix Lemma 8). *Let F be a totally real field for which the Leopoldt conjecture for p is valid. And let F_∞ be the cyclotomic $\boldsymbol{Z}_p$-extension, and M the maximal abelian p-ramified p-extension of F respectively. Put*

$$\alpha(F)=\frac{(w(F(\mu_p))hR_pE_p(1, F))}{\sqrt{\delta}}\,. \tag{10}$$

Then we have

$$\#\mathrm{Gal}(M/F_\infty)=p^{v_p(\alpha(F))}\,,$$

where $w(F(\mu_p))$ is the number of the roots of unity contained in $F(\mu_p)$, h is the class number of F, R_p is the p-adic regulator of F, δ is the absolute value of the discriminant of F, and v_p is the p-adic valuation normalized by $v_p(p)=1$. ■

In this lemma let $F=K^+$. Then we have

$$\mathrm{Gal}(M/K_\infty^+)=1 \iff \alpha(K^+)\in\boldsymbol{Z}_p^\times\,. \tag{11}$$

Let

$$\boldsymbol{Q}=\boldsymbol{Q}_0\subset\boldsymbol{Q}_1\subset\cdots\subset\boldsymbol{Q}_n\subset\cdots\subset\boldsymbol{Q}_\infty$$

be the cyclotomic $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}$. And define an integer ν by $\boldsymbol{Q}_\infty\cap K^+=\boldsymbol{Q}_{\nu-1}$. Then it follows that ($p$-part of $w(K)$)$=p^\nu$. Now to connect the algebraic results in the above

with analytic objects, we need another lemma.

LEMMA 3 (Colmez [Col]). *We use the notation in Lemma* 2. *Put* $\zeta_p(F, s)=L_p(s, \omega_F^0)$. *Then we have*

$$\lim_{s\to 1}(s-1)\zeta_p(F, s)=\frac{2^{n-1}hR_pE_p(1, F)}{\sqrt{\delta}},$$

where $n=[F : \boldsymbol{Q}]$. *In particular, if the Leopoldt conjecture is valid for* F, *then* $\zeta_p(F, s)$ *has a pole at* $s=1$ *of order* 1 *and the residue is given by the above formula.* ■

We apply this lemma to K^+. Under the assumption that the Leopoldt conjecture is valid for K^+, we have

$$\operatorname{Res}(\zeta_p(K^+, s), s=1)=\frac{2^{n-1}hR_pE_p(1, K^+)}{\sqrt{\delta}}\neq 0. \tag{12}$$

By (10), (11) and (12) we obtain

$$\operatorname{Gal}(M/K_\infty^+)=1 \iff w(K)\operatorname{Res}(\zeta_p(K^+, s), s=1)\in \boldsymbol{Z}_p^\times .$$

It can be seen $\zeta_p(K^+, s)=\prod_{i=2, i:\text{even}}^{d} L_p(s, \omega_k^i)$, and by (7) and (8) we have

$$(u^s-u)\zeta_p(K^+, s)=\prod_{i=2, i:\text{even}}^{d} H(u^s-1, \omega_k^{1-i}).$$

It follows from (9) that the both sides of the above equation are analytic, and by the expansion of u^s-u:

$$u^s-u=u(s-1)\log_p(u)+\text{higher terms},$$

we obtain

$$u\log_p(u)\operatorname{Res}(\zeta_p(K^+, s), s=1)=\prod_{i=2, i:\text{even}}^{d} H(u^1-1, \omega_k^{1-i}).$$

On the other hand, we have

$$v_p(u\log(u))=v_p(u-1)=v_p(w(K))$$

by the definition of u. This yields

$$v_p(w(K)\operatorname{Res}(\zeta_p(K^+, s), s=1))=v_p\left(\prod_{i=2, i:\text{even}} H(u^1-1, \omega_k^{1-i})\right).$$

Since $H(u^1-1, \omega_k^{1-i})$'s are p-adic integers, we finally obtain

$$\operatorname{Gal}(M/K_\infty^+)=1 \iff H(u^1-1, \omega_k^{1-i})\in \boldsymbol{Z}_p^\times \qquad (2\leq i\leq d : \text{even}).$$

We rewrite the condition of the right hand side. We have, for $j\not\equiv 0 \pmod d$,

$$\begin{aligned} H(u^1-1, \omega_k^{1-j}) &\equiv H(u^{1-j}-1, \omega_k^{1-j}) \pmod{p} \\ &= L_p(1-j, \omega_k^j) \quad \text{(by (7))} \\ &= \zeta^*(1-j, k) \quad \text{(by (6))} \\ &= (p\text{-adic unit}) \times \zeta(1-j, k) \quad \text{(by (1))}. \end{aligned} \tag{13}$$

For $j \equiv 0 \pmod{d}$, we have

$$\begin{aligned} H(u^1-1, \omega_k^{1-j}) &\equiv H(u^{1-j}-1, \omega_k^{1-j}) \pmod{p} \\ &= (u^{1-j}-u)L_p(1-j, \omega_k^j) \quad \text{(by (7), (8))} \\ &= (u^{1-j}-u)\zeta^*(1-j, k) \quad \text{(by (6))} \\ &= (p\text{-adic unit}) \times (u^{1-j}-u)\zeta(1-j, k) \quad \text{(by (1))}. \end{aligned}$$

Let $j=d$, and we have $v_p(u^{1-d}-u)=v$, because $(p, d)=1$, Hence we have

$$H(u^1-1, \omega_k^{1-d}) \in \boldsymbol{Z}_p^\times \iff p^v\zeta(1-d, k) \in \boldsymbol{Z}_p^\times . \tag{14}$$

Combining (13) and (14), the proof of Theorem 1 is complete.

5. Proof of Theorem 2.

Let h, R, δ be the class number, the regulator and the absolute value of the discriminant of L respectively. Moreover let h^+, R^+, δ^+ be the corresponding objects for L^+, and w the number of the roots of unity contained in L. We can prove a class number formula for L by the same method used by Greenberg in his paper [Gre1]. Namely, we have

$$ah^- = \frac{w}{2^{t+1}} \prod_{i=1, i:\text{odd}}^{f} L^*(0, \omega_k^{ei}), \tag{15}$$

where $h^- = h/h^+$ and the integer t is determined by the formula $R/R^+ = 2^t$ (see Proposition 4.16 [Was]) and the integer a is determined by the formula

$$a = \lim_{s \to 0} \frac{E_p(s, L)}{E_p(s, L^+)}.$$

Note that, since no element of $S(L^+)$ splits in L/L^+, a is a power of 2, so a p-adic unit. Also note that

$$v_p(w) = \begin{cases} 0 & \text{if } e \neq 1 \\ v & \text{if } e = 1 . \end{cases}$$

By (5) we can rewrite (15) by the language of p-adic L-functions. In fact, we have

$$w \prod_{i=1,\, i:\text{odd}}^{f} L^*(0, \omega_k^{ei}) = w \prod_{i=1,\, i:\text{odd}}^{f} L_p(0, \omega_k^{ei+1}) . \tag{16}$$

As in the proof of Theorem 1 we obtain

$$\begin{aligned}
&(p\text{-adic unit}) \times w \prod_{i=1,\, i:\text{odd}}^{f} L_p(0, \omega_k^{ei+1}) \\
&\equiv w \prod_{i=1,\, i:\text{odd}}^{f} L_p(1-(ei+1), \omega_k^{ei+1}) \qquad (\mathrm{mod}\, p) \\
&= w \prod_{i=1,\, i:\text{odd}}^{f} \zeta^*(1-(ei+1), k) \\
&= (p\text{-adic unit}) \times w \prod_{i=1,\, i:\text{odd}}^{f} \zeta(1-(ei+1), k) .
\end{aligned} \tag{17}$$

Combining (15), (16), (17) and using the p-integrality of $\zeta(1-(ei+1), k)$ or $p^{\nu}\zeta(1-d, k)$, the proof of Theorem 2 is complete.

References

[Ada] N. ADACHI, Generalization of Kummer's criterion for divisibility of class numbers, J. Number Theory, **5** (1973), 253–265.

[Bru] A. BRUMER, On the units of algebraic number fields, Mathematika, **14** (1967), 121–124.

[Can] A. CANDIOTTI, Computation of Iwasawa invariants and K_2, Comp. Math., **29** (1974), 89–111.

[Coa] J. COATES, p-adic L-functions and Iwasawa's theory, *Algebraic Number Fields* (Durham Symposium, 1975; ed. by A. Fröhlich), 269–353, Academic Press, 1977.

[Co-Si] J. COATES and W. SINNOTT, On p-adic L-functions over totally real fields, Invent. Math., **24** (1974), 253–279.

[Co-Wi] J. COATES and A. WILES, Kummer's criterion for Hurwitz numbers, *Algebraic Number Theory* (Kyoto Conference, 1975; ed. by S. Iyanaga), 9–23, Japan Soc. Promotion Sci., 1977.

[Col] P. COLMEZ, Résidu en $s=1$ des fonctions zêta p-adique, Invent. Math., **91** (1988), 371–389.

[De-Ri] P. DELIGNE and K. RIBET, Values of abelian L-functions at negative integers over totally real fields, Invent. Math., **59** (1980), 227–286.

[Gre1] R. GREENBERG, A generalization of Kummer's criterion, Invent. Math., **21** (1973), 247–254.

[Gre2] R. GREENBERG, On the Iwasawa invariants of totally real number fields, Amer. J. Math., **98** (1976), 263–284.

[Iwa] K. IWASAWA, *Lectures on p-Adic L-Functions*. Ann. of Math. Studies, **74** (1972), Princeton Univ. Press.

[Kud] A. KUDO, On a generalization of a theorem of Kummer, Mem. Fac. Sci. Kyushu Univ. Ser. A, **29** (1978), 255–261.

[Leo] H. W. LEOPOLDT, Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, J. Reine Angew. Math., **199** (1958), 165–174.

[Sha] I. SHAFAREVICH, Extensions with given ramification points, (in Russian), Publ. Math. Inst. Haut. Etud. Sci., **18** (1964), 295–319.

[Sie] C. L. SIEGEL, Über die Fourierschen Koeffizienten von Modulformen, Nachr. Akad. Wiss. Göttingen

Math.-Phys. Kl., **3** (1970), 15–56.

[Was] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, Graduate Texts in Math., **83** (1982), Springer-Verlag.

[Wil] A. WILES, The Iwasawa conjecture for totally real fields, Ann. of Math., **131** (1990), 493–540.

Present Address:
DEPARTMENT OF MATHEMATICS, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY
OKUBO, SHINJUKU-KU, TOKYO 169, JAPAN