On the \( \mu \)-invariants of cyclotomic fields

by

KENKICHI IWASAWA (Princeton, N.J.)

Let \( p \) be an odd prime. For each \( n \geq 0 \), let \( \kappa_n \) denote the cyclotomic field of \( p^{n+1} \)-th roots of unity and let \( p^\nu \), \( \nu \geq 0 \), be the highest power of \( p \) which divides the class number of \( \kappa_n \). It is known (see [1]) that for all sufficiently large \( n \), the exponent \( \nu_n \) is given by a formula

\[
\nu_n = 2\lambda_n + \nu p^n + \nu
\]

where \( \lambda_n, \mu, \nu \) are integers \((\lambda_n, \mu, \nu \geq 0)\), independent of \( n \). In the present paper, we shall prove that

\[
\mu < p - 1.
\]

Let \( \mathbb{Z}_p \) denote the ring of \( p \)-adic integers and let \( A \) be the ring of all formal power series in an indeterminate \( T \) with coefficients in \( \mathbb{Z}_p \):

\[ A = \mathbb{Z}_p[[T]]. \]

We shall first prove a lemma on \( A \)-modules.(1)

A \( A \)-module \( Y \) is called elementary if \( Y \) is the direct sum of a finite number of \( A \)-modules of the form \( A/p^m, m \geq 0 \), where \( p \) is prime ideals of height 1 in \( A \). Let \( X \) be a noetherian torsion \( A \)-module. Then there exist an elementary \( A \)-module \( X \) and a morphism

\[
f: X \rightarrow Y
\]

such that both the kernel and the cokernel of \( f \) are finite modules. Let

\[ Y = \sum A/p^m_i
\]

be the direct decomposition for \( Y \) and let

\[
\mu = \sum m_i,
\]

where the sum is taken over all indices \( i \) such that \( P_i = pA \). The integer \( \mu \) is then uniquely determined for \( X \) by the above and hence is denoted by \( \mu(X) \).

(1) For the theory of \( A \)-modules, see [3].
that the order of $X^{-}/T X^{-}$ is just equal to the highest power of $p$ which divides $h^{-}$. Hence, applying the above lemma for $X^{-}$, we see that

$$p^p - h^{-}.$$

On the other hand, the classical class number formula for $k$ states that

$$h^{-} = 2p \prod_{\chi} \left( 1 - \frac{1}{2p} \sum_{a=1}^{p-1} a \chi(a) \right),$$

where the product is taken over all Dirichlet characters $\chi$ defined mod $p$ with $\chi(-1) = -1$. Since

$$\left| \sum_{a=1}^{p-1} a \chi(a) \right| < \sum_{a=1}^{p-1} a = \frac{(p-1)p}{2},$$

we have

$$h^{-} < 2^p - p(p-1)^{(p-1)/2} \leq p^{(p-1)/2}.$$

It then follows that

$$\mu^{-} < (p-1)/2$$

so that

$$\mu < p - 1,$$

q.e.d.

Instead of the above elementary argument, we may estimate $h^{-}$ also by using

$$|L(1; \chi)| < 2 \log p, \quad \chi \neq 1.$$

We then see that for any given real number $\sigma > 1/2$, there exists an integer $N(\sigma)$ such that

$$\mu < N(\sigma)$$

whenever $p > N(\sigma)$. It is also clear that by the same method, we can find an upper bound for the $\mu$-invariant of a so-called $Z_p$-extension $K/k$ in many special cases. In particular, if $K$ has only one prime divisor which divides the rational prime $p$ (as in the special case discussed above), then

$$\mu(K/k) \leq \log h/\log p,$$

where $h$ is the class number of $k$.

References


PRINCETON UNIVERSITY

Received on 21. 3. 1971

(147)