J. Math. Soc. Japan
Vol. 49, No. 4, 1997

Greenberg's conjecture and the Iwasawa polynomial

By Hiroki SUMIDA

(Received Feb. 8, 1995)
(Revised Aug. 8, 1995)

Introduction.

Let k be a finite extension of the field $\boldsymbol{Q}$ of rational numbers and p a fixed prime number. A Galois extension K of k is called a $\boldsymbol{Z}_p$-extension when the Galois group $\mathrm{Gal}(K/k)$ is topologically isomorphic to the additive group $\boldsymbol{Z}_p$ of p-adic integers. Let K be a $\boldsymbol{Z}_p$-extension of k, $k_n \subset K$ the unique cyclic extension over k of degree p^n and A_n the p-Sylow subgroup of the ideal class group of k_n. We denote by $\# A$ the number of elements of a finite set A.

Iwasawa proved the following theorem (see [**I2**]).

THEOREM (Iwasawa). *There exist three integers* $\lambda=\lambda(K/k)$, $\mu=\mu(K/k)$ *and* $\nu=\nu(K/k)$ *such that*

$$\# A_n = p^{\lambda n+\mu p^n+\nu}$$

for all sufficiently large n.

Every k has at least one $\boldsymbol{Z}_p$-extension called the cyclotomic $\boldsymbol{Z}_p$-extension. We denote by k_∞ the cyclotomic $\boldsymbol{Z}_p$-extension of k.

GREENBERG'S CONJECTURE. *If* k *is a totally real number field, then*

$$\lambda(k_\infty/k) = \mu(k_\infty/k) = 0.$$

In other words the maximal unramified abelian p-*extension of* k_∞ *is a finite extension.*

By [**I1**], this conjecture is true for $k=\boldsymbol{Q}$ and p arbitrary. As experimental results, this conjecture has been verified for $p=3$ and many real quadratic fields with small discriminants in [**C**], [**G1**], [**FK**], [**FKW**], [**F**], [**Kr**], [**T**] and [**FT**].

The main purpose of this paper is to give a "good" necessary and sufficient condition for Greenberg's conjecture. The condition is given in terms of some p-ramified abelian p-extensions of k_n and the Iwasawa polynomial associated to k. Here a "good" condition means that it can be checked for n as little as possible. To check it, we need a lot of data (an "approximate" Iwasawa polynomial, basis of the ideal class group, that of the unit group and that of the