WARING'S PROBLEM FOR ALGEBRAIC NUMBER FIELDS AND PRIMES OF THE FORM $(p^r - 1)/(p^d - 1)$

Dedicated to Hans Rademacher on the occasion of his seventieth birthday

BY

PAUL T. BATEMAN AND ROSEMARIE M. STEMMLER[1]

1. Introduction

Let K be an algebraic number field of finite degree n over the rationals, and let $J(K)$ be its ring of integers. If m is a positive integer greater than unity, let $J_m(K)$ be the additive group generated by the m^{th} powers of the elements of $J(K)$. Clearly $J_m(K)$ is a subring of $J(K)$. Needless to say, $J_m(K)$ is that subset of $J(K)$ in which Waring's problem for m^{th} powers is to be considered. The identity

$$m!\, x = \sum_{k=0}^{m-1} (-1)^{m-1-k} \binom{m-1}{k} \{(x+k)^m - k^m\}$$

shows that

$$m!\, J(K) \subset J_m(K) \subset J(K).$$

Hence $J_m(K)$ consists of certain of the residue classes of $J(K)$ modulo $m!\, J(K)$. Further $J_m(K)$ can be determined in a particular case by an examination of the quotient ring $J(K)/\{m!\, J(K)\}$. This determination can be rather complicated, especially when m is composite.

When m is a prime q, the situation is somewhat simpler than in the general case. In particular, it is easy to characterize those algebraic number fields K for which $J_q(K) = J(K)$. We shall do this in this paper. Examples of our main result are as follows: (A) $J_3(K) = J(K)$ unless either 3 is ramified[2] in $J(K)$ or 2 has in $J(K)$ a prime ideal factor of second degree, (B) $J_{11}(K) = J(K)$ unless 11 is ramified in $J(K)$, (C) $J_{31}(K) = J(K)$ unless either 31 is ramified in $J(K)$ or 2 has in $J(K)$ a prime ideal factor of fifth degree or 5 has in $J(K)$ a prime ideal factor of third degree. For most primes q the situation is analogous to that for $q = 11$, that is, we *usually* can say that $J_q(K) = J(K)$ if and only if q is not ramified in $J(K)$. This generalizes the familiar result [10] that $J_2(K) = J(K)$ if and only if 2 is not ramified in $J(K)$.

The primes for which complications occur are those special primes q ex-

Received April 24, 1961; received in revised form August 16, 1961.

[1] This work was supported by the Office of Naval Research.

[2] The phrase "q is ramified in $J(K)$" means that q is divisible by the square of some prime ideal in $J(K)$. By the so-called ramification theorem (see [6]) the condition that q is ramified in $J(K)$ is equivalent to the condition that q divides the discriminant of K. Accordingly our results could easily be modified by replacing the former condition by the latter.