A CHARACTERIZATION OF ALGEBRAIC NUMBER FIELDS WITH CLASS NUMBER TWO

L. CARLITZ

Let $\mathcal{Z} = \mathbb{R}(\theta)$ denote an algebraic number field over the rationals with class number $h$. It is familiar that $h = 1$ if and only if unique factorization into prime holds for the integers of $\mathcal{Z}$. For fields with $h = 2$ we have the following criterion.

**Theorem.** The algebraic number field $\mathcal{Z}$ has class number $\leq 2$ if and only if for every nonzero integer $\alpha \in \mathcal{Z}$ the number of primes $\pi_i$ in every factorization

$$\alpha = \pi_1 \pi_2 \cdots \pi_k$$

depends only on $\alpha$.

Suppose first that $h = 2$ and consider the factorization into prime ideals

$$\alpha = p_1 \cdots p_s r_1 \cdots r_t,$$

where the $p_i$ are principal ideals while the $r_j$ are not. Then

$$p_i = (\pi_i) \quad (j = 1, \ldots, s).$$

Since $h = 2$, it follows that

$$r_\alpha r_j = (\rho_{ij}) \quad (i, j = 1, \ldots, t);$$

moreover $t$ must be even, $= 2u$, say. Thus every factorization into primes implied by (2), for example

Received by the editors August 3, 1959.

1 Research sponsored by National Science Foundation grant NSF G-9425.
where $\epsilon$ is a unit, will contain exactly $s+u$ primes.

We now show that when $h>2$, there occur factorizations (1) with different values of $k$. The proof makes use of the fact that every class of ideals contains at least one prime ideal. (For proof of a much stronger result see [1]).

Assume first the existence of a class $A$ of period $m>2$. Let $p$ be a prime ideal in $A$ and $p'$ a prime ideal in $A^{-1}$. Then we have

$$ p^m = (\pi), \quad p'^m = (\pi'), \quad pp' = (\pi_1), $$

and it is easily verified that $\pi, \pi', \pi_1$ are primes. Clearly (3) implies

$$ \pi_1 = \epsilon \pi', $$

where $\epsilon$ is a unit.

In the next place assume the existence of two classes $A_1, A_2$ each of period 2 such that $A_3 = A_1A_2$ is not principal. Choose prime ideals $p_j \in A_j$ ($j=1, 2, 3$). Then we have

$$ p_j^2 = (\pi_j) \quad (j = 1, 2, 3), \quad p_1p_2p_3 = (\pi), $$

and again it is easily verified that $\pi_1, \pi_2, \pi_3, \pi$ are all primes. From (5) we get

$$ \pi^2 = \pi_1\pi_2\pi_3. $$

Using (5) and (6) it is evident that when $h>2$, the number of primes $k$ in (1) is not independent of the factorization.

Since the case $h=1$ requires no further discussion, this completes the proof of the theorem.

**Reference**


Duke University