A CHARACTERIZATION OF ALGEBRAIC NUMBER FIELDS WITH CLASS NUMBER TWO¹

L. CARLITZ

Let \( Z = \mathbb{Q}(\theta) \) 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 \( Z \). For fields with \( h = 2 \) we have the following criterion.

**Theorem.** The algebraic number field \( Z \) has class number \( \leq 2 \) if and only if for every nonzero integer \( \alpha \in \mathbb{Z} \) the number of primes \( \pi_j \) 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

\[
(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{r}_1 \cdots \mathfrak{r}_t,
\]

where the \( \mathfrak{p}_j \) are principal ideals while the \( \mathfrak{r}_j \) are not. Then

\[
\mathfrak{p}_j = (\pi_j) \quad (j = 1, \ldots, s).
\]

Since \( h = 2 \), it follows that

\[
\mathfrak{r}_i \mathfrak{r}_j = (\rho_{ij}) \quad (i, j = 1, \ldots, t);
\]

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

---

¹ Research sponsored by National Science Foundation grant NSF G-9425.
\[ \alpha = e\pi_1 \cdots \pi_u \rho_1 \cdots \rho_{l-1}, \]

where \( e \) 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

\[ \pi_1 = e\pi\pi', \]

where \( e \) 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 \( p_1 \subset A_j \) (\( j = 1, 2, 3 \)). 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**