S. Ullom
Nagoya Math. J.
Vol. 34 (1969), 153-167

NORMAL BASES IN GALOIS EXTENSIONS OF NUMBER FIELDS

S. ULLOM*

Introduction

The notion of module together with many other concepts in abstract algebra we owe to Dedekind [2]. He recognized that the ring of integers O_K of a number field was a free $\boldsymbol{Z}$-module. When the extension K/F is Galois, it is known that K has an algebraic normal basis over F. A fractional ideal of K is a Galois module if and only if it is an ambiguous ideal. Hilbert [4, §§105-112] used the existence of a normal basis for certain rings of integers to develop the theory of root numbers—their decomposition already having been studied by Kummer.

Let K/F be a Galois extension of number fields. A necessary condition that O_K have a normal basis was given by Speiser [9], namely that K/F be tamely ramified. Hilbert [4, Theorem 132] showed O_K has a normal basis when $K/\boldsymbol{Q}$ is abelian and the degree of $K/\boldsymbol{Q}$ is prime to the discriminant of $K/\boldsymbol{Q}$. E. Noether [7] proved that if K/F is tamely ramified, then O_K has a normal basis everywhere locally. When $K/\boldsymbol{Q}$ is abelian with $G = G(K/\boldsymbol{Q})$, Leopoldt [6] gave a complete structure theory for O_K as a $\boldsymbol{Z}G$-module using Gauss sums as generators. His theory uses in a crucial way Kronecker's theorem that every absolutely abelian field is a subfield of a cyclotomic field and that the base ring of integers $\boldsymbol{Z}$ is a principal ideal ring. Fröhlich [3] using "Kummer invariants" considered the case when K/F is a Kummer extension and gave necessary and sufficient conditions that O_K have a normal basis. Yokoi [11] using the structure theory of integral representations of cyclic groups of prime order described the integral representations afforded by O_K, $K/\boldsymbol{Q}$ a cyclic extension of prime degree.

Received October 16, 1967.
Revised July 15, 1968.
* This research is partially supported by National Science Foundation Contract Number GP-1837 and GP-6010.