ABELIAN GALOIS EXTENSIONS OF RINGS CONTAINING ROOTS OF UNITY

BY
L. N. CHILDS[1]

Let R be a commutative ring and A a Galois extension of R with abelian group G of exponent n. Then A is a rank one projective $R[G]$-module and is a free $R[G]$-module iff A has a normal basis. If R is connected, and contains $1/n$ and a primitive n-th root of unity, then $R[G]$ decomposes into the direct sum $\oplus R_i$ of copies of R (as rings), so that as $R[G]$-module, $A = \oplus A_j$, a direct sum of rank one projective R-modules. In this paper we first show (Theorem 1) that in this situation this decomposition makes A into a kind of generalized group ring with nicely described G-structure, so that if all the A_i are isomorphic to R, i.e., A has a normal basis, then A is a projective group algebra.

We then give two applications of Theorem 1. In Section 2 we investigate for central Galois extensions the relationship between Theorem 1 and a similar result of Kanzaki, to obtain a description of central abelian extensions with normal basis.

The set of isomorphism classes of all Galois extensions of R with abelian group G which are R-algebras forms an abelian group, with a subgroup consisting of classes of extensions which have normal basis. In Section 3 we use Theorem 1 and a result of G. Garfinkel and M. Orzech to compute the group of Galois extensions modulo those with normal basis when R and G satisfy the hypotheses cited above.

I wish to thank M. Orzech for suggesting some useful improvements.

0. Definitions and notation

All rings have units. A commutative ring R will be called connected if it has no idempotents but 0 and 1.

Let A be a ring, G a finite group of automorphisms, and $R = A^G$, the fixed ring of G. Assume R is contained in the center of A. Then A is a Galois extension of R with group G if there exist $x_1 \cdots x_n$, $y_1 \cdots y_n$ in A so that $\sum_i x_i \sigma(y_i) = \delta_{1,\sigma}$ for all σ in G. This particular choice of definition of Galois extension is equivalent to several other standard conditions (since [CHR 1.3(b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d) (e) $\Rightarrow$ (a)] remains valid). In particular, A is a separable R-algebra [D1, Theorem 1].

If A, A' are Galois extensions of R with group G, we say A and A' are isomorphic as Galois extensions if there is an R-algebra isomorphism of A onto A' which is at the same time a G-module homomorphism.

Received November 22, 1968.
[1] Research partially supported by a National Science Foundation grant at Northwestern University.