

# *Hopf Algebras and Galois Extensions of an Algebra*

H. F. KREIMER & M. TAKEUCHI

**Introduction.** Let  $R$  be a given commutative ring with identity element 1, and let  $J$  be a given Hopf algebra over  $R$  which is a finitely generated, projective  $R$ -module. Conditions under which an  $R$ -algebra  $B$  may be called a  $J$ -Galois extension of a subalgebra  $A$  are investigated in the first part of this paper. These conditions seem modestly restrictive, and in the case of a commutative algebra  $B$  they appear to be weaker than conditions imposed by S. U. Chase and M. E. Sweedler in their definition of a commutative Galois  $J$ -algebra [3]. But the structure of a Hopf algebra is used to derive various properties of a  $J$ -Galois extension. For example a  $J$ -Galois extension of an  $R$ -algebra  $A$  is finitely generated and projective as either a left or right  $A$ -module; and in particular the earlier definition of a commutative Galois  $J$ -algebra is seen to be a special instance of a  $J$ -Galois extension as defined here.

In the second part of the paper, the concept of a normal basis for a  $J$ -Galois extension is introduced and explored. A simple criterion for the existence of a normal basis when the kernel of the augmentation or counit map of the dual Hopf algebra  $J^*$  is contained in the Jacobson radical of  $J^*$  is developed; and applications to  $p$ -groups of automorphisms, derivations, and higher derivations of an algebra over a ring of prime characteristic  $p$  are given.

The following notation and elementary facts will be used throughout this paper. For any object  $X$  in a category, let the identity morphism for  $X$  also be denoted by the symbol  $X$ . An  $R$ -module will always be assumed to be unital, and the symbols  $\otimes$  and  $\text{Hom}$  will denote respectively tensor product and group of module homomorphisms for pairs of  $R$ -modules unless some other module structure is indicated by subscripts. For  $R$ -modules  $X$  and  $Y$ ,  $T$  will denote the  $R$ -module isomorphism of  $X \otimes Y$  onto  $Y \otimes X$  such that  $T(x \otimes y) = y \otimes x$  for  $x$  in  $X$  and  $y$  in  $Y$ , and  $X^*$  will denote the dual module  $\text{Hom}(X, R)$ . If  $x \in X$  and  $\phi \in X^*$ , let  $\langle \phi, x \rangle$  denote the value of  $\phi$  at  $x$ ; and if  $f$  is an  $R$ -module homomorphism of  $X$  into  $Y$ , let  $f^*$  denote the adjoint map of  $Y^*$  into  $X^*$ . If  $X$  is a finitely generated, projective  $R$ -module; then so is  $X^*$ , and there are natural isomorphisms by which  $X$  may be identified with  $X^{**}$  and  $X^* \otimes Y^*$  may be identified with  $(X \otimes Y)^*$ . Moreover elements  $v$  and  $w$  of  $X \otimes Y$  are equal if and only if  $(\phi \otimes Y)(v) = (\phi \otimes Y)(w)$  for every