NORMAL BASES OF CYCLIC FIELDS OF PRIME-POWER DEGREE

By Sam Perlis

If Z is a normal field of degree n over F with automorphism group $G = (I, S_2, \cdots, S_n)$, a normal basis of Z/F is any basis of the form $(u, u^{S_2}, \cdots, u^{S_n})$. That such a basis always exists is well known (see [2; 32, footnote], [3], [4; bibliography], [5; bibliography]). We consider fields Z which are cyclic of degree $n = p^e$ over F, p being any prime, and obtain necessary and sufficient conditions for a quantity u of Z to generate a normal basis of Z/F. (When the conjugates of u form a basis of Z/F we shall say that u "generates" a normal basis of Z/F.) The structure of the extensions Z/F has been studied by A. A. Albert [1; IX] and his structure theorems are used here. The result is simplest in the case of characteristic p: the conjugates of a quantity u form a basis of Z/F if and only if the trace of u in Z/F is not zero. A particularly simple choice of u is given for this case. In the final section earlier results are applied to cyclotomic fields Z/F such that F contains a primitive p-th root of unity.

1. **Some lemmas.** We first consider cyclic fields of arbitrary finite degree over a field F.

Lemma 1. *Let Z be a cyclic field of degree n over F with generating automorphism S and a normal basis generated by a quantity v. Then a quantity $u = c_0v + c_1v^S + \cdots + c_{n-1}v^{S^{n-1}}$ of Z (c_i in F) generates a normal basis of Z/F if and only if the polynomials*

$$f(\lambda) = c_0 + c_1\lambda + \cdots + c_{n-1}\lambda^{n-1}, \qquad g(\lambda) = \lambda^n - 1 \tag{1}$$

are relatively prime.

We must examine the matrix T expressing the conjugates of u in terms of the basis $(v, \cdots, v^{S^{n-1}})$, and find the conditions under which it is non-singular. This matrix is

$$T = \left\| \begin{matrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ c_1 & c_2 & \cdots & c_0 \end{matrix} \right\|. \tag{2}$$

If a matrix A is defined to be the special case of T obtained by setting $c_1 = 1$, and $c_i = 0$ for $i \neq 1$, we have

$$T = c_0 + c_1A + \cdots + c_{n-1}A^{n-1} = f(A),$$

Received January 7, 1942; presented to the American Mathematical Society December 29, 1941.