THE GALOIS GROUP OF $x^n + x - t$

DAVID R. HAYES

1. Introduction. Suppose one wishes to make some computations in the finite field $\mathbf{F}_q$ of q elements, where $q = p^n$ is a prime power. One must first find an irreducible polynomial of degree n over the prime field $\mathbf{F}_p$. Chowla [2] has pointed out the advantages of knowing *a priori* that irreducibles of a simple form always exist and has suggested that perhaps there is always an irreducible of the form $x^n + x + a$, $a \in F_p$, at least for fixed n and all large p. In fact, Chowla conjectured that the number $N(p)$ of such irreducibles over $\mathbf{F}_p$ is asymptotic as $p \to \infty$ to p/n. In establishing this conjecture Cohen [3] and Ree [4] independently proved that

$$N(p) = \frac{p}{n} + O(p^{\frac{1}{2}}), \tag{1}$$

where the implied constant depends only on n. Both proofs, which use a function field analog of the Čebotarev density theorem, require an explicit knowledge of the Galois group of the polynomial $x^n + x - t$ over the function field $\mathbf{F}_p(t)$ for large p. This Galois group was, in fact, already known from previous work of Birch and Swinnerton-Dyer [1] who proved a general result of which the following theorem is a special case.

THEOREM 1. *Let K be the splitting field of $\phi(x) = x^n + x - t$ over $k = \mathbf{F}_p(t)$. Then K/k is Galois; and if $p \nmid n(n-1)$, then $G =$ Gal (K/k) is the full symmetric group S_n on n letters, and the field of constants of K/k is $\mathbf{F}_p$.*

The proof provided in [1] for this theorem proceeds by first "lifting" the polynomial to characteristic 0 and then using the theory of Riemann surfaces—a technique described by the authors themselves as an "inelegant device". In this note I give another proof of this theorem which does not leave characteristic p. The idea of the proof is still the same: one examines the decomposition groups at the ramified primes. But instead of Riemann surface theory, I use the Hurwitz formula for the genus of a covering, which is valid in any characteristic. These methods are easily adapted so as to provide a proof of the full theorem of Birch and Swinnerton-Dyer [1; Lemma 3].

2. Proof of Theorem 1. Note that $\phi(x)$ is separable since the roots of its derivative are all algebraic over $\mathbf{F}_p$. So K/k is certainly Galois. Further, $\phi(x)$ is irreducible since it has degree 1 in t. Therefore, the Galois group of $\phi(x)$ is transitive as a permutation group on the roots of $\phi(x)$. Let $\mathbf{F}_p^+$ be the algebraic

Received November 27, 1972. This paper was supported in part by NSF Grant GP-29103.