PACIFIC JOURNAL OF MATHEMATICS
Vol. 78, No. 1, 1978

ON THE DEGREE OF THE SPLITTING FIELD OF AN IRREDUCIBLE BINOMIAL

DAVID GAY AND WILLIAM YSLAS VÉLEZ

Let x^m-a be irreducible over a field F. We give a new proof of Darbi's formula for the degree of the splitting field of x^m-a and investigate some of its properties. We give a more explicit formula in case the only roots of unity in F are ± 1.

A formula for the degree of the splitting field of an irreducible binomial over a field F of characteristic 0 was given in 1926 in the following:

THEOREM (*Darbi* [1]). *Let ζ_m denote a primitive mth-root of unity and let $x^m-a \in F[x]$ be irreducible with root α. Define an integer k as follows:*

$$k = \max\{l: l \mid m \quad \text{and} \quad \alpha^{m/l} \in F(\zeta_m)\}\,. \tag{1}$$

Then the degree of the splitting field of $x^m - a$ is $m\phi_F(m)/k$, where $\phi_F(m) = [F(\zeta_m): F]$.

In § 1 of this paper we give a new proof of this theorem which, with an appropriate interpretation of the symbols above, will also be valid when char $F > 0$. In § 2, with the aid of a theorem of Schinzel, we obtain some properties of the number k, defined as in (1). Finally in § 3, we will express k explicitly as a function of a and m for a field F of characteristic 0 such that the only roots of unity in F are ± 1.

1. **Proof of Darbi's theorem for arbitrary characteristic.** Let char $F = p > 0$ and let m be a positive integer. Set $m = m_0 p^f$, with $(m_0, p) = 1$ and set $\zeta_m = \zeta_{m_0}$. Thus $\phi_F(m) = \phi_F(m_0)$.

Our first step is to reduce the proof of the general theorem to a proof of the separable case, that is, to the case where char $F \nmid m$. Indeed, let char $F = p > 0$ and $x^m - a$ be irreducible over F with root α. The splitting field of $x^m - a$ is $F(\alpha, \zeta_m) = F(\alpha^{p^f}, \alpha^{m_0}, \zeta_{m_0})$, which in turn is the compositum, over F, of $F(\alpha^{p^f}, \zeta_{m_0})$, a separable extension of F, and $F(\alpha^{m_0})$, a purely-inseparable extension. Thus, if Theorem 1 were true for the separable case, $x^{m_0} - a$ (with splitting field $F(\alpha^{p^f}, \zeta_{m_0})$), then we would have:

$$[F(\alpha, \zeta_{m_0}): F] = p^f(m_0\phi_F(m_0)/k) = m\phi_F(m)/k\,.$$