A Note on Morse Polynomials

Peter Müller

October 24, 2011

Let $f(X) \in K[X]$ be a polynomial over a field K of degree $n > 0$. Then $f(X)$ is called a *Morse polynomial* if the following holds: The derivative $f'(X)$ has $n-1$ distinct roots $\alpha_1, \ldots, \alpha_{n-1}$ in an algebraic closure of K, and the elements $f(\alpha_i)$, $i = 1, 2, \ldots, n-1$, are pairwise distinct.

Let t be a transcendental over K. In [Hil92] Hilbert proved that $\mathrm{Gal}(f(X) - t/\mathbb{C}(t)) = S_n$, where S_n is the symmetric group on the n roots of $f(X) - t$.

Hilbert's proof uses Riemann surfaces and the interpretation of the Galois group as a monodromy group. Using lifts to characteristic 0, Birch and Swinnerton–Dyer extended Hilbert's result to fields of positive characteristic, see [BSD59, Lemma 3]. Another approach is given in the proof of [Ser92, Theorem 4.4.5]. While that proof does not use topology anymore, it still uses non-trivial tools from valuation theory.

In this note we give a more elementary argument, based on the simple observation that a Morse polynomial is functionally indecomposable.

Theorem (Birch–Swinnerton, Dyer)**.** *Let $f(X) \in K[X]$ be a Morse polynomial of degree n. Then* $\mathrm{Gal}(f(X) - t/\mathbb{C}(t)) = S_n$.

Proof. Let p be the characteristic of K. Note that p does not divide n, as $f'(X)$ has degree $n-1$, and $p \neq 2$, as $f'(X)$ is separable. In particular, $f(X) - t$ is separable over $K(t)$.

We claim that $f(X)$ is not a composition of polynomials of smaller degree over K: Suppose that $f(X) = g(h(X))$, so $f'(X) = g'(h(X))h'(X)$ with $\deg(g'(X)) \geq 1$. We may assume that $h(X)$ is monic. Note that $g'(X)$ and $h'(X)$ are separable. Let β be a root of $g'(X)$, and γ_1, γ_2 be roots of $h(X) - \beta$. Then γ_1, γ_2 are roots of $f'(X)$, so $\gamma_1 = \gamma_2$ in view of $f(\gamma_1) = g(\beta) = f(\gamma_2)$. Thus $h(X) = (X - \gamma)^e + \beta$, where $e > 1$ because h is not linear. But then γ is

not only a root of $g'(h(X))$, but also a root of $h'(X)$, contrary to separability of $f'(X)$.

Furthermore, there is no composition $f(X) = g(h(X))$ for rational functions g, h of smaller degree: If that were the case, then it is easy to see that there is a linear fractional function $\mu(X)$ such that $g(\mu(X))$ and $\mu^{-1}(h(x))$ are polynomials.

Thus by Lüroth's theorem, there is no field properly between $K(x)$ and $K(t)$, where x is a root of $f(X) - t$. Thus $G = \mathrm{Gal}(f(X) - t/K(t))$ acts primitively on the conjugates of x.

Every multiple root of $f(X) - \lambda$ for some λ is a root of $f'(X)$. The Morse assumption shows the following: Let α be a root of $f'(X)$, and set $\lambda = f(\alpha)$. Then $f(X) - \lambda = (X - \rho)^2 h(X)$, where $h(X)$ is separable with $h(\rho) \neq 0$. Since the characteristic p is not 2, this shows (by standard arguments) that G contains a transposition. But a finite primitive permutation group which contains a transposition is symmetric. (This can be seen as follows: Let $i \sim j$ if $i = j$ or if G contains the transposition (i, j). Then $\sim$ is an equivalence relation, for if $(i, j), (j, k) \in G$ with $i \neq k$, then $(j, k)(i, j)(j, k) = (i, k) \in G$. Also, the action of G preserves $\sim$, so the equivalence classes are a block system, which by primitivity is the whole set which G acts on. Thus G contains all the transpositions of this set, and the claim follows.) □

References

[BSD59] B. J. Birch and H. P. F. Swinnerton-Dyer. Note on a problem of Chowla. *Acta Arith.*, 5:417–423 (1959), 1959.

[Hil92] D. Hilbert. Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. *J. Reine Angew. Math.*, 110:104–129, 1892.

[Ser92] J.-P. Serre. *Topics in Galois Theory.* Jones and Bartlett, Boston, 1992.

Institut für Mathematik, Universität Würzburg, Campus Hubland Nord, 97074 Würzburg, Germany
E-mail: peter.mueller@mathematik.uni-wuerzburg.de