Value Sets of Polynomials on Hilbertian Fields

Peter Müller

May 9, 2005

In [JM90] Jankowski and Marlewski prove by elementary methods that if f and g are polynomials in $\mathbb{Q}[X]$, then $f(\mathbb{Q}) = g(\mathbb{Q})$ implies the existence of $a, b \in \mathbb{Q}$ with $f(X) = g(aX + b)$. Here $f(\mathbb{Q})$ denotes the value set of f on $\mathbb{Q}$. We extend their assertion to coefficient fields which are Hilbertian. For instance, any finitely generated field (like a number field) is Hilbertian. For this result, and many related topics, see [FJ86].

Theorem 0.1. *Let k be a Hilbertian field. Let $f, g \in k[X]$ be non–constant polynomials with $g(k) \subseteq f(k)$. Then there is a polynomial $p \in k[X]$ with $g(X) = f(p(X))$. If $g(k) = f(k)$, then p is linear.*

Proof. Let X and Y be indeterminants over k. Set

$$f(X) - g(Y) = A_1(X, Y) \cdot A_2(X, Y) \cdots A_t(X, Y)$$

with irreducible polynomials A_i. As k is Hilbertian, there are infinitely many $r \in k$ such that $A_i(X, r)$ is irreducible for $i = 1, 2, \dots, t$. On the other hand, for each such r, there is an $s \in k$ with $f(s) - g(r) = 0$, i.e. $A_i(s, r) = 0$ for some i, depending on r. Thus there exists an index i such that $A_i(X, r)$ is irreducible and has a zero in X for infinitely many $r \in k$. So A_i has degree 1 in X. Therefore

$$f(X) - g(Y) = h(X, Y) \cdot (X \cdot v(Y) - u(Y))$$

with $h \in k[X, Y]$, $u, v \in k[Y]$, and v non–zero. Now specialize X, setting $X = u(Y)/v(Y)$. We get

$$f(\frac{u(Y)}{v(Y)}) = g(Y) .$$

As $p(Y) = u(Y)/v(Y)$ is integral over $k[Y]$, p is a polynomial.

Now suppose $f(k) = g(k)$. Then $g(X) = f(p(X))$ and $f(X) = g(q(X))$ with $p, q \in k[X]$. Comparing the degrees yields the assertion. □

Remark 0.2. The above problem is related to a question of Davenport. Here, for $f, g \in \mathbb{Z}[X]$, the condition $f(\mathbb{Q}) = g(\mathbb{Q})$ is weakened to $\bar{f}(\mathbb{F}_p) = \bar{g}(\mathbb{F}_p)$ for almost all primes p (where $\bar{f}$ denotes the reduction of coefficients modulo p). There are examples, like $f(X) = X^8$, $g(X) = 16X^8$, where the above condition doesn't imply $f(\mathbb{Q}) = g(\mathbb{Q})$. See [FJ86, 19.6] and [Mül98] for variations and partial results about this problem.

References

[FJ86] M. Fried, M. Jarden, *Field Arithmetic*, Springer–Verlag, Berlin Heidelberg (1986).

[JM90] L. Jankowski, A. Marlewski, *On the rational polynomials having the same image of the rational number set*, Funct. Approx. Comment. Math. (1990), **19**, 139–148.

[Mül98] P. Müller, *Kronecker conjugacy of polynomials*, Trans. Amer. Math. Soc. (1998), **350**, 1823–1850.

Mathematisches Institut, Universität Würzburg, Am Hubland, 97074 Würzburg, Germany

E-mail: `Peter.Mueller@mathematik.uni-wuerzburg.de`