Generic Polynomials are Descent-Generic

Gregor Kemper
IWR, Universität Heidelberg, Im Neuenheimer Feld 368
69 120 Heidelberg, Germany
email Gregor.Kemper@iwr.uni-heidelberg.de

January 8, 2001

Abstract

Let $g(X) \in K(t_1, \ldots, t_m)[X]$ be a generic polynomial for a group G in the sense that every Galois extension N/L of infinite fields with group G and $K \leq L$ is given by a specialization of $g(X)$. We prove that then also every Galois extension whose group is a subgroup of G is given in this way.

Let K be a field and G a finite group. Let us call a monic, separable polynomial $g(t_1, \ldots, t_m, X) \in K(t_1, \ldots, t_m)[X]$ **generic** for G over K if the following two properties hold.

(1) The Galois group of g (as a polynomial in X over $K(t_1, \ldots, t_m)$) is G.

(2) If L is an infinite field containing K and N/L is a Galois field extension with group G, then there exist $\lambda_1, \ldots, \lambda_m \in L$ such that N is the splitting field of $g(\lambda_1, \ldots, \lambda_m, X)$ over L.

We call g **descent-generic** if it satisfies (1) and the stronger property

(2') If L is an infinite field containing K and N/L is a Galois field extension with group $H \leq G$, then there exist $\lambda_1, \ldots, \lambda_m \in L$ such that N is the splitting field of $g(\lambda_1, \ldots, \lambda_m, X)$ over L.

DeMeyer [2] proved that the existence of an irreducible descent-generic polynomial for a group G over an infinite field K is equivalent to the existence of a generic extension S/R for G over K in the sense of Saltman [6]. Ledet [5] proved that the existence of a generic polynomial for a group G over an infinite field K is equivalent to the existence of a generic extension S/R of G over K. Thus for K infinite the existence of a generic polynomial for G implies the existence of a descent-generic polynomial for G. In this note we prove the following stronger result.

Theorem 1. *Every generic polynomial $g(t_1, \ldots, t_m, X)$ for G over K is descent-generic.*

Proof. G has a faithful, transitive permutation representation $G \hookrightarrow S_n$, by which it acts on the rational function field $K(x_1, \ldots, x_n)$. $K(x_1, \ldots, x_n)$ is Galois over $K(x_1, \ldots, x_n)^G$ with group G, hence there exist $p_1, \ldots, p_m \in K(x_1, \ldots, x_n)^G$ such that $K(x_1, \ldots, x_n)$ is the splitting field of $f(X) := g(p_1, \ldots, p_m, X)$ over $K(x_1, \ldots, x_n)^G$. Write

$$f(X) = \prod_{h \in Z} (X - h),$$

where $Z \subset K(x_1, \ldots, x_n)$ is the set of zeros of f. Let d_0 be the least common multiple of the denominators of the coefficients of $g(X)$. Then $d_0(p_1, \ldots, p_m) \neq 0$. Let d be the numerator of

Mathematics Subject Classification (2000): 12F10, 12F12.

$d_0(p_1, \ldots, p_m)$. For every $\sigma \in G \setminus \{1\}$ there exists a $h_\sigma \in Z$ such that $\sigma(h_\sigma) \neq h_\sigma$. Choose $0 \neq s \in K[x_1, \ldots, x_n]$ such that with $S := K[x_1, \ldots, x_n, s^{-1}]$ we have

$$Z \cup \{p_1, \ldots, p_m\} \cup \{(\sigma(h_\sigma) - h_\sigma)^{-1} \mid 1 \neq \sigma \in G\} \cup \{d^{-1}\} \subset S.$$

Now let N/L be a Galois extension of infinite fields with Galois group $H \leq G$. Then by Lemma 2 (see below) there exists an H-equivariant homomorphism $\psi\colon S \to N$ of K-algebras. Set $\lambda_i := \psi(p_i)$. Then $\lambda_i \in N^H = L$, $g(\lambda_1, \ldots, \lambda_m, X)$ is defined (no zero-division), and we have

$$g(\lambda_1, \ldots, \lambda_m, X) = \psi(f(X)) = \prod_{h \in Z} (X - \psi(h)).$$

Let $N' \subseteq N$ be the field extension of L generated by the $\psi(h)$ with $h \in Z$. We are done if we can show that $N' = N$. Indeed, for $1 \neq \sigma \in H$ we have

$$0 \neq \psi(\sigma(h_\sigma) - h_\sigma) = \sigma((\psi(h_\sigma)) - \psi(h_\sigma),$$

hence σ does not fix N'. By Galois theory, $N = N'$ follows. □

The proof required the following lemma, which is more or less well-known (see Kuyk [4] and Saltman [6]). We give a short proof for the convenience of the reader.

Lemma 2. *Let $G \leq S_n$ be a transitive permutation group and N/L a Galois extension of infinite fields with group G. Let $s \in N[x_1, \ldots, x_n]$ be a non-zero polynomial. Then there exist $\alpha_1, \ldots, \alpha_n \in N$ such that*

(a) $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ for all $\sigma \in G$, where $\sigma(\alpha_i)$ denotes the Galois action, and

(b) $s(\alpha_1, \ldots, \alpha_n) \neq 0$.

Proof. Let $\{\sigma(\vartheta) \mid \sigma \in G\}$ be a normal basis of N/L. For $i \in \{1, \ldots, n\}$, choose $\sigma \in G$ with $\sigma(1) = i$ and set

$$\beta_i := \sum_{\rho \in G_1} \sigma\rho(\vartheta) \quad \text{and} \quad \widetilde{\beta}_i := \sum_{j=1}^{n} \beta_i^{j-1} x_j,$$

where $G_1 \leq G$ is the stabilizer of 1. Then the β_i are pairwise distinct and $\tau(\beta_i) = \beta_{\tau(i)}$ for all $\tau \in G$. The determinant of the transition matrix from the x_i to the $\widetilde{\beta}_i$ is $\prod_{i<j}(\beta_j - \beta_i) \neq 0$. Thus the $\widetilde{\beta}_i$ are algebraically independent over N, so $g(x_1, \ldots, x_n) := s(\widetilde{\beta}_1, \ldots, \widetilde{\beta}_n) \neq 0$. Hence by the infinity of L there exist $\xi_1, \ldots, \xi_n \in L$ such that $g(\xi_1, \ldots, \xi_n) \neq 0$, and the $\alpha_i := \sum_{j=1}^{n} \xi_j \cdot \beta_i^{j-1}$ satisfy (a) and (b). □

Remark. (a) Although the proofs of the results of DeMeyer [2] and Ledet [5] mentioned above are constructive, one cannot use these proofs to obtain Theorem 1. Indeed, it is often necessary in Ledet's construction to add further indeterminates to $t_1, \ldots, t_m$. Therefore a polynomial with a larger number of parameters may arise when passing from a generic polynomial to a generic extension and from this to a descent-generic polynomial. Moreover, a generic polynomial need not be irreducible, but DeMeyer's construction always yields an irreducible descent-generic polynomial.

(b) In DeMeyer's proof that an irreducible descent-generic polynomial g gives rise to a generic extension (the "easier" direction), the irreducibility of g is not used. Thus Ledet's result is a direct consequence of Theorem 1 together with DeMeyer's result.

(c) Theorem 1 is well-suited for applications. For example, the result, due to Abhyankar [1], that every finite Galois extension of a field L containing $\mathbb{F}_q$ is the splitting field of a polynomial of the form

$$X^{q^m} + t_1 X^{q^{m-1}} + \cdots + t_{m-1} X^q + t_m X \qquad (*)$$

(a "q-vectorial" polynomial) follows from the fact that ($*$) defines a generic polynomial for $\mathrm{GL}_n(\mathbb{F}_q)$ (see Kemper and Mattig [3]).

(d) The property (1) of generic polynomials was not used in the proof of Theorem 1, so in fact we proved that the properties (2) and (2') are equivalent.

References

[1] Shreeram S. Abhyankar, *Galois Embeddings for Linear Groups*, Trans. Amer. Math. Soc. **352** (2000), 3881–3912.

[2] Frank R. DeMeyer, *Generic Polynomials*, J. of Algebra **84** (1983), 441–448.

[3] Gregor Kemper, Elena Mattig, *Generic Polynomials with Few Parameters*, J. Symbolic Comput. **30** (2000), 843–857.

[4] W. Kuyk, *On a Theorem of E. Noether*, Nederl. Akad. Wetensch. Proc. Ser. A **67** (1964), 32–39.

[5] Arne Ledet, *Generic Extensions and Generic Polynomials*, J. Symbolic Comput. **30** (2000), 867–872.

[6] David J. Saltman, *Generic Galois Extensions and Problems in Field Theory*, Adv. in Math. **43** (1982), 250–283.