

Generic Polynomials with Few Parameters

Gregor Kemper* and Elena Mattig

12 November, 1999

Abstract

We call a polynomial $g(t_1, \dots, t_m, X)$ over a field K generic for a group G if it has Galois group G as a polynomial in X , and if every Galois field extension N/L with $K \subseteq L$ and $\text{Gal}(N/L) \leq G$ arises as the splitting field of a suitable specialization $g(\lambda_1, \dots, \lambda_m, X)$ with $\lambda_i \in L$. We discuss how the rationality of the invariant field of a faithful linear representation leads to a generic polynomial which is often particularly simple and therefore useful. Then we consider various examples and applications in characteristic 0 and in positive characteristic. These include results on so-called vectorial polynomials and a generalization of an embedding criterion given by Abhyankar. We give recursive formulas for generic polynomials over a field of defining characteristic for the groups of upper unipotent and upper triangular matrices, and explicit formulas for generic polynomials for the groups $\text{GU}_2(q^2)$ and $\text{GO}_3(q)$.

Introduction

In inverse Galois theory (see Malle and Matzat [15]) one is interested in obtaining polynomials which have a given group as Galois group. It is even more desirable to have a polynomial which parametrizes all polynomials with a given group, or at least all Galois field extensions having this group. A typical example is the polynomial $X^2 - t$, which parametrizes all \mathbb{Z}_2 -extensions over a field of characteristic not 2. Such polynomials are called generic (see in Section 1 for a more precise definition).

A classical way to obtain generic polynomials was given by Noether [18], who proved that if the invariant field $K(x_1, \dots, x_n)^G$ of a permutation group $G \leq S_n$ is purely transcendental (= rational) over K , then a generic polynomial for G exists, and has n parameters. The question whether $K(x_1, \dots, x_n)^G$ is rational is known as Noether's problem. In this paper we start by showing that the rationality of the invariant field $K(V)^G$ of a faithful linear representation leads to a generic polynomial in $m = \dim(V)$ parameters. In fact, polynomials arising in this way have the stronger property that they parametrize exactly all Galois extensions having a *subgroup* of G as Galois group. We present a more general construction principle for generic polynomials (having this subgroup-property), which depends on the rationality of the invariant field of a suitable subfield of $K(x_1, \dots, x_n)$. Constructing generic polynomials from linear representations does not provide any new existence proofs for generic polynomials, since by the so-called no-name lemma (see Miyata [16]) the rationality of $K(V)^G$ implies the rationality of the invariant field of some faithful permutation representation. However, the generic polynomials arising from linear representations usually have fewer parameters and are simpler than generic polynomials obtained from permutation representations. Such polynomials are useful for theoretical and computational purposes. For example, searches for polynomials with certain embedding properties become much easier to perform if a simple generic polynomial is provided.

In the second section we consider some examples and applications. We obtain some particularly nice generic polynomials for small groups in characteristic 0 (or coprime to the group order). In

*The author gratefully acknowledges financial support by the Deutsche Forschungsgemeinschaft.

characteristic dividing the group order, our methods reach much further. We give simple generic polynomials for the general linear group, the special linear group, and the affine linear group, each in defining characteristic. As applications, we prove that every finite Galois extension in characteristic p is the splitting field of a vectorial polynomial (which was independently proved by Abhyankar [1]), and generalize a theorem by Abhyankar [1] on certain central embedding problems. Moreover, we obtain recursion formulas which give generic polynomials for the groups of upper unipotent and upper triangular matrices, and we explicitly give generic polynomials for the unitary groups $\mathrm{GU}_n(q^2)$ and the orthogonal groups $\mathrm{GO}_3(q)$ for q odd, again in defining characteristic.

We would like to thank B. Heinrich Matzat for valuable comments on a first version of this paper and for raising our interest in generic polynomials, and Shreeram S. Abhyankar for a brief but very fruitful meeting in Dagstuhl. We also thank the anonymous referees for some valuable comments.

1 Generic polynomials and rationality

We start by giving a definition of a generic polynomial, which follows DeMeyer [5].

Definition 1. *Let K be a field and G a finite group. A separable polynomial $g(t_1, \dots, t_m, X) \in K(t_1, \dots, t_m)[X]$ with coefficients in the rational function field $K(t_1, \dots, t_m)$ is called **generic** for G over K if the following two properties hold.*

- (a) *The Galois group of g (as a polynomial in X) is G .*
- (b) *If L is an infinite field containing K and N/L is a Galois field extension with Galois group $H \leq G$, then there exist $\lambda_1, \dots, \lambda_m \in L$ such that N is the splitting field of $g(\lambda_1, \dots, \lambda_m, X)$ over L .*

Remark 2. (a) Many authors (see Smith [23], Lecacheux [12], Ledet [13]) define generic polynomials as polynomials satisfying Definition 1(a), and Definition 1(b) only for $H = G$. It was proved by Ledet [14] that the existence of a generic polynomial in this sense implies the existence of a generic polynomial in the sense of Definition 1. All examples known to the authors seem to suggest the stronger assertion that both concepts of generic polynomials actually coincide.

- (b) The main result of DeMeyer [5] states that the existence of a generic polynomial (in the sense of Definition 1) for a group G over an infinite field K is equivalent to the existence of a generic extension in the sense of Saltman [19] for G over K . DeMeyer gives a procedure to obtain a generic extension from a generic polynomial and vice versa.
- (c) By Saltman [20], the existence of a generic extension for G over an infinite field K is equivalent to the condition that the invariant field $K(V_{\mathrm{reg}})^G$ of G acting by the regular representation is retract rational over K (see the definition in [20]). \triangleleft

For a finitely generated field extension L over K we say that $\varphi_1, \dots, \varphi_m \in L$ form a **minimal basis** if they generate L over K and are algebraically independent. Thus L/K is purely transcendental if and only if a minimal basis exists. The first goal is to prove the following general principle for the construction of generic polynomials.

Theorem 3. *Let K be a field, G a group acting on the rational function field $K(x_1, \dots, x_n)$ by permutations of the indeterminates, and let F be a G -stable intermediate field between K and $K(x_1, \dots, x_n)$ such that G acts faithfully on F . Assume that the fixed field F^G is purely transcendental over K . Then there exists a generic polynomial for G over K .*

More, precisely, let $\varphi_1, \dots, \varphi_m \in F^G$ be a minimal basis and choose a finite, G -stable subset $\mathcal{M} \subset F$ such that $F = F^G(\mathcal{M})$. Set

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) \in F^G[X].$$

Then $f(X) = g(\varphi_1, \dots, \varphi_m, X)$ with $g \in K(t_1, \dots, t_m)[X]$, and g is a generic polynomial for G over K .

Proof. Since the φ_i are algebraically independent, $K(t_1, \dots, t_m)$ is isomorphic to F^G , and a splitting field of g is isomorphic to $F^G(\mathcal{M}) = F$. Since the $y \in \mathcal{M}$ are pairwise distinct, f and therefore g is separable, and

$$\text{Gal}(g(X)) = \text{Gal}(F/F^G) = G.$$

It remains to prove property (b) of Definition 1. Choose $0 \neq d_0 \in K[t_1, \dots, t_m]$ such that $d_0 \cdot g \in K[t_1, \dots, t_m, X]$, and let $d \in K[x_1, \dots, x_n]$ be the numerator of $d_0(\varphi_1, \dots, \varphi_m)$. Furthermore, choose a non-zero polynomial $h \in K[x_1, \dots, x_n]$ such that $K[x_1, \dots, x_n, h^{-1}]$ contains d^{-1} , \mathcal{M} , all φ_i , and $\text{discr}_X(f)^{-1}$.

Let N/L be a Galois field extension with group $H \leq G$ as in Definition 1(b). By Lemma 4 (see below) there exist $\alpha_1, \dots, \alpha_n \in N$ such that

$$\sigma(\alpha_i) = \alpha_{\sigma(i)} \quad \text{for } \sigma \in H, \quad \text{and} \quad h(\alpha_1, \dots, \alpha_n) \neq 0.$$

Here $\sigma(i)$ is defined by the permutation action of G on the x_i , e.i., $\sigma(x_i) = x_{\sigma(i)}$. Thus

$$\Psi: K[x_1, \dots, x_n, h^{-1}] \rightarrow N, \quad x_i \mapsto \alpha_i$$

defines a homomorphism of K -algebras which commutes with the H -actions. Set $\lambda_i := \Psi(\varphi_i)$. Then $\lambda_i \in N^H = L$, and $g(\lambda_1, \dots, \lambda_m, X)$ is well-defined since $d^{-1} \in K[x_1, \dots, x_n, h^{-1}]$. We have

$$\prod_{y \in \mathcal{M}} (X - \Psi(y)) = \Psi(f) = g(\lambda_1, \dots, \lambda_m, X).$$

Therefore $N' := L(\Psi(\mathcal{M})) \subseteq N$ is the splitting field of $g(\lambda_1, \dots, \lambda_m, X)$ over L . By way of contradiction, assume that $N' \subsetneq N$. By Galois theory, there exists a $\sigma \in H \setminus \{1\}$ which fixes N' element-wise. Again by Galois theory and since $F = F^G(\mathcal{M})$, there is a $y \in \mathcal{M}$ such that $\sigma(y) \neq y$. Therefore $\sigma(y) - y$ is a divisor of $\text{discr}_X(f)$, and it follows that $\sigma(\Psi(y)) - \Psi(y) = \Psi(\sigma(y) - y)$ divides $\Psi(\text{discr}_X(f))$. But $\Psi(\text{discr}_X(f)) \neq 0$ since $\text{discr}_X(f)^{-1} \in K[x_1, \dots, x_n, h^{-1}]$. It follows that $\sigma(\Psi(y)) \neq \Psi(y)$, in contradiction to the statement that σ fixes N' . This completes the proof. \square

The proof required the following lemma. We omit the proof, since the lemma is implicitly contained in Kuyk [11]. See also Saltman [19].

Lemma 4. *Let $G \leq S_n$ be a permutation group and N/L a Galois extension of infinite fields with Galois group G . Let $f \in N[x_1, \dots, x_n]$ be a non-zero polynomial. Then there exist $\alpha_1, \dots, \alpha_n \in N$ such that*

- (a) $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ for all $\sigma \in G$, where $\sigma(\alpha_i)$ denotes the Galois action, and
- (b) $f(\alpha_1, \dots, \alpha_n) \neq 0$.

Remark 5. (a) The referee of this paper pointed out to us that under the hypotheses of Theorem 3 the invariant field $K(x_1, \dots, x_n)^G$ is retract rational. Indeed, we have an epimorphism

$$(K(x_1, \dots, x_n) \otimes_K F)^G \rightarrow K(x_1, \dots, x_n)^G, \quad f \otimes g \mapsto fg,$$

for which the map $f \mapsto f \otimes 1$ is a section. But $(K(x_1, \dots, x_n) \otimes_K F)^G$ is purely transcendental over F^G by the no-name lemma (see Miyata [16]), and therefore purely transcendental over K by the hypothesis. From this the retract rationality follows.

- (b) All examples of generic polynomials known to the authors can be viewed as instances of Theorem 3. This includes the generic polynomials for many abelian groups given by Saltman [19, Theorem 2.1], which in some cases exist even though Noether's problem has a negative answer. \triangleleft

In geometric terms the situation of Theorem 3 is as follows: G acts faithfully on a reduced affine K -scheme X of finite type such that the quotient $X//G$ is isomorphic to an affine m -space $\mathbb{A}^m(K)$. Moreover, we have a G -equivariant, dominant rational morphism $V \rightarrow X$ with V a permutation representation of G . Indeed, one can choose \mathcal{M} to be integral over $K[\varphi_1, \dots, \varphi_m]$, and X as the spectrum of the K -algebra R generated by \mathcal{M} and the φ_i . Then $X//G = \text{Spec}(R^G) = \text{Spec}(K[\varphi_1, \dots, \varphi_m])$. The dominant rational morphism $V \rightarrow X$ comes from the embedding $F \subseteq K(x_1, \dots, x_n)$ (see Hartshorne [6, Chapter I, Theorem 4.4]).

A reduced K -scheme X of finite type with a faithful G -action, together with a G -equivariant, dominant rational morphism $V \rightarrow X$ is often called a **compression** of V . The minimal dimension of a compression X of V is called the **essential dimension** of G (see Buhler and Reichstein [3]) and denoted by $\text{ed}_K(G)$. The essential dimension does not depend on the choice of the faithful linear representation V . It follows that the number m of parameters of a generic polynomial obtained from Theorem 3 is bounded from below by the essential dimension $\text{ed}_K(G)$. In fact, Buhler and Reichstein [3, Theorem 7.5] proved that $\text{ed}_K(G)$ is the minimal number of parameters in a so-called versal polynomial for G , but this is weaker than a generic polynomial, or even a polynomial satisfying Definition 1(a) and Definition 1(b) for $H = G$.

Example 6. In this example we assume that the characteristic of K is zero.

- (a) If G is abelian of rank r , then $\text{ed}_K(G) \geq r$, with equality if K contains a primitive e -th root of unity with $e = \exp(G)$ (Buhler and Reichstein [3, Theorem 6.1]). Thus a generic polynomial for G has at least r parameters.
- (b) If G is not cyclic or dihedral of order not divisible by 4, then $\text{ed}_K(G) > 1$ (Buhler and Reichstein [3, Theorem 6.2]). Thus generic polynomials with only one parameter can only exist for cyclic groups or dihedral groups of order not divisible by 4. \triangleleft

An important question is which schemes with a G -action arise as compressions of permutation representations. This is clearly the case if V is a faithful linear representation, since V is an epimorphic image of a free KG -module of finite rank, i.e., of a direct sum of copies of the regular representation. Using this, we deduce that a positive answer to Noether's problem for a faithful linear representation of G leads to a generic polynomial. If V is a linear representation of G , we write $K[V]$ for the symmetric algebra of V^* and $K(V)$ for the field of fractions of $K[V]$. $K(V)$ is a rational function field with a basis of V^* as indeterminates, and can be interpreted as the field of rational function on V . G acts on $K(V)$, and we denote the invariant field by $K(V)^G$.

Theorem 7. *Let G be a finite group and V an m -dimensional, faithful linear representation of G over a field K . Assume that $K(V)^G = K(\varphi_1, \dots, \varphi_m)$ (which implies that the φ_i form a minimal basis), and choose a finite, G -stable subset $\mathcal{M} \subset K(V)$ such that $K(V) = K(V)^G(\mathcal{M})$. Set*

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) \in K(V)^G[X],$$

so $f(X) = g(\varphi_1, \dots, \varphi_m, X)$ with $g \in K(\varphi_1, \dots, \varphi_m)[X]$. Then $g(X)$ is a generic polynomial for G over K .

If, moreover, the φ_i are homogeneous with

$$\deg(\varphi_1) = 1 \quad \text{and} \quad \deg(\varphi_2) = \dots = \deg(\varphi_m) = 0, \tag{1}$$

and if $\mathcal{M} \subset V^*$, then also $g(1, t_2, \dots, t_m, X)$ is a generic polynomial (in $m - 1$ parameters) for G .

Remark 8. By Kemper [8, Proposition 1.1], a minimal basis $\varphi_1, \dots, \varphi_m$ satisfying (1) exists if and only if there is a minimal basis of homogeneous rational invariants, and the only element of G acting as a scalar matrix is the identity. \triangleleft

Proof of Theorem 7. The first assertion follows immediately by Theorem 3 since $K(V)$ can be embedded G -equivariantly into the function field $K(\tilde{V})$ of a permutation module \tilde{V} (see above).

To prove the second assertion we take $F = K(V)_0$, the field of homogeneous rational functions of degree 0. Then $K(V) = F(\varphi_1)$, since $h \cdot \varphi_1^{-\deg(h)}$ lies in F_0 for any homogeneous $h \in K(V)$. This implies that G acts faithfully on F . We now claim that $F^G = K(\varphi_2, \dots, \varphi_m)$. Writing $N := K(\varphi_2, \dots, \varphi_m)$, we have $N \leq F^G$. The invariant φ_1 is transcendental over F^G , and on the other hand $K(V)^G$ has transcendence degree 1 over N , hence F^G/N is an algebraic extension. But $K(V)^G$ is a purely transcendental extension of N containing F^G , so we conclude that $F^G = N$.

Now $\{y/\varphi_1 \mid y \in \mathcal{M}\} \subset F$ is a G -stable subset which generates F as an extension of F^G . We have

$$\prod_{y \in \mathcal{M}} (X - y/\varphi_1) = \varphi_1^{-|\mathcal{M}|} \cdot f(\varphi_1 \cdot X) = g(1, \varphi_2, \dots, \varphi_m, X),$$

so the second assertion follows by Theorem 3. \square

2 Applications

We now consider various applications of Theorem 7, which divide naturally into two cases: the modular case where $|G|$ is divisible by the characteristic of K , and the non-modular case, where the characteristic is 0 or coprime to the group order.

2.1 Generic polynomials in characteristic 0 or coprime to $|G|$

In this section we always assume that the characteristic of K does not divide the group order $|G|$.

Abelian groups. Let G be an abelian group of exponent e and assume that K contains a primitive e -th root of unity. Then G is isomorphic to a linear group of the form

$$\left\{ \begin{pmatrix} \zeta_1 & & \\ & \ddots & \\ & & \zeta_m \end{pmatrix} \mid \zeta_i \in K, \zeta_i^{n_i} = 1 \right\}$$

with n_i positive integers. The invariant ring is generated by $x_1^{n_1}, \dots, x_m^{n_m}$. With $\mathcal{M} := \{\zeta x_i \mid i = 1, \dots, m, \zeta^{n_i} = 1\}$, Theorem 7 yields the generic polynomial

$$g(t_1, \dots, t_m, X) = (X^{n_1} - t_1) \cdots (X^{n_m} - t_m).$$

Thus Kummer theory can be viewed as a special example of Theorem 7. By Example 6(a), g has the least possible number of parameters.

Z_3 and Z_4 . We want to obtain generic polynomials for the cyclic groups Z_3 and Z_4 of orders 3 and 4 without making assumptions on roots of unity in the ground field. For $G = Z_3$ we use the representation given by the matrix $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. With $x_3 := -x_1 - x_2$ and $s_2 := x_1x_2 + x_1x_3 + x_2x_3$ we have rational invariants

$$\varphi_1 := \frac{x_1x_2x_3}{s_2}, \quad \varphi_2 := \frac{s_2^3}{(x_1x_2x_3)^2}, \quad \varphi_3 := \frac{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)}{x_1x_2x_3},$$

which generate the invariant field and satisfy the discriminant relation

$$\varphi_3^2 = -27 - 4\varphi_2.$$

Therefore φ_1 and φ_3 form a minimal basis if $\text{char}(K) \neq 2$, and with $\mathcal{M} := \{2x_1, 2x_2, 2x_3\}$ we obtain

$$\prod_{y \in \mathcal{M}} (X - y) = X^3 - \varphi_1^2(27 + \varphi_3^2) \cdot X + 2\varphi_1^3(27 + \varphi_3^2).$$

The second part of Theorem 7 (with a slight change of variables) leads to the generic polynomial

$$g(t, X) = X^3 - 3(1 + 3t^2) \cdot X + 2(1 + 3t^2)$$

for $G = Z_3$, which is over any field K with $\text{char}(K) \notin \{2, 3\}$. The generic polynomial for Z_3 given by Seidelmann [21] has two parameters and is somewhat more complicated.

For $G = Z_4$ we use the representation given by the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. We have invariants

$$\varphi_1 := x_1^2 + x_2^2 \quad \text{and} \quad \varphi_2 := \frac{x_1^2 - x_2^2}{x_1 x_2},$$

which satisfy

$$(\varphi_2^2 + 4)x_1^4 - \varphi_1(\varphi_2^2 + 4)x_1^2 + \varphi_1^2 = 0 \quad \text{and} \quad x_2 = \frac{(\varphi_2^2 + 4)x_1^3 - \varphi_1(\varphi_2^2 + 2)x_1}{\varphi_1 \varphi_2}.$$

Therefore $K(x_1, x_2)^G = K(\varphi_1, \varphi_2)$. Taking $\mathcal{M} = \{\pm\varphi_1/x_1, \pm\varphi_1/x_2\}$, we obtain

$$\prod_{y \in \mathcal{M}} (X - y) = X^4 - \varphi_1(\varphi_2^2 + 4)X^2 + \varphi_1^2(\varphi_2^2 + 4).$$

Replacing φ_1 by $-\varphi_1/2$ and φ_2 by $2\varphi_2$, we obtain

$$g(t_1, t_2, X) = X^4 + 2t_1(t_2^2 + 1) \cdot X^2 + t_1^2(t_2^2 + 1)$$

as a generic polynomial for Z_4 over any field K of characteristic not 2. Again this is simpler than the generic polynomial given by Seidelmann [21].

Dihedral groups. The dihedral group $G = D_n$ of order $2n$ has a faithful two-dimensional representation over a field containing $\zeta_n + \zeta_n^{-1}$, with ζ_n a primitive n -th root of unity. This representation is a reflection representation, hence the invariant ring is isomorphic to a polynomial ring by the theorem of Shephard, Todd and Chevalley. Therefore a generic polynomial for G over K exists. For $n = 2$, we obtain

$$g(t_1, t_2, X) = X^4 + t_1 X^2 + t_2^2$$

as a generic polynomial for the Klein 4-group. For $n = 4$, we have

$$g(t_1, t_2, X) = X^4 + t_1 X^2 + t_2$$

as a generic polynomial for D_4 . Both generic polynomials are over any field which is not of characteristic 2 (since $\zeta_n + \zeta_n^{-1} = -2$ or 0 for $n = 2$ or 4 , respectively), and they are much simpler than the ones given by Seidelmann [21]. By Example 6(b), the number of parameters is minimal. The existence of generic polynomials for the dihedral groups D_4 and D_8 was proved by Black [2].

(Near-) reflection groups. Some other interesting groups have reflection representations, such as $\text{SL}_2(3)$. Since the (two-dimensional) reflection representation is defined over a field containing $\sqrt{-3}$, we obtain a generic polynomial in two parameters over such a field.

By Kemper [8, Corollary 1.4] the following condition suffices to guarantee that the invariant field of G is purely transcendental: there exists a reflection group \tilde{G} containing G which is generated by G together with the scalar matrices contained in \tilde{G} . In fact, in this case the fields of invariants of degree 0 of G and of \tilde{G} coincide. In this way, groups such as A_5 can be reached, since $\{\pm 1\} \times A_5$ occurs as the complex reflection group G_{23} in the classification of Shephard and Todd [22]. We obtain a generic polynomial $g(t_1, t_2, X)$ for A_5 over a field containing $\sqrt{5}$. This polynomial is of degree 12 and can be printed in about five lines. In similar ways, there exists a generic polynomial in two parameters for the group $\text{PSL}_2(7)$ over $\mathbb{Q}(\sqrt{-7})$.

2.2 Modular applications

Some groups have faithful linear representations of particularly small dimension over a field of characteristic dividing the group order. Typical examples are classical groups with their defining representation. This has two consequences. First, the chances of finding a minimal basis for the invariant field of such a representation are fairly high, and second, the resulting generic polynomials have few parameters and are quite simple. In this section we will give a few examples.

The general and special linear group. Let V be an m -dimensional vector space over the finite field \mathbb{F}_q . Then we have

$$\prod_{y \in V^*} (X - y) = X^{q^m} + c_1 X^{q^{m-1}} + \cdots + c_{m-1} X^q + d^{q-1} X \quad (2)$$

(see Wilkerson [25]). Obviously the c_i are invariant under $G := \mathrm{GL}(V)$, and so is $c_m := d^{q-1}$. The c_i are called the **Dickson invariants**, and generate the invariant ring $\mathbb{F}_q[V]^G$. This can be seen by a Galois theoretic argument (again see Wilkerson [25]). Setting $\mathcal{M} := V^*$, we deduce from Theorem 7 that

$$g(t_1, \dots, t_m, X) = X^{q^m} + t_1 X^{q^{m-1}} + \cdots + t_{m-1} X^q + t_m X \quad (3)$$

is a generic polynomial for $G = \mathrm{GL}_m(q)$ over \mathbb{F}_q . Dividing by X also yields a generic polynomial. The polynomial d in Equation (2) turns out to be $\mathrm{SL}(V)$ -invariant, and it is easy to see that for an intermediate group G between $\mathrm{SL}(V)$ and $\mathrm{GL}(V)$ with $[\mathrm{GL}(V) : G] = e$ the invariants $c_1, \dots, c_{m-1}, d^{(q-1)/e}$ form a minimal basis of $K(V)^G$. Hence G has the generic polynomial

$$g(t_1, \dots, t_m, X) = X^{q^m-1} + t_1 X^{q^{m-1}-1} + \cdots + t_{m-1} X^{q-1} + t_m^e.$$

A polynomial of the form (3) (with t_i arbitrary) is called **q -vectorial** of q -degree m , since the evaluation map given by $g(X)$ is \mathbb{F}_q -linear (see Abhyankar [1]). Since every finite group has a faithful representation over \mathbb{F}_q , we see that every finite Galois extension N of a field L containing \mathbb{F}_q is the splitting field of a q -vectorial polynomial $g(X)$ over L . Moreover, if the Galois group has a faithful linear representation of degree m over \mathbb{F}_q , then the q -degree of $g(X)$ can be chosen to be m . This was independently proved by Abhyankar [1].

The following theorem gives polynomials which are “generic” for field extensions for which certain embedding problems are solvable. Here we call an embedding problem $G \rightarrow \mathrm{Gal}(N/L)$ solvable if there exists a Galois extension M of L containing N , and an isomorphism $G \xrightarrow{\sim} \mathrm{Gal}(M/L)$ such that the composition of this isomorphism with the restriction map $\mathrm{Gal}(M/L) \rightarrow \mathrm{Gal}(N/L)$ is the given epimorphism $G \rightarrow \mathrm{Gal}(N/L)$. For general information on embedding problems we refer the reader to Malle and Matzat [15, Chapter IV].

Theorem 9. *Let $G \leq \mathrm{GL}_n(q)$ be a linear group over a finite field, and let $Z \leq G$ be a subgroup consisting of scalar matrices. Set $H := G/Z$ and $e := |Z|$. Let N be a Galois extension of a field L containing \mathbb{F}_q such that $\mathrm{Gal}(N/L) = H$ and the embedding problem $G \rightarrow \mathrm{Gal}(N/L)$ is solvable. Then N is the splitting field of a polynomial of the form*

$$g(X) = X^{(q^m-1)/e} + \lambda_1 X^{(q^{m-1}-1)/e} + \cdots + \lambda_{n-1} X^{(q-1)/e} + \lambda_n$$

with $\lambda_i \in L$.

Proof. Let M/K be a solution of the embedding problem $G \rightarrow \mathrm{Gal}(N/L)$. By the above remark, M is the splitting field of a polynomial

$$h(X) = X^{q^m-1} + \lambda_1 X^{q^{m-1}-1} + \cdots + \lambda_{n-1} X^{q-1} + \lambda_n$$

with $\lambda_i \in L$, and Z acts on the roots of $h(X)$ by multiplication with e -th roots of unity. Let N' be the extension of L generated by the e -th powers of the roots of $h(X)$. Then N' is the splitting field of $g(X)$, with $g(X)$ as in the statement of the theorem. We have to show that $N' = N$. Clearly Z fixes N' , hence $N' \subseteq M^Z = N$. By Galois theory it remains to show that every $\sigma \in G$ fixing N' lies in Z . So assume that $\sigma(\vartheta^e) = \vartheta^e$ for all roots ϑ of $h(X)$. Then ϑ is an eigenvector of σ with respect to an e -th root of unity as eigenvalue. Observe that the roots of $X \cdot h(X)$ form an m -dimensional \mathbb{F}_q -vector space. By the above, this vector space consists entirely of eigenvectors. If $0 \neq \vartheta_1, \vartheta_2$ were two eigenvectors with distinct eigenvalues, then $\vartheta_1 + \vartheta_2$ would not be an eigenvector. Therefore there exists only one eigenvalue, and we conclude that σ is a scalar matrix lying in Z . This completes the proof. \square

Remark 10. Abhyankar [1] proved the following special case of Theorem 9: G is an intermediate group between $\mathrm{SL}_m(q)$ and $\mathrm{GL}_m(q)$, where $q - 1$ divides m , and Z is the group of all scalar matrices. Under these hypotheses, he also obtained a converse statement: If a Galois extension N/L with group G/Z comes from a polynomial $g(X)$ as in Theorem 9, then the embedding problem $G \rightarrow \mathrm{Gal}(N/L)$ is solvable. Under the weaker hypotheses of Theorem 9, this converse is false in general (for example, $m = 1$, $Z = G$ and $L = N = \overline{\mathbb{F}_q}$, an algebraic closure). \triangleleft

Affine linear groups. Further interesting examples are given by the affine linear group or the special affine linear groups, or intermediate groups. Suppose that H is an intermediate group between $\mathrm{SL}_m(q)$ and $\mathrm{GL}_m(q)$, and let e be the index of H in $\mathrm{GL}_m(q)$. The corresponding affine group is $G := \mathbb{F}_q^m \rtimes H$, where H acts naturally on \mathbb{F}_q^m . For $H = \mathrm{GL}_n(q)$ we obtain the affine linear group $\mathrm{AGL}_m(q)$. A faithful linear representation is given by

$$((a_1, \dots, a_m), A) \mapsto \begin{pmatrix} 1 & 0 & \cdots & 0 \\ a_1 & & & \\ \vdots & & A & \\ a_m & & & \end{pmatrix},$$

where $(a_1, \dots, a_m) \in \mathbb{F}_q^m$ and $A \in H$. Let the action on indeterminates x_0, x_1, \dots, x_m be given by this representation. We have invariants

$$c_0 := \prod_{a_1, \dots, a_m \in \mathbb{F}_q} (x_0 + a_1 x_1 + \cdots + a_m x_m)$$

and furthermore the Dickson invariants c_1, \dots, c_{m-1} and $b := d^{(q-1)/e}$ arising from the equation

$$\prod_{a_1, \dots, a_m \in \mathbb{F}_q} (X + a_1 x_1 + \cdots + a_m x_m) = X^{q^m} + c_1 X^{q^{m-1}} + \cdots + c_{m-1} X^q + d^{q-1} X$$

(see (2)). The only common zero of c_0, \dots, c_{m-1}, b in $\overline{\mathbb{F}_q}^m$ is the origin and the degree product of these invariants equals $|G|$, hence by Smith [24, Prop. 5.5.5] we conclude that

$$\mathbb{F}_q[x_0, \dots, x_n]^G = \mathbb{F}_q[c_0, \dots, c_{m-1}, b].$$

Thus we have a minimal basis of $\mathbb{F}_q(x_0, \dots, x_n)^G$, which we change now in order to apply the second part of Theorem 7. Set

$$\varphi_0 := c_0/b^e, \quad \varphi_i := \varphi_0^{q^{m-i}-q^m} \cdot c_i \quad (0 < i < m), \quad \text{and} \quad \varphi_m := \varphi_0^{(1-q^m)/e} \cdot b.$$

Then $c_0 = \varphi_0^{q^m} \varphi_m^e$, $c_i = \varphi_0^{q^m - q^{m-i}} \cdot \varphi_i$ ($0 < i < m$), and $b = \varphi_0^{(q^m-1)/e} \cdot \varphi_m$. Hence the φ_i provide another minimal basis, and $\deg(\varphi_0) = 1$ and $\deg(\varphi_i) = 0$ for $i > 0$. Choosing $\mathcal{M} :=$

$\{-x_0 + a_1x_1 + \cdots + a_mx_m \mid a_i \in \mathbb{F}_q\}$, we obtain from (2)

$$\begin{aligned} \prod_{y \in \mathcal{M}} (X - y) &= (X + x_0)^{q^m} + c_1(X + x_0)^{q^{m-1}} + \cdots + c_{m-1}(X + x_0)^q + d^{q-1}(X + x_0) \\ &= X^{q^m} + c_1X^{q^{m-1}} + \cdots + c_{m-1}X^q + b^eX + c_0 \\ &= X^{q^m} + \varphi_0^{q^m - q^{m-1}}\varphi_1 \cdot X^{q^{m-1}} + \cdots + \varphi_0^{q^m - q}\varphi_{m-1} \cdot X^q + \varphi_0^{q^m - 1}\varphi_m^e \cdot X + \varphi_0^{q^m} \varphi_m^e. \end{aligned}$$

By Theorem 7, this yields the generic polynomial given in the following theorem.

Theorem 11. *Let $\mathrm{SL}_m(q) \leq H \leq \mathrm{GL}_m(q)$ with $e := [\mathrm{GL}_m(q) : H]$, and let $G := \mathbb{F}_q^m \rtimes H$ be the corresponding affine group. Then*

$$g(X) = X^{q^m} + t_1 \cdot X^{q^{m-1}} + \cdots + t_{m-1} \cdot X^q + t_m^e \cdot X + t_m^e$$

is a generic polynomial for G over \mathbb{F}_q .

This is in particular interesting for $m = 1$. Here we obtain the generic polynomial

$$g(X) = X^q + t^e X + t^e.$$

Specializing further to $e = q - 1$ and replacing X by tX , we obtain the Artin-Schreier polynomial $g(X) = X^q + X + t$ as a generic polynomial for the additive group \mathbb{F}_q . Thus the above polynomial may be viewed as a generalization of Artin-Schreier polynomials.

P -groups. If K is a field of positive characteristic p and G a p -group, then by Miyata [16], $K(V)^G$ is purely transcendental over K for every representation V . Thus by Theorem 7 there exists a generic polynomial for every p -group. Miyata's proof uses the fact that with an appropriate choice of a basis the elements of G act as upper triangular matrices with 1's on the main diagonal. Of particular interest is the group $U_m(q)$ of all upper triangular matrices with entries in \mathbb{F}_q and 1's on the main diagonal, since every p -group can be embedded into some $U_m(q)$. The invariant ring of $U_m(q)$ is isomorphic to a polynomial ring generated by the products over orbits of the variables x_1, \dots, x_m (see Smith [24, Proposition 5.5.5]). The following theorem gives a recursion formula for the ensuing generic polynomials for $U_m(q)$.

Theorem 12. *Define polynomials $g_m(X) \in \mathbb{F}_q(t_1, \dots, t_{m-1})[X]$ by $g_2(X) := X^q - X - t_1$ and the recursion formula*

$$g_{m+1}(X) := g_m(X)^q - t_{m-1}^{q-1}g_m(X) - t_m.$$

Then $g_m(X)$ is a generic polynomial for $U_m(q)$ over \mathbb{F}_q . Therefore a Galois field extension N/L with $\mathbb{F}_q \subseteq L$ has a p -group as Galois group if and only if N is the splitting field of a specialization of a polynomial $g_m(X)$ as above.

Proof. For $U_{m+1}(q)$ we have generating invariants

$$\varphi_0 = x_1 \quad \text{and} \quad \varphi_i = \prod_{a_1, \dots, a_i \in \mathbb{F}_q} (a_1x_1 + \cdots + a_ix_i + x_{i+1}) \quad (0 < i \leq m).$$

In order to use Theorem 7 we choose $\mathcal{M}_{m+1} = \{a_1x_1 + \cdots + a_mx_m + x_{m+1}\}$. Set

$$\begin{aligned} f_{m+1}(X) &:= \prod_{y \in \mathcal{M}_{m+1}} (X - y) \quad \text{and} \\ h_{m+1}(X) &:= \prod_{a_1, \dots, a_m \in \mathbb{F}_q} (X - (a_1x_1 + \cdots + a_mx_m)). \end{aligned}$$

Then

$$f_{m+1}(X) = h_{m+1}(X - x_{m+1}) = h_{m+1}(X) - h_{m+1}(x_{m+1}) = h_{m+1}(X) - \varphi_m, \quad (4)$$

since $h_{m+1}(X)$ is a q -vectorial polynomial by Equation (2). We have

$$h_2(X) = \prod_{a \in \mathbb{F}_q} (X - ax_1) = X^q - X$$

and hence $f_2(X) = X^q - X - \varphi_1$, which yields $g_2(X)$. We have to prove the recursion formula

$$f_{m+1}(X) = f_m(X)^q - \varphi_{m-1}^{q-1} f_m(X) - \varphi_m,$$

which by (4) is equivalent to

$$h_{m+1}(X) = h_m(X)^q - \varphi_{m-1}^{q-1} h_m(X).$$

Both sides are monic of degree q^m in X , so we must show that for $b_1, \dots, b_m \in \mathbb{F}_q$, $X = b_1x_1 + \dots + b_mx_m$ is a zero of the right hand side. But we have

$$\begin{aligned} h_m(b_1x_1 + \dots + b_mx_m) &= \prod_{a_1, \dots, a_{m-1} \in \mathbb{F}_q} ((b_1 - a_1)x_1 + \dots + (b_{m-1} - a_{m-1})x_{m-1} + b_mx_m) = \\ &= h_m(b_mx_m) = b_m\varphi_{m-1}, \end{aligned}$$

hence the right hand side specializes to $b_m^q\varphi_{m-1}^q - b_m\varphi_{m-1}^q = 0$. This completes the proof. \square

Example 13. For $U_3(p)$, which is the Heisenberg group H_{p^3} , we obtain

$$g(X) = X^{p^2} - (1 + t_1^{p-1})X^p + t_1^{p-1}X - t_2$$

as a generic polynomial over \mathbb{F}_p . This ties in nicely with a result by Ledet [13], who constructed generic polynomials for H_{p^3} over fields of characteristic not equal to p

Upper triangular matrices. It is even easier to give a recursion formula for generic polynomials for the group of upper triangular matrices in $\mathrm{GL}_n(q)$.

Proposition 14. Define polynomials $g_m(X) \in \mathbb{F}_q(t_1, \dots, t_m)[X]$ by $g_1(X) := X^q - t_1X$ and the recursion formula

$$g_m(X) := g_{m-1}(X)^q - t_m g_{m-1}(X).$$

Then $g_m(X)$ is a generic polynomial for the group $B_m(q)$ of all upper triangular matrices in $\mathrm{GL}_m(q)$.

Proof. We have generating invariants $\varphi_1 := x_1^{q-1}$ and

$$\varphi_i := \prod_{a_1, \dots, a_{i-1} \in \mathbb{F}_q} (a_1x_1 + \dots + a_{i-1}x_{i-1} + x_i)^{q-1} \quad (2 \leq i \leq n).$$

Choose $\mathcal{M}_m := \{a_1x_1 + \dots + a_mx_m \mid a_1, \dots, a_m \in \mathbb{F}_q\}$ and set $f_m(X) := \prod_{y \in \mathcal{M}_m} (X - y)$. Then

$$f_1 = X^q - \varphi_1 X,$$

which yields g_1 as a generic polynomial. Moreover, we have

$$f_m(X) = \prod_{a \in \mathbb{F}_q} f_{m-1}(X - a_mx_m) = f_{m-1}(X)^q - f_{m-1}(X) \cdot f_{m-1}(x_m)^{q-1} = f_{m-1}(X)^q - \varphi_m f_{m-1}(X),$$

which proves the recursion formula. \square

The unitary group $\mathrm{GU}_2(q^2)$. It is known by Carlisle and Kropholler [4] that the invariant field of the general unitary group $\mathrm{GU}_n(q^2)$ acting on the natural module is rational. We give a generic polynomial for the case $n = 2$.

Proposition 15. *Let $G = \mathrm{GU}_2(q^2)$ be the general unitary group defined over \mathbb{F}_{q^2} . Then the polynomial*

$$g(X) = X^{(q^2-1)(q+1)} - t_1^{q-1} X^{q(q^2-1)} - t_2 X^{q^2-1} + t_1^{q^2-1}$$

is generic for G over \mathbb{F}_{q^2} .

Proof. We choose the hermitian form as $x_1^q x_2 + x_1 x_2^q$. Let V be the natural KG -module. By Carlisle and Kropholler [4], a minimal basis of $\mathbb{F}_{q^2}(V)^G$ is given by

$$\varphi_1 := x_1^q x_2 + x_1 x_2^q \quad \text{and} \quad \varphi_2 := \frac{x_1^{q^3} x_2 + x_1 x_2^{q^3}}{\varphi_1}.$$

Choose $\omega \in \mathbb{F}_{q^2}$ with $\omega^{q-1} = -1$. The factorization $\varphi_1 = x_2 \prod_{a \in \mathbb{F}_q} (x_1 + a\omega x_2)$ implies that

$$\mathcal{M} := \{bx_2 \mid b \in \mathbb{F}_{q^2}^\times\} \cup \{b(x_1 + a\omega x_2) \mid b \in \mathbb{F}_{q^2}^\times, a \in \mathbb{F}_q\}$$

is G -stable. We have

$$\begin{aligned} \prod_{y \in \mathcal{M}} (X - y) &= (X^{q^2-1} - x_2^{q^2-1}) \prod_{a \in \mathbb{F}_q} \left(X^{q^2-1} - \frac{(x_1 + a\omega x_2)^{q^2}}{x_1 + a\omega x_2} \right) \\ &= \frac{(x_2 X^{q^2-1} - x_2^{q^2}) (x_1 X^{q^2-1} - x_1^{q^2})^q + (x_1 X^{q^2-1} - x_1^{q^2}) (x_2 X^{q^2-1} - x_2^{q^2})^q}{\varphi_1} \\ &= X^{(q^2-1)(q+1)} - \varphi_1^{q-1} X^{q(q^2-1)} - \varphi_2 X^{q^2-1} + \varphi_1^{q^2-1}. \end{aligned}$$

This yields the generic polynomial $g(X)$. □

The orthogonal groups $\mathrm{GO}_3(q)$. It is a bit more difficult to give generic polynomials for the orthogonal groups $\mathrm{GO}_3(q)$.

Proposition 16. *Let $G = \mathrm{GO}_3(q)$ be the general orthogonal group with q an odd prime power. Then the polynomial*

$$g(X) = X^{q^2-1} - t_3 X^{q-1} + t_2^{q-1} - \frac{F(t_2) - F(0)}{t_2}$$

with $F(Y) := (t_1 X^{2(q-1)} - 2(Y + t_1^{(q+1)/2}) X^{q-1} + t_1^q)^{(q+1)/2}$ is generic for G over \mathbb{F}_q . Observe that $g(X)$ is monic of degree $q^2 - 1$ and has coefficients in $\mathbb{F}_q[t_1, t_2, t_3]$.

Proof. We may assume that G is defined by the quadratic form $x_1^2 - x_2^2 + x_3^2$. By Carlisle and Kropholler [4], the invariants $x_1^{q^i+1} - x_2^{q^i+1} + x_3^{q^i+1}$ ($0 \leq i \leq 2$) form a minimal basis for $K(V)^G$, where $K = \mathbb{F}_q$, and V is the natural module. We choose generators

$$\begin{aligned} \varphi_1 &:= x_1^2 - x_2^2 + x_3^2, \\ \varphi_2 &:= x_1^{q+1} - x_2^{q+1} + x_3^{q+1} - \varphi_1^{\frac{q+1}{2}}, \\ \varphi_3 &:= \frac{x_1^{q^2+1} - x_2^{q^2+1} + x_3^{q^2+1} - \varphi_1^{\frac{q^2+1}{2}}}{\varphi_2}. \end{aligned}$$

(In fact, the φ_i generate $K[V]^G$ as a polynomial ring, but we do not need this result.)

For $v \in V$ we denote the linear form on V given by $w \mapsto \langle v, w \rangle$ by $v^* \in V^*$. By Witt's extension theorem, the set $\mathcal{M} := \{v^* \mid v \in V \setminus \{0\} \text{ is isotropic}\}$ is one G -orbit, which has length $q^2 - 1$ (see Jacobson [7, Section 6.10]). We have that $x_1 - x_2 \in \mathcal{M}$ is a divisor of φ_2 . Hence all $v^* \in \mathcal{M}$ divide φ_2 . We can therefore choose a system of representatives \mathcal{M}_0 of the K^\times -orbits on \mathcal{M} such that

$$\varphi_2 = \prod_{y \in \mathcal{M}_0} y.$$

Now we have

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) = \prod_{y \in \mathcal{M}_0} (X^{q-1} - y^{q-1}) = \frac{1}{\varphi_2} \prod_{y \in \mathcal{M}_0} (yX^{q-1} - y^q).$$

The K -linear map $\Phi: V^* \rightarrow K[V][X]$, $y \mapsto yX^{q-1} - y^q$ extends to a homomorphism $\Phi: K[V] \rightarrow K[V][X]$ of K -algebras, which allows us to express the above equation as $f(X) = \Phi(\varphi_2)/\varphi_2$. We have

$$\begin{aligned} \Phi(x_i^2) &= x_i^2 X^{2(q-1)} - 2x_i^{q+1} X^{q-1} + x_i^{2q} \quad \text{and} \\ \Phi(x_i^{q+1}) &= x_i^{q+1} X^{q^2-1} - x_i^{2q} X^{q(q-1)} - x_i^{q^2+1} X^{q-1} + x_i^{q^2+q}, \end{aligned}$$

which after an easy computation leads to

$$\begin{aligned} \varphi_2 f(X) &= \varphi_2 \left(X^{q^2-1} - \varphi_3 X^{q-1} + \varphi_2^{q-1} \right) + \left(\varphi_1 X^{2(q-1)} - 2\varphi_1^{\frac{q+1}{2}} X^{q-1} + \varphi_1^q \right)^{\frac{q+1}{2}} \\ &\quad - \left(\varphi_1 X^{2(q-1)} - 2(\varphi_2 + \varphi_1^{\frac{q+1}{2}}) X^{q-1} + \varphi_1^q \right)^{\frac{q+1}{2}}. \end{aligned}$$

From this the claimed generic polynomial $g(X)$ follows by Theorem 7. \square

Other reflection groups. It is not true in the modular case that the invariant ring of a reflection group is always isomorphic to a polynomial ring (see Nakajima [17], Kemper and Malle [9]). However, it is true by Kemper and Malle [10] that the invariant field of every finite irreducible reflection group is purely transcendental over the ground field. Therefore every group which has a faithful irreducible reflection representation over a field K has a generic polynomial over K . Since the minimal bases are given explicitly in [10], these generic polynomials could be computed (given enough storage space and time for the hard cases). In particular, the general linear, orthogonal, symplectic and unitary groups have generic polynomials over their field of definition. (Here the rationality of the invariant fields is already known by Carlisle and Kropholler [4].)

The rationality of the invariant field can also be shown for some groups which are ‘‘close’’ to reflection groups (see Kemper [8]). This applies, for example, to the commutator subgroups $\Omega_n(q)$ of $\text{GO}_n(q)$ for q and n odd. These groups are simple, and $\Omega_3(q) \cong \text{PSL}_2(q)$. The second part of Theorem 7 therefore yields the existence of generic polynomials for $\text{PSL}_2(q)$ over \mathbb{F}_q in two parameters. Although these polynomials can be computed explicitly for given values of q , no general formula is known to date.

References

- [1] Shreeram S. Abhyankar, *Galois Embeddings for Linear Groups*, Trans. Amer. Math. Soc. **352** (2000), 3881–3912.
- [2] Elena V. Black, *Deformations of Dihedral 2-Group Extensions of Fields*, Trans. Amer. Math. Soc. **351** (1999), 3229–3241.

- [3] Joe Buhler, Zinovy Reichstein, *On the Essential Dimension of a Finite Group*, *Compos. Math.* **106** (1997), 159–179.
- [4] David Carlisle, Peter H. Kropholler, *Rational Invariants of Certain Orthogonal and Unitary Groups*, *Bull. London Math. Soc.* **24** (1992), 57–60.
- [5] Frank R. DeMeyer, *Generic Polynomials*, *J. of Algebra* **84** (1983), 441–448.
- [6] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, Heidelberg, Berlin 1977.
- [7] Nathan Jacobson, *Basic Algebra*, vol. 1, Freeman, New York 1985.
- [8] Gregor Kemper, *A Constructive Approach to Noether's Problem*, *Manuscripta Math.* **90** (1996), 343–363.
- [9] Gregor Kemper, Gunter Malle, *The Finite Irreducible Linear Groups with Polynomial Ring of Invariants*, *Transformation Groups* **2** (1997), 57–89.
- [10] Gregor Kemper, Gunter Malle, *Invariant Fields of Finite Irreducible Reflection Groups*, *Math. Ann.* **315** (1999), 569–586.
- [11] W. Kuyk, *On a Theorem of E. Noether*, *Nederl. Akad. Wetensch. Proc. Ser. A* **67** (1964), 32–39.
- [12] Odile Lecacheux, *Constructions de polynomes generiques a groupe de Galois resoluble*, *Acta Arith.* **86** (1998), 207–216.
- [13] Arne Ledet, *Generic and Explicit Realisation of Small p -Groups*, *J. Symbolic Comput.* **30** (2000), 859–865.
- [14] Arne Ledet, *Generic Extensions and Generic Polynomials*, *J. Symbolic Comput.* **30** (2000), 867–872.
- [15] Gunter Malle, B. Heinrich Matzatz, *Inverse Galois Theory*, Springer-Verlag, Berlin, Heidelberg 1999.
- [16] Takehiko Miyata, *Invariants of Certain Groups I*, *Nagoya Math. J.* **41** (1971), 69–73.
- [17] Haruhisa Nakajima, *Invariants of Finite Groups Generated by Pseudo-Reflections in Positive Characteristic*, *Tsukuba J. Math.* **3** (1979), 109–122.
- [18] Emmy Noether, *Gleichungen mit vorgeschriebener Gruppe*, *Math. Ann.* **78** (1918), 221–229.
- [19] David J. Saltman, *Generic Galois Extensions and Problems in Field Theory*, *Adv. in Math.* **43** (1982), 250–283.
- [20] David J. Saltman, *Retract Rational Fields and Cyclic Galois Extensions*, *Israel J. Math* **47** (1984), 165–215.
- [21] F. Seidelmann, *Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich*, *Math. Ann.* **78** (1918), 230–233.
- [22] G. C. Shephard, J. A. Todd, *Finite Unitary Reflection Groups*, *Canad. J. Math.* **6** (1954), 274–304.
- [23] Gene Ward Smith, *Generic Cyclic Polynomials of Odd Degree*, *Commun. Algebra* **19** (1991), 3367–3391.
- [24] Larry Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, Wellesley, Mass. 1995.

- [25] Clarence Wilkerson, *A Primer on the Dickson Invariants*, Amer. Math. Soc. Contemp. Math. Series **19** (1983), 421–434.

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

Lena Mattig
Fachbereich 06 Mathematik und Informatik
Universität Gesamthochschule Essen
Universitätsstr. 2
45 117 Essen 1
Germany
lena.mattig@uni-essen.de