On the Essential Dimension of a Finite Group

J. Buhler
Department of Mathematics, Reed College, Portland, OR 97202 USA

Z. Reichstein
Department of Mathematics, Oregon State University, Corvallis, OR 97331 USA

December 31, 1995

Abstract. Let $f(x) = \sum a_i x^i$ be a monic polynomial of degree n whose coefficients are algebraically independent variables over a base field k of characteristic 0. We say that a polynomial $g(x)$ is generating (for the symmetric group) if it can be obtained from $f(x)$ by a non-degenerate Tschirnhaus transformation. We show that the minimal number $\mathrm{d}_k(n)$ of algebraically independent coefficients of such a polynomial is at least $[n/2]$. This generalizes a classical theorem of Felix Klein on quintic polynomials and is related to an algebraic form of Hilbert's 13-th problem.

Our approach to this question (and generalizations) is based on the idea of the "essential dimension" of a finite group G: the smallest possible dimension of an algebraic G-variety over k to which one can "compress" a faithful linear representation of G. We show that $d_k(n)$ is just the essential dimension of the symmetric group S_n. We give results on the essential dimension of other groups. In the last section we relate the notion of essential dimension to versal polynomials and discuss their relationship to the generic polynomials of Kuyk, Saltman and DeMeyer.

1. Introduction

Let k be a field of characteristic 0. All fields in this paper will be assumed to contain k and all field embeddings will fix k pointwise. All algebraic varieties will be assumed to be irreducible. These varieties and all maps between them will always be defined over k.

Suppose

$$p(x) = x^n + a_1 x^{n-1} + \ldots + a_n \tag{1}$$

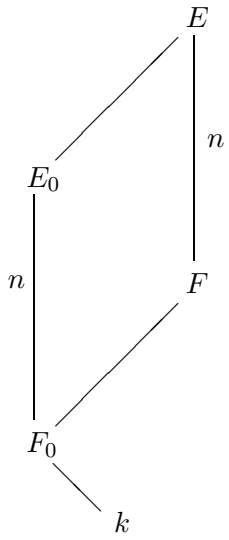
is a general polynomial of degree n. That is, we assume that the coefficients $a_1, \ldots, a_n$ are algebraically independent indeterminates over k. We would like to reduce the number of independent coefficients by means of a non-degenerate Tschirnhaus transformation, i.e., by considering equations satisfied by

$$t = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} \pmod{p(x)}\,, \tag{2}$$

where the $r_0, \ldots, r_{n-1}$ are rational functions in the coefficients a_i. For example, when $n = 2$, the equation satisfied by $t = x + a_1/2$ is of the form $q(t) = t^2 - c = 0$ which has only one independent parameter. By

a similar transformation, the general cubic polynomial can be shifted to get a polynomial in which the coefficient of t^2 is 0; by scaling the general cubic can be further reduced to the 1-parameter form $p(t) = t^3 + at + a$. Similarly, the general quartic polynomial can be written in the 2-parameter form $t^4 + at^2 + bt + b$. Later we will see that in this case the number of parameters cannot be reduced to one.

One way to formalize this question is as follows. Suppose that E/F is a field extension of degree n. We say that this extension is *defined* over a field $F_0 \subset F$ if there exists an extension E_0/F_0 of degree n contained in E such that $E_0F = E$. (Note that this also implies $E_0 \cap F = F_0$.)



In other words, E/F is defined over F_0 if there exists a primitive element α whose minimal polynomial has all of its coefficients in F_0. We define the *essential dimension* of E/F over k, or $\mathrm{ed}_k(E/F)$ for short, to be the minimal value of $\mathrm{trdeg}_k(F_0)$, where $\mathrm{trdeg}_k(F_0)$ denotes the transcendence degree of F_0 over k. This is the minimal number of independent parameters one needs to write down a generating polynomial for E over F.

Now let $p(x)$ be a general polynomial as in (1). Set $K = k(a_i)$ and $L = K[x]/(p)$. The minimal number of parameters required to represent p is simply the essential dimension $\mathrm{ed}_k(L/K)$; we shall denote this number by $\mathrm{d}_k(n)$. Our earlier observations can now be summarized by saying that

$$\mathrm{d}_k(2) = \mathrm{d}_k(3) = 1, \quad \mathrm{d}_k(4) = 2.$$

A classical result of Hermite [11] shows that after a suitable substitution a general polynomial of degree 5 can be written in the form $t^5 + at^3 + bt + b$. Thus $\mathrm{d}_k(5) \leq 2$. Felix Klein proved that $\mathrm{d}_k(5) \neq 1$ (which he

called "Kronecker's Theorem"); see [13], [4], and [19]. Thus $\mathrm{d}_k(5) = 2$. In degree 6 one can use a theorem of Joubert [12] to show that there exists a general polynomial of the form $t^6 + at^4 + bt^2 + ct + c$; see also Richmond [17]. This proves that $\mathrm{d}_k(6) \leq 3$. (For modern proofs of Hermite's and Joubert's results see Coray [5].) We shall later see that $\mathrm{d}_k(6)$ is, in fact, equal to 3.

One of the main results of this paper is the following generalization of the above-mentioned theorem of Felix Klein.

THEOREM 1.1. $\mathrm{d}_k(n)$ *is a (not necessarily strictly) increasing function of* n. *Moreover* $\mathrm{d}_k(n+2) \geq \mathrm{d}_k(n)+1$. *In particular,* $\mathrm{d}_k(n) \geq [n/2]$ *for any* $n \geq 1$.

For a proof of Theorem 1.1 see Corollary 4.3 and Theorem 6.5. The best upper bound on $\mathrm{d}_k(n)$ we have is $\mathrm{d}_k(n) \leq n-3$ for all $n \geq 5$; see Theorem 6.5(c). We note that the result $\mathrm{d}_k(4) > 1$ was only briefly mentioned in Klein (see also [19]) since quartic equations are solvable and hence, from the nineteenth century perspective, less interesting.

The smallest value of n for which these results do not establish the exact value of $\mathrm{d}_k(n)$ is 7; we do not know whether $\mathrm{d}_k(7)$ equals 3 or 4. This question has a tangential relationship to Hilbert's 13-th problem, the most straightforward form of which asks whether or not a seventh degree algebraic function can be expressed in terms of continuous functions of two arguments. This was settled by Kolmogorov and Arnold, and a number of generalizations have been obtained (see, for example, the references listed in [10, Lorentz, p. 419]). Hilbert also implied that the question can be interpreted purely algebraically; this approach to the 13-th problem is discussed at some length in his 1927 paper [9]. Additional algebraic interpretations of Hilbert's 13-th Problem have been given by Arnold and Shimura [10, p. 45-46], and by Abhyankar [1]. To be more precise about the relationship between the algebraic form of Hilbert's 13-th Problem and and the value of $\mathrm{d}_k(7)$, we consider a variant of $d_k(n)$ defined as follows. Let $p(x)$ be the general polynomial of degree n as in (1) and let $K = k(a_1, \dots, a_n)$ be as above. We now want to reduce the number of independent coefficients of p by means of a more general non-degenerate Tschirnhaus transformation (2) where $r_0, \dots, r_{n-1}$ are radical expressions in $a_1, \dots, a_n$ and elements of k. In other words, rather than requiring that $r_0, \dots, r_{n-1}$ lie in K as we did before, we now allow them to lie in the solvable closure K^{solv} of K. It is easy to see that $p(x)$ remains irreducible over K^{solv} for any $n \geq 5$. Let $M = K^{solv}[x]/(p(x))$. We now define $\mathrm{d}'_k(n)$ to be the essential dimension of the extension M/K^{solv}. Our definition clearly implies $\mathrm{d}'_k(n) \leq \mathrm{d}_k(n)$.

Hilbert [9] gave upper bounds on $\mathrm{d}'_k(n)$ for $n \leq 9$. In particular, he showed that $\mathrm{d}'_k(5) = 1$, $\mathrm{d}'_k(6) \leq 2$ and $\mathrm{d}'_k(7) \leq 3$. The question of whether or not $\mathrm{d}'_k(6)$ is actually equal to 2, explicitly mentioned by Hilbert in [9], was recently settled in the affirmative by Abhyankar [1]. (The proof uses a sextic surface constructed in Abyankhar's thesis [2].) The question of whether or not $\mathrm{d}'_k(7)$ is equal to 3 is an algebraic version of Hilbert's 13th problem. To the best of our knowledge, it is still open. In fact, we are not aware of any (non-trivial) lower bounds on $\mathrm{d}'_k(n)$ for any $n \geq 7$.

Our investigation of $\mathrm{d}_k(n)$ led us to a closer examination of the notion of essential dimension. We study it from a more geometric point of view in Sections 2 and 3. Let G be a finite group and let $G \longrightarrow GL(V)$ be a faithful finite-dimensional representation of G. Consider algebraic k-varieties Y with a faithful G-action for which there exists a dominant G-equivariant rational map $V \longrightarrow Y$ defined over k. The essential dimension of G is the minimal possible dimension of Y as above. We show that this number depends only on G and not on the representation we started out with; see Theorem 3.1. We call it the essential dimension of G over k or $\mathrm{ed}_k(G)$ for short. In Section 4 we explore a number of consequences of Theorem 3.1. In particular, we also show that the number $\mathrm{d}_k(n)$ we introduced earlier is equal to $\mathrm{ed}_k(\mathrm{S}_n)$; see Corollary 4.2.

This brings us to the question of computing $\mathrm{ed}_k(\mathrm{S}_n)$ and, more generally, $\mathrm{ed}_k(G)$ for an arbitrary finite group G. In principle, since $\mathrm{ed}_k(G)$ is an invariant of G it should be describable in terms of the group structure of G. We give such a description for abelian groups (when k has appropriate roots of unity; see Theorem 6.1) but we appear to be rather far from being able to give a general formula for $\mathrm{ed}_k(G)$ for an arbitrary group G. However, in Section 5, we prove a result which can be viewed as a step towards such a formula. Namely, if H is a cyclic central subgroup of G then under suitable conditions $\mathrm{ed}_k(G) = \mathrm{ed}_k(G/H) + 1$; see Theorem 5.3 and Corollary 5.5. These results are used in Section 6 to classify groups of essential dimension 1 and to compute and estimate $\mathrm{ed}_k(G)$ for some specific G, including abelian, symmetric, and alternating groups. Klein's proof of "Kronecker's Theorem" was actually accomplished by proving, in our language, that $\mathrm{ed}_k(\mathrm{A}_5) > 1$. This inequality is a special case of Theorem 6.7, which gives a lower bound on the essential dimension of alternating groups.

Finally, in Section 7 we relate the essential dimension of a finite group G to "versal" polynomials. This notion is related to Saltman's work [18] on generic field extensions; see also Demeyer [6], Kuyk [14] and our Remark 7.2. Our construction is somewhat different; its general form can be traced back at least to Grothendieck [8, Sections 2, 3]. Our

main result here is that $\mathrm{ed}_k(G)$ is the minimal number of algebraically independent coefficients for a versal polynomial with galois group G; see Theorem 7.5.

We thank S. Abhyankar, R. Guralnick, H. W. Lenstra, D. Saltman and D. Thakur for informative conversations. We are also grateful to J-P. Serre for reading several earlier versions of this paper and giving us a number of very helpful suggestions.

2. Galois Extensions

The notion of essential dimension of a finite extension E/F, introduced in the previous section, arises naturally in the geometric context when E is galois over F. In this section we take a closer look at this situation.

For convenience, we repeat the basic definition.

DEFINITION 2.1. Let E/F be a finite field extension of degree n.

(a) We say that E/F is *defined* over a subfield F_0 of F if there exists an extension E_0/F_0 of degree n such that $E_0 \subset E$ and $E_0F = E$.

(b) The essential dimension of E/F, which we will usually abbreviate as $\mathrm{ed}_k(E/F)$, is the minimal value of $\mathrm{trdeg}_k(F_0)$ as F_0 ranges over all fields for which E/F defined over F_0.

LEMMA 2.2. *Let E/F be a finite galois extension with galois group G. Then there is a galois extension E_1/F_1 with group G such that $E_1F = E$ and $\mathrm{trdeg}_k(F_1) = \mathrm{ed}_k(E/F)$. In other words, in the above definition of the essential dimension of E/F, we may assume without loss of generality that E_0 is G-invariant, the G-action on E_0 is faithful, and $F_0 = E_0^G$.*

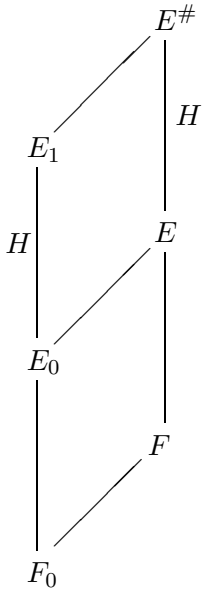
Proof. Choose E_0/F_0 as in the definition of essential dimension for E/F. Since E is galois over F, it contains a normal closure E_1 of E_0 over F_0. Let $F_1 = E_1^G$. By our construction E_1 is G-invariant, the G-action on E_1 is faithful (because $E_1F = E$), and $[E_1 : F_1] = n$. Moreover, since E_1 is a finite extension of F_0, we have $\mathrm{trdeg}_k(F_1) = \mathrm{trdeg}_k(E_1) = \mathrm{trdeg}_k(F_0) = \mathrm{ed}_k(E/F)$, as desired.

LEMMA 2.3. *Let E/F be a field extension of degree n and let $E^\#$ be the normal closure of E over F. Then $\mathrm{ed}_k(E/F) = \mathrm{ed}_k(E^\#/F)$.*

Proof. Denote the galois group $\mathrm{Gal}(E^\#/F)$ by G and its subgroup $\mathrm{Gal}(E^\#/E)$ by H. By Lemma 2.2 there exists a G-invariant subfield E_1 of $E^\#$ on which G acts faithfully and such that $\mathrm{trdeg}_k(E_1) = \mathrm{ed}_k(E^\#/F)$. Denote E_1^G by F_1, as above. Now set $E_0 = E_1^H$ and $F_0 = F_1$. Then $E_0 \subset E$,

$$[E_0 : F_0] = [G : H] = [E : F]$$

and $E_0F = E_1^H F = (E_1F)^H = (E^\#)^H = E$. Thus $\mathrm{ed}_k(E/F) \leq \mathrm{trdeg}_k(F_0) = \mathrm{ed}_k(E^\#/F)$.



To prove the opposite inequality, choose E_0/F_0 such that $F_0 \subset F$, $[E_0 : F_0] = n$, $E_0F = E$ and $\mathrm{trdeg}_k(F_0) = \mathrm{ed}_k(E/F)$. Since $E^\#$ is galois over F, it contains a normal closure E_1 of E_0 over F_0. By our construction G acts faithfully on E_1, $E_1F = E^\#$ and $\mathrm{trdeg}_k(E_1) = \mathrm{trdeg}_k(F_0) = \mathrm{ed}_k(E/F)$. This shows that $\mathrm{ed}_k(E/F) \geq \mathrm{ed}_k(E^\#/F)$ and thus completes the proof of the lemma.

We now define the notion of essential dimension in the geometric setting. First we introduce some terminology.

Let G be a finite group and let X be an (irreducible) algebraic variety. We call X a *G-variety* if it is equipped with a regular algebraic action $G \times X \longrightarrow X$. A subvariety $Y \subset X$ is called a *G-subvariety* if Y is G-invariant. A G-variety is *faithful* if every non-trivial element of G acts in a non-trivial way, i.e., the induced map $G \longrightarrow \mathrm{Aut}(X)$ is injective. A rational map $X \longrightarrow Y$ is called a rational *G-map* if it commutes with the action of G. *Linear* G-varieties or *representations of* G will be of special interest to us in the sequel. In this case X is a vector space and the G-action is given by a group homomorphism $G \longrightarrow GL(X)$.

We record the following simple observation for future reference.

LEMMA 2.4. *Let G be a finite group and let X be a G-variety defined over k. Denote the algebraic closure of k by $\overline{k}$.*

(a) Assume $X(k)$ is dense in $X(\overline{k})$. Then X is faithful if and only if G acts freely on a non-empty open subset of $X(k)$.

(b) Assume X is a k-unirational variety. Then X is faithful if and only if G acts freely on a non-empty open subset of $X(k)$.

Proof. (a) One implication is obvious: if G acts freely on a non-empty open subset of $X(k)$ then X is faithful. To prove the converse we may assume without loss of generality that $k = \overline{k}$. For $g \in G$ let $X(k)^g$ be the set of all points of $X(k)$ fixed by g. Since X is faithful, $X(k)^g$ is a proper closed subset of $X(k)$ for every $g \neq 1_G$. Let Z be the union of all these sets. Then $X \setminus Z$ is a dense open subset on which G acts freely.

(b) If X is k-unirational then $X(k)$ is dense in $X(\overline{k})$ and part (a) applies.

Given a faithful G-variety X, consider a dominant rational G-map $f : X \longrightarrow Y$ where Y is also faithful. Such a dominant map can be thought of as a "compression" of the G-action on X. Furthermore, since the G-action on Y is faithful, this process does not lead to loss of "essential information" about the original action on X. Thus it is natural to ask how much a given faithful G-action can be compressed.

DEFINITION 2.5. Let X be a faithful G-variety. The *essential dimension* of X is the minimal dimension of a faithful G-variety Y such that there exists a dominant rational G-map $f : X \longrightarrow Y$. We shall denote this number by $\mathrm{ed}_k(X)$.

Remark 2.6. Let k' be a finite extension of k and let X be a faithful G-variety defined over k. Our definition than implies that $\mathrm{ed}_k(X) \geq \mathrm{ed}_{k'}(X)$. Equality does not always hold; see Remark 6.4.

It is now easy to see that our geometric Definition 2.5 of essential dimension is closely related to the algebraic Definition 2.1.

LEMMA 2.7. *Let X be a faithful G-variety, let $E = k(X)$ be the field of rational functions on X and let $F = E^G$ be the field of G-invariant rational functions on X. Then* $\mathrm{ed}_k(X) = \mathrm{ed}_k(E/F)$.

Proof. Dominant rational G-equivariant maps $f : X \longrightarrow Y$ are in 1-1 correspondence with G-invariant subfields E_0 of E. Here $E_0 = k(Y)$. Moreover, G acts faithfully on Y if and only if it acts faithfully on E_0. Since $\dim(Y) = \mathrm{trdeg}_k(E_0)$, our assertion is a direct consequence of Lemma 2.2.

3. Essential Dimension of a Group

The purpose of this section is to prove that essential dimension of a linear action depends only on the group G and not on the corresponding faithful representation. We will also show that faithful linear representations have maximal essential dimension among all faithful G-varieties. More precisely, we shall prove the following theorem.

THEOREM 3.1. *Let G be a finite group.*

(a) There exists a faithful G-variety Z with the following property. For every faithful linear G-variety W, there exists a dominant rational G-map $W \longrightarrow Z$.

(b) The essential dimension of a faithful linear representation of a finite group G depends only on the group and not on the representation. We shall call this number the essential dimension of G and denote it by $\mathrm{ed}_k(G)$.

(c) Let X be a faithful G-variety. Then $\mathrm{ed}_k(X) \leq \mathrm{ed}_k(G)$.

As noted earlier, part (c) can be interpreted as saying that linear G-varieties are "least compressible" among all faithful G-varieties.

Let $V_{reg} = k[G]$ be the group algebra of G. The points of V_{reg} are of the form $\sum a_g g$ where the sum is taken over all $g \in G$. We shall view V_{reg} as a linear G-variety with the G-action given by the *(left) regular representation*, i.e.

$$h \sum_g a_g g = \sum_g a_g (hg) \ .$$

LEMMA 3.2. *(a) Let $a, b \in V_{reg}$. Assume that the G-orbit of a has $\mid G \mid$ distinct elements. Then there exists a (regular) G-morphism $\alpha : V_{reg} \longrightarrow V_{reg}$ such that $\alpha(a) = b$.*

(b) Let Y and C be affine G-invariant k-subvarieties of V_{reg} such that $C \neq V_{reg}$. Assume that the G-action on Y is faithful. Then there exists a G-morphism $\beta : V_{reg} \longrightarrow V_{reg}$ such that $\beta(Y) \not\subset C$.

Proof. Given a polynomial $p \in k[V_{reg}]$ we define the morphism $\alpha_p : V_{reg} \longrightarrow V_{reg}$ by

$$\alpha_p(x) \longrightarrow \sum_{g \in G} p(g^{-1}x) g$$

for every $x \in V_{reg}$. By construction α_p is a G-morphism, since for any $h \in G$

$$\alpha_p(hx) \longrightarrow \sum_{g \in G} p(g^{-1}hx) g = \sum_{g' = h^{-1}g \in G} p(g'^{-1}x) h g' = h \alpha_p(x) \ .$$

(a) Let $b = \sum b_g g$. By our assumption $g(a) \neq h(a)$ if g and h are distinct elements of G. Thus we can choose $p(x) \in k[V_{reg}]$ such that $p(g^{-1}a) = b_g$. Now let $\alpha = \alpha_p$. Then $\alpha(a) = b$, as desired.

(b) First assume that Y has a k-point a whose orbit has $\mid G \mid$ distinct elements. In this case part (b) is an easy consequence of part (a): we simply choose a k-point $b \notin C$, find $\alpha : V_{reg} \longrightarrow V_{reg}$ such that $\alpha(a) = b$ and let $\beta = \alpha$.

Now we turn to the general case. Let W_d be vector space of polynomials of degree $\leq d$ on V_{reg}. One easily checks that the set P_d of all p such that $\alpha_p(Y) \subset C$ is closed in W_d. In order to complete the proof of the lemma we need to show that $P_d \neq W_d$ for some $d \geq 1$. Assume the contrary: $P_d = W_d$ for every d. Let k' be a finite field extension of k. Since $P_d(k) = W_d(k)$ is dense in $W_d(k')$, we see that $P_d(k') = W_d(k')$. On the other hand, we can choose k' so that $Y(k')$ contains a point a with exactly $\mid G \mid$ elements in its orbit. Then as we noted above, there exist a $p \in k'[V_{reg}]$ such that $\alpha_p(Y) \not\subset C$. If p is a polynomial of degree d, this means $p \notin P_d$. In other words, $P_d(k') \neq W_d(k')$, a contradiction.

LEMMA 3.3. *Let W be a faithful linear G-variety. Then* $\mathrm{ed}_k(W) \geq \mathrm{ed}_k(V_{reg})$.

Proof. Let $f : W \longrightarrow Z$ be a dominant rational G-map such that Z is faithful and $\dim(Z) = \mathrm{ed}_k(W)$. Then there is an open G-invariant subset Z_0 of Z and an open G-invariant subset W_0 of W such that f restricts to a surjective morphism $W_0 \longrightarrow Z_0$. By our construction Z is a k-unirational variety. Thus Lemma 2.4(b) implies that we can choose $w \in W_0(k)$ such that the G-orbit of $z = f(w) \in Z_0(k)$ contains exactly $\mid G \mid$ points. Define a G-morphism $\phi : V_{reg} \longrightarrow W$ by $\phi(\sum a_g g) = \sum a_g g(w)$ and consider the composition map $f \circ \phi : V_{reg} \longrightarrow Z$. Let U be the closure of image of $f \circ \phi$ in Z. Since $f \circ \phi(1_G) = z$, we see that $z \in U$. By our choice of z this implies that the G-action on U is faithful.

We have thus constructed a dominant rational G-map $V_{reg} \longrightarrow U$ defined over k. Since U is a faithful G-variety, we have

$$\mathrm{ed}_k(V_{reg}) \leq \dim(U) \leq \dim(Z) = \mathrm{ed}_k(W) \ ,$$

as desired.

LEMMA 3.4. *Let X be a faithful G-variety of essential dimension d. Then there exists a dominant rational G-map $X \longrightarrow Y$ such that Y is a d-dimensional faithful affine G-subvariety of V_{reg}.*

Proof. By the definition of essential dimension there exists a dominant rational G-map $f : X \longrightarrow Z$ where Z is a faithful d-dimensional

G-variety. Let $\lambda \in k(Z)$ be a primitive element for the finite field extension $k(Z)^G \subset k(Z)$. Then $\Lambda : z \longrightarrow \sum a_g g$ where $a_g = g(\lambda)(z)$ is a rational G-map $Z \longrightarrow V_{reg}$. Let Y be the closure of $\Lambda(Z)$. We want to show that the composite map $f \circ \Lambda : X \longrightarrow Y$ has the properties claimed in the lemma. Since $\dim(Y) \leq \dim(Z) = d$, it is enough to show that Y is a faithful G-variety. Note that the function field $k(Y)$ can be identified with the subfield of $k(X)$ generated by λ and its translates. By our choice of λ, G acts faithfully on this subfield.

We are now ready to proceed with the proof of Theorem 3.1.

Proof of Theorem 3.1:. Choose a faithful G-variety Z and a dominant rational G-map $f : V_{reg} \longrightarrow Z$ such that $\dim(Z) = \mathrm{ed}_k(V_{reg})$. We will prove that this variety has the property claimed in part (a) of Theorem 3.1.

By Lemma 2.4(b) there exists a dense open subset $Z_0 \subset Z$ such that G acts freely on $Z_0(k)$. Let U be a dense open subset of V_{reg} such that f is regular on U and $f(U) \subset Z_0$. Let C be the complement of U in V_{reg}.

Now consider a faithful G-variety X of essential dimension d. By Lemma 3.4 there exists a dominant rational G-map $\gamma : X \longrightarrow Y$ where Y is a faithful d-dimensional G-subvariety of V_{reg}. By Lemma 3.2(b) there exists a G-morphism $\beta : V_{reg} \longrightarrow V_{reg}$ defined over k such that $\beta(Y) \not\subset C$. By our choice of C this means that the composite rational map

$$f \circ \beta \circ \gamma : X \longrightarrow V_{reg} \longrightarrow V_{reg} \longrightarrow Z \tag{3}$$

is well-defined. Moreover, the closure $Z' \subset Z$ of its image intersects Z_0 non-trivially. Hence, the G-action on Z' is faithful. Thus

$$\mathrm{ed}_k(X) \leq \dim(Z') \leq \dim(Z) = \mathrm{ed}_k(V_{reg}) \ . \tag{4}$$

If $X = W$ is a linear G-variety then by Lemma 3.3 $\mathrm{ed}_k(W) \geq \mathrm{ed}_k(V_{reg})$. Thus (4) implies (i) $\mathrm{ed}_k(W) = \mathrm{ed}_k(V_{reg})$ and (ii) $\dim(Z') = \dim(Z)$. Part (b) of Theorem 3.1 is an immediate consequence of (i). Moreover, (3) is the map whose existence is asserted in Theorem 3.1(a). Since $\mathrm{ed}_k(G) = \mathrm{ed}_k(V_{reg})$, part (c) follows from (4).

4. Elementary Properties

In this section we explore the consequences of Theorem 3.1.

LEMMA 4.1. *(a) If H is a subgroup of G then* $\mathrm{ed}_k(H) \le \mathrm{ed}_k(G)$.

(b) If G is a direct product of H_1 and H_2 then $\mathrm{ed}_k(G) \le \mathrm{ed}_k(H_1) + \mathrm{ed}_k(H_2)$.

Proof. (a) Obvious from the definition.

(b) For $i = 1, 2$ let W_i be a faithful representation of H_i and $\alpha_i : W_i \longrightarrow Y_i$ be a dominant rational H_i-map to a faithful H_i-variety Y_i such that $\dim(Y_i) = \mathrm{ed}_k(H_i)$. Then $W = W_1 \times W_2$ is a faithful G-representation and $Y = Y_1 \times Y_2$ is a faithful G-variety for the natural (componentwise) action of $G = H_1 \times H_2$. Moreover, $\alpha_1 \times \alpha_2 : W \longrightarrow Y$ is a dominant rational G-map. Thus $\mathrm{ed}_k(G) \le \mathrm{ed}_k(Y) = \mathrm{ed}_k(H_1) + \mathrm{ed}_k(H_2)$.

COROLLARY 4.2. *Let G be a transitive subgroup of S_n, let $x_1, \dots, x_n$ be independent variables over k and let $\mathbf{F}_G$ be the fixed field for the natural (permutation) action of G on $E = k(x_1, \dots, x_n)$. Then*

$$\mathrm{ed}_k(\mathbf{F}_G(x_1)/\mathbf{F}_G) = \mathrm{ed}_k(G).$$

In particular, the number $\mathrm{d}_k(n)$, defined in the introduction, is equal to $\mathrm{ed}_k(S_n)$.

Proof. Note that E is the normal closure of $\mathbf{F}_G(x_1)$ over $\mathbf{F}_G$. Thus by Lemma 2.3 $\mathrm{ed}_k(\mathbf{F}_G(x_1)/\mathbf{F}_G) = \mathrm{ed}_k(E/\mathbf{F}_G)$. Now let V be the faithful n-dimensional representation of G where the G-action is given by permuting the elements of a fixed basis. Then we can identify E with $k(V)$ as fields with a G-action. In other words, $\mathrm{ed}_k(E/\mathbf{F}_G) = \mathrm{ed}_k(V) = \mathrm{ed}_k(G)$; see Theorem 3.1(b).

To prove the last assertion of the corollary, recall that we defined $\mathrm{d}_k(n)$ as $\mathrm{ed}_k(\mathbf{F}_G(x_1)/\mathbf{F}_G)$ where $G = \mathrm{S}_n$.

COROLLARY 4.3. $\mathrm{d}_k(n)$ *is a increasing function of n. That is,* $\mathrm{d}_k(n) \le \mathrm{d}_k(n+1)$ *for every $n \ge 1$.*

Proof. Since $\mathrm{S}_n \subset \mathrm{S}_{n+1}$, we have $\mathrm{ed}_k(\mathrm{S}_n) \le \mathrm{ed}_k(\mathrm{S}_{n+1})$, see Lemma 4.1(a). In other words, $\mathrm{d}_k(n) \le \mathrm{d}_k(n+1)$ by Corollary 4.2.

LEMMA 4.4. $\mathrm{ed}_k(G) = 0$ *if and only if* $G = \{1\}$.

Proof. Consider a faithful representation V of G. By Lemmas 2.2 and 2.7, $\mathrm{ed}_k(G) = 0$ if and only if there exists a G-invariant subfield E_0 of $k(V)$ such that G acts faithfully on E_0, and E_0 is algebraic over k. Since $k(V)$ is a purely transcendental extension of k, and k is algebraically closed in $k(V)$, this is only possible if $E_0 = k$. In particular, G acts trivially on E_0. This action is faithful if and only if $G = \{1\}$.

Remark 4.5. Assume $\mathrm{ed}_k(G) \ge 2$ (this will always be true unless G is cyclic or odd dihedral; see Lemma 4.4 and Theorem 6.2). Then we

can find a faithful G-variety X such that the inequality of Theorem 3.1(c) is strict. In fact: for any finite group G there exists a curve with a faithful G-action.

Proof. Since G is isomorphic to a subgroup of S_n for some n, it is enough to show that for any $n \geq 2$ there exists a curve X_n with a faithful S_n-action.

To construct such a curve we need an irreducible polynomial $p(x)$ over $k(t)$ with galois group S_n. Since $k(t)$ is a Hilbertian field (see [7, Thm. 12.10]), $p(x)$ can be obtained by specializing the algebraically independent coefficients of the generic polynomial $x^n + a_1 x^{n-1} + \ldots + a_n$ in $k(t)$.

Let L be the splitting field of $p(x)$ over $K(t)$. Since L is a finite extension of $k(t)$, $\mathrm{trdeg}_k(L) = 1$. Thus L is the function field of a unique smooth projective curve X_n. The S_n-action on L translates into a (regular) faithful S_n-action on X_n.

5. Central Extensions

In this section we will prove that if G is a central extension of G' by a cyclic group of prime order then, under suitable hypotheses, $\mathrm{ed}_k(G) = \mathrm{ed}_k(G') + 1$.

We begin by recalling some well-known definitions concerning discrete valuations. Let F be a field and let $\nu\colon F^* \longrightarrow \mathbf{Z}$ be a discrete valuation. Note: we assume $\nu(F^*) = \mathbf{Z}$. As usual, we define $F_i = \nu^{-1}(i) \cup \{0\}$ and $F_{\geq i}$ = union of all F_j with $j \geq i$. Then $F_{\geq 0}$ is a local ring with maximal ideal $F_{\geq 1}$ and fraction field F. Denote the residue field by $\widetilde{F} = F_{\geq 0}/F_{\geq 1}$. Then $F_{\geq 1}/F_{\geq 2}$ is a 1-dimensional vector space over $\widetilde{F}$.

LEMMA 5.1. *Assume that $\nu\colon F^* \longrightarrow \mathbf{Z}$ is a discrete valuation on a field F, and that the residue field $\widetilde{F}$ has characteristic 0. Let σ be an automorphism of F of finite order which preserves ν, i.e., $\nu \circ \sigma = \nu$. Assume that the automorphisms of $\widetilde{F}$ and $F_{\geq 1}/F_{\geq 2}$ induced by σ are trivial. Then σ is the identity automorphism of F.*

Proof. This is a standard fact which says, in essence, that there is no wild ramification in characteristic zero. It is easily derived from [20, Cor. 2, Prop. IV.7] by passing to the completion and noting that σ acts trivially on both $\widetilde{F}$ and $F_{\geq 1}/F_{\geq 2}$ if and only if it acts trivially on $F_{\geq 0}/F_{\geq 2}$.

For completeness we also sketch a direct proof. First one can show that for $n = 0, 1, \ldots$ if $x \in F_n$ then $\sigma(x) = x + y$ where $y \in F_{\geq n+1}$.

This is obvious when $n = 0, 1$ and the general statement follows by induction.

It remains to show that $y = 0$, i.e., $\sigma(x) = x$. Assume the contrary: $\nu(y) = j$ for some $j \geq n + 1$. Since $\sigma(y) = y + z$ where $z \in F_{\geq j+1}$, we have $\sigma^m(x) = x + my$ modulo $F_{\geq j+1}$ for any $m \geq 0$. Since $\mathrm{char}\,(F_{\geq 0}/F_{\geq j+1}) = \mathrm{char}\,(\widetilde{F}) = 0$, this implies that σ has infinite order, contradicting our hypothesis.

LEMMA 5.2. *Assume that $\nu\colon F^* \longrightarrow \mathbf{Z}$ is a discrete valuation on a field F whose residue field $\widetilde{F}$ is of characteristic 0. Let G be a finite group of ν-preserving automorphisms of F. Moreover, assume that elements of G fix the roots of unity in $\widetilde{F}$. If $\tau \in G$ induces a trivial automorphism on $\widetilde{F}$ then τ lies in the center of G.*

Proof. We want to show that any element $\tau' \in G$ commutes with τ. Indeed, consider the commutator σ of τ and τ'. We want to prove that $\sigma = id_F$. Note that σ acts trivially of $\widetilde{F}$. Thus by Lemma 5.1 it is sufficient to show that σ also acts trivially on $T = F_{\geq 1}/F_{\geq 2}$. Since T is a 1-dimensional vector space over $\widetilde{F}$, the action of τ on it is given by multiplication by a root of unity ω. Since $\tau'(\omega) = \omega$, one easily checks that σ acts trivially on T.

Now we come to our key result.

THEOREM 5.3. *Let G be a finite group and let H be a cyclic subgroup of G of prime order p. Assume that*

(a) H is central.

(b) There exists a character $\chi\colon G \longrightarrow k^*$ which is non-trivial on H,

(c) H can be properly contained in a central cyclic subgroup H' of order r only if the base field k does not have a primitive r-th root of unity.

Then $\mathrm{ed}_k(G) = \mathrm{ed}_k(G/H) + 1$.

Remark 5.4. Note that if k contains a primitive p^m-th root of unity for sufficiently large m (namely $m \geq$ the p-exponent of $G/[G, G]$) then condition (b) is equivalent to $H \cap [G, G] = \{1\}$. Indeed, denote the latter condition by (b'). It is clear that (b) implies (b'). To prove the converse it is enough to lift a non-trivial character of H to the finite abelian group $G/[G, G]$. This can always be done; see, e.g., [15, p. 49]. We also remark that condition (c) is immediate if H is maximal among the cyclic subgroups of the center of G.

We now proceed with the proof of Theorem 5.3.

Proof. Let W be a faithful representation of G/H and let V_0 be the 1-dimensional representation of G given by χ. By our assumption on χ, $V = W \oplus V_0$ is a faithful representation of G. In particular, $G \subset \chi(G) \times G/H$. By Lemma 4.1 we have

$$\mathrm{ed}_k(G) \leq \mathrm{ed}_k(G/H) + \mathrm{ed}_k(\chi(G)) \ .$$

Since $\chi(G)$ has a 1-dimensional faithful representation V_0, we have $\mathrm{ed}_k(\chi(G)) \leq 1$ and thus

$$\mathrm{ed}_k(G) \leq \mathrm{ed}_k(G/H) + 1 \ .$$

It remains to prove the opposite inequality. Denote $\mathrm{ed}_k(G)$ by d. By Lemma 2.7 there exists a G-invariant subfield $F \subset k(V)$ such that $\mathrm{trdeg}_k F = d$ and G acts faithfully on F. Since W is a G-invariant hyperplane in V, it defines a G-invariant discrete valuation $\mu\colon k(V)^* \longrightarrow \mathbf{Z}$ where $\mu(\alpha)$ is the "order of vanishing of α on W" for any $0 \neq \alpha \in k(V)$. Note that the valuation ring $k(V)_{\geq 0}$ consists of those rational functions α on V whose domain of definition intersects W, and the maximal ideal $k(V)_{\geq 1}$ is the set of all α which restrict to 0 on W. Thus the residue field $\widetilde{k(V)}$ is naturally isomorphic to the field $k(W)$ of rational functions on W via an isomorphism which respects the G-action. Moreover, since H acts trivially on W, its action on $k(V)_{\geq 0}$ descends to a trivial action on $\widetilde{k(V)} = k(W)$.

We now restrict μ to F. First note that $\mu(F^*) \neq (0)$. Indeed, assume the contrary. Then $F \subset k(V)_{\geq 0}$. Taking the quotient by the ideal $k(V)_{\geq 1}$ gives a G-equivariant embedding of fields $F \hookrightarrow \widetilde{k(V)}$. Since H acts trivially on $\widetilde{k(V)}$, it also acts trivially on F. But G acts faithfully on F, a contradiction. Thus $\mu(F^*) = r\mathbf{Z}$ for some positive integer r. Then $\nu = (1/r)\mu\colon F^* \longrightarrow \mathbf{Z}$ is a G-invariant valuation. Clearly $F_{\geq 0} \subset k(V)_{\geq 0}$, $F_{\geq 1} \subset k(V)_{\geq 1}$ and $\widetilde{F} \subset \widetilde{k(V)} = k(W)$. Since $F_{\geq 0}$ is a local domain and $F_{\geq 1}$ is a maximal ideal, we have

$$\mathrm{trdeg}_k \widetilde{F} \leq \mathrm{trdeg}_k F - 1 = d - 1 \ . \tag{5}$$

(Since $F_{\geq 1}$ is a principal ideal, we actually have equality; however, this fact will not be needed in the sequel.) We claim that G/H acts faithfully on $\widetilde{F}$. Indeed, assume the contrary: there exists a subgroup H' of G such that H' properly contains H and the H'-action on $\widetilde{F}$ is trivial. By Lemma 5.2 H' is central in G. Note that Lemma 5.2 applies in this setting because k is algebraically closed in $k(W)$ (and thus in $\widetilde{F}$) which implies that elements of G automatically preserve all roots of unity. Denote the order of H' by r. Consider the action of H' on

$F_{\geq 1}/F_{\geq 2}$. Since $F_{\geq 1}/F_{\geq 2}$ is a 1-dimensional vector space over $\widetilde{F}$, this action cannot be faithful. Otherwise H' would be cyclic and $\widetilde{F}$ would contain a primitive r-th root of unity. This root of unity would then have to lie in k, contradicting our assumption (c). Therefore, there exists an element $h \in H'$ which acts trivially on both $\widetilde{F}$ and $F_{\geq 1}/F_{\geq 2}$. By Lemma 5.1, h acts trivially on F. Thus the G-action on F is not faithful. This contradiction proves the claim.

We are now ready to finish the proof of the theorem. Since G/H acts faithfully on $\widetilde{F} \subset k(W)$, we have $\mathrm{ed}_k(G/H) \leq \mathrm{trdeg}_k \widetilde{F}$; see Lemma 2.7. From (5) we conclude that $\mathrm{ed}_k(G/H) \leq d - 1 = \mathrm{ed}_k(G) - 1$, i.e., $\mathrm{ed}_k(G) \geq \mathrm{ed}_k(G/H) + 1$, as desired.

COROLLARY 5.5. *Let p be a prime integer, let k be a field containing a primitive p-th root of unity and let G_0 be a finite group and let $G = G_0 \times \mathbf{Z}/p\mathbf{Z}$. Assume that the center of G_0 is a p-group (possibly trivial). Then* $\mathrm{ed}_k(G) = \mathrm{ed}_k(G_0) + 1$.

Proof. Let $H = \{1\} \times \mathbf{Z}/p\mathbf{Z}$. Then G and H satisfy the conditions of Theorem 5.3 and $G/H = G_0$.

In the sequel we will only use Corollary 5.5 rather than Theorem 5.3 itself. However, the assumptions of Theorem 5.3 are, indeed, more general, even if k is assumed to contain all roots of unity. In other words, there are groups G satisfying the conditions of Theorem 5.3 which are not direct products of H and G/H. We thank R. Guralnick for helping us construct one such example with $|\ G\ | = p^4$.

6. Further Examples

6.1. Abelian Groups

We begin by determining the essential dimension of a finite abelian group. Recall that the *rank* of such a group is equal to the smallest number of elements which generate it. It can also be thought of as the maximal number r such that $(\mathbf{Z}/p\mathbf{Z})^r$ is contained in G for some prime number p. Let m be the exponent of G and suppose that the base field k contains a primitive m-th root of unity. Then every representation of G is a direct sum of characters. Since the dual group $\hat{G}$ is isomorphic to G, the rank r is equal to the smallest dimension of a faithful linear representation of G; see e.g., [15].

THEOREM 6.1. *Let G be a finite abelian group of exponent m. Assume that the base field k contains a primitive m-th root of unity. Then the essential dimension of G is equal to its rank.*

This result can be interpreted as saying that an r-dimensional faithful representation of G is "incompressible", i.e. it cannot be G-rationally mapped onto a faithful G-variety of dimension $\leq r-1$.

Proof. Since G has an r-dimensional faithful representation, it is enough to show that $\mathrm{ed}_k(G) \geq r$. Since G contains a copy of $(\mathbf{Z}/p\mathbf{Z})^r$, we may assume without loss of generality that $G = (\mathbf{Z}/p\mathbf{Z})^r$; see Lemma 4.1(a). The theorem now follows from Corollary 5.5.

6.2. Groups of Essential Dimension One

THEOREM 6.2. *Assume that k is a field containing all roots of unity and that G is a finite group. Then $\mathrm{ed}_k(G) = 1$ if and only if G is isomorphic to a cyclic group $\mathbf{Z}/n\mathbf{Z}$ or a dihedral group D_m where m is odd.*

Proof. (a) Assume $\mathrm{ed}_k(G) = 1$ and let W be a faithful representation of G. Then there exists a faithful G-curve Y and a dominant rational G-map $W \longrightarrow Y$. This implies, in particular, that Y is a rational curve and G is isomorphic to a subgroup of $\mathrm{Aut}(Y) = \mathrm{PSL}_2(k)$. The finite subgroups of $\mathrm{PSL}_2(k)$ were classified by Felix Klein. According to this classification, G is isomorphic to $C_n = \mathbf{Z}/n\mathbf{Z}$, D_n, A_4, S_4 or A_5; see e.g., [13, Chapter 1]. (Recall that $\mathrm{char}\,(k) = 0$ throughout this paper. The classification of finite subgroups of $\mathrm{PSL}_2(k)$ is somewhat different if $\mathrm{char}\,(k) \neq 0$.)

It remains to determine which of these groups have essential dimension 1. The groups C_n and D_m with m odd lift to $GL_2(k)$. The natural projection $k^2\backslash\{0\} \longrightarrow \mathbf{P^1}(k)$ shows that these groups have essential dimension 1; see Lemma 4.4. Each of the remaining groups contains a copy of $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Hence, by Lemma 4.1(a) and Theorem 6.1 their essential dimensions are ≥ 2.

Remark 6.3. Theorem 6.1 cannot be extended to non-commutative groups. Here by the rank of a non-commutative group G we mean the maximal rank of an abelian subgroup in contains. Assume G is a group whose order is a product of distinct odd primes. Then G has rank 1. On the other hand, by Theorem 6.2 $\mathrm{ed}_k(G) = 1$ if and only if G is cyclic. For all other G we have $\mathrm{ed}_k(G) > 1 = \mathrm{rank}(G)$.

Remark 6.4. If k does not contain all roots of unity then we may have to further restrict our list. In this case the question of computing $\mathrm{ed}_k(G)$ leads to interesting arithmetic problems even for cyclic groups G; for related results see [16].

6.3. Symmetric Groups

The essential dimension of the symmetric group S_n is of special interest to us. Recall that it is equal to the number $d(n)$ defined in the introduction; see Corollary 4.2.

THEOREM 6.5. *Let k be an arbitrary field of characteristic 0. Then*

(a) $\mathrm{ed}_k(S_{n+2}) \geq \mathrm{ed}_k(S_n) + 1$ *for any* $n \geq 1$.

(b) $\mathrm{ed}_k(S_n) \geq [n/2]$ *for any* $n \geq 1$.

(c) $\mathrm{ed}_k(S_n) \leq n - 3$ *for any* $n \geq 5$.

(d) $\mathrm{ed}_k(S_4) = \mathrm{ed}_k(S_5) = 2$, $\mathrm{ed}_k(S_6) = 3$.

Proof. (a) Since S_{n+2} contains $\mathrm{S}_n \times \mathbf{Z}/2\mathbf{Z}$, the desired inequality follows from Corollary 5.5 and Lemma 4.1(a).

(b) We use induction on n. Note that $\mathrm{ed}_k(1) = 0$ and $\mathrm{ed}_k(2) = 1$. The induction step is given by part (a).

(c) Consider the natural action of S_n on the n-dimensional vector space $V = k^n$. By Theorem 3.1(b), $\mathrm{ed}_k(\mathrm{S}_n) = \mathrm{ed}_k(V)$. Thus it is enough to construct an S_n-invariant subfield F of $k(x_1, \dots, x_n)$ such that the S_n-action on F is faithful and $\mathrm{trdeg}_k(F) \leq n-3$. Let F be the extension of k which is generated by the cross-ratios

$$[x_i : x_j : x_l : x_m] = (x_m - x_i)(x_l - x_j)(x_m - x_j)^{-1}(x_l - x_i)^{-1} \qquad (6)$$

as i, j, l, m range over all unordered 4-tuples of distinct integers between 1 and n. The symmetric group S_n permutes these cross-ratios among themselves. Thus our field F is S_n-invariant. Moreover, for $n \geq 5$ no non-trivial element of S_n fixes every one of the cross-ratios in (6). Thus S_n acts faithfully on F.

It remains to show that $\mathrm{trdeg}_k F \leq n-3$. Note that we may assume without loss of generality that k is algebraically closed. Indeed, if $\overline{k}$ is the algebraic closure of k then

$$\mathrm{trdeg}_k F = \mathrm{trdeg}_{\overline{k}}(F \otimes_k \overline{k}) \ .$$

The inclusion $F \subset k(x_1, \dots, x_n)$ induces a dominant rational map $f : (\mathbf{P^1})^n \longrightarrow Y$ where Y is a k-variety whose function field is F. Consider the diagonal $\mathrm{PSL}_2(k)$-action on $(\mathbf{P^1})^n$. Since the cross-ratios (6) are PSL_2-invariant, the fibers of f are unions of PSL_2-orbits. For $n \geq 5$ a generic PSL_2-orbit in $(\mathbf{P^1})^n$ is 3-dimensional. Thus a generic fiber of f has dimension ≥ 3. By the fiber dimension theorem we conclude that $\dim(Y) \leq n - 3$. (Note that f is dominant and k is algebraically closed.) In other words, $\mathrm{trdeg}_k F \leq n - 3$, as desired.

(d) Parts (b) and (c) imply $\mathrm{ed}_k(\mathrm{S}_5) = 2$ and $\mathrm{ed}_k(\mathrm{S}_6) = 3$. Part (b) also implies, $\mathrm{ed}_k(\mathrm{S}_4) \geq 2$. Since S_4 is a subgroup of S_5, the opposite inequality follows from Lemma 4.1(a).

Remark 6.6. An alternative way to phrase our argument in part (b) is as follows. Note that the subgroup of S_n generated by the transpositions $(2i-1, 2i)$ $(i = 1, \dots, [n/2])$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^{[n/2]}$. The inequality of part (b) now follows from a special case of Theorem 6.1:

$$\mathrm{ed}_k((\mathbf{Z}/2\mathbf{Z})^r) = r. \tag{7}$$

One cannot, however, get a sharper lower bound on $\mathrm{ed}_k(S_n)$ in this way since the rank of an abelian subgroup of S_n is always $\leq [n/2]$; see [3, Thm. 2.3(b)].

J-P. Serre has found another proof of (7). Briefly, suppose that all extensions with galois group $(\mathbf{Z}/2\mathbf{Z})^r$ can be parametrized with m parameters (see section 7 for the connection with essential dimension). Then all quadratic forms of rank r can be parametrized with m parameters, since they arise (essentially) as trace forms of "multiquadratic" equations

$$f(x) = (x^2 - a_1)(x^2 - a_2)...(x^2 - a_r) \ .$$

Serre proves that the r-th Stiefel-Whitney class of this form is generically nonzero. On the other hand, if $m < r$ then $H^r(F)$ is zero for a field F of transcendence degree m over an algebraically closed field. Thus $m \geq r$, as desired.

6.4. Alternating Groups

THEOREM 6.7. *Let k be an arbitrary field of characteristic 0. Then*

(a) $\mathrm{ed}_k(A_{n+4}) \geq \mathrm{ed}_k(A_n) + 2$ *for any* $n \geq 4$.

(b) $\mathrm{ed}_k(A_4) = \mathrm{ed}_k(A_5) = 2$.

(c) $\mathrm{ed}_k(A_n) \geq 2[n/4]$ *for any* $n \geq 4$.

Proof. (a) The group A_{n+4} contains $A_n \times A_4$ and A_4 contains $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Thus by Lemma 4.1(a),

$$\mathrm{ed}_k(A_{n+4}) \geq \mathrm{ed}_k(A_n \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \ .$$

The desired inequality now results from applying Corollary 5.5 (twice) to the group $A_n \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

(b) The inequalities $\mathrm{ed}_k(A_4)$ and $\mathrm{ed}_k(A_5) \geq 2$ follow from Lemma 4.1(a) and Theorem 6.1, since both groups contain $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. The opposite inequalities follow from Theorem 6.5(d).

(c) The claimed inequality clearly holds for $n = 4, 5, 6$ and 7; see part (b). The general case now follows from part (a) by induction on n.

7. Versal Polynomials

In this section we introduce and study *versal polynomials*. Our main result is Theorem 7.5 which relates versal polynomials with galois group G to the essential dimension $\mathrm{ed}_k(G)$.

Recall that throughout this paper all fields contain the base field k, which is of characteristic 0, and all field embeddings fix k pointwise.

If $p(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in F[t]$ is a monic irreducible polynomial, then a *specialization* of p is a polynomial $q(t) \in K[t]$ over a field K, such that there is a ring homomorphism $\phi\colon k[a_1, \ldots, a_n] \to K$ with $q(t) = t^n + \phi(a_1)t^{n-1} + \cdots \phi(a_n)$.

Let L/K be a finite field extension of degree n and let $L^{\#}$ be the normal closure of L over K. The group $G = \mathrm{Gal}(L^{\#}/K)$ acts on the n right cosets of its subgroup $\mathrm{Gal}(L^{\#}/L)$. This defines an embedding

$$\tau : G \hookrightarrow \mathrm{S}_n \tag{8}$$

of G as a transitive subgroup of S_n. Renumbering the n right cosets of $\mathrm{Gal}(L^{\#}/L)$, we see that τ is defined up to conjugacy in S_n. By abuse of terminology we shall refer to τ by simply saying that G is a *transitive permutation group*. We will also refer to this permutation group as the galois group of the (possibly non-galois) extension L/K or of any defining polynomial for this extension (over K.) For the remainder of this section we fix a transitive permutation group G as in (8).

DEFINITION 7.1. Let G be a transitive permutation group. An irreducible polynomial $p(t) \in F[t]$ with galois group G over F is said to be *versal* for G if for every extension L/K of degree n with group G there is a specialization $q(t)$ of $p(t)$ such that L/K is a root field of q, i.e., L is isomorphic to $K[t]/(q(t))$.

Remark 7.2. Our definition is similar to the definition of a generic polynomial in [6] (which is, in turn, closely related to the notion of generic extension in [18]) but is not identical to it. Aside from the fact that we work with non-galois extensions and permutation (rather than abstract) groups, there are two main differences. First of all, we do not require the field F to be a purely transcendental extension of k. Consequently, while the existence of generic polynomials in the sense of [6] is a rather delicate question, versal polynomials always exist; see below. Secondly, a specialization of a versal polynomial (in the sense we defined above) may not have galois group G. We use the term versal instead of generic to emphasize these distinctions.

Our first observation is that there is a natural smallest field F_p which can play the role of F in the definition. Let $p(t)$ be a versal polynomial for a transitive permutation group G. Let L be a root field of $p(t)$ and $L^{\#}$ be its normal closure over F. Let $y_1, \cdots, y_n$ be the roots of p in L. Then G permutes the y_i according to (8) and therefore acts on the field $k(y_1, \ldots, y_n)$. Let $F_p = k(y_1, \ldots, y_n)^G$ be the fixed field under that action. The coefficients of $p(t)$ lie in F_p, and the galois group of p over F_p is equal to G (as a permutation group.) Thus there is no loss of generality in assuming that $F = F_p$. Note that by our construction $F_p/k(a_1, \ldots, a_n)$ is an algebraic extension.

Our next observation is that versal polynomials exist for any transitive permutation group G. Indeed, let $x_1, \ldots, x_n$ be algebraically independent over k and set $\mathbf{F}_G = k(x_1, \ldots, x_n)^G$ and

$$p(t) \;=\; (t - x_1)(t - x_2) \cdots (t - x_n) \;=\; t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbf{F}_G[t].$$

Note that this is the same polynomial we considered in (1). The galois group of p over $\mathbf{F}_G$ is equal to G (as a permutation group.) Since the coefficients a_i are algebraically independent over k, p can be specialized to any polynomial over any field, and therefore p is versal.

Now we consider a generalization of this construction along the lines suggested in the introduction.

DEFINITION 7.3. Let $x_1, \ldots, x_n$ be independent variables over k and let $\mathbf{F}_G = k(x_1, \ldots, x_n)^G$. An irreducible polynomial $p(t) \in \mathbf{F}_G[t]$ of degree n is said to be a *generating polynomial* for G if $\mathbf{F}_G(x_1)$ is a root field of $p(t)$ over $\mathbf{F}_G$, i.e., $\mathbf{F}_G(x_1) \simeq \mathbf{F}_G[t]/(p(t))$.

THEOREM 7.4. *A generating polynomial for G is versal for G.*

The argument we present below is a similar to the proof of [18, Theorem 5.1]; see also [14, Theorem 1].

Proof. Let $p(t) = t^n + b_1 t^{n-1} + \ldots + b_n \in \mathbf{F}_G[t]$ be a generating polynomial as in Definition 7.3. Then $p(t)$ is the minimal polynomial over $\mathbf{F}_G$ for an element y such that $\mathbf{F}_G(y) = \mathbf{F}_G(x_1)$. For $i = 0, 1, \ldots, n-1$ write y^i as an $\mathbf{F}_G$-linear combination of the powers of x_1:

$$y^i = \sum_{j=0}^{n-1} f_{ij} x_1^j \,. \tag{9}$$

Let $f = \det([f_{ij}]) \in \mathbf{F}_G$ be the determinant of the the matrix $[f_{ij}]$. Then y generates $\mathbf{F}_G(x_1)$ over $\mathbf{F}_G$ if and only if $f \neq 0$. Let $y = y_1, y_2, \ldots, y_n$ be the conjugates of y under G, i.e., the roots of p in $k(x_1, \ldots, x_n)$. Write

$f_{ij}, y_i \in k(x_1, \ldots, x_n)$ as rational functions over a common denominator:

$$f_{ij} = g_{ij}/d, \quad y_i = v_i/d, \quad g_{ij}, v_i, d \in k[x_1, \ldots, x_n].$$

Let $q = \det(g_{ij})d \in k[x_1, \ldots, x_n]$.

In order to show that p is versal, we consider an extension L/K of degree n with galois group G. Let $L^\#$ be the normal closure of L in K. Recall that the right cosets of $H = \mathrm{Gal}(L^\#/L)$ in G can be numbered from 1 to n so that G permutes them according to (8). Since the embedding in (8) is only defined up to conjugacy, we may assume without loss of generality that the coset $H = 1_G H$ corresponds to 1. Let $\phi_i : L^\# \longrightarrow L^\#$ be a representative of the i-th coset. Note that the restrictions $\phi_1, \ldots, \phi_n$ to L are the n distinct embeddings of L in $L^\#$ over K.

We now view L as an n-dimensional vector space over K. Let $U_1 \subset L$ be the set of generators for the extension $K \subset L$. Then U_1 is Zariski-open in $L \simeq K^n$ and is defined over K. By the primitive element theorem it is nonempty. Let U_2 be the set of all $x \in L$ such that $q(\phi_1(x), \ldots, \phi_n(x)) \neq 0$. By [15, Theorem VI.12.1, p. 309] and linear independence of characters, the embeddings ϕ_i are algebraically independent. Hence, U_2 is also non-empty and Zariski-open. In particular, we conclude that the set $U = U_1 \cap U_2$ is a non-empty Zariski-open subset of L defined over K.

Next we choose $z \in U$ and define a ring homomorphism

$$k[x_1, \ldots, x_n] \longrightarrow L^\#$$

by sending x_i to $\phi_i(z)$ for $i = 1, \ldots, n$. Note that $\phi_1(z) = z$. By our choice of z, this homomorphism extends to a homomorphism $\mu : R \longrightarrow L^\#$ where $R = k[x_1, \ldots, x_n, y_1, \ldots, y_n, f_{ij}, 1/d, 1/f]$. Since L/K has galois group G, this homomorphism is G-equivariant. Thus μ sends elements of $\mathbf{F}_G = k(x_1, \ldots, x_n)^G$ to K and elements of $\mathbf{F}_G(x_1)$ to $K(z) = L$. In particular, the coefficients $b_1, \ldots, b_n$ of $p(t)$, lie in R (up to sign they are symmetric polynomials in $y_1, \ldots, y_n$) and $\mu(b_1), \ldots, \mu(b_n)$ lie in K.

Now consider the polynomial $\mu(p) = t^n + \mu(b_1)t^{n-1} + \ldots + \mu(b_n)$. Its roots are $\mu(y) = \mu(y_1), \mu(y_2), \ldots, \mu(y_n) \in L^\#$. In order to show that $p(t)$ is versal, it is sufficient to verify that the root field of $\mu(p)$ over K is L, i.e., $K(\mu(y)) = L$. Applying μ to both sides of (9), and remembering that $\mu(x_1) = z$, we obtain

$$\mu(y)^i = \sum_{j=0}^{n-1} \mu(f_{ij}) z^j \ .$$

Note that since $1/d \in R$, we have $f_{ij} \in R$ for every i, j. Thus $\mu(f_{ij})$ are well-defined elements of K. Moreover, by our choice of z, the determinant $\mu(f)$ of the above system is a non-zero element of K. Thus $K(\mu(y)) = K(z) = L$, as desired.

Given a transitive permutation group G, we would like to choose a versal polynomial $p(t) \in F[t]$ for G in the most economical way. In other words, we would like to define $p(t)$ so that it would have the minimal possible number of algebraically independent coefficients. Note that this number is equal to the minimal possible value of $\operatorname{trdeg}_k(F)$. Indeed, recall that for a given versal polynomial p we have a canonical choice of the field of definition $F = F_p$ and that for this choice of F the extension $F/k(a_1, \dots, a_n)$ is algebraic.

Our next result shows that this number is, in fact, equal to the essential dimension of G. In particular, it depends only on the abstract group G, and not on n or a specific realization of G as a permutation group.

THEOREM 7.5. *There exists a versal polynomial for a transitive permutation group G with $\operatorname{ed}_k(G)$ algebraically independent coefficients (over k). There does not exists a versal polynomial with fewer than $\operatorname{ed}_k(G)$ algebraically independent coefficients.*

Proof. Let $p(t)$ be a versal polynomial for G with the minimal number of algebraically independent coefficients. We shall denote this number by m. We want to prove that $m = \operatorname{ed}_k(G)$.

By Definition 7.1 this polynomial can be specialized to a polynomial $q(t)$ which generates the extension $\mathbf{F}_G(x_1)/\mathbf{F}_G$. In other words, q is a generating polynomial. By Theorem 7.4 $q(t)$ is also versal. Since $q(t)$ is a specialization of $p(t)$, it cannot have more than m algebraically independent coefficients. By our choice of m, it cannot have fewer than m algebraically independent coefficients either. This proves that we only need to consider generating polynomials, i.e., m is the minimal possible number of algebraically independent coefficients of a generating polynomial for G.

Note that a field F_0 contains the coefficients of some generating polynomial if and only if the extension $\mathbf{F}_G(x_1)/\mathbf{F}_G$ is defined over F_0; see Definition 2.1(a). Thus m is the minimal value of $\operatorname{trdeg}_k(F_0)$ among all such F_0. In other words, $m = \operatorname{ed}_k(\mathbf{F}_G(x_1)/\mathbf{F}_G)$; see Definition 2.1(b). By Corollary 4.2 this number equals $\operatorname{ed}_k(G)$, as claimed.

COROLLARY 7.6. *Every field extension $F \subset E$ of degree n (with $k \subset F$) is defined over a field F_0 such that $\operatorname{trdeg}_k(F_0) \leq \operatorname{ed}_k(S_n)$.*

Proof. Let $G \hookrightarrow \mathrm{S}_n$ be the galois group of E/F and let $p(t)$ be a versal polynomial for G with $m = \operatorname{ed}_k(G)$ algebraically independent

coefficients. This polynomial can then be specialized to a polynomial $q(t) = t^n + b_1 t^{n-1} + \ldots + b_n \in F[t]$ whose root field over F is E. In other words, E/F is defined over the field $F_0 = k(b_1, \ldots, b_n)$. Since q is a specialization of p, we have $\operatorname{trdeg}_k(F_0) \leq m$. Finally, note that $m = \operatorname{ed}_k(G) \leq \operatorname{ed}_k(\mathrm{S}_n)$; see Lemma 4.1(a).

References

1. Abhyankar, S. S., 1995, *Hilbert's Thirteenth Problem*, preprint.
2. Abhyankar, S. S., 1955, On the ramification of algebraic functions, *American J. of Math.* *77* 572–592.
3. Aschbacher, M. and Guralnick, R., 1989, On abelian quotients of primitive groups, *Proceedings AMS* 107, 89–95.
4. Brauer, R., 1934, Über die Kleinsche Theorie der algebraischen Gleichungen, *Math. Ann.* 110, 473-500; also in *Richard Brauer: Collected Papers* vol. 3. pp. 570-597.
5. Coray, D., 1987, Cubic hypersurfaces and a result of Hermite, *Duke J. Math.* 54, 657–670.
6. DeMeyer, F., 1982, Generic polynomials, *J. Algebra* **84** (1982), 441–448.
7. Fried, M., and Jarden, M., 1986, *Field Arithmetic*, Springer-Verlag, Berlin, Heidelberg and New York, 1986.
8. Grothendieck, A., 1958, La torsion homologique et les sections rationnelles, Exposè 5, *Seminaire C. Chevalley, Anneaux de Chow et applications*, 2nd année, IHP, 1958.
9. Hilbert, D., 1927, Über die Gleichung neunten Grades, *Mathematische Annalen* 97, 243–250.
10. Hilbert, D., 1900, Mathematical problems. Lecture delivered before the international congress of mathematicians at Paris in 1900, in *Mathematical developments arising from Hilbert Problems*, Proceedings of Symposia in Pure Mathematics 28 (1976), American Mathematical Society.
11. Hermite, C., 1861, Sur l'invariant du dix-huitiéme ordre des formes du cinquième degré, *J. Crelle* 59, 304–305.
12. Father Joubert, 1867, Sur l'equation du sixième degré, *C-R. Acad. Sc. Paris* 64, 1025–1029.
13. Klein, F., 1884, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Teubner, Leipzig, 1884. English translation: *Lectures on the icosahedron and solution of equations of the fifth degree*, translated by G.G. Morrice, 2nd and rev. edition, New York, Dover Publications, 1956.
14. Kuyk, W., 1964, On a theorem of E. Noether, *Nederl. Acad. Wetensch. Proc. Ser. A* 67, 32–39.
15. Lang. S., 1993, *Algebra* (Third Edition) Addison-Wesley Publishing Company, Reading, Massachusetts, 1993.
16. H. W. Lenstra, Jr., 1974, Rational Functions Invariant under a Finite Abelian Group, *Inventiones math.* 25, 299-325.
17. Richmond H. W., 1900, Note on the invariants of a binary sextic, *Quarterly J. of Math.* 31, 57–59.
18. Saltman, D., 1982, Generic galois extensions and problems in field theory, *Advances in Math.* 43, 250–283.
19. Serre, J.-P., 1978, Extensions icosaédriques, in *Collected Papers*, vol. III, pp. 550—554

20. Serre, J.-P., 1979, *Local Fields*, Graduate Texts in Mathematics 67, Springer-Verlag, Berlin.
21. Serre, J.-P., 1992, *Topics in Galois Theory*, Research Notes in Mathematics, v. 1, Jones and Bartlett, Boston.
22. Swan, R., 1983, Noether's Problem in Galois Theory, in *Emmy Noether in Bryn Mawr* (ed. B. Srinivasan and J. Sally), Springer-Verlag, York, Berlin.