Utrecht University

Faculty of Science
Department of Mathematics

Master Thesis

Essential Dimension

Author:
Joost Franssen

Supervisor:
Prof. dr. G. L. M. Cornelissen

Second reader:
Prof. dr. F. Beukers

June 6, 2019

Preface

Introduction

Essential dimension is a notion that encapsulates the minimal number of parameters necessary to describe an object. The formal concept was introduced for general polynomials and for finite groups by Buhler and Reichstein in 1997 (see [3]). The notion has its origins in the centuries old question of reducing the number of coefficients of a general polynomial by means of polynomial elimination. This was done for the purpose of finding the roots of said polynomial using radicals. For example, think of 'completing the square' to obtain the quadratic formula, or the method employed by Cardano to eliminate the quadratic term of the general cubic polynomial (see [23, p. 16]), wherefrom he derived his famous formula. Say we have a general polynomial of degree $n \in \mathbb{N}$

$$p(X) \coloneqq X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$$

with algebraically independent coefficients $a_1, \ldots, a_n$ over some field $\Bbbk$. Let $K \coloneqq \Bbbk(a_1, \ldots, a_n)$. Set $Y = T(X)$ for some polynomial

$$T(X) \coloneqq t_{n-1}X^{n-1} + \cdots + t_1 X + t_0$$

for suitable coefficients $t_0, \ldots, t_{n-1} \in K$. Upon eliminating X from the equations $p(X) = 0$ and $Y = T(X)$, we obtain a new polynomial

$$q(Y) \coloneqq Y^n + b_1 Y^{n-1} + \cdots + b_{n-1}Y + b_n$$

with coefficients in K. The polynomial q can be computed explicitly as the resultant of $p(X)$ and $Y - T(X)$. Its roots are precisely the images of the roots of p under T. The goal here is to choose the t_i in such a way that the resulting polynomial q has fewer algebraically independent coefficient than p; i.e., that the transcendence degree of $\Bbbk(b_1, \ldots, b_n)$ over $\Bbbk$ is lower. The above procedure is called a *Tschirnhaus transformation*.

Let us look at an example. Consider, for instance with $\Bbbk = \mathbb{Q}$, the general quadratic polynomial

$$p(X) = X^2 + a_1 X + a_2$$

over $K = \Bbbk(a_1, a_2)$. Let α_1 and α_2 be the roots of p in some field extension of K. Completing the square lets us write p as follows:

$$p(X) = \left(X + \tfrac{a_1}{2}\right)^2 + a_2 - \tfrac{a_1^2}{4}.$$

Consider $Y = T(X) = X + \frac{a_1}{2}$. Upon eliminating X, we obtain

$$q(Y) = Y^2 + a_2 - \tfrac{a_1^2}{4}.$$

Observe that the roots of q are precisely $\alpha_i + \frac{a_1}{2} = T(\alpha_i)$ for $i = 1, 2$. Thus q is a Tschirnhaus transform of p via T. Moreover, we see that q is defined over the field $\Bbbk\left(a_2 - \frac{a_1^2}{4}\right)$, which is of transcendence degree 1 over $\Bbbk$, whereas $\operatorname{trdeg}_{\Bbbk}(K) = 2$.

Tschirnhaus himself allowed T, and therefore q, to have coefficients in a radical extension of K. In [31] he found a suitable T to eliminate both the quadratic and linear terms of the general cubic polynomial. Thereby he managed to find the roots in terms of radicals in a different way than Cardano originally did. Later, in 1786, Bring applied Tschirnhaus transformations (allowing radicals as well) to eliminate the quartic, cubic, and quadratic terms of the general quintic polynomial (see [1]) in an effort to find the

roots using radicals. Subsequently, Jerrard, independently of Bring, also discovered this using Tschirnhaus transformations, which was published in 1834 ([22, pp. 398–399]). He moreover generalized Bring's result by showing that the terms of degree $n-1$, $n-2$, and $n-3$ can all simultaneously be brought to zero for any $n \geq 4$ using Tschirnhaus transformations that allow radical expressions as coefficients.
The question of reducing the number of coefficients is also related to an algebraic version of Hilbert's thirteenth problem about the general septic polynomial. By Jerrard's result, the general septic's sixth, fifth, and fourth power terms can be removed; the constant term a_7 can be made 1 using the transformation $T(X) = \frac{X}{\sqrt[7]{a_7}}$, yielding the form $p(X) = X^7 + b_1X^3 + b_2X^2 + b_3X + 1$. The roots of p can be seen as an algebraic function of the three variables b_1, b_2, and b_3. Hilbert's problem now asks whether this algebraic function can be written as the composition of finitely many bivariate functions. Originally, Hilbert asked in [13] about continuous functions, but in a later paper [14] raised the question of "the existence of *algebraic* functions of this kind". Thus an algebraic version of this problem asks whether the roots of p can be expressed using algebraic functions that only depend on two variables. In order to answer this question it is useful to look at Tschirnhaus transformations. Namely, the answer would be affirmative, if one finds a Tschirnhaus transform q, whose coefficients only depend on two variables, instead of three.

We shall only consider the stricter version of Tschirnhaus transformations, where the coefficients of T are required to lie in K itself. Applying such a Tschirnhaus transformation leaves the basic algebraic properties of the roots intact. Namely, the root field $K[Y]/(q)$ of the Tschirnhaus transform q is isomorphic to the root field $K[X]/(p)$ of p. The converse is also true: If some polynomial $q' \in K[Y]$ satisfies $K[Y]/(q') \cong K[X]/(p)$, then q' can be obtained from p via some Tschirnhaus transformation $T' \in K[X]$. Therefore, p and the resulting Tschirnhaus transform q can be deemed equivalent. The polynomial q is defined over the subfield $F \coloneqq \Bbbk(b_1, \ldots, b_n) \subseteq K$. If the transcendence degree of F over $\Bbbk$ is strictly lower than that of K, we have found a polynomial equivalent to p that depends on fewer algebraically independent parameters—which is precisely what happened in the example above for the general quadratic. This leads us to the following question.

Question: *What is the minimal transcendence degree over $\Bbbk$ of such fields F, over which a Tschirnhaus transform q of p is defined?*

This number is called the *essential dimension of p over $\Bbbk$*, which we denote by $\mathrm{d}_{\Bbbk}(n)$, where $n = \deg p$. Thus the 'minimal number of parameters necessary to describe p' is the minimal transcendence degree of F. The precise value of $\mathrm{d}_{\Bbbk}(n)$, as well as lower and upper bounds, is what Buhler and Reichstein thoroughly investigated in their original paper [3] over a field of characteristic 0. However, instead of utilizing Tschirnhaus transformations, they employ tools from algebraic geometry. They define the notion of essential dimension for faithful G-varieties; algebraic varieties on which a finite group G acts faithfully. Eventually, this gives rise to the concept of essential dimension of a finite group G, denoted $\mathrm{ed}_{\Bbbk}(G)$. The connection to general polynomials comes from the result that $\mathrm{ed}_{\Bbbk}(\mathrm{S}_n) = \mathrm{d}_{\Bbbk}(n)$, where S_n is the symmetric group of degree n. They prove in particular, for a field $\Bbbk$ of characteristic 0, the exact values

$$\mathrm{d}_{\Bbbk}(2) = \mathrm{d}_{\Bbbk}(3) = 1,\ \mathrm{d}_{\Bbbk}(4) = \mathrm{d}_{\Bbbk}(5) = 2,\ \text{and}\ \mathrm{d}_{\Bbbk}(6) = 3, \tag{1}$$

and the bounds

$$\mathrm{d}_{\Bbbk}(n+2) \geq \mathrm{d}_{\Bbbk}(n) + 1 \text{ and, for } n \geq 5,\ \mathrm{d}_{\Bbbk}(n) \leq n - 3. \tag{2}$$

Thereby they reproduced the results $\mathrm{d}_{\Bbbk}(5) \leq 2$, which can be derived from a result of Hermite's in 1861 in [12], and $\mathrm{d}_{\Bbbk}(5) \geq 2$ by a theorem of Klein in [18, §II.V.11]. Moreover, they improved the result $\mathrm{d}_{\Bbbk}(6) \leq 3$ obtained by Joubert ([16]) and Richmond ([25]).

We shall take a close look at the methods used by Buhler and Reichstein in order to generalize the results that they obtained. Since their requirement that $\Bbbk$ have characteristic 0 is rather strong, we set out to explore whether this assumption is necessary and, if it is dropped, which restrictions we must put on the ground field instead. We therefore ask ourselves the following.

Question: *Which restrictions on $\Bbbk$ are absolutely necessary for which the assertions made in* [3] *related to $\mathrm{d}_{\Bbbk}(n)$ can be generalized?*

Question: *Which proofs of* [3] *will still (mostly) work in this more general setting?*

It turns out that it is necessary that $\Bbbk$ be an infinite field in order to define the essential dimension of a finite group in the same way as Buhler and Reichstein did. In Theorem 4.15 we managed to prove the results in (1) and (2) for an arbitrary infinite field $\Bbbk$ of characteristic unequal to 2. Moreover, we

obtained similar results in the case that $\operatorname{char}\Bbbk = 2$; in Theorem 4.20 we show in particular that

$$\mathrm{d}_{\Bbbk}(2) = \mathrm{d}_{\Bbbk}(3) = 1,\ \mathrm{d}_{\Bbbk}(4) = \mathrm{d}_{\Bbbk}(5) = 2,\ \text{and}\ \mathrm{d}_{\Bbbk}(6) \in \{2,3\}, \tag{3}$$

and

$$\mathrm{d}_{\Bbbk}(n+3) \geq \mathrm{d}_{\Bbbk}(n)+1 \text{ provided that } n \neq 4 \text{ and } \zeta_3 \in \Bbbk, \text{ and, if } n \geq 5,\ \mathrm{d}_{\Bbbk}(n) \leq n-3. \tag{4}$$

Here ζ_3 denotes a primitive third root of unity. Moreover, for any characteristic we were able to generalize all assertions made in [3] that were necessary to prove the above results, which shows that the methods used by Buhler and Reichstein work in a much more general setting than in which they introduced them.

Before we are able to obtain these results in Chapter 4, we need to lay the groundwork. We start in Chapter 1 by formally defining the essential dimension of a finite, separable field extension. Therefrom comes the notion of essential dimension of a general polynomial. We explore the precise relation it has with Tschirnhaus transformations and how they can be utilized to find upper bounds, which we do. We end the chapter with our first results on the value of $\mathrm{d}_{\Bbbk}(n)$ for $1 \leq n \leq 4$.
As mentioned above, Buhler and Reichstein used concepts from algebraic geometry to further their research. Whence we delve into some preliminary notions about algebraic varieties in Chapter 2. We explore in detail the diverse notions of 'points' a variety may admit, and some aspects of base change. These results shall prove to be invaluable in the last two chapters.
Chapter 3 is where we finally start to follow [3]. Here we develop the theory of essential dimension for an algebraic variety, on which a finite group acts faithfully, over a field $\Bbbk$ of arbitrary characteristic. We introduce linear varieties, wherewith we later attain the concept of essential dimension of a finite group. We generalize many statements proved in [3] that are necessary for this. We have meticulously looked at each of those assertions and proofs in [3] to decide whether the statement is still true in arbitrary characteristic and which proofs still work. We then accordingly adjusted the statements or laid milder conditions than $\operatorname{char}\Bbbk = 0$ (the only condition being that $\Bbbk$ be infinite for some claims). We also tweaked the proofs where necessary, or replaced them entirely.
Finally, in Chapter 4 we define the essential dimension of a finite group G, denoted $\mathrm{ed}_{\Bbbk}(G)$. We continue to follow [3], although some of the main results that generalize those of [3] are due to [17]. We first explore some properties of $\mathrm{ed}_{\Bbbk}(G)$, before moving on to the relation to general polynomials. We prove that $\mathrm{ed}_{\Bbbk}(\mathrm{S}_n) = \mathrm{ed}_{\Bbbk}(n)$, and in Theorems 4.15 and 4.20 we obtain the results (1) and (2) for $\operatorname{char}\Bbbk \neq 2$, and (3) and (4) for $\operatorname{char}\Bbbk = 2$. We end this chapter by describing our process of our unsuccessful attempt to determine the exact value of $\mathrm{d}_{\Bbbk}(6)$ over characteristic 2, which hopefully will be useful to others willing to attempt this.

About the Proofs Presented

The proofs that we present here come from various sources. Some are entirely our own, some are inspired by others' proof, and some are obtained from an external source. This section aims to document the primary contributions that we have made and to discuss some of the issues with the proofs that we have found. The majority of the proofs obtained elsewhere have been almost completely rewritten in order to fill in as many useful details as we could so that each proof become more legible and easier to understand. We thereby chose to sacrifice brevity or elegance for clarity.

- The proofs of Proposition 1.10 and the necessary lemmas are our own. Only part of this assertion is mentioned in [15, Proposition 6.1.14].
- The necessary Tschirnhaus transformations that we use in Examples 1.15, 1.16, and 1.17 were found by us, for which we made use of `Mathematica`.
- The exploration in Section 2.2 about the diverse notions of 'points' of varieties is primarily our own work, bar some preliminaries taken from [9].
- The proofs of Proposition 3.17 and Corollary 3.18, which constitute [3, Lemma 2.4], require some extra work. The original proofs in [3] lacked a lot of details that we add in, some of which are non-trivial without the assumption that $\operatorname{char} \Bbbk = 0$. Moreover, the requirement that $\Bbbk$ be infinite is naturally implicit in their proofs, because their ground field is of characteristic 0.
- The statement proved in Theorem 3.13 is given in [3, Lemma 2.7], but the corresponding proof we could not follow, let alone reproduce. We give a different proof, which moreover immediately yields the useful Corollary 3.14.
- One of the main intermediate results to define the notion of essential dimension for a finite group is Lemma 3.22, which is [3, Lemma 3.2]. In part (a) we construct the polynomial p ourselves (at the time of writing we were unaware of the theory of Lagrange interpolation polynomials).
  The original proof of part (b) in [3] seems to present an incorrect argument. In their notation, they consider the subset P_d of W_d, the latter of which corresponds to our $\mathscr{W}_d(\Bbbk)$, and the former to the equivalent of our $P_{d,\overline{\Bbbk}}$ as if it were defined over $\Bbbk$ directly—which is not quite our $P_{d,\Bbbk}$. The problem is that they subsequently act as if P_d were a variety in its own right with $\Bbbk'$-points for an algebraic extension $\Bbbk'/\Bbbk$, even though they have only defined P_d as a subset of the $\Bbbk$-points of a variety. We have corrected this oddity in our proof of part (b) of Lemma 3.22. Namely, we first base change to the algebraic closure $\overline{\mathscr{W}}_d$, define $P_{d,\overline{\Bbbk}}$ as a subset of the $\overline{\Bbbk}$-points there, wherefrom we can simply set $P_{d,\Bbbk}$ to be the intersection of $P_{d,\overline{\Bbbk}}$ and $\overline{\mathscr{W}}_d(\Bbbk)$. Subsequently, we can prove the assertion in $\overline{\mathscr{V}}_G$, before finally showing that this implies that the statement also holds in $\mathscr{V}_G$.
- We give a dissimilar proof of [3, Lemma 3.3] in Lemma 3.23. We do utilize the clever trick from [3] of choosing a primitive element of the field extension $\Bbbk(\mathscr{Y})/\Bbbk(\mathscr{Y})^G$ to assure that the G-action on the variety $\mathfrak{X}$ is faithful, but the remainder of the proof is different.
- The proof of Proposition 4.3 is entirely our own. The statement comes from [3, Lemma 4.1(b)], however we were unable to generalize their proof to an arbitrary infinite ground field $\Bbbk$. Since in characteristic 0 every reduced variety is automatically geometrically reduced, one finds that the fiber product $\mathscr{Y}_1 \times_{\Bbbk} \mathscr{Y}_2$ of two varieties $\mathscr{Y}_1$ and $\mathscr{Y}_2$ is automatically reduced by [28, Lemma 32.6.7(2)], and therefore is a variety as well. In our case, when $\Bbbk$ can have characteristic different from 0, this is not necessarily true. This could possibly be remedied by considering the reduction $(\mathscr{Y}_1 \times_{\Bbbk} \mathscr{Y}_2)_{\mathrm{red}}$, but we decided to give a different proof instead.
- Proposition 4.16 is based on a lemma by Ohm in [24], but we made a small improvement. In our notation, Ohm assumes that Y is transcendental over both L and E, while we only assume that Y is transcendental over L. This required an extra small step in the proof to make sure that the extension $L(Y)/E(Y)$ is algebraic. In [15, Proposition 8.1.1] the authors also drop this assumption, but they do not account for this in their proof.
- The proof of Proposition 4.24 is our own, even though a slightly stronger version is presented in [17, Proposition 5.10].

Acknowledgments

I would primarily like to express my gratitude to my supervisor prof. dr. Cornelissen. Not only did he provide various invaluable suggestions that benefited this thesis greatly, but he also helped me with several proofs, and provided useful references for my research. During our regular meetings he always took the time to explain things to me that I did not understand, or think with me to solve a problem I was facing. He moreover kept me motivated and enthused about the subject by helping me plan the course we could take, while letting me also be free to choose what I deemed interesting or useful. It has been an absolute pleasure to work with him.
My thanks also goes to prof. dr. Beukers for taking the time to be the second reader of this thesis.
Finally, I would like to thank my family and friends for their continued support throughout.

Notation and Conventions

All rings that we use are assumed to be commutative and unitary. For the precise definition of an algebraic variety see Definition 2.1.
Every remark tacitly assumes the notation of the part that directly precedes it.
We use the symbols $\square$, $\star$, $\diamond$, and $\lozenge$ to denote the end of a proof, definition, remark, and example, respectively. Other symbols and notation that we use are listed in the table below.

A_G	The $\Bbbk$-algebra $\Bbbk[\{X_\sigma \mid \sigma \in G\}]$.
$\mathbb{A}^n_\Bbbk$	The n-dimensional affine space $\operatorname{Spec} \Bbbk[X_1, \dots, X_n]$.
A_n	The alternating group of degree n.
$\operatorname{Aut}(A)$	The group of automorphisms of A.
$\operatorname{char} \Bbbk$	The characteristic of the field $\Bbbk$.
$\mathrm{Cr}_n(\Bbbk)$	The Cremona group of order n over $\Bbbk$.
$\mathrm{d}_\Bbbk(n)$	The essential dimension of the n-th degree general polynomial over $\Bbbk$ (Definition 1.6).
e	The neutral element of G.
$\operatorname{ed}_\Bbbk(L/K)$	The essential dimension of the field extension L/K over $\Bbbk$ (Definition 1.1).
$\operatorname{ed}_\Bbbk(G \circlearrowright \mathcal{X})$	The essential dimension of a faithful G-variety $\mathcal{X}$ over $\Bbbk$ (Definition 3.12).
$\operatorname{ed}_\Bbbk(G)$	The essential dimension of the finite group G over $\Bbbk$ (Definition 4.1).
E^G	The subfield of E consisting of all elements fixed by the group G.
f^T	The Tschirnhaus transform of a polynomial f via T (Definition 1.7).
$f \sim g$	$g = f^T$ for some Tschirnhaus transformation T (Proposition 1.10).
$\operatorname{Frac}(A)$	The field of fractions of an integral domain A.
$\varphi^\sharp$	The map on structure sheaves of a morphism φ of algebraic varieties (Definition 2.1).
G	A finite group.
$\mathrm{GL}_n(\Bbbk)$	The general linear group of order n over $\Bbbk$.
$\operatorname{Hom}_\Bbbk(\mathcal{X}, \mathcal{Y})$	The set of $\Bbbk$-morphisms $\mathcal{X} \to \mathcal{Y}$ between varieties.
$\Bbbk$	An arbitrary ground field; assumed to be infinite in Chapter 4.
$\Bbbk_p$, $\Bbbk_{\neq p}$	$\Bbbk$ with characteristic indicated by the subscript (Section 4.2).
$\overline{\Bbbk}$	An algebraic closure of $\Bbbk$.
$\Bbbk(\mathcal{X})$	The function field of a variety $\mathcal{X}$.
$K[X]^{\mathrm{sim}}$	The set of non-constant, monic polynomials with only simple roots over a field K (Proposition 1.10).
$\kappa(P)$	The residue field $\mathcal{O}_{\mathcal{X},P}/\mathfrak{m}_{\mathcal{X},P}$ of a point P of a variety $\mathcal{X}$ (Section 2.2).
$m_{\alpha/F}$	The minimal polynomial of an element α over a field F, where α lies in some algebraic extension of F.
$\mathbb{N}$	The set $\{1, 2, 3, \dots\}$ of natural numbers.
$\mathbb{N}_0$	$\mathbb{N} \cup \{0\}$.
$\operatorname{nil}(R)$	The nilradical of a ring R.
$\operatorname{ord}(\sigma)$	The order of the element σ in a group.
$\mathcal{O}_\mathcal{X}$	The structure sheaf of an algebraic variety $\mathcal{X}$ (Definition 2.1).
$\mathcal{O}_{\mathcal{X},P}$, $\mathfrak{m}_{\mathcal{X},P}$	The stalk of $\mathcal{O}_\mathcal{X}$ at a point $P \in \mathcal{X}$ and its maximal ideal, respectively (Definition 2.1).
$\mathrm{PGL}_n(\Bbbk)$	The projective general linear group of order n over $\Bbbk$.
$\operatorname{Res}(f, g)$	The resultant of two polynomials f and g.
$R^\times$	The group of units of a ring R.
S_n	The symmetric group of degree n.
$\operatorname{Spec} A$	The spectrum of a ring A.
$\operatorname{trdeg}_F(E)$	The transcendence degree of a field E over a subfield F.
$\mathcal{V}(\mathfrak{a})$	The set $\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{a} \subseteq \mathfrak{p}\}$, where $\mathfrak{a} \subseteq \Bbbk[X_1, \dots, X_n]$ is an ideal.
$\mathcal{V}_G$	The faithful G-variety $\operatorname{Spec} A_G$.
$\mathcal{X}(\Bbbk)$	The set of $\Bbbk$-rational points of a variety $\mathcal{X}$ (Section 2.2).
$\mathcal{X}_{\Bbbk'}$	The base change $\mathcal{X} \times_\Bbbk \Bbbk'$ of $\mathcal{X}$ to a field extension $\Bbbk'$ of $\Bbbk$ (Section 2.2).
$\mathcal{X} \times_\Bbbk \mathcal{Y}$	The fiber product of two varieties $\mathcal{X}$ and $\mathcal{Y}$ over $\Bbbk$.
$\mathcal{X} \dashrightarrow \mathcal{Y}$	A rational map between algebraic varieties (Definition 2.3).
$\mathcal{Z}(\mathfrak{a})$	The subset $\{\alpha \in \Bbbk^n \mid f(\alpha) = 0 \text{ for all } f \in \mathfrak{a}\}$ of $\Bbbk^n$, where $\mathfrak{a} \subseteq \Bbbk[X_1, \dots, X_n]$ is an ideal.
$Z(G)$	The center of the group G.
ζ_n	A primitive n-th root of unity.

Contents

Chapter 1

Essential Dimension of a General Polynomial

Throughout this chapter we fix a field $\Bbbk$, all fields that we consider are assumed to contain $\Bbbk$, and homomorphisms of such fields are $\Bbbk$-linear.

Let $n \in \mathbb{N}$ and let $\{a_1, \dots, a_n\}$ be a set of algebraically independent elements over $\Bbbk$. Set $K \coloneqq \Bbbk(a_1, \dots, a_n)$, and let

$$p(X) \coloneqq X^n + a_1 X^{n-1} + \cdots + a_n \in K[X] \tag{1.5}$$

be the general polynomial of degree n over $\Bbbk$. The field K has transcendence degree n over $\Bbbk$. Our goal is to reduce the number of transcendental elements necessary to 'describe' p. That is to say, we want to find a subfield $F \subseteq K$ with minimal transcendence degree over $\Bbbk$ such that p is 'equivalent' to a polynomial defined over F. This equivalence will turn out to be in terms of so-called Tschirnhaus transformations. With such a subfield F, $\operatorname{trdeg}_{\Bbbk}(F)$ is called the *essential dimension* of p over $\Bbbk$. We shall now formally define this and show the relation to Tschirnhaus transformations. We end this chapter with some examples for p of low degree.
The original idea of essential dimension came from a paper by Buhler and Reichstein [3].

Definition 1.1 (Essential dimension of a field extension)**.** Let K be a field and L a separable field extension of degree $n \in \mathbb{N}$. Let $F \subseteq K$ be a subfield. We say that L/K is *defined over* F, if there exists a field extension E/F of degree n with $E \subseteq L$ such that $EK = L$. For such an extension E/F we also say that L/K is *defined over* E/F. See Figure 1.1.
The *essential dimension of* L/K *over* $\Bbbk$ is the minimal transcendence degree of F over $\Bbbk$, where F runs over all fields over which L/K is defined. We denote this by $\operatorname{ed}_{\Bbbk}(L/K)$. ☆

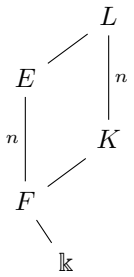


Figure 1.1: L/K defined over E/F.

It turns out that in the above situation, where a finite, separable extension L/K is defined over E/F, also E/F is a separable extension. The proof we present here comes from [17, Lemma 2.2].

***Lemma* 1.2.** *Let L/K be a separable field extension of degree $n \in \mathbb{N}$. Let $F \subseteq K$ be a subfield, and E/F be an extension such that L/K is defined over E/F. Then E is separable over F.*

Proof. If $\operatorname{char} \Bbbk = 0$, we are done. So suppose that $\operatorname{char} \Bbbk =: p > 0$. Let E^p be the field of all p-th powers of elements of E. By [19, Corollary 6.10], E/F is separable if and only if $E^p F = E$. Consider

the surjective field homomorphism $\varphi\colon E \otimes_F K \to EK$ induced by $\alpha \otimes \beta \mapsto \alpha\beta$. As K-vector spaces, $E \otimes_F K \cong F^n \otimes_F K \cong K^n$, and $EK = L \cong K^n$. Thus φ is also injective by the Rank-Nullity Theorem, wherefore $E \otimes_F K \cong EK$ as fields. By restricting φ to $E^pF \otimes_F K$, we moreover see that $E^pF \otimes_F K \cong (E^pF)K$. Let $V \coloneqq E/(E^pF)$, where the quotient is taken as an F-vector space. Consider the following short exact sequence of vector spaces over F:

$$0 \to E^pF \to E \to V \to 0.$$

Since any field is faithfully flat over a subfield, tensoring with K over F gives the short exact sequence

$$0 \to E^pF \otimes_F K \to E \otimes_F K \to V \otimes_F K \to 0,$$

which, with the isomorphisms above, becomes

$$0 \to (E^pF)K \to EK \to V \otimes_F K \to 0. \tag{1.6}$$

Since L/K is separable, $L^pK = L$. Therefore,

$$L = L^pK = (EK)^pK = E^p(K^pK) = E^pK = (EF)^pK = (E^pF^p)K = (E^pF)K.$$

Thus the injection $(E^pF)K \to EK$ in (1.6) is also surjective. Subsequently, $V \otimes_F K = 0$. Since K is faithfully flat over F, this implies that $V = 0$. That is to say, $E = E^pF$. We conclude that E/F is separable. □

We shall regularly deal with finite Galois extensions L/K with Galois group G. To find a field extension E/F, over which L/K is defined, it is sufficient to find a subfield $E \subseteq L$ on which G acts faithfully. We prove this assertion below.

***Lemma* 1.3.** *Let L/K be a finite Galois extension with Galois group G. Let $E \subseteq L$ be a subfield on which G acts faithfully. Set $F \coloneqq E^G$. Then L/K is defined over E/F and* $\operatorname{ed}_{\Bbbk}(L/K) \leq \operatorname{trdeg}_{\Bbbk}(E)$.

Proof. Because E/F is Galois, we have $[E : F] = \#G = [L : K]$. Since G fixes F and $F \subseteq L$, it follows that $F \subseteq K$, because $K = L^G$. It remains to show that $EK = L$. Since $E \subseteq EK$ and G acts faithfully on E, we see that only the neutral element of G fixes EK. Because $K \subseteq EK \subseteq L$, it follows from the Galois correspondence that $L = EK$. Thus L/K is defined over E/F and hence $\operatorname{ed}_{\Bbbk}(L/K) \leq \operatorname{trdeg}_{\Bbbk}(F) = \operatorname{trdeg}_{\Bbbk}(E)$. □

The following lemma, which we shall need later on, allows us to only consider Galois extensions E/F if L/K is Galois itself (see also [3, Lemma 2.2]).

***Lemma* 1.4.** *If L/K is a finite Galois extension of degree n with Galois group G, then there exists a Galois extension E/F with Galois group G, over which L/K is defined, such that* $\operatorname{ed}_{\Bbbk}(L/K) = \operatorname{trdeg}_{\Bbbk}(F)$.

Proof. Let E'/F' be a field extension, over which L/K is defined, such that $\operatorname{ed}_{\Bbbk}(L/K) = \operatorname{trdeg}_{\Bbbk}(F')$. Since E'/F' is separable by Lemma 1.2, there exists an $\alpha \in E'$ such that $E' = F'(\alpha)$. Moreover, since $E'K = L$, it follows that $L \cong K(\alpha)$, and so the minimal polynomial $m_{\alpha/F'}$ of α over F' remains irreducible over K. Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of $m_{\alpha/F'}$ in some extension field of F'. Since L/K is Galois and $\alpha \in L$, it follows that $\alpha_1, \ldots, \alpha_n \in L$. The normal closure E of E' over F' is $F'(\alpha_1, \ldots, \alpha_n)$, hence $E \subseteq L$.
Each $\sigma \in G$ is fully determined by to which α_i it sends α. Since E contains all α_i, it follows that G acts faithfully on E via $\sigma \mapsto \sigma|_E$. Let $F \coloneqq E^G$. Since E/F' is Galois and $F' \subseteq F \subseteq E$, we see that E/F is Galois. Therefore, $[E : F] = n$. Since $\{\sigma|_E \mid \sigma \in G\}$ is a group of n different automorphisms of E, it follows that G is (isomorphic to) the Galois group of E/F.
By Lemma 1.3, L/K is defined over E/F. Finally, we see that $\operatorname{trdeg}_{\Bbbk}(F) = \operatorname{trdeg}_{\Bbbk}(E) = \operatorname{trdeg}_{\Bbbk}(F') = \operatorname{ed}_{\Bbbk}(L/K)$. □

The following assertion lets us work with Galois extensions instead of just separable ones, as taking normal closures makes no difference. This is [3, Lemma 2.3].

***Lemma* 1.5.** *Let L/K be a separable field extension of finite degree. Let $L^{\#}$ be the normal closure of L. Then* $\operatorname{ed}_{\Bbbk}(L^{\#}/K) = \operatorname{ed}_{\Bbbk}(L/K)$.

Proof. To show equality we show both inequalities. Let G be the Galois group of $L^\#/K$.
We start with '$\geq$'. Let $E \subseteq L^\#$ be a subfield on which G acts faithfully such that $L^\#/K$ is defined over E/E^G and $\mathrm{ed}_\Bbbk(L^\#/K) = \mathrm{trdeg}_\Bbbk(E)$, which exists by Lemma 1.4. Let $H \leq G$ be the subgroup corresponding to $K \subseteq L \subseteq L^\#$. Clearly $E^H \subseteq (L^\#)^H = L$, thus $E^H K$ is an intermediate field between K and L. Any element of G that fixes $E^H K$ has to belong to H; clearly any element of H fixes $E^H K$. Thus, by the Galois correspondence, $E^H K = L$. Finally, since also $[E^H : E^G] = [G : H] = [L : K]$, we see that L/K is defined over E^H/E^G. Consequently, $\mathrm{ed}_\Bbbk(L/K) \leq \mathrm{trdeg}_\Bbbk(E^G) = \mathrm{trdeg}_\Bbbk(E) = \mathrm{ed}_\Bbbk(L^\#/K)$.
For the converse inequality we let E/F be a field extension over which L/K is defined such that $\mathrm{ed}_\Bbbk(L/K) = \mathrm{trdeg}_\Bbbk(E)$. Since $E \subseteq L$, we may take a normal closure $E^\#$ of E over F inside $L^\#$. In particular, the action of G on $L^\#$ restricts to an action on $E^\#$. Furthermore, because $EK = L$ and G fixes K, this action is faithful. Now Lemma 1.3 tells us that $\mathrm{ed}_\Bbbk(L^\#/K) \leq \mathrm{trdeg}_\Bbbk(E^\#) = \mathrm{trdeg}_\Bbbk(E) = \mathrm{ed}_\Bbbk(L/K)$. □

Using Definition 1.1 we can define the essential dimension of the general polynomial p in (1.5).

Definition 1.6 (Essential dimension of a general polynomial)**.** Let $n \in \mathbb{N}$. Let $\{a_1, \ldots, a_n\}$ be algebraically independent over $\Bbbk$, $K \coloneqq \Bbbk(a_1, \ldots, a_n)$, and $p(X) \coloneqq X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$. Let $L \coloneqq K[X]/(p)$. Note that p is irreducible and separable over K, hence L/K is a separable field extension of degree n. We define the *essential dimension of p over $\Bbbk$* to be $\mathrm{ed}_\Bbbk(L/K)$, which we denote by $\mathrm{d}_\Bbbk(n)$. ☆

To see why this definition encapsulates the minimal number of parameters necessary to describe the general polynomial p, we need to delve into when we deem polynomials equivalent. We got the main idea for this equivalence from [15, pp. 141–142].

Let $L \coloneqq K[X]/(p)$ as in Definition 1.6, and let E/F be a field extension over which L/K is defined such that $\mathrm{d}_\Bbbk(n) = \mathrm{trdeg}_\Bbbk(F)$. Since E/F is separable, there exists a primitive element $\beta \in E$ such that $E = F(\beta)$. Let $\mathfrak{m}_{\beta/F}$ be the minimal polynomial of β over F. Since, by assumption, $EK = L$, we have $K(\beta) \cong L$, wherefore $\mathfrak{m}_{\beta/F}$ remains irreducible over K. Hence $L \cong K[X]/(\mathfrak{m}_{\beta/F})$. We thus see that the root fields of p and $\mathfrak{m}_{\beta/F}$ over K are the same. This means in particular that their respective Galois groups over K coincide.
Let $\overline{X} \in K[X]/(\mathfrak{m}_{\beta/F})$ be the residue class of X. Consider the image $T(\overline{X}) \in L$ of $\overline{X}$ under the K-isomorphism $\varphi\colon K[X]/(\mathfrak{m}_{\beta/F}) \xrightarrow{\sim} L$, where T is a polynomial over K. Since $\overline{X} \in L$ corresponds to a root of p (by definition of L), we see that the roots of $\mathfrak{m}_{\beta/F}$ are all of the form $T(\alpha)$ for a root α of p in some extension field of K; we have the following commutative diagram:

$$\begin{array}{ccccc}
 & & \overline{X} & \longmapsto & \alpha \\
T(\overline{X}) & K[X]/(p) & \xrightarrow{\sim} & K(\alpha) & T(\alpha) \\
\uparrow & \wr\uparrow\varphi & & \wr\uparrow & \uparrow \\
\overline{X} & K[X]/(\mathfrak{m}_{\beta/F}) & \xrightarrow{\sim} & K(\beta) & \beta \\
 & & \overline{X} & \longmapsto & \beta.
\end{array}$$

Since p and $\mathfrak{m}_{\beta/F}$ are separable, T is injective on the roots of p. Thus if $\alpha_1, \ldots, \alpha_n$ are said roots, then $\mathfrak{m}_{\beta/F}(X) = \prod_{i=1}^n (X - T(\alpha_i))$. This leads us to the following definition.

Definition 1.7 (Tschirnhaus transformation)**.** Let K be a field and $T \in K[X]$ a polynomial. Let $f \in K[X]$ be a non-constant, monic polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$ in some extension field of K. A *Tschirnhaus transformation* is a map $f \mapsto f^T$, where

$$f^T(X) \coloneqq \prod_{i=1}^n (X - T(\alpha_i)).$$

When we say that T is a Tschirnhaus transformation, we mean the map $(\bullet)^T$. The resulting polynomial f^T is the *Tschirnhaus transform of f by T*. ☆

Remark 1.8. We need only consider Tschirnhaus transformations with $\deg T < n$. If $\deg T \geq n$, we can use long division of T by f to obtain polynomials $q, T' \in K[X]$ such that $T = qf + T'$, where $\deg T' < n$. We then have $T(\alpha_i) = q(\alpha_i) f(\alpha_i) + T'(\alpha_i) = T'(\alpha_i)$ for every i. Therefore, $f^T = f^{T'}$. ✧

Remark 1.9. One can use the resultant to explicitly compute the polynomial f^T. Write $f(X) = X^n + c_1X^{n-1} + \cdots + c_n \in K[X]$ and $T(X) = t_{n-1}X^{n-1} + \cdots t_1X + t_0 \in K[X]$. Letting Y be another variable, consider $g(Y) \coloneqq \operatorname{Res}(f(X), Y - T(X))$. Explicitly,

$$g(Y) = \det \begin{pmatrix} 1 & c_1 & \cdots & c_n & & \\ & \ddots & \ddots & \ddots & \ddots & \\ & & 1 & c_1 & \cdots & c_n \\ -t_{n-1} & -t_{n-2} & \cdots & Y - t_0 & & \\ & \ddots & \ddots & \ddots & \ddots & \\ & & -t_{n-1} & -t_{n-2} & \cdots & Y - t_0 \end{pmatrix}$$

with the matrix of size $(\deg(T) + n) \times (\deg(T) + n)$, whose diagonal is $(\overbrace{1, \ldots, 1}^{\deg T \text{ entries}}, \overbrace{Y - t_0, \ldots, Y - t_0}^{n \text{ entries}})$. Thus $g(Y)$ is a polynomial in Y of degree n with coefficients in K. Moreover, the coefficient of Y^n is the determinant of the upper-left $(\det T) \times (\det T)$-square matrix; this is a triangular matrix with only 1's on the diagonal. Whence g is monic. As is well known, the resultant of two polynomials is zero if and only if those polynomials have a common root. As polynomials of X, we are considering $f(X)$ and $Y - T(X)$. All roots of f are $\alpha_1, \ldots, \alpha_n$. For any α_i, setting $Y = T(\alpha_i)$, we see that $f(X)$ and $T(\alpha_i) - T(X)$ have the root α_i in common. Whence $g(T(\alpha_i)) = 0$. Conversely, if $g(\beta) = 0$ for some β in an extension field of K, then $f(X)$ and $\beta - T(X)$ have a common root. Thus for some α_j, we have $\beta - T(\alpha_j) = 0$. We therefore infer that $g = f^T$. Note that this in particular shows that $f^T \in K[X]$. ✧

One polynomial being a Tschirnhaus transform of another is not actually an equivalence relation in general. Fortunately, it is on a certain subset of polynomials, which for our purposes is more than sufficient. Namely, we have the following proposition.

***Proposition* 1.10.** *Let K be a field and let $K[X]^{\mathrm{sim}}$ be the set of non-constant, separable, monic polynomials over K. For $f, g \in K[X]^{\mathrm{sim}}$ we define the relation $\sim$ via*

$$f \sim g \ :\Longleftrightarrow\ g = f^T \text{ for some } T \in K[X].$$

This relation is an equivalence relation.

Remark 1.11. We call a polynomial (not necessarily irreducible) *separable* if all of its roots are simple. That is, in some algebraic closure all of its roots are distinct and the number of distinct roots equals the degree of the polynomial. In some literature one finds that a polynomial is called separable if all of its irreducible factors over the ground field have only simple roots. For our purposes the former definition is more convenient. ✧

Before we prove Proposition 1.10, we need a series of lemmas. We retain the definitions of $K[X]^{\mathrm{sim}}$ and the relation $\sim$.

***Lemma* 1.12.** *Let K be a field. Let $f, g \in K[X]^{\mathrm{sim}}$ and assume they are irreducible. Then $f \sim g$ if and only if $K[X]/(f) \cong K[X]/(g)$.*

Proof. For the direct implication let $T \in K[X]$ be such that $g = f^T$. Observe that $\deg f = \deg f^T = \deg g$. Consider the map $\tilde{\varphi}\colon K[X] \to K[X]/(f)$ defined by $\tilde{\varphi}(X) \coloneqq T(\overline{X})$. Consider $g \circ T$. Since f only has simple roots and each root of f is also a root of $g \circ T$, it follows that $f \mid g \circ T$. Therefore, $\tilde{\varphi}(g(X)) = g(T(\overline{X})) = 0$ in $K[X]/(f)$. Thus $(g) \subseteq \ker \tilde{\varphi}$, which means that $\tilde{\varphi}$ factors through $K[X]/(g)$, inducing a homomorphism $\varphi\colon K[X]/(g) \to K[X]/(f)$. Since g is irreducible, $K[X]/(g)$ is a field. It follows from $\varphi(1) = 1 \neq 0$ that φ is injective. Finally, $K[X]/(g)$ and $K[X]/(f)$ have the same degree over K, so φ is an isomorphism.
The converse implication follows from the argument after Definition 1.6. □

***Lemma* 1.13.** *Let K be a field. Let $f \in K[X]$ be monic, separable, and irreducible of degree $n \in \mathbb{N}$, and let $T \in K[X]$. If f^T is separable, then it is irreducible.*

Proof. Let G be the Galois group of f over K and let $\alpha_1, \ldots, \alpha_n$ be the roots of f. Then $L \coloneqq K(T(\alpha_1), \ldots, T(\alpha_n))$ is the splitting field of f^T over K. The fact that f^T is separable implies that L/K is Galois and that T is injective on the set of roots of f. For any $\sigma \in G$ and any α_i, we have $\sigma(T(\alpha_i)) = T(\sigma(\alpha_i)) = T(\alpha_j)$ for some j. Thus restricting σ from the splitting field of f over K to

L gives a well-defined homomorphism $L \to L$. Since $\sigma^{-1}|_L$ is its inverse, $\sigma|_L$ is an automorphism of L, and so $\sigma|_L \in \mathrm{Gal}(L/K)$. For any two α_i and α_j there exists a $\tau \in G$ such that $\tau(\alpha_i) = \alpha_j$. Then $\tau|_L \in \mathrm{Gal}(L/K)$ satisfies $\tau|_L(T(\alpha_i)) = T(\alpha_j)$. Therefore, $\mathrm{Gal}(L/K)$ acts transitively on the roots of f^T, wherefrom follows that f^T is irreducible. □

***Lemma* 1.14.** *Let K be a field and let $f, g \in K[X]^{\mathrm{sim}}$. Suppose that f and g have the same degree n. Let $s, t \in \mathbb{N}$, and write $f = f_1 \cdots f_s$ and $g = g_1 \cdots g_t$, where the $f_i, g_j \in K[X]^{\mathrm{sim}}$ are irreducible. Then $f \sim g$ if and only if $s = t$ and for some permutation $\sigma \in \mathrm{S}_s$ we have for all i that $f_i \sim g_{\sigma(i)}$.*

Proof. First we prove the direct implication. Let $T \in K[X]$ such that $g = f^T$. Fix an i and consider f_i^T. Note that $f_i^T \mid f^T$, wherefore f_i^T is separable. Since f_i is separable and irreducible, Lemma 1.13 implies that f_i^T is irreducible as well. Thus $f_i^T = g_j$ for some j. Since $g_j = g_{j'}$ if and only if $j = j'$, we get a well-defined map $\sigma\colon \{1, \dots, s\} \to \{1, \dots, t\}$ sending i to j if $f_i \sim g_j$ via T.
We show that σ is injective. Suppose for i and i' we have $f_i^T = g_j = f_{i'}^T$. Let β be a root of g_j. Then there is a root α of f_i and a root α' of $f_{i'}$ such that $T(\alpha) = \beta = T(\alpha')$. Since f and g have the same number of roots and all of their respective roots are distinct, T is injective on the set of roots of f. Thus $\alpha = \alpha'$, and so $f_i = f_{i'}$, which in turn means that $i = i'$. So σ is injective. This implies that $t \geq s$.
We now have

$$\sum_{j=1}^{t} \deg(g_j) = n = \sum_{i=1}^{s} \deg(f_i) = \sum_{i=1}^{s} \deg(g_{\sigma(i)}).$$

This means that if some j were not reached by σ, the corresponding g_j would have degree 0. This cannot happen, so σ is bijective. Consequently, $t = s$, $\sigma \in \mathrm{S}_s$, and $f_i \sim g_{\sigma(i)}$ for all i.
To prove the converse implication, we assume that $s = t$, and that, without loss of generality, $g_i = f_i^{T_i}$ for some $T_i \in K[X]$ with $\deg T_i < \deg f_i$. Since the f_i are irreducible and pairwise distinct, we have, by the Chinese Remainder Theorem,

$$\prod_{i=1}^{s} K[X]/(f_i) \cong K[X]/(f).$$

Let $T \in K[X]$ be a lift of the image of $(T_1, \dots, T_s)$ under this isomorphism. Then $T \equiv T_i \bmod f_i$ for every i, and so, due to Remark 1.8, $f_i^T = f_i^{T_i}$. Therefore, $g = f_1^T \cdots f_s^T = f^T$. Whence $f \sim g$. □

Proof of Proposition 1.10. We show that $\sim$ is an equivalence relation. Let $f, g, h \in K[X]^{\mathrm{sim}}$. Via $T = X$, $f \sim f$, thus $\sim$ is reflexive.
Suppose $f \sim g$, i.e., $g = f^T$ for some $T \in K[X]$. As in the proof of Lemma 1.14, write $f = f_1 \cdots f_s$ and $g = g_1 \cdots g_s$ with the f_i and g_j monic and irreducible such that $g_i = f_i^T$. Then $f_i \sim g_i$, and so Lemma 1.12 implies that $K[X]/(f_i) \cong K[X]/(g_i)$, wherefrom the same lemma concludes that $g_i \sim f_i$. Thus $g \sim f$ by Lemma 1.14, wherefore $\sim$ is symmetric.
Assume that $f \sim g$ and $g \sim h$ with $g = f^T$ and $h = g^{T'}$ for some $T, T' \in K[X]$. Then $h = \left(f^T\right)^{T'} = f^{T' \circ T}$. Thus $f \sim h$, and so $\sim$ is transitive. □

Let us get back to our general polynomial $p(X) = X^n + \cdots + a_n$ over $K = \Bbbk(a_1, \dots, a_n)$. Write again $L = K[X]/(p)$. We may now deduce that it is sufficient to consider Tschirnhaus transformations to express the essential dimension $\mathrm{d}_\Bbbk(n)$ of p, so long as said Tschirnhaus transformation is injective on the roots of the polynomial it is applied to. We have seen that, if L/K is defined over E/F, where $\mathrm{trdeg}_\Bbbk(F) = \mathrm{d}_\Bbbk(n)$, then we can find a Tschirnhaus transformation T such that $p^T \in F[X]$ and $E \cong F[X]/(p^T)$; this is the construction below Definition 1.6.
We can also use Tschirnhaus transformations to find upper bounds for $\mathrm{d}_\Bbbk(n)$. Let T be a Tschirnhaus transformation of p, which is injective on its roots. The Tschirnhaus transform p^T is defined over some subfield $F \subseteq K$. Now p^T is irreducible by Lemma 1.13. Write $E \coloneqq F[X]/(p^T)$. Then Lemma 1.12 asserts that $KE = K[X]/(p^T) \cong L$. Hence L/K is defined over E/F, and so $\mathrm{d}_\Bbbk(n) \leq \mathrm{trdeg}_\Bbbk(F)$. We illustrate a way of utilizing this for $n = 2, 3, 4$ with a series of examples.

Example 1.15. For $n = 2$ we have $p(X) = X^2 + a_1 X + a_2$. Consider the Tschirnhaus transformation $T(X) \coloneqq \frac{a_1}{a_2} X$. One explicitly computes

$$p^T(Y) = \begin{vmatrix} 1 & a_1 & a_2 \\ -\frac{a_1}{a_2} & Y & 0 \\ 0 & -\frac{a_1}{a_2} & Y \end{vmatrix} = Y^2 + \frac{a_1^2}{a_2} Y + \frac{a_1^2}{a_2}.$$

Setting $b \coloneqq \frac{a_1^2}{a_2}$, we see that $p^T(X) = X^2 + bX + b \in \Bbbk(b)[X]$. It now follows that

$$\mathrm{d}_\Bbbk(2) \leq 1, \tag{1.7}$$

because $\mathrm{trdeg}_\Bbbk(\Bbbk(b)) = 1$. ◊

Example 1.16. Take $n = 3$. Then $p(X) = X^3 + a_1X^2 + a_2X + a_3$. First assume that $\mathrm{char}\,\Bbbk \neq 3$. We can apply the standard trick to eliminate the quadratic term. Namely, take the Tschirnhaus transformation $T(X) \coloneqq X + \frac{a_1}{3}$. Then

$$q(X) \coloneqq p^T(X) = X^3 + b_1X + b_2,$$

where

$$b_1 \coloneqq a_2 - \tfrac{a_1^2}{3} \quad \text{and} \quad b_2 \coloneqq a_3 + \tfrac{2a_1^3}{27} - \tfrac{a_1a_2}{3}.$$

We can reduce this even further with the same transformation as in the case of $n = 2$. That is, consider $T'(X) \coloneqq \frac{b_1}{b_2}X$. Then

$$q^{T'}(X) = X^3 + cX + c,$$

where $c \coloneqq \frac{b_1^3}{b_2^2}$. Thus $\mathrm{d}_\Bbbk(3) \leq 1$, provided that $\mathrm{char}\,\Bbbk \neq 3$.
The same result can be obtained in the case that $\mathrm{char}\,\Bbbk = 3$. Starting from the original polynomial p, letting instead $T(X) \coloneqq a_1X^2 + (a_1^2 + a_2)X$ yields

$$p^T(X) = X^3 + b_1X + b_2,$$

where

$$b_1 \coloneqq a_1^3a_3 + a_2^3 - a_1^2a_2^2 \quad \text{and} \quad b_2 \coloneqq a_2^3a_3 - a_1^4a_2a_3 - a_1^3a_3^2.$$

Applying again the Tschirnhaus transformation T' from before, we see that $\mathrm{d}_\Bbbk(3) \leq 1$ also for $\mathrm{char}\,\Bbbk = 3$. Hence

$$\mathrm{d}_\Bbbk(3) \leq 1 \tag{1.8}$$

holds for any field $\Bbbk$. ◊

Example 1.17. In the case of $n = 4$, $p(X) = X^4 + a_1X^3 + \cdots + a_4$ over $K = \Bbbk(a_1, \ldots, a_4)$. Assume that $\mathrm{char}\,\Bbbk \neq 2$. As usual, applying $T(X) \coloneqq X + \frac{a_1}{4}$ to p eliminates the cubic term:

$$q(X) \coloneqq p^T(X) = X^4 + b_1X^2 + b_2X + b_3$$

with the $b_i \in K$. Similarly as for degrees 2 and 3, we can apply $T'(X) \coloneqq \frac{b_2}{b_3}X$ to obtain

$$q^{T'}(X) = X^4 + c_1X^2 + c_2X + c_2$$

with $c_1, c_2 \in \Bbbk(b_1, b_2, b_3)$. This shows that $\mathrm{d}_\Bbbk(4) \leq 2$ if $\mathrm{char}\,\Bbbk \neq 2$.
In case $\mathrm{char}\,\Bbbk = 2$, similarly to degree 3, we can apply a different transformation to get rid of the cubic term of p. Namely, instead of T as above, consider $T(X) \coloneqq X^2 + a_1X$. Then

$$p^T(X) = X^4 + b_1X^2 + b_2X + b_3,$$

where

$$b_1 \coloneqq a_2^2 + a_1a_3, \quad b_2 \coloneqq a_1a_2a_3 + a_1^2a_4 + a_3^2, \quad \text{and} \quad b_3 \coloneqq a_1^2a_2a_4 + a_1a_3a_4 + a_4^2.$$

Applying again T' as before, we find that $p^T \sim X^4 + c_1X^2 + c_2X + c_2$, and so $\mathrm{d}_\Bbbk(4) \leq 2$ also for $\mathrm{char}\,\Bbbk = 2$. Whence

$$\mathrm{d}_\Bbbk(4) \leq 2 \tag{1.9}$$

over any field $\Bbbk$. ◊

We have now seen some upper bounds for the essential dimension for some small n. Finding lower bounds however seems to be a lot trickier. This is because instead of finding an explicit Tschirnhaus transformation, for a lower bound we would have to show that no such transformation can exist. We do have the following lower bound, which may intuitively seem trivial.

***Proposition* 1.18.** *Let $n \in \mathbb{N}$, $\{a_1, \ldots, a_n\}$ algebraically independent over $\Bbbk$, $K \coloneqq \Bbbk(a_1, \ldots, a_n)$, and $p(X) \coloneqq X^n + \cdots + a_n \in K[X]$ the general polynomial. Then $\mathrm{d}_\Bbbk(n) = 0$ if and only if $n = 1$.*

For the proof we need another proposition.

***Proposition* 1.19.** *Let $k/\Bbbk$ be an algebraic extension of fields. Then $\mathrm{d}_k(n) \leq \mathrm{d}_\Bbbk(n)$.*

Proof. Take the notation of Proposition 1.18. Since $k/\Bbbk$ is algebraic, p remains irreducible over $kK = k(a_1, \ldots, a_n)$. Let $T \in K[X]$ be a Tschirnhaus transformation such that p^T is defined over a subfield $F \subseteq K$ with $\mathrm{trdeg}_\Bbbk(F) = \mathrm{d}_\Bbbk(n)$. Then $T \in (kK)[X]$ and $p^T \in (kF)[X]$. Since $k/\Bbbk$ is algebraic, $\mathrm{trdeg}_k(kF) = \mathrm{trdeg}_\Bbbk(kF) = \mathrm{trdeg}_\Bbbk(F)$. Thus $\mathrm{d}_k(n) \leq \mathrm{trdeg}_k(kF) = \mathrm{d}_\Bbbk(n)$. □

Proof of Proposition 1.18. Suppose $\mathrm{d}_\Bbbk(n) = 0$. Let $\overline{\Bbbk}$ be an algebraic closure of $\Bbbk$. Proposition 1.19 implies that $\mathrm{d}_{\overline{\Bbbk}}(n) = 0$. Then $p \sim q$ for some polynomial q defined over a field $F \supseteq \overline{\Bbbk}$ with $\mathrm{trdeg}_{\overline{\Bbbk}}(F) = 0$. Such an extension is algebraic, and since $\overline{\Bbbk}$ is algebraically closed, $F = \overline{\Bbbk}$. Lemma 1.13 implies that q is irreducible over $\overline{\Bbbk}$. This can only happen if $\deg q = 1$. Hence $n = 1$.
Conversely, if $n = 1$, then $p = X + a_1 \in K = \Bbbk(a_1)$, and the Tschirnhaus transformation $T(X) = 0$ suffices. □

Proposition 1.18 shows in particular that $\mathrm{d}_\Bbbk(n) \geq 1$ for $n \geq 2$. Combining this with (1.7), (1.8), and (1.9) gives us the results displayed in Table 1.1.

n	1	2	3	4
$\mathrm{d}_\Bbbk(n)$	0	1	1	1 or 2

Table 1.1: Essential dimension of p for small values of n.

What we learn from this is that it seems to become very complicated very quickly to determine the essential dimension as the degree of the general polynomial increases. We therefore shall need a different approach. In the next chapters we shall develop the theory of essential dimension first for certain algebraic varieties and therefrom for finite groups. We shall see that we can relate the essential dimension of the general polynomial of degree n to the essential dimension of the symmetric group S_n.

Chapter 2

Notions of Algebraic Varieties

Again fix a field $\Bbbk$. All fields that we will consider are assumed to contain $\Bbbk$, homomorphisms of such fields are $\Bbbk$-linear, and all algebraic varieties are defined over $\Bbbk$, unless stated otherwise. An algebraic closure of $\Bbbk$ will be denoted by $\overline{\Bbbk}$.

In this chapter we shall repeat some definitions and concepts from algebraic geometry in order to establish notation and conventions. Most of these we have adopted from [11, §§II.1–3]. We take a precise look at the various notions of 'points' a variety admits and consider some properties of base change.

2.1 Preliminaries

Definition 2.1 (Algebraic variety)**.** An *algebraic variety* (over $\Bbbk$) is a reduced, geometrically irreducible, separated scheme of finite type over $\Bbbk$.
We usually write an algebraic variety as $(\mathcal{X}, \mathcal{O}_\mathcal{X})$, where $\mathcal{X}$ is the underlying topological space and $\mathcal{O}_\mathcal{X}$ is the structure sheaf. We may also by abuse of notation leave the structure sheaf implicit and call $\mathcal{X}$ an algebraic variety. Moreover, the word 'algebraic' shall generally be left out. If $U \subseteq \mathcal{X}$ is an open subset, then $\mathcal{O}_\mathcal{X}(U)$ is the $\Bbbk$-algebra of sections on U. For a point $P \in \mathcal{X}$, we write $\mathcal{O}_{\mathcal{X},P}$ for the stalk of $\mathcal{O}_\mathcal{X}$ at P.
If $(\mathcal{Y}, \mathcal{O}_\mathcal{Y})$ is another variety, a ($\Bbbk$-)morphism $(\mathcal{X}, \mathcal{O}_\mathcal{X}) \to (\mathcal{Y}, \mathcal{O}_\mathcal{Y})$ is a pair $(\varphi, \varphi^\sharp)$, where $\varphi\colon \mathcal{X} \to \mathcal{Y}$ is a continuous map of the underlying topological spaces, and $\varphi^\sharp\colon \mathcal{O}_\mathcal{Y} \to \varphi_*\mathcal{O}_\mathcal{X}$ is a morphism of sheaves on $\mathcal{Y}$, where for any open $V \subseteq \mathcal{Y}$, $(\varphi_*\mathcal{O}_\mathcal{X})(V) \coloneqq \mathcal{O}_\mathcal{X}(\varphi^{-1}(V))$. Thus for any such V we get an induced $\Bbbk$-algebra homomorphism $\varphi^\sharp_V\colon \mathcal{O}_\mathcal{Y}(V) \to \mathcal{O}_\mathcal{X}(\varphi^{-1}(V))$. We often may just write $\varphi\colon \mathcal{X} \to \mathcal{Y}$ to mean the morphism $(\varphi, \varphi^\sharp)$. For each point $P \in \mathcal{X}$ the induced homomorphism of local rings $\varphi^\sharp_P\colon \mathcal{O}_{\mathcal{Y},\varphi(P)} \to \mathcal{O}_{\mathcal{X},P}$ is required to be a local homomorphism. ☆

Remark 2.2. It is worth pointing out that the above definition gives us some nice properties of our varieties. That $\mathcal{X}$ is integral (reduced and irreducible) and of finite type over $\Bbbk$ implies that for any affine open $U \subseteq \mathcal{X}$, we have $(U, \mathcal{O}_\mathcal{X}|_U) \cong (\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$, where A is a finitely generated, integral $\Bbbk$-algebra (a $\Bbbk$-algebra that is also an integral domain). Moreover, $\mathcal{X}$ is irreducible as a topological space, and so has a unique generic point. Separated in particular implies that the intersection of finitely many affine opens is again affine. That $\mathcal{X}$ is of finite type over $\Bbbk$ also implies that $\mathcal{X}$ is quasi-compact and hence, in particular, can be covered by a finite number of affine opens. For more details we refer to [11, §§II.1–3]; in particular Propositions 2.2–2.3 and Exercises 3.1–3.3. ✧

We shall also need the notion of a rational map.

Definition 2.3. Let $\mathcal{X}$ and $\mathcal{Y}$ be varieties. A *rational map* $\varphi\colon \mathcal{X} \dashrightarrow \mathcal{Y}$ is an equivalent class of pairs $(U, {}_U\varphi)$, where $U \subseteq \mathcal{X}$ is a non-empty, open subset, and ${}_U\varphi\colon U \to \mathcal{Y}$ is a morphism. Two pairs $(U, {}_U\varphi)$ and $(V, {}_V\varphi)$ are equivalent if and only if for some non-empty open $W \subseteq U \cap V$ the morphisms ${}_U\varphi|_W$ and ${}_V\varphi|_W$ coincide. We call φ *dominant* if there is a representative $(U, {}_U\varphi)$ such that its image ${}_U\varphi(U)$ is dense in $\mathcal{Y}$. ☆

Remark 2.4. Let $\eta \in \mathcal{X}$ and $\xi \in \mathcal{Y}$ be the generic points. The generic point is contained in every open subset, so we may speak of $\varphi(\eta)$. Recall that φ is dominant if and only if $\varphi(\eta) = \xi$. Note that therefore *every* representative of φ has dense image in $\mathcal{Y}$ if one has. ✧

Remark 2.5. An injective $\Bbbk$-algebra homomorphism $f\colon A \to B$ between finitely generated, integral $\Bbbk$-algebras induces a dominant (rational) map $\varphi\colon \operatorname{Spec} B \to \operatorname{Spec} A$. This is because the generic point of $\operatorname{Spec} B$ and $\operatorname{Spec} A$ is the zero ideal, wherefore, by injectivity, $\varphi((0)) = f^{-1}((0)) = (0) \in \operatorname{Spec} A$. ✧

2.2 Base Change and Points

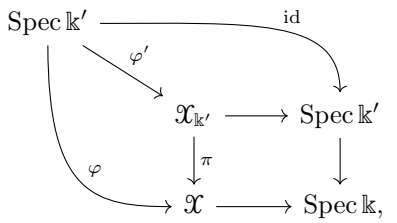
Let $\mathcal{X}$ be a variety over $\Bbbk$. There are several established notions of 'points' of $\mathcal{X}$. The *geometric points* are the elements of the underlying topological space of $\mathcal{X}$. A subset of these are the *closed points*: those $P \in \mathcal{X}$ for which the singleton $\{P\}$ is a closed subset of $\mathcal{X}$. In the case of an affine variety these points are precisely the maximal ideals.
For any point $P \in \mathcal{X}$ we have the local ring $\mathcal{O}_{\mathcal{X},P}$ and its unique maximal ideal $\mathfrak{m}_{\mathcal{X},P} \subset \mathcal{O}_{\mathcal{X},P}$. The *residue field* $\kappa(P)$ of P is the quotient $\mathcal{O}_{\mathcal{X},P}/\mathfrak{m}_{\mathcal{X},P}$. For instance, if $\eta \in \mathcal{X}$ is the generic point, then $\kappa(\eta) = \Bbbk(\mathcal{X})$.
Now let $\Bbbk'/\Bbbk$ be an algebraic field extension. We call a point $P \in \mathcal{X}$ a $\Bbbk'$-*rational point* if there exists a $\Bbbk$-embedding $\kappa(P) \hookrightarrow \Bbbk'$. We denote the set of such points by $\mathcal{X}(\Bbbk') \subseteq \mathcal{X}$. The closed points are precisely those points $P \in \mathcal{X}$ with $\kappa(P)/\Bbbk$ algebraic or, equivalently, finite (see [9, Proposition 3.33]). Thus the set of closed points is precisely $\mathcal{X}(\overline{\Bbbk})$, the set of $\overline{\Bbbk}$-rational points. The closed points are particularly important, because they are dense in $\mathcal{X}$ by [9, Proposition 3.35].
A ($\Bbbk$-)morphism $\operatorname{Spec}\Bbbk' \to \mathcal{X}$ is called a $\Bbbk'$-*valued point* of $\mathcal{X}$. The image of such a morphism is precisely one geometric point. The set of these points is denoted by $\operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X})$. There is a close relation between $\Bbbk'$-rational points and $\Bbbk'$-valued points. The image $\varphi((0)) \in \mathcal{X}$ of some $\varphi\colon \operatorname{Spec}\Bbbk' \to \mathcal{X}$ is a $\Bbbk'$-rational point, and for every $\Bbbk'$-rational point $P \in \mathcal{X}(\Bbbk')$ there is a morphism $\operatorname{Spec}\Bbbk' \to \mathcal{X}$ with image P. However, this morphism is generally not unique. More precisely, we have a one-to-one correspondence

$$\operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X}) \longleftrightarrow \{(P, \iota) \mid P \in \mathcal{X} \text{ and } \iota\colon \kappa(P) \hookrightarrow \Bbbk'\}, \tag{2.1}$$

where the ι fix $\Bbbk$ pointwise. For more details we refer to [9, §3.4].
An advantage of the $\Bbbk'$-valued points is that they give a nice correspondence with fiber products in the following sense. Let $\mathcal{Y}$ be another variety over $\Bbbk$. We write $\mathcal{X} \times_{\Bbbk} \mathcal{Y}$ for the fiber product $\mathcal{X} \times_{\operatorname{Spec}\Bbbk} \mathcal{Y}$ of $\mathcal{X}$ and $\mathcal{Y}$ over $\Bbbk$. Then the $\Bbbk'$-valued points of $\mathcal{X} \times_{\Bbbk} \mathcal{Y}$ correspond precisely to the pairs of $\Bbbk'$-valued points of $\mathcal{X}$ and of $\mathcal{Y}$. This is because the fiber product of schemes is a categorical product in the category of schemes, and so

$$\operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X} \times_{\Bbbk} \mathcal{Y}) \cong \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X}) \times \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{Y}) \tag{2.2}$$

as sets. This bijection does not generally hold for the $\Bbbk'$-rational points. On these points, $\mathcal{X}(\Bbbk')$, we can use topological properties, because we have the subspace topology from $\mathcal{X}$. Note that when $\Bbbk' = \Bbbk$, (2.1) gives a bijection between the $\Bbbk$-valued points and the $\Bbbk$-rational points, hence we have the best of both worlds. We then usually do not distinguish both kinds of points and call them simply $\Bbbk$-*points*. In particular, (2.2) becomes $(\mathcal{X} \times_{\Bbbk} \mathcal{Y})(\Bbbk) \cong \mathcal{X}(\Bbbk) \times \mathcal{Y}(\Bbbk)$ as sets.
In general, we can do a base change to $\Bbbk'$. Namely, we let $\mathcal{X}_{\Bbbk'} \coloneqq \mathcal{X} \times_{\Bbbk} \Bbbk' \coloneqq \mathcal{X} \times_{\operatorname{Spec}\Bbbk} \operatorname{Spec}\Bbbk'$. It turns out that the $\Bbbk'$-valued points of $\mathcal{X}_{\Bbbk'}$ correspond bijectively to the $\Bbbk'$-valued points of $\mathcal{X}$. Note that, since we deem $\mathcal{X}_{\Bbbk'}$ a variety over $\Bbbk'$, the $\Bbbk'$-valued points are $\Bbbk'$-morphisms, not just $\Bbbk$-morphisms. We thus consider $\operatorname{Hom}_{\Bbbk'}(\operatorname{Spec}\Bbbk', \mathcal{X}_{\Bbbk'}) \subseteq \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X}_{\Bbbk'})$ and check what happens when we apply (2.2). Any $\Bbbk'$-morphism $\varphi'\colon \operatorname{Spec}\Bbbk' \to \mathcal{X}_{\Bbbk'}$ fits in the commutative diagram



where π is the projection and $\varphi \coloneqq \pi \circ \varphi'$. The correspondence (2.2) yields

$$\operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X}_{\Bbbk'}) \cong \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X}) \times \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \operatorname{Spec}\Bbbk').$$

However, we only want to look at the $\Bbbk'$-morphisms $\operatorname{Spec}\Bbbk' \to \mathcal{X}_{\Bbbk'}$, excluding those that are merely $\Bbbk$-morphisms. Since the above correspondence sends any such $\Bbbk'$-morphism φ' to the pair (φ, id), we obtain for this subset the following bijections of sets:

$$\operatorname{Hom}_{\Bbbk'}(\operatorname{Spec}\Bbbk', \mathcal{X}_{\Bbbk'}) \cong \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X}) \times \{\mathrm{id}_{\operatorname{Spec}\Bbbk'}\} \cong \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X}).$$

Thus indeed, on the left we have the $\Bbbk'$-valued points of $\mathcal{X}_{\Bbbk'}$, and on the right the $\Bbbk'$-valued points of $\mathcal{X}$. With this construction we can no longer see the $\Bbbk$-rational points inside the $\Bbbk'$-rational points, because the variety $\mathcal{X}_{\Bbbk'}$ is considered over $\Bbbk'$, wherefore every residue field is a field extension of $\Bbbk'$. Fortunately, we can remedy this. Let $b\colon \operatorname{Spec}\Bbbk' \to \operatorname{Spec}\Bbbk$ be the (unique) $\Bbbk$-morphism induced by the inclusion $\Bbbk \hookrightarrow \Bbbk'$. We then have a map $\operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk, \mathcal{X}) \to \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X})$, $\varphi \mapsto \varphi \circ b$. We show that this map is injective. Suppose $\varphi, \psi\colon \operatorname{Spec}\Bbbk \to \mathcal{X}$ satisfy $\varphi \circ b = \psi \circ b$. Then $\varphi \circ b((0)) = \psi \circ b((0)) \in \mathcal{X}(\Bbbk)$, and so φ and ψ have the same $\Bbbk$-rational point in their image. By (2.1), $\varphi = \psi$. Now we have an inclusion

$$\mathcal{X}(\Bbbk) \cong \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk, \mathcal{X}) \hookrightarrow \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk', \mathcal{X}) \cong \operatorname{Hom}_{\Bbbk'}(\operatorname{Spec}\Bbbk', \mathcal{X}_{\Bbbk'}) \cong \mathcal{X}_{\Bbbk'}(\Bbbk'). \tag{2.3}$$

We shall write $\mathcal{X}_{\Bbbk'}(\Bbbk)$ for the image of $\mathcal{X}(\Bbbk)$ inside $\mathcal{X}_{\Bbbk'}(\Bbbk')$. This image consists of precisely those points $P' \in \mathcal{X}_{\Bbbk'}$ for which $\pi(P') \in \mathcal{X}(\Bbbk)$. The construction above just gives an identification between $\mathcal{X}(\Bbbk)$ and $\mathcal{X}_{\Bbbk'}(\Bbbk)$ as sets. Usually when we look at the $\Bbbk$-rational points, we also want to consider the topology.

***Proposition* 2.6.** *Let $\mathcal{X}$ be a variety over $\Bbbk$, $\Bbbk'/\Bbbk$ an algebraic field extension, and $\pi\colon \mathcal{X}_{\Bbbk'} \to \mathcal{X}$ the projection of the base change of $\mathcal{X}$ to $\Bbbk'$. Then π is an open surjection.*

Proof. Surjectivity and openness are local on the target, so we may assume that $\mathcal{X} = \operatorname{Spec} A$ for some finitely generated, integral $\Bbbk$-algebra A. Then $\mathcal{X}_{\Bbbk'} = \operatorname{Spec}(A \otimes_{\Bbbk} \Bbbk')$ and $\pi = \operatorname{Spec}\iota$, where ι is the inclusion $A \hookrightarrow A \otimes_{\Bbbk} \Bbbk'$, $a \mapsto a \otimes 1$. Since $\Bbbk \hookrightarrow \Bbbk'$ is an integral extension of rings, so is $A \hookrightarrow A \otimes_{\Bbbk} \Bbbk'$. Thus, by 'going up', there lies a prime $\mathfrak{q} \subset A \otimes_{\Bbbk} \Bbbk'$ over every prime $\mathfrak{p} \subset A$. That is to say, for each $\mathfrak{p} \in \mathcal{X}$ there is a $\mathfrak{q} \in \mathcal{X}_{\Bbbk'}$ such that $\pi(\mathfrak{q}) = \mathfrak{p}$.
That π is open follows from [28, Lemma 10.40.10]. □

Next we want to restrict π to $\mathcal{X}_{\Bbbk'}(\Bbbk)$ and show that it becomes a homeomorphism onto $\mathcal{X}(\Bbbk)$. This will take a few steps. We first recall a useful fact from commutative algebra, which we shall need.

***Lemma* 2.7.** *Let R and R' be commutative rings and $f\colon R \to R'$ a surjective homomorphism. Let $\mathfrak{p} \subset R$ be a prime ideal. If $\ker f \subseteq \mathfrak{p}$, then $f(\mathfrak{p})$ is a prime ideal of R'.*

Proof. Let $x', y' \in R'$ with $x'y' \in f(\mathfrak{p})$. Let $x, y \in R$ with $f(x) = x'$ and $f(y) = y'$, and pick a $z \in \mathfrak{p}$ such that $f(z) = x'y'$. Then $xy - z \in \ker f$, and so $xy \in \mathfrak{p}$. Thus either x or y belongs to $\mathfrak{p}$, and so x' or y' lies in $f(\mathfrak{p})$. □

***Lemma* 2.8.** *Let $\mathcal{X}$ be a variety over $\Bbbk$, $\Bbbk'/\Bbbk$ an algebraic extension, and $\pi\colon \mathcal{X}_{\Bbbk'} \to \mathcal{X}$ the projection. Let $P \in \mathcal{X}$ be a closed point, and $Q \in \mathcal{X}_{\Bbbk'}$ such that $\pi(Q) = P$. Then Q is a closed point. Moreover, if $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals corresponding to P and Q, respectively, in some affine opens, then $\kappa(Q) \cong (\kappa(P) \otimes_{\Bbbk} \Bbbk')/\varpi(\mathfrak{q})$, where $\varpi\colon A \otimes_{\Bbbk} \Bbbk' \to (A/\mathfrak{p}) \otimes_{\Bbbk} \Bbbk'$ is the natural map.*

Proof. By restricting to an affine open neighborhood of P, we may assume that $\mathcal{X}$ is affine, say, $\mathcal{X} = \operatorname{Spec} A$. Let $\mathfrak{p} \subset A$ and $\mathfrak{q} \subset A \otimes_{\Bbbk} \Bbbk'$ be prime ideals corresponding to P and Q, respectively. Observe that $\mathfrak{q}$ contracts to $\mathfrak{p}$ under $A \hookrightarrow A \otimes_{\Bbbk} \Bbbk'$, because $\pi(Q) = P$. To show that Q is a closed point, we have to show that $\mathfrak{q}$ is a maximal ideal.
Let $\varpi\colon A \otimes_{\Bbbk} \Bbbk' \to (A/\mathfrak{p}) \otimes_{\Bbbk} \Bbbk'$ be the natural map; note that it is surjective. We first show that $\varpi(\mathfrak{q})$ is prime in $(A/\mathfrak{p}) \otimes_{\Bbbk} \Bbbk'$. To do this, we show that $\ker\varpi \subseteq \mathfrak{q}$ and apply Lemma 2.7. Let $\alpha \in \ker\varpi$. Write $\alpha = \sum_{i=1}^{m}(a_i \otimes b_i)$ with $m \in \mathbb{N}$, $a_1, \dots, a_m \in A$, and $b_1, \dots, b_m \in \Bbbk'$ linearly independent over $\Bbbk$. Now $\varpi(\alpha) = \sum_{i=1}^{m}(\bar{a}_i \otimes b_i) = 0$. By the equational criterion for vanishing [8, Lemma 6.4], there are finitely many $\lambda_{ij} \in \Bbbk$ and $\bar{a}'_j \in A/\mathfrak{p}$ such that for each i

$$\sum_j \lambda_{ij}\bar{a}'_j = \bar{a}_i, \tag{2.4}$$

and for each j

$$\sum_{i=1}^{m} \lambda_{ij} b_i = 0. \tag{2.5}$$

Upon lifting (2.4) to A, we get elements $a''_i \in \mathfrak{p}$ such that $\sum_j \lambda_{ij} a'_j = a_i - a''_i$ for every i. We now have

$$\alpha = \sum_{i=1}^{m}\left(a''_i + \sum_j \lambda_{ij}a'_j\right) \otimes b_i = \sum_{i=1}^{m}(a''_i \otimes b_i) + \sum_{i=1}^{m}\left(\sum_j \lambda_{ij}a'_j \otimes b_i\right).$$

The second summation in the final expression becomes zero:

$$\sum_{i=1}^{m}\left(\sum_j \lambda_{ij} a'_j \otimes b_i\right) = \sum_{i=1}^{m}\sum_j \lambda_{ij}\left(a'_j \otimes b_i\right) = \sum_j \sum_{i=1}^{m} \lambda_{ij}\left(a'_j \otimes b_i\right) = \sum_j a'_j \otimes \left(\sum_{i=1}^{m} \lambda_{ij} b_i\right) = 0,$$

where the final equality follows from (2.5). Whence $\alpha = \sum_{i=1}^{m}(a''_i \otimes b_i)$. This means that every element of the kernel of ϖ can be written as a sum of pure tensors $a\otimes b$ with $a \in \mathfrak{p}$. Note that $\varpi(a\otimes b) = 0\otimes b = 0$. Thus we reduce to the case where $\alpha = a \otimes b$ with $a \in \mathfrak{p}$. Then $a \otimes b = (a \otimes 1)(1 \otimes b) \in \mathfrak{p}(A \otimes_{\Bbbk} \Bbbk')$, the extension of $\mathfrak{p}$ under $A \hookrightarrow A \otimes_{\Bbbk} \Bbbk'$. Since $\mathfrak{q}$ contracts to $\mathfrak{p}$, we have $\mathfrak{p}(A \otimes_{\Bbbk} \Bbbk') \subseteq \mathfrak{q}$. Therefore, $\alpha \in \mathfrak{q}$, and so $\ker \varpi \subseteq \mathfrak{q}$. Combined with the fact that ϖ is surjective, this implies that $\varpi(\mathfrak{q})$ is a prime ideal by Lemma 2.7.

Next we show that $\mathfrak{q}$ is maximal. Since P is a closed point, $\mathfrak{p}$ is a maximal ideal, and hence $A/\mathfrak{p}$ is an algebraic field extension of $\Bbbk$. The extension $\Bbbk \hookrightarrow \Bbbk'$ is integral, thus so is $A/\mathfrak{p} \hookrightarrow (A/\mathfrak{p}) \otimes_{\Bbbk} \Bbbk'$. Since $\dim(A/\mathfrak{p}) = 0$, because it is a field, the same holds for $(A/\mathfrak{p}) \otimes_{\Bbbk} \Bbbk'$. Whence $\varpi(\mathfrak{q})$ is a maximal ideal. The kernel of the composition

$$A \otimes_{\Bbbk} \Bbbk' \to (A/\mathfrak{p}) \otimes_{\Bbbk} \Bbbk' \to ((A/\mathfrak{p}) \otimes_{\Bbbk} \Bbbk')/\varpi(\mathfrak{q})$$

is precisely $\mathfrak{q}$. The composition is surjective onto a field, hence $\mathfrak{q}$ is a maximal ideal, wherefore Q is a closed point. Moreover,

$$\kappa(Q) \cong (A \otimes_{\Bbbk} \Bbbk')/\mathfrak{q} \cong ((A/\mathfrak{p}) \otimes_{\Bbbk} \Bbbk')/\varpi(\mathfrak{q}) \cong (\kappa(P) \otimes_{\Bbbk} \Bbbk')/\varpi(\mathfrak{q}). \qquad \square$$

Let us also recall a simple fact from topology that is going to be very useful.

***Lemma* 2.9.** *Let $f\colon X \to Y$ be a continuous, open, surjective map of topological spaces. Let $S \subseteq X$ be a subspace and suppose that $f^{-1}(f(S)) = S$. Then $f|_S\colon S \to f(S)$ is an open surjection.*

Proof. Let $U \cap S \subseteq S$ be an open set, where $U \subseteq X$ is open. Clearly $f(U \cap S) \subseteq f(U) \cap f(S)$. Let $y \in f(U) \cap f(S)$. There is an $x \in U$ such that $f(x) = y$. Since $y \in f(S)$, $x \in f^{-1}(f(S)) = S$. Hence $x \in U \cap S$, and so $y \in f(U \cap S)$. Now $f(U \cap S) = f(U) \cap f(S)$, which is open in $f(S)$, because $f(U)$ is open. $\square$

Now we have enough material to prove the homeomorphic relation between $\mathfrak{X}_{\Bbbk'}(\Bbbk)$ and $\mathfrak{X}(\Bbbk)$ via π.

***Proposition* 2.10.** *Let $\mathfrak{X}$ be a variety over $\Bbbk$, $\Bbbk'/\Bbbk$ an algebraic extension, and $\pi\colon \mathfrak{X}_{\Bbbk'} \to \mathfrak{X}$ the projection. Then the restriction $\pi|_{\mathfrak{X}_{\Bbbk'}(\Bbbk)}\colon \mathfrak{X}_{\Bbbk'}(\Bbbk) \to \mathfrak{X}(\Bbbk)$ is a homeomorphism.*

Proof. We show in the following order that the map in question is well-defined, injective, and an open surjection.

Let $P' \in \mathfrak{X}_{\Bbbk'}(\Bbbk)$ and let $\varphi'\colon \operatorname{Spec}\Bbbk' \to \mathfrak{X}_{\Bbbk'}$ be the corresponding $\Bbbk'$-morphism. Then, by construction of $\mathfrak{X}_{\Bbbk'}(\Bbbk)$, $\pi \circ \varphi'$ factors as $\varphi \circ b$ with $\varphi \in \operatorname{Hom}_{\Bbbk}(\operatorname{Spec}\Bbbk, \mathfrak{X})$ and $b\colon \operatorname{Spec}\Bbbk' \to \operatorname{Spec}\Bbbk$. Now $\pi(P') = \pi(\varphi'((0))) = \varphi \circ b((0)) \in \mathfrak{X}(\Bbbk)$. Thus $\pi|_{\mathfrak{X}_{\Bbbk'}(\Bbbk)}$ maps into $\mathfrak{X}(\Bbbk)$.

Let $P', Q' \in \mathfrak{X}_{\Bbbk'}(\Bbbk)$ and let $\varphi', \psi' \in \operatorname{Hom}_{\Bbbk'}(\operatorname{Spec}\Bbbk', \mathfrak{X}_{\Bbbk'})$ be the corresponding $\Bbbk'$-valued points. We have $\pi \circ \varphi' = \varphi \circ b$ and $\pi \circ \psi' = \psi \circ b$ with $\varphi, \psi\colon \operatorname{Spec}\Bbbk \to \mathfrak{X}$. Suppose $\pi(P') = \pi(Q')$. This means that $\varphi \circ b((0)) = \psi \circ b((0))$. Consequently, $\varphi = \psi$, and so $\pi \circ \varphi' = \pi \circ \psi'$. By the universal property of the fiber product, $\varphi' = \psi'$. Thus $P' = Q'$ and hence injectivity follows.

It now remains to show that $\pi|_{\mathfrak{X}_{\Bbbk'}(\Bbbk)}$ is open and surjective. Since π is an open surjection by Proposition 2.6, for openness it suffices to show that $\pi^{-1}(\pi(\mathfrak{X}_{\Bbbk'}(\Bbbk))) = \mathfrak{X}_{\Bbbk'}(\Bbbk)$ due to Lemma 2.9. We shall show that any $P \in \mathfrak{X}(\Bbbk)$ comes only from a point $P' \in \mathfrak{X}_{\Bbbk'}(\Bbbk)$, which implies both surjectivity and openness. So let $P \in \mathfrak{X}(\Bbbk)$ and let $P' \in \mathfrak{X}_{\Bbbk'}$ such that $\pi(P') = P$. By Lemma 2.8, $\kappa(P') \cong \Bbbk \otimes_{\Bbbk} \Bbbk' \cong \Bbbk'$. This means that $P' \in \mathfrak{X}_{\Bbbk'}(\Bbbk')$. Thus there is a $\varphi' \in \operatorname{Hom}_{\Bbbk'}(\operatorname{Spec}\Bbbk', \mathfrak{X}_{\Bbbk'})$ such that $\varphi'((0)) = P'$. Then $\pi \circ \varphi'$ induces a local ring homomorphism $\mathcal{O}_{\mathfrak{X},P} \to \mathcal{O}_{\operatorname{Spec}\Bbbk',(0)} = \Bbbk'$ on stalks, which means that it sends the maximal ideal $\mathfrak{m}_{\mathfrak{X},P}$ of $\mathcal{O}_{\mathfrak{X},P}$ into the maximal ideal (0) of $\Bbbk'$. Thus $\mathfrak{m}_{\mathfrak{X},P}$ is in the kernel of this map, which therefore factors through $\mathcal{O}_{\mathfrak{X},P}/\mathfrak{m}_{\mathfrak{X},P} = \kappa(P) = \Bbbk$. Whence $\pi \circ \varphi'$ factors through $\operatorname{Spec}\Bbbk$, giving rise to a map $\varphi\colon \operatorname{Spec}\Bbbk \to \mathfrak{X}$ with image P such that $\pi \circ \varphi' = \varphi \circ b$. By the universal property of the fiber product, $\varphi' = (\varphi \circ b) \times_{\Bbbk} \mathrm{id}_{\operatorname{Spec}\Bbbk'}$, the latter being the map obtained following the construction of $\mathfrak{X}_{\Bbbk'}(\Bbbk)$ in (2.3). Hence $P' \in \mathfrak{X}_{\Bbbk'}(\Bbbk)$.

We now conclude that $\pi|_{\mathfrak{X}_{\Bbbk'}(\Bbbk)}$ is a continuous, open bijection onto $\mathfrak{X}(\Bbbk)$, i.e., a homeomorphism. $\square$

Besides the projection morphism, any morphism between varieties restricts to a map between their respective $\Bbbk'$-rational points for any algebraic extension $\Bbbk'/\Bbbk$.

***Proposition* 2.11.** *Let $\varphi\colon \mathcal{X} \to \mathcal{Y}$ be a morphism of varieties. Let $\Bbbk'/\Bbbk$ be an algebraic extension. Then φ restricts to $\mathcal{X}(\Bbbk') \to \mathcal{Y}(\Bbbk')$.*

Proof. Let $P \in \mathcal{X}(\Bbbk')$. Then φ induces a local ring homomorphism $\varphi_P^\sharp\colon \mathcal{O}_{\mathcal{Y},\varphi(P)} \to \mathcal{O}_{\mathcal{X},P}$; that is, $\varphi_P^\sharp\big(\mathfrak{m}_{\mathcal{Y},\varphi(P)}\big) \subseteq \mathfrak{m}_{\mathcal{X},P}$. The composition of $\varphi_P^\sharp$ with the quotient map to $\mathcal{O}_{\mathcal{X},P}/\mathfrak{m}_{\mathcal{X},P}$ therefore factors through $\mathcal{O}_{\mathcal{Y},\varphi(P)}/\mathfrak{m}_{\mathcal{Y},\varphi(P)}$; thusly we obtain the commutative diagram

$$\begin{array}{ccccc} \mathcal{O}_{\mathcal{Y},\varphi(P)} & \xrightarrow{\varphi_P^\sharp} & \mathcal{O}_{\mathcal{X},P} & \twoheadrightarrow & \kappa(P). \\ & \searrow & & \nearrow & \\ & & \kappa(\varphi(P)) & & \end{array}$$

Consequently, there is an embedding $\kappa(\varphi(P)) \hookrightarrow \kappa(P) \hookrightarrow \Bbbk'$, wherefore $\varphi(P) \in \mathcal{Y}(\Bbbk')$. □

In particular, a morphism induces a map on $\Bbbk$-rational points. In the case of affine spaces $\mathbb{A}^n_\Bbbk$ the converse is also true. In the literature one may find that affine varieties are identified with their $\Bbbk$-rational points, often implicitly. For the sake of preciseness, we shall explicitly construct a way this identification can be used for affine spaces. Fix an $n \in \mathbb{N}_0$ and let $A \coloneqq \Bbbk[X_1, \dots, X_n]$, the polynomial ring in n variables over $\Bbbk$. The n-dimensional affine space $\mathbb{A}^n_\Bbbk$ is defined to be $\operatorname{Spec} A$. On $\mathbb{A}^n_\Bbbk$ we have the usual Zariski topology, whose closed sets are $\mathcal{V}(\mathfrak{a}) \coloneqq \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{a} \subseteq \mathfrak{p}\}$, where $\mathfrak{a} \subseteq A$ is an ideal. On the other hand one finds the space $\Bbbk^n$ endowed also with the Zariski topology. In the latter case this means that the closed sets of $\Bbbk^n$ are of the form $\mathcal{Z}(\mathfrak{a}) \coloneqq \{\alpha \in \Bbbk^n \mid f(\alpha) = 0 \text{ for all } f \in \mathfrak{a}\}$, where again $\mathfrak{a} \subseteq A$ is an ideal. The concepts are similar, but the actual objects in question are quite different. The following proposition shows the precise relation that we have.

***Proposition* 2.12.** *Let $A \coloneqq \Bbbk[X_1, \dots, X_n]$ be the polynomial ring in n variables, and consider the n-dimensional affine space $\mathbb{A}^n_\Bbbk = \operatorname{Spec} A$. Then $\mathbb{A}^n_\Bbbk(\Bbbk)$ with the induced subspace topology is homeomorphic to $\Bbbk^n$ endowed with the Zariski topology.*

Proof. Let $\mathfrak{m} \in \mathbb{A}^n_\Bbbk(\Bbbk)$. Then $A/\mathfrak{m} \cong \kappa(\mathfrak{m}) = \Bbbk$. Any map $A \to \Bbbk$ is completely determined by fixed elements $\alpha_1, \dots, \alpha_n \in \Bbbk$ via $X_i \mapsto \alpha_i$. Thus $\mathfrak{m}$ is the kernel of some map $A \to \Bbbk$, $f \mapsto f(\alpha)$ for some $\alpha \in \Bbbk^n$. That is, $\mathfrak{m} = \mathfrak{m}_\alpha \coloneqq \{f \in A \mid f(\alpha) = 0\} = (X_1 - \alpha_1, \dots, X_n - \alpha_n)$. Clearly this α is uniquely determined by $\mathfrak{m}$. Thus we get a bijection $\psi\colon \mathbb{A}^n_\Bbbk(\Bbbk) \to \Bbbk^n$ by sending $\mathfrak{m}_\alpha$ to α.
Let $\mathfrak{a} \subseteq A$ be an ideal. A point α belongs to $\mathcal{Z}(\mathfrak{a})$ if and only if each polynomial in $\mathfrak{a}$ vanishes at α if and only if $\mathfrak{a} \subseteq \mathfrak{m}_\alpha$ if and only if $\mathfrak{m}_\alpha \in \mathcal{V}(\mathfrak{a})$. Thus $\psi^{-1}(\mathcal{Z}(\mathfrak{a})) = \mathcal{V}(\mathfrak{a}) \cap \mathbb{A}^n_\Bbbk(\Bbbk)$ and $\psi(\mathcal{V}(\mathfrak{a}) \cap \mathbb{A}^n_\Bbbk(\Bbbk)) = \mathcal{Z}(\mathfrak{a})$. All closed sets of $\Bbbk^n$ and $\mathbb{A}^n_\Bbbk(\Bbbk)$ are of these forms, wherefore ψ is continuous and closed, and hence a homeomorphism. □

This identification allows us to prove a useful fact for later use.

***Lemma* 2.13.** *Assume that $\Bbbk$ is infinite. Let $\mathcal{X}$ be a $\Bbbk$-unirational variety, i.e., a variety equipped with a dominant, rational map $\mathbb{A}^n_\Bbbk \dashrightarrow \mathcal{X}$ for some $n \in \mathbb{N}_0$. Then $\mathcal{X}_{\overline{\Bbbk}}(\Bbbk)$ is dense in $\mathcal{X}_{\overline{\Bbbk}}(\overline{\Bbbk})$.*

Proof. We first show that $\mathbb{A}^n_{\overline{\Bbbk}}(\Bbbk)$ is dense in $\mathbb{A}_{\overline{\Bbbk}}(\overline{\Bbbk})$. From Proposition 2.12 this boils down to showing that $\Bbbk^n$ is dense in $\overline{\Bbbk}^n$ for the Zariski topology. Let $\mathcal{Z}(\mathfrak{a}) \subseteq \overline{\Bbbk}^n$ be the closure of $\Bbbk^n$, where $\mathfrak{a} \subseteq \overline{\Bbbk}[X_1, \dots, X_n]$ is an ideal. Any $f \in \mathfrak{a}$ vanishes on all of $\Bbbk^n$. Since $\Bbbk$ is infinite, this implies that f is the zero polynomial. Hence $\mathfrak{a} = 0$, which means that $\mathcal{Z}(\mathfrak{a}) = \overline{\Bbbk}^n$, and so $\Bbbk^n$ is dense in $\overline{\Bbbk}^n$.
The given dominant, rational map $\mathbb{A}^n_\Bbbk \dashrightarrow \mathcal{X}$ extends to a dominant, rational map $\mathbb{A}^n_{\overline{\Bbbk}} \dashrightarrow \mathcal{X}_{\overline{\Bbbk}}$, because it still sends the generic point to the generic point. Let $U \subseteq \mathbb{A}^n_{\overline{\Bbbk}}$ be a non-empty open, and $\varphi\colon U \to \mathcal{X}_{\overline{\Bbbk}}$ a morphism representing this rational map. Since $\mathbb{A}^n_\Bbbk(\Bbbk)$ is dense in $\mathbb{A}^n_{\overline{\Bbbk}}(\overline{\Bbbk})$, which in turn is dense in $\mathbb{A}^n_{\overline{\Bbbk}}$, it follows that $\mathbb{A}^n_{\overline{\Bbbk}}(\Bbbk)$ is dense in $\mathbb{A}^n_{\overline{\Bbbk}}$. From this follows that $U(\Bbbk)$ is dense in U. Subsequently, $\varphi(U(\Bbbk))$ is dense in $\operatorname{im}\varphi$, which in turn is dense in $\mathcal{X}_{\overline{\Bbbk}}$. Thus $\varphi(U(\Bbbk))$ is dense in $\mathcal{X}_{\overline{\Bbbk}}$. A morphism sends $\Bbbk$-points to $\Bbbk$-points, wherefrom follows that $\varphi(U(\Bbbk)) \subseteq \mathcal{X}_{\overline{\Bbbk}}(\Bbbk)$. This implies that $\mathcal{X}_{\overline{\Bbbk}}(\Bbbk)$ is dense in $\mathcal{X}_{\overline{\Bbbk}}(\overline{\Bbbk})$. □

Chapter 3

Essential Dimension of Algebraic Varieties

We again fix a field $\Bbbk$. All fields that we will consider are assumed to contain $\Bbbk$, homomorphisms of such fields are $\Bbbk$-linear, and all algebraic varieties are defined over $\Bbbk$, unless stated otherwise. An algebraic closure of $\Bbbk$ will be denoted by $\overline{\Bbbk}$.

In this chapter we shall define the essential dimension of algebraic varieties. We are interested in a specific type of variety, namely ones on which a finite group acts in a certain way.

3.1 Group Actions on Varieties

Henceforth we fix a finite group G and we denote its neutral element by e.

Definition 3.1 (G-variety)**.** A variety $(\mathfrak{X}, \mathcal{O}_\mathfrak{X})$ is called a *G-variety* if it is endowed with a group action $\rho\colon G \to \mathrm{Aut}(\mathfrak{X}, \mathcal{O}_\mathfrak{X})$. That is to say, each $\sigma \in G$ induces an automorphism $\rho(\sigma) = ({}_\mathfrak{X}\sigma, {}_\mathfrak{X}\sigma^\sharp)$ on $(\mathfrak{X}, \mathcal{O}_\mathfrak{X})$ in such a way that $\rho(e)$ is the identity and for all $\sigma, \tau \in G$, $\rho(\sigma\tau) = \rho(\sigma) \circ \rho(\tau)$. We call $\mathfrak{X}$ a *faithful G-variety* if G acts faithfully, i.e., if ρ is injective. ☆

Notation. If G acts on some algebraic object A, be it a variety, an algebra, or a field, we usually denote the automorphism on A induced by an element $\sigma \in G$ using a preceding subscript: ${}_A\sigma\colon A \to A$. Sometimes this subscript will be omitted when this causes no confusion and is more convenient.

Remark. If $B \subseteq A$ such that the action on A restricts to B, i.e., for each $\sigma \in G$ we have ${}_A\sigma(B) \subseteq B$, then we say that B is *G-invariant*. Note that by this we—as opposed to some of the literature—do *not* mean that the action on A becomes trivial on B. ✧

Morphisms of varieties induce homomorphisms on stalks between the corresponding points. If we apply this to automorphisms arising from a group action and the stalk at the generic point, then the following proposition provides us with a group action on the function field.

***Proposition* 3.2.** *Let $\mathfrak{X}$ be a G-variety and let $\eta \in \mathfrak{X}$ be the generic point. The action of G on $\mathfrak{X}$ induces a group action on the function field $\Bbbk(\mathfrak{X}) = \mathcal{O}_{\mathfrak{X},\eta}$.*

Proof. Let $\sigma \in G$. Since the induced map ${}_\mathfrak{X}\sigma$ on the underlying topological space is surjective, it is dominant, and so ${}_\mathfrak{X}\sigma(\eta) = \eta$. We therefore have an induced $\Bbbk$-algebra homomorphism ${}_\mathfrak{X}\sigma^\sharp_\eta\colon \mathcal{O}_{\mathfrak{X},\eta} \to \mathcal{O}_{\mathfrak{X},\eta}$. Because G acts on $\mathfrak{X}$, we have for any two $\sigma, \tau \in G$ the equality ${}_\mathfrak{X}(\sigma\tau)^\sharp = {}_\mathfrak{X}\tau^\sharp \circ {}_\mathfrak{X}\sigma^\sharp$. Going to the stalk at η yields in particular that ${}_\mathfrak{X}(\sigma\tau)^\sharp_\eta = {}_\mathfrak{X}\tau^\sharp_\eta \circ {}_\mathfrak{X}\sigma^\sharp_\eta$. That ${}_\mathfrak{X}e^\sharp$ is the identity means that for any open $U \subseteq \mathfrak{X}$, the map ${}_\mathfrak{X}e^\sharp_U\colon \mathcal{O}_\mathfrak{X}(U) \to \mathcal{O}_\mathfrak{X}(U)$ is the identity. Thus we immediately obtain that ${}_\mathfrak{X}e^\sharp_\eta = \mathrm{id}_{\mathcal{O}_{\mathfrak{X},\eta}}$. Consequently, ${}_\mathfrak{X}(\sigma^{-1})^\sharp_\eta$ is the inverse of ${}_\mathfrak{X}\sigma^\sharp_\eta$. We conclude that G acts on $\Bbbk(\mathfrak{X})$ via $\sigma \mapsto {}_\mathfrak{X}\sigma^\sharp_\eta$. □

It turns out that the obtained group action on the function field has the nice property of retaining the distinct actions of different elements of G. The converse is also true. This means that two elements of G act differently on the variety if and only if they act differently on the function field. The following two assertions make this more precise.

***Proposition* 3.3.** *Let $\mathfrak{X}$ be a variety, $\eta \in \mathfrak{X}$ its generic point, and $(\varphi, \varphi^\sharp)$ an automorphism. Then $(\varphi, \varphi^\sharp)$ is the identity on $(\mathfrak{X}, \mathcal{O}_\mathfrak{X})$ if and only if the induced automorphism $\varphi^\sharp_\eta$ is the identity on $\mathcal{O}_{\mathfrak{X},\eta}$.*

Proof. In the proof of Proposition 3.2 we have already seen that the direct implication is true.
We prove the converse implication. Consider the identity morphism $(\mathrm{id}, \mathrm{id}^\sharp)\colon (\mathfrak{X}, \mathcal{O}_\mathfrak{X}) \to (\mathfrak{X}, \mathcal{O}_\mathfrak{X})$. Observe that $\mathrm{id}^\sharp_\eta$ is the identity map on $\mathcal{O}_{\mathfrak{X},\eta}$, hence $\mathrm{id}^\sharp_\eta = \varphi^\sharp_\eta$ by assumption. Then [28, Lemma 28.40.4(1)] asserts that there is a non-empty open $U \subseteq \mathfrak{X}$ such that $\mathrm{id}\,|_U = \varphi|_U$. Since $\mathfrak{X}$ is separated, this implies that $(\varphi, \varphi^\sharp) = (\mathrm{id}, \mathrm{id}^\sharp)$, as desired. □

***Corollary* 3.4.** *Let $\mathfrak{X}$ be a G-variety. Then G acts faithfully on $\mathfrak{X}$ if and only if G acts faithfully on $\Bbbk(\mathfrak{X})$.*

Proof. Let $\eta \in \mathfrak{X}$ be the generic point. Consider the following conditions:

(i) for all $\sigma \in G$, $({}_\mathfrak{X}\sigma, {}_\mathfrak{X}\sigma^\sharp)$ is the identity on $(\mathfrak{X}, \mathcal{O}_\mathfrak{X})$ if and only if $\sigma = e$;
(ii) for all $\sigma \in G$, ${}_\mathfrak{X}\sigma^\sharp_\eta$ is the identity on $\Bbbk(\mathfrak{X})$ if and only if $\sigma = e$.

The first condition means that G acts faithfully on $(\mathfrak{X}, \mathcal{O}_\mathfrak{X})$; the second one says exactly that G acts faithfully on $\Bbbk(\mathfrak{X})$. For every $\sigma \in G$, Proposition 3.3 says that $({}_\mathfrak{X}\sigma, {}_\mathfrak{X}\sigma^\sharp)$ is the identity if and only if ${}_\mathfrak{X}\sigma^\sharp_\eta$ is the identity. Thus the left-hand side condition in (i) and (ii) are equivalent for any $\sigma \in G$. This just means that (i) and (ii) are equivalent, which is what we wanted to show. □

In the case of affine varieties we also have a nice relation between a group action on a finitely generated, integral $\Bbbk$-algebra, and a group action on its spectrum.

***Proposition* 3.5.** *Let A be a finitely generated, integral $\Bbbk$-algebra. Suppose that G acts on A via $\sigma \mapsto {}_A\sigma\colon A \to A$ in such a way that ${}_A(\sigma\tau) = {}_A\tau \circ {}_A\sigma$ for any $\sigma, \tau \in G$ (this is essentially a right group action written on the left). This induces an action on $\mathfrak{X} \coloneqq \operatorname{Spec} A$. Moreover, G acts faithfully on A if and only if G acts faithfully on $\mathfrak{X}$.*

Proof. From [11, Proposition II.2.3] we get an injection $\mathrm{Aut}(A) \hookrightarrow \mathrm{Aut}(\mathfrak{X})$. Moreover, if $f, g \in \mathrm{Aut}(A)$ induce respectively $(\varphi, \varphi^\sharp), (\psi, \psi^\sharp) \in \mathrm{Aut}(\mathfrak{X})$, then $f \circ g$ induces $(\psi, \psi^\sharp) \circ (\varphi, \varphi^\sharp)$. Note that the order of composition is reversed.
Thus for each $\sigma \in G$ the automorphism ${}_A\sigma\colon A \to A$ induces uniquely an automorphism $({}_\mathfrak{X}\sigma, {}_\mathfrak{X}\sigma^\sharp)$ on $\mathfrak{X}$. Because for $\sigma, \tau \in G$ we have ${}_A(\sigma\tau) = {}_A\tau \circ {}_A\sigma$, the induced automorphisms on $\mathfrak{X}$ are the same: $({}_\mathfrak{X}(\sigma\tau), {}_\mathfrak{X}(\sigma\tau)^\sharp) = ({}_\mathfrak{X}\sigma, {}_\mathfrak{X}\sigma^\sharp) \circ ({}_\mathfrak{X}\tau, {}_\mathfrak{X}\tau^\sharp)$. Moreover, $e \in G$ yields ${}_Ae = \mathrm{id}_A$, wherefore this induces the identity on $\mathfrak{X}$. Whence the composition $G \to \mathrm{Aut}(A) \hookrightarrow \mathrm{Aut}(\mathfrak{X})$, $\sigma \mapsto {}_A\sigma \mapsto ({}_\mathfrak{X}\sigma, {}_\mathfrak{X}\sigma^\sharp)$, is a group action of G on $\mathfrak{X}$.
Finally, since the second map of this composition is an injection, we see that $G \to \mathrm{Aut}(A)$ is injective if and only if $G \to \mathrm{Aut}(\mathfrak{X})$ is injective. Thus the last assertion also holds. □

Remark 3.6. From [11, Proposition II.2.3] we also get for any $\sigma \in G$ the equality ${}_\mathfrak{X}\sigma^\sharp_\mathfrak{X} = {}_A\sigma$. This is compatible with composition, so the group action on A can be recovered from the one it induces on $\mathfrak{X}$. ✧

Often we want to restrict to an affine, open subset of a variety, because the variety as a whole is usually less tractable. The following lemma helps with this for G-varieties.

***Lemma* 3.7.** *Let $\mathfrak{X}$ be a G-variety and let $U \subseteq \mathfrak{X}$ be a non-empty, open subset. Then there exists a non-empty, affine, G-invariant open $V \subseteq U$.*

Proof. Without loss of generality we may assume that U is affine. We omit the subscript of the induced morphisms by G for the sake of notational clarity. Let $V \coloneqq \bigcap_{\tau \in G} \tau^{-1}(U)$, which is a subset of U. Since U is affine, so is $\tau^{-1}(U)$ for each τ. It now follows that V is a non-empty, affine open, because G is finite and $\mathfrak{X}$ is irreducible and separated. For every $\sigma \in G$ we have

$$\sigma(V) = \bigcap_{\tau \in G} \sigma\big(\tau^{-1}(U)\big) = \bigcap_{\tau \in G} \big(\tau\sigma^{-1}\big)^{-1}(U) = V,$$

because as τ goes through all element of G, so does $\tau\sigma^{-1}$. □

Remark 3.8. If the action of G on $\mathfrak{X}$ is faithful, then the action of G on V is faithful as well (and vice versa): Suppose for $\sigma, \tau \in G$ we have ${}_V\sigma = {}_V\tau$. This means that ${}_\mathfrak{X}\sigma|_V = {}_\mathfrak{X}\tau|_V$. Then the fact that $\mathfrak{X}$ is separated implies that ${}_\mathfrak{X}\sigma = {}_\mathfrak{X}\tau$. Consequently, $\sigma = \tau$, as G acts faithfully on $\mathfrak{X}$. Hence G acts faithfully on V. ✧

We shall need to relate different G-varieties to each other, so we need a concept of morphisms between them that respect the group actions.

Definition 3.9. Let $\mathcal{X}$ and $\mathcal{Y}$ be G-varieties. A morphism $\varphi\colon \mathcal{X} \to \mathcal{Y}$ of varieties is called *G-equivariant* if φ commutes with the actions of G. That is to say, for every $\sigma \in G$ we have the equality $\varphi \circ {}_{\mathcal{X}}\sigma = {}_{\mathcal{Y}}\sigma \circ \varphi$ of morphisms. Such a morphism is also called a *G-map*. ☆

In the affine case these G-maps may arise from G-equivariant homomorphisms between finitely generated, integral $\Bbbk$-algebras on which G acts. We prove this in the following lemma.

***Lemma* 3.10.** *Let A and B be finitely generated, integral $\Bbbk$-algebras. Let G act on both of them. Let $f\colon A \to B$ be a homomorphism of $\Bbbk$-algebras that commutes with the action of G. Then the induced morphism $\varphi\colon \operatorname{Spec} B \to \operatorname{Spec} A$ is G-equivariant.*

Proof. For every $\sigma \in G$ the homomorphisms ${}_{B}\sigma \circ f$ and $f \circ {}_{A}\sigma$ on A induce respectively $\varphi \circ {}_{\operatorname{Spec} B}\sigma$ and ${}_{\operatorname{Spec} A}\sigma \circ \varphi$. These are equal, because ${}_{B}\sigma \circ f = f \circ {}_{A}\sigma$ by assumption. □

Analogous to rational maps of varieties, we do not want to restrict ourselves only to G-maps that are defined on the entire source space.

Definition 3.11. Let $\mathcal{X}$ and $\mathcal{Y}$ be G-varieties. A *rational, G-equivariant map* (or *rational G-map*) is a rational map $\varphi\colon \mathcal{X} \dashrightarrow \mathcal{Y}$ such that for every $\sigma \in G$ the rational maps $\varphi \circ {}_{\mathcal{X}}\sigma$ and ${}_{\mathcal{Y}}\sigma \circ \varphi$ are equal; this means that there is a non-empty open $U \subseteq \mathcal{X}$ and a morphism $\psi\colon U \to \mathcal{Y}$ such that (U, ψ) is a representative for both $\varphi \circ {}_{\mathcal{X}}\sigma$ and ${}_{\mathcal{Y}}\sigma \circ \varphi$. ☆

We now have enough material to come to the definition of essential dimension of faithful G-varieties.

Definition 3.12 (Essential dimension of a faithful G-variety)**.** Let $\mathcal{X}$ be a faithful G-variety. Let $\mathcal{Y}$ be a G-variety. We say that $\mathcal{X}$ is *defined over* $\mathcal{Y}$, if $\mathcal{Y}$ is faithful, and if there exists a dominant, rational G-map $\mathcal{X} \dashrightarrow \mathcal{Y}$. The *essential dimension of $\mathcal{X}$ over* $\Bbbk$ is the minimal dimension of $\mathcal{Y}$, where $\mathcal{Y}$ ranges over all G-varieties over which $\mathcal{X}$ is defined. We denote this number by $\operatorname{ed}_{\Bbbk}(G \circlearrowright \mathcal{X})$. ☆

From algebraic geometry we know that the dimension of a variety $\mathcal{X}$ is the transcendence degree of its function field. The following theorem asserts a similar relation for essential dimension: It relates the essential dimension of a faithful G-variety to the essential dimension of its function field over the subfield fixed by G. This relation is stated in [3, Lemma 2.7], but the proof below is our own.

***Theorem* 3.13.** *Let $\mathcal{X}$ be a faithful G-variety. Let $L \coloneqq \Bbbk(\mathcal{X})$ and $K \coloneqq L^G$. Then*

$$\operatorname{ed}_{\Bbbk}(G \circlearrowright \mathcal{X}) = \operatorname{ed}_{\Bbbk}(L/K). \tag{3.1}$$

Proof. We shall prove the desired equality by proving both inequalities.
First we prove '$\geq$' in (3.1). Let $\mathcal{Y}$ be a G-variety over which $\mathcal{X}$ is defined such that $\operatorname{ed}_{\Bbbk}(G \circlearrowright \mathcal{X}) = \dim(\mathcal{Y})$. Let $\varphi\colon \mathcal{X} \dashrightarrow \mathcal{Y}$ be the given dominant, rational G-map. Let $U \subseteq \mathcal{X}$ be open and non-empty, and let $(U, {}_{U}\varphi)$ represent φ. Let $\eta \in \mathcal{X}$ and $\xi \in \mathcal{Y}$ be the generic points. Note that ${}_{U}\varphi(\eta) = \xi$, because φ is dominant. Since $\eta \in U$, we get a $\Bbbk$-algebra homomorphism on stalks ${}_{U}\varphi^{\sharp}_{\eta}\colon \mathcal{O}_{\mathcal{Y},\xi} \to \mathcal{O}_{U,\eta}$. Since U is dense in $\mathcal{X}$, we have $\mathcal{O}_{U,\eta} = \mathcal{O}_{\mathcal{X},\eta}$, wherefore we get a G-equivariant monomorphism $\Bbbk(\mathcal{Y}) \hookrightarrow \Bbbk(\mathcal{X})$ of fields that fixes $\Bbbk$. Let E be the image of $\Bbbk(\mathcal{Y})$ in $L = \Bbbk(\mathcal{X})$. Since G acts faithfully on E, Lemma 1.3 shows that

$$\operatorname{ed}_{\Bbbk}(L/K) \leq \operatorname{trdeg}_{\Bbbk}(E) = \dim(\mathcal{Y}) = \operatorname{ed}_{\Bbbk}(G \circlearrowright \mathcal{X}). \tag{3.2}$$

Next we prove '$\leq$' in (3.1). Let E/F be a field extension over which L/K is defined such that $\operatorname{ed}_{\Bbbk}(L/K) = \operatorname{trdeg}_{\Bbbk}(F)$. Because L/K is a Galois extension with Galois group G, we may assume that E/F is Galois as well with the same Galois group by Lemma 1.4. We now want to construct a dominant, rational G-map $\mathcal{X} \dashrightarrow \mathcal{Y}$, where $\mathcal{Y}$ is a faithful G-variety with $\Bbbk(\mathcal{Y}) = E$.

Construction of $\mathcal{Y}$. Let $U \subseteq \mathcal{X}$ be a non-empty, affine, open subset; say, $U = \operatorname{Spec} A$, where A is a finitely generated, integral $\Bbbk$-algebra. Since $\operatorname{Frac}(A) \cong L$, it follows that L is finitely generated over $\Bbbk$. Whence so is E by [2, §V.15, Corollary 3, p. V.118]. Say E is generated by $y_1, \ldots, y_m \in E$. Let B be the $\Bbbk$-algebra generated by all G-orbits of the y_i; that is to say, $B \coloneqq \Bbbk\big[\{{}_{E}\tau(y_i) \mid \tau \in G\}_{i=1}^{m}\big]$; note that here ${}_{E}\tau = {}_{\mathcal{X}}\tau^{\sharp}_{\eta}|_{E}$. Clearly $\operatorname{Frac}(B) = E$ and, by construction, the action of G on E restricts to B. Consequently, G acts faithfully on B.
Let $\mathcal{Y} \coloneqq \operatorname{Spec} B$. From Proposition 3.5 we obtain a faithful G-action on $\mathcal{Y}$. This action arises in such a way that ${}_{\mathcal{Y}}\sigma^{\sharp}_{\mathcal{Y}} = {}_{B}\sigma$ for every $\sigma \in G$. We have $\Bbbk(\mathcal{Y}) = \operatorname{Frac}(B) = E$, as we wanted. We still need to

check that $\mathcal{Y}$ is geometrically irreducible, but for this we shall utilize the following construction.

Construction of $\mathcal{X} \dashrightarrow \mathcal{Y}$. For each $\tau \in G$ and $i \in \{1, \dots, m\}$ let $V_{\tau,i} \subseteq \mathcal{X}$ be a non-empty open such that ${}_E\tau(y_i) \in \mathcal{O}_{\mathcal{X}}(V_{\tau,i})$. Since G is finite and there are finitely many i, the intersection of all these sets is again open. Thus, by Lemma 3.7, there is a non-empty, affine, open subset $V \subseteq \bigcap_{\tau\in G}\bigcap_{i=1}^{m} V_{\tau,i}$ on which G acts. Say $V = \operatorname{Spec} C$ for a finitely generated, integral $\Bbbk$-algebra C. Note that $\mathcal{O}_{\mathcal{X}}(V) \cong C$ and so G acts on C via $\sigma \mapsto {}_{\mathcal{X}}\sigma_V^{\sharp}$. We then have an inclusion $\iota\colon B \hookrightarrow C$. This is indeed injective: If $f \in \ker \iota$, then $f|_V = 0$, and so $(V, f|_V)$ is zero in $\Bbbk(\mathcal{Y}) \subseteq \Bbbk(\mathcal{X})$. Since $B \subseteq \Bbbk(\mathcal{Y})$, it follows that $f = 0$.
We can now show that $\mathcal{Y}$ is geometrically irreducible. For this we just need to check that the nilradical of $B \otimes_{\Bbbk} \overline{\Bbbk}$ is prime. Note that V is geometrically irreducible, because $\mathcal{X}$ is. Since $B \hookrightarrow C$ and $\overline{\Bbbk}$ is flat over $\Bbbk$, we get an inclusion $B \otimes_{\Bbbk} \overline{\Bbbk} \hookrightarrow C \otimes_{\Bbbk} \overline{\Bbbk}$. The nilradical of $C \otimes_{\Bbbk} \overline{\Bbbk}$ is a prime ideal, because V is geometrically irreducible. The contraction of this ideal to $B \otimes_{\Bbbk} \overline{\Bbbk}$ is precisely $\operatorname{nil}(B \otimes_{\Bbbk} \overline{\Bbbk})$, which is therefore prime as well.
Next we show that ι commutes with the G-action on B and C. For this we must show that $\iota \circ {}_B\sigma = {}_{\mathcal{X}}\sigma_V^{\sharp} \circ \iota$ for every $\sigma \in G$. We have the commutative diagram

$$\begin{array}{ccc} \mathcal{O}_{\mathcal{X}}(V) & \xrightarrow{{}_{\mathcal{X}}\sigma_V^{\sharp}} & \mathcal{O}_{\mathcal{X}}(V) \\ \big\downarrow & & \big\downarrow \\ \mathcal{O}_{\mathcal{X},\eta} & \xrightarrow{{}_{\mathcal{X}}\sigma_{\eta}^{\sharp}} & \mathcal{O}_{\mathcal{X},\eta}, \end{array}$$

where the vertical maps are inclusions. Thus, upon regarding $C \subseteq \mathcal{O}_{\mathcal{X},\eta}$, we have ${}_{\mathcal{X}}\sigma_V^{\sharp} = {}_{\mathcal{X}}\sigma_{\eta}^{\sharp}|_C$. Moreover, by construction, ${}_B\sigma = {}_{\mathcal{X}}\sigma_{\eta}^{\sharp}|_B$. Since B and C are subalgebras of $\mathcal{O}_{\mathcal{X},\eta}$, and ι is just a simple inclusion, it commutes automatically with the group actions.
Let φ be the morphism $\operatorname{Spec} C \to \mathcal{Y}$ induced by ι. Since ι is injective, φ is dominant. Lemma 3.10 implies that φ is G-equivariant. From this we conclude that (V, φ) is a representative of a dominant, rational G-map $\mathcal{X} \dashrightarrow \mathcal{Y}$. We now have obtained that $\mathcal{X}$ is defined over $\mathcal{Y}$. Consequently,

$$\operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) \leq \dim(\mathcal{Y}) = \operatorname{trdeg}_{\Bbbk}(E) = \operatorname{trdeg}_{\Bbbk}(F) = \operatorname{ed}_{\Bbbk}(L/K). \tag{3.3}$$

Combining (3.2) and (3.3) yields the desired equality $\operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) = \operatorname{ed}_{\Bbbk}(L/K)$. □

***Corollary* 3.14.** *Let $\mathcal{X}$ be a faithful G-variety. Then there exists an affine G-variety $\mathcal{Y}$ over which $\mathcal{X}$ is defined such that* $\operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) = \dim(\mathcal{Y})$.

Proof. Construct $\mathcal{Y}$ as in the proof of Theorem 3.13. It then follows together with (3.3) that

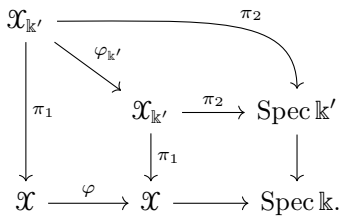
$$\operatorname{ed}_{\Bbbk}\big(\Bbbk(\mathcal{X})/\Bbbk(\mathcal{X})^G\big) = \operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) \leq \dim(\mathcal{Y}) = \operatorname{ed}_{\Bbbk}\big(\Bbbk(\mathcal{X})/\Bbbk(\mathcal{X})^G\big).$$

Thus $\operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) = \dim(\mathcal{Y})$. □

We shall need to apply the basics lain in Section 2.2 with group actions. Fortunately, group actions fit nicely onto this, as we see in the following two propositions.

***Proposition* 3.15.** *Let $\mathcal{X}$ be a G-variety and $\Bbbk'/\Bbbk$ an algebraic extension. The action of G on $\mathcal{X}$ extends to $\mathcal{X}_{\Bbbk'}$. Moreover, G acts faithfully on $\mathcal{X}$ if and only if G acts faithfully on $\mathcal{X}_{\Bbbk'}$.*

Proof. Let $\pi_1\colon \mathcal{X}_{\Bbbk'} \to \mathcal{X}$ and $\pi_2\colon \mathcal{X}_{\Bbbk'} \to \operatorname{Spec} \Bbbk'$ be the projections. Let $\varphi \in \operatorname{Aut}(\mathcal{X})$. This map extends to $\mathcal{X}_{\Bbbk'}$ via the unique morphism $\varphi_{\Bbbk'}$ that fits the commutative diagram



Let $\psi \in \operatorname{Aut}(\mathcal{X})$. Then

$$\pi_1 \circ (\varphi_{\Bbbk'} \circ \psi_{\Bbbk'}) = \varphi \circ \pi_1 \circ \psi_{\Bbbk'} = (\varphi \circ \psi) \circ \pi_1 = \pi_1 \circ (\varphi \circ \psi)_{\Bbbk'}.$$

Similarly, $\pi_2 \circ (\varphi_{\Bbbk'} \circ \psi_{\Bbbk'}) = \pi_2 = \pi_2 \circ (\varphi \circ \psi)_{\Bbbk'}$. Thus, by the universal property of the fiber product, $\varphi_{\Bbbk'} \circ \psi_{\Bbbk'} = (\varphi \circ \psi)_{\Bbbk'}$. Clearly $(\mathrm{id}_{\mathfrak{X}})_{\Bbbk'} = \mathrm{id}_{\mathfrak{X}_{\Bbbk'}}$. Consequently, we get a well-defined group homomorphism $\rho\colon \mathrm{Aut}(\mathfrak{X}) \to \mathrm{Aut}(\mathfrak{X}_{\Bbbk'})$. Moreover, we show that ρ is injective. Suppose $\varphi \in \ker \rho$. Then $\varphi_{\Bbbk'} = \mathrm{id}_{\mathfrak{X}_{\Bbbk'}}$. Hence,

$$\varphi \circ \pi_1 = \pi_1 \circ \varphi_{\Bbbk'} = \pi_1.$$

Because π_1 is surjective, $\varphi = \mathrm{id}_{\mathfrak{X}}$. Thus ρ is injective. The composition $G \to \mathrm{Aut}(\mathfrak{X}) \hookrightarrow \mathrm{Aut}(\mathfrak{X}_{\Bbbk'})$ of the action on $\mathfrak{X}$ and ρ defines a group action on $\mathfrak{X}_{\Bbbk'}$. Moreover, this composition is injective if and only if the first map is injective. Thus G acts faithfully on $\mathfrak{X}$ if and only if on $\mathfrak{X}_{\Bbbk'}$. □

The following builds upon Proposition 2.12 in that it suffices to define and check certain properties of morphisms between affine spaces on their $\Bbbk$-points only.

***Proposition* 3.16.** *Let $n, m \in \mathbb{N}_0$, $A \coloneqq \Bbbk[X_1, \dots, X_n]$, $B \coloneqq \Bbbk[Y_1, \dots, Y_m]$, so that* $\operatorname{Spec} A$ *and* $\operatorname{Spec} B$ *are the n- and m-dimensional affine spaces, respectively. Suppose that $\varphi\colon \Bbbk^n \to \Bbbk^m$ is a map given by $\varphi = (\varphi_1, \dots, \varphi_m)$, where each $\varphi_j \in A$. Then φ extends to a morphism $\tilde{\varphi}\colon \mathbb{A}^n_{\Bbbk} \to \mathbb{A}^m_{\Bbbk}$ such that on the $\Bbbk$-points $\tilde{\varphi}$ is precisely φ under the identification ψ from Proposition 2.12. Moreover, every morphism $\mathbb{A}^n_{\Bbbk} \to \mathbb{A}^m_{\Bbbk}$ arises in this way. Finally, let G act on the affine spaces; if φ is G-equivariant, then so is $\tilde{\varphi}$.*

Proof. Given $\varphi\colon \Bbbk^n \to \Bbbk^m$, define $\varphi^*\colon B \to A$ by $f \mapsto f \circ \varphi$. Then φ^* is a $\Bbbk$-algebra homomorphism and therefore induces a morphism $\tilde{\varphi}\colon \mathbb{A}^n_{\Bbbk} \to \mathbb{A}^m_{\Bbbk}$. We need to show that $\psi \circ \tilde{\varphi} \circ \psi^{-1} = \varphi$. Let $\alpha \in \Bbbk^n$ and let $\psi^{-1}(\alpha) = \mathfrak{m}_\alpha \subset A$ be the corresponding maximal ideal. Then

$$\tilde{\varphi}(\mathfrak{m}_\alpha) = (\varphi^*)^{-1}(\mathfrak{m}_\alpha) = \{f \in B \mid f \circ \varphi \in \mathfrak{m}_\alpha\} = \{f \in B \mid f(\varphi(\alpha)) = 0\} = \mathfrak{m}_{\varphi(\alpha)} \subset B.$$

Note that $\psi\big(\mathfrak{m}_{\varphi(\alpha)}\big) = \varphi(\alpha)$. Thus indeed $\psi \circ \tilde{\varphi} \circ \psi^{-1}(\alpha) = \varphi(\alpha)$.
Conversely, let $\tilde{\varphi}\colon \mathbb{A}^n_{\Bbbk} \to \mathbb{A}^m_{\Bbbk}$ be a morphism. Let $\tilde{\varphi}_{\Bbbk} \coloneqq \Bbbk^n \to \Bbbk^m$ be the corresponding map on $\Bbbk$-points obtained via ψ. For each j, let $\varphi_j \coloneqq \tilde{\varphi}^\sharp_{\mathbb{A}^m_{\Bbbk}}(Y_j) \in A$, and let $\varphi \coloneqq (\varphi_1, \dots, \varphi_m)$. We need to show that $\tilde{\varphi}_{\Bbbk} = \varphi$. By construction, $\tilde{\varphi}^\sharp_{\mathbb{A}^m_{\Bbbk}}\colon f \mapsto f \circ \varphi$. Since $\tilde{\varphi} = \operatorname{Spec}(\tilde{\varphi}^\sharp_{\mathbb{A}^m_{\Bbbk}})$, we have for any $\alpha \in \Bbbk^n$

$$\mathfrak{m}_{\varphi(\alpha)} = \left(\tilde{\varphi}^\sharp_{\mathbb{A}^m_{\Bbbk}}\right)^{-1}(\mathfrak{m}_\alpha) = \tilde{\varphi}(\mathfrak{m}_\alpha) = \mathfrak{m}_{\tilde{\varphi}_{\Bbbk}(\alpha)}.$$

Whence $\varphi = \tilde{\varphi}_{\Bbbk}$. This means that $\tilde{\varphi}$ arises from its restriction to $\Bbbk$-points via the above construction.
Now suppose G acts on the affine spaces and assume that φ is G-equivariant. It suffices to show that φ^* is G-equivariant by Lemma 3.10. The action of G on $\Bbbk^n$ is induced by the one on $\mathbb{A}^n_{\Bbbk}$; that is, ${}_{\Bbbk^n}\sigma = \psi \circ {}_{\mathbb{A}^n_{\Bbbk}}\sigma \circ \psi^{-1}$. From the above argument we find that ${}_A\sigma = {}_{\Bbbk^n}\sigma^*$. Due to the assumption that $\varphi \circ {}_{\Bbbk^n}\sigma = {}_{\Bbbk^m}\sigma \circ \varphi$, we obtain

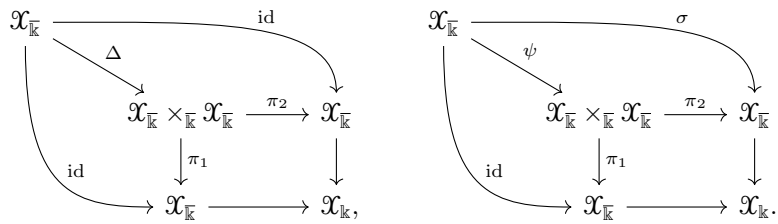
$${}_A\sigma \circ \varphi^* = {}_{\Bbbk^n}\sigma^* \circ \varphi^* = (\varphi \circ {}_{\Bbbk^n}\sigma)^* = ({}_{\Bbbk^m}\sigma \circ \varphi)^* = \varphi^* \circ {}_{\Bbbk^m}\sigma^* = \varphi^* \circ {}_B\sigma.$$

Thus φ^*, and thereby $\tilde{\varphi}$, is G-equivariant. □

For certain G-varieties its rational points can be very useful to determine whether G acts faithfully. The following assertions show this. It shall become a handy tool to assure that the varieties we consider are faithful. The following two statements constitute [3, Lemma 2.4]; the proof we give here is based on that reference.

***Proposition* 3.17.** *Let $\mathfrak{X}$ be a G-variety, and assume that $\mathfrak{X}_{\overline{\Bbbk}}(\Bbbk)$ is dense in $\mathfrak{X}_{\overline{\Bbbk}}(\overline{\Bbbk})$. Then G acts faithfully on $\mathfrak{X}$ if and only if there exists a non-empty open of $\mathfrak{X}(\Bbbk)$ on which G acts freely.*

Proof. For the converse implication, let $U \subseteq \mathfrak{X}(\Bbbk)$ be a non-empty open on which G acts freely. If $\sigma \in G$ acts trivially on $\mathfrak{X}$, then in particular for any $P \in U$, ${}_{\mathfrak{X}}\sigma(P) = P$. Then ${}_{\mathfrak{X}}\sigma|_U$ has a fixed point, wherefore $\sigma = e$ by the free action of G. Thus G acts faithfully on $\mathfrak{X}$.
We prove the direct implication in four steps. We only use the action of G on $\mathfrak{X}_{\overline{\Bbbk}}$ and shall omit the preceding subscript for the automorphisms of $\mathfrak{X}_{\overline{\Bbbk}}$ induced by elements of G.
Step 1. Fix a $\sigma \in G$. We show that the set of $\overline{\Bbbk}$-points of $\mathfrak{X}_{\overline{\Bbbk}}$ fixed by σ, denoted $\mathfrak{X}_{\overline{\Bbbk}}(\overline{\Bbbk})^\sigma$, is closed in $\mathfrak{X}_{\overline{\Bbbk}}(\overline{\Bbbk})$. Consider the following two commutative diagrams



We show that $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\sigma = \psi^{-1}(\operatorname{im}\Delta) \cap \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$. Recall that $(\mathcal{X}_{\mathbb{k}} \times_{\mathbb{k}} \mathcal{X}_{\mathbb{k}})(\overline{\mathbb{k}}) \cong \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}}) \times \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$ as sets via $P \mapsto (\pi_1(P), \pi_2(P))$.
For '$\subseteq$', pick a point $P \in \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\sigma$. As $\sigma(P) = P$, we have $\pi_i(\Delta(P)) = \pi_i(\psi(P))$ for $i = 1, 2$. Hence $\psi(P) = \Delta(P)$, and so $P \in \psi^{-1}(\operatorname{im}\Delta) \cap \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$.
Conversely, for '$\supseteq$', if $P \in \psi^{-1}(\operatorname{im}\Delta) \cap \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$, then there exists a $Q \in \mathcal{X}_{\mathbb{k}}$ such that $\psi(P) = \Delta(Q)$. Then

$$\sigma(P) = \pi_2 \circ \psi(P) = \pi_2 \circ \Delta(Q) = Q = \pi_1 \circ \Delta(Q) = \pi_1 \circ \psi(P) = P.$$

This means that $P \in \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\sigma$. So $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\sigma = \psi^{-1}(\operatorname{im}\Delta) \cap \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$. Since $\mathcal{X}$ is separated and ψ is continuous, it follows that $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\sigma$ is closed in $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$.
Step 2. Fix a $\sigma \in G$ and suppose that $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\sigma = \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$. We show that $\sigma = e$. By Lemma 3.7, there is an affine open $U \subseteq \mathcal{X}_{\overline{\mathbb{k}}}$ op which G acts. Since $\mathcal{X}_{\overline{\mathbb{k}}}$ is still separated under the base change, G acts faithfully on U. Thus we may assume that $\mathcal{X}_{\overline{\mathbb{k}}}$ is affine. Say $\mathcal{X}_{\overline{\mathbb{k}}} = \operatorname{Spec} A$, where A is a finitely generated $\overline{\mathbb{k}}$-algebra, whose nilradical is a prime ideal (because $\mathcal{X}$ is geometrically irreducible). The equality $\mathcal{X}_{\overline{\mathbb{k}}}(\overline{\mathbb{k}})^\sigma = \mathcal{X}_{\overline{\mathbb{k}}}(\overline{\mathbb{k}})$ means that σ fixes all maximal ideals of A. Let $\mathfrak{p} \subset A$ be a prime ideal. By continuity of σ^{-1}, $\sigma(\mathcal{V}(\mathfrak{p})) = \mathcal{V}(\mathfrak{a})$ for some ideal $\mathfrak{a} \subseteq A$. Trivially, $\sigma(\mathfrak{p}) \in \mathcal{V}(\mathfrak{a})$, wherefore $\mathfrak{a} \subseteq \sigma(\mathfrak{p})$. This implies that $\mathcal{V}(\sigma(\mathfrak{p})) \subseteq \sigma(\mathcal{V}(\mathfrak{p}))$. Applying this twice, we find

$$\mathcal{V}(\mathfrak{p}) = \sigma^{-1} \circ \sigma(\mathcal{V}(\mathfrak{p})) \supseteq \sigma^{-1}(\mathcal{V}(\sigma(\mathfrak{p}))) \supseteq \mathcal{V}(\sigma^{-1} \circ \sigma(\mathfrak{p})) = \mathcal{V}(\mathfrak{p}).$$

Thus all the set containments are actually equalities, from which follows that $\sigma(\mathcal{V}(\mathfrak{p})) = \mathcal{V}(\sigma(\mathfrak{p}))$. Consequently, making use of the Nullstellensatz,

$$\sigma(\mathfrak{p}) = \bigcap_{\mathfrak{m} \supseteq \sigma(\mathfrak{p})} \mathfrak{m} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \sigma(\mathfrak{m}) = \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m} = \mathfrak{p},$$

where all $\mathfrak{m}$ are maximal ideals of A. We have now found that σ is the identity on $\mathcal{X}_{\overline{\mathbb{k}}}$, wherefore $\sigma = e$ by the faithfulness of the action on $\mathcal{X}_{\overline{\mathbb{k}}}$.
Step 3. We no longer assume affineness of $\mathcal{X}_{\overline{\mathbb{k}}}$. Let

$$U \coloneqq \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}}) \setminus \left(\bigcup_{\substack{\tau \in G \\ \tau \neq e}} \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\tau \right).$$

Since each $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\tau$ is closed, and G is finite, U is open. We claim that this is a non-empty open on which G acts freely. If U were empty, then all the $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\tau$ for $\tau \neq e$ together would cover $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$. For each $\tau \neq e$, let $Z_\tau \subseteq \mathcal{X}_{\overline{\mathbb{k}}}$ be a closed subset such that $Z_\tau \cap \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}}) = \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\tau$. Then the union of these closed sets is closed and contains the dense set $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$. Hence the union of the Z_τ covers $\mathcal{X}_{\overline{\mathbb{k}}}$. By irreducibility of $\mathcal{X}_{\overline{\mathbb{k}}}$, there is a $\sigma \neq e$ such that $\mathcal{X}_{\overline{\mathbb{k}}} = Z_\sigma$. However, this implies that $\mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\sigma = \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})$, which contradicts *Step 2*. Whence U is non-empty.
To see that G acts on U and that this action is free, let $\sigma \in G$ and $P \in U$. Suppose $\sigma(P) \notin U$. Since $\sigma(P)$ is a $\overline{\mathbb{k}}$-point, there is some $\tau \neq e$ such that $\tau(\sigma(P)) = \sigma(P)$ by the definition of U. Hence P is a fixed point of $\sigma^{-1}\tau\sigma$. But $P \in U$, so $\sigma^{-1}\tau\sigma = e$. This implies that $\tau = e$, which is a contradiction. Thus $\sigma(P) \in U$. The action on U is free, because if $\sigma(P) = P$, then $P \in \mathcal{X}_{\mathbb{k}}(\overline{\mathbb{k}})^\sigma$, which implies that $\sigma = e$.
Step 4. We need to translate our $U \subseteq \mathcal{X}_{\overline{\mathbb{k}}}(\overline{\mathbb{k}})$ first to the $\mathbb{k}$-points of $\mathcal{X}_{\overline{\mathbb{k}}}$, and then to $\mathcal{X}(\mathbb{k})$. Since, by assumption, $\mathcal{X}_{\overline{\mathbb{k}}}(\mathbb{k})$ is dense in $\mathcal{X}_{\overline{\mathbb{k}}}(\overline{\mathbb{k}})$, the intersection $U \cap \mathcal{X}_{\overline{\mathbb{k}}}(\mathbb{k})$ is a non-empty, open subset of $\mathcal{X}_{\overline{\mathbb{k}}}(\mathbb{k})$. Let $\pi\colon \mathcal{X}_{\overline{\mathbb{k}}} \to \mathcal{X}$ be the projection of the base change to $\overline{\mathbb{k}}$. Proposition 2.10 implies that $V \coloneqq \pi(U \cap \mathcal{X}_{\overline{\mathbb{k}}}(\mathbb{k}))$ is a non-empty, open subset of $\mathcal{X}(\mathbb{k})$. Since π commutes with the G-action, G also acts freely on V. Thus V is the desired open. □

***Corollary* 3.18.** *Assume that $\mathbb{k}$ is infinite. Let $\mathcal{X}$ be a $\mathbb{k}$-unirational G-variety. Then G acts faithfully on $\mathcal{X}$ if and only if there exists a non-empty open of $\mathcal{X}(\mathbb{k})$ on which G acts freely.*

Proof. Since $\mathbb{k}$ is infinite, by Lemma 2.13, $\mathcal{X}_{\overline{\mathbb{k}}}(\mathbb{k})$ is dense in $\mathcal{X}_{\overline{\mathbb{k}}}(\overline{\mathbb{k}})$, and so Proposition 3.17 applies. □

3.2 Linear Varieties

Our group G can act on various varieties with different essential dimension. It turns out that the maximum essential dimension of all G-varieties is attained by so-called *linear* G-varieties. Moreover, all these linear G-varieties have the same essential dimension. This shall lead to the definition of essential dimension of a finite group.

Definition 3.19. A *linear variety* is a variety isomorphic to $\mathbb{A}^n_{\Bbbk}$ for some $n \in \mathbb{N}_0$. ☆

Remark 3.20. One can create a linear variety from a finite-dimensional vector space. For such a vector space W of dimension n let $e_1, \dots, e_n$ be a basis, and consider $A \coloneqq \Bbbk[X_1, \dots, X_n]$. Then, by Proposition 2.12, $\mathcal{W} \coloneqq \operatorname{Spec} A$ is a linear variety with $\mathcal{W}(\Bbbk) \cong W$ in such a way that a point $w_1e_1 + \cdots + w_ne_n \in W$ corresponds to the ideal $(X_1 - w_1, \dots, X_n - w_n) \in \mathcal{W}(\Bbbk)$. Choosing a basis identifies W with $\Bbbk^n$. Thus, if G acts on W, then we also get an action of G on $\mathcal{W}$, as Proposition 3.16 shows. ✧

Remark 3.21. If $\mathcal{W}$ is any linear G-variety, then its $\Bbbk$-points form a vector space $\mathcal{W}(\Bbbk)$. The action we get on $\mathcal{W}(\Bbbk)$ gives us a map $G \to \operatorname{Aut}(\mathcal{W}(\Bbbk))$. This is a representation of G. ✧

Consider the $\Bbbk$-vector space W_G freely generated over $\Bbbk$ by the elements of G. For each $\tau \in G$, we denote by e_τ the corresponding basis element of W_G. The regular representation of G is the group action of G on W_G, where σ acts on a basis element e_τ by ${}_{W_G}\sigma(e_\tau) = e_{\sigma\tau}$. We have seen that the $\Bbbk$-points of an affine space is just a $\Bbbk$-vector space by the identification of Proposition 2.12. We can therefore interpret W_G as the set of $\Bbbk$-points of some affine space $\mathbb{A}^{\#G}_{\Bbbk}$. For each $\tau \in G$, let X_τ be a variable; then consider the polynomial algebra $A_G \coloneqq \Bbbk[\{X_\tau \mid \tau \in G\}]$. Now let $\mathcal{V}_G$ be $\operatorname{Spec} A_G$. Then $\mathcal{V}_G \cong \mathbb{A}^{\#G}_{\Bbbk}$ and $\mathcal{V}_G(\Bbbk) \cong W_G$. From Proposition 3.16 we obtain that the action of W_G extends through A_G to $\mathcal{V}_G$. The extension to A_G is obtained by letting $\sigma \in G$ act on A_G by ${}_{A_G}\sigma \colon f \mapsto f \circ {}_{W_G}\sigma$. From this we see that ${}_{A_G}\sigma(X_\tau) = X_{\sigma^{-1}\tau}$. The action then extends to $\mathcal{V}_G$ as usual by Proposition 3.5. We shall generally identify $\mathcal{V}_G(\Bbbk)$ with W_G and, justified by Proposition 3.16, often just define morphisms on $\mathcal{V}_G(\Bbbk)$.
For a polynomial $p \in A_G$ we define a morphism $\alpha_p \colon \mathcal{V}_G \to \mathcal{V}_G$ as follows. On the $\Bbbk$-points we set

$$\begin{aligned} \alpha_p \colon W_G &\longrightarrow W_G \\ v &\longmapsto \sum_{\tau \in G} p\big({}_{W_G}\tau^{-1}(v)\big) e_\tau. \end{aligned}$$

Note that $p \circ {}_{W_G}\tau^{-1} = {}_{A_G}\tau^{-1}(p) \in A_G$, thus this indeed induces an endomorphism of $\mathcal{V}_G$. We henceforth only need the action on $\mathcal{V}_G(\Bbbk)$, so we omit the preceding subscript W_G to make the notation less cluttered. If $\sigma \in G$ and $v \in \mathcal{V}_G(\Bbbk)$, then

$$\alpha_p(\sigma(v)) = \sum_{\tau \in G} p\big(\tau^{-1}(\sigma(v))\big) e_\tau = \sum_{\tau \in G} p\Big(\big(\sigma^{-1}\tau\big)^{-1}(v)\Big) e_\tau.$$

Upon substituting $\gamma \coloneqq \sigma^{-1}\tau$, we obtain

$$= \sum_{\gamma \in G} p\big(\gamma^{-1}(v)\big) e_{\sigma\gamma} = \sigma\left(\sum_{\gamma \in G} p\big(\gamma^{-1}(v)\big) e_\gamma\right) = \sigma(\alpha_p(v)).$$

Therefore, α_p is G-equivariant. A good choice for the polynomial p can give us some useful endomorphism of $\mathcal{V}_G$ that we shall need later. The following lemma makes use of this. This is [3, Lemma 3.2]; the proof given below was inspired by the one given in that paper.

***Lemma* 3.22.**

(a) *Let $v, w \in \mathcal{V}_G(\Bbbk)$ and assume that v has a full G-orbit; i.e., an orbit containing $\#G$ distinct elements. Then there exists a G-endomorphism of $\mathcal{V}_G$ sending v to w.*

(b) *Now assume that $\Bbbk$ is infinite. Let $\mathfrak{X} \subseteq \mathcal{V}_G$ be a closed, faithful G-subvariety, and let $U \subseteq \mathcal{V}_G$ be a non-empty, open subset on which G acts. Then there exists a G-morphism $\beta \colon \mathcal{V}_G \to \mathcal{V}_G$ such that $\beta(\mathfrak{X}) \cap U \neq \emptyset$.*

Proof.

(a) Write $v = \sum_{\tau \in G} v_\tau e_\tau$ with $v_\tau \in \Bbbk$, and similarly for w. We concretely give a polynomial p such that α_p is the desired endomorphism. Consider the Lagrange polynomial

$$p \coloneqq \sum_{\gamma \in G} w_\gamma \prod_{\varsigma \in G} \prod_{\substack{\sigma \in G \\ v_\sigma \neq v_\varsigma}} \frac{X_{\gamma^{-1}\varsigma} - v_\sigma}{v_\varsigma - v_\sigma}; \qquad p \circ \tau^{-1} = \sum_{\gamma \in G} w_\gamma \prod_{\varsigma \in G} \prod_{\substack{\sigma \in G \\ v_\sigma \neq v_\varsigma}} \frac{X_{\tau\gamma^{-1}\varsigma} - v_\sigma}{v_\varsigma - v_\sigma}.$$

We need to show that for every $\tau \in G$ we have $p\big(\tau^{-1}(v)\big) = w_\tau$. In $p\big(\tau^{-1}(v)\big)$ the term $\gamma = \tau$ becomes

$$w_\tau \prod_{\varsigma \in G} \prod_{\substack{\sigma \in G \\ v_\sigma \neq v_\varsigma}} \frac{v_{\tau\tau^{-1}\varsigma} - v_\sigma}{v_\varsigma - v_\sigma} = w_\tau \cdot 1 = w_\tau.$$

When $\gamma \neq \tau$, we show that there is a factor $\frac{v_{\tau\gamma^{-1}\varsigma} - v_\sigma}{v_\varsigma - v_\sigma}$ that vanishes, so that all terms $\gamma \neq \tau$ be zero. For some $\varsigma \in G$ we want that the second product contain the factor corresponding to $\sigma = \tau\gamma^{-1}\varsigma$; then trivially $v_{\tau\gamma^{-1}\varsigma} - v_\sigma = 0$. The problem is that v_σ might equal v_ς, wherefore this factor would not appear. We argue by contradiction. Suppose that for every $\varsigma \in G$ we have $v_\varsigma = v_{\tau\gamma^{-1}\varsigma}$. Then $v = \big(\tau\gamma^{-1}\big)^{-1}(v)$. Since v has a full G-orbit, this means that $\big(\tau\gamma^{-1}\big)^{-1} = e$. Hence $\gamma = \tau$, which is a contradiction. Thus every term $\gamma \neq \tau$ of $p\big(\tau^{-1}(v)\big)$ vanishes.
We now see that $p\big(\tau^{-1}(v)\big) = w_\tau$ for every $\tau \in G$. Consequently, $\alpha_p(v) = w$.

(b) Let $d \in \mathbb{N}_0$. For every monomial $\prod_{\tau\in G} X_\tau^{c_\tau}$ with each $c_\tau \in \mathbb{N}_0$ we let X_{c_G} be a new variable, where c_G is the tuple $(c_\tau)_{\tau\in G}$. Then define

$$B_d \coloneqq \Bbbk\left[\left\{ X_{c_G} \;\middle|\; c_G = (c_\tau)_{\tau\in G} \in \mathbb{N}_0^{\#G}, \sum_{\tau\in G} c_\tau \leq d \right\}\right] \text{ and } \mathscr{W}_d \coloneqq \operatorname{Spec} B_d.$$

A point $p \in \mathscr{W}_d(\Bbbk)$ corresponds to a tuple of elements of $\Bbbk$ indexed by the c_G. If we interpret every component of p as the coefficient of the corresponding monomial $\prod_{\tau\in G} X_\tau^{c_\tau}$, then p corresponds to a polynomial of A_G of total degree at most d. We therefore may view $\mathscr{W}_d(\Bbbk) \subseteq A_G$.
Let us denote by a bar the base change to the algebraic closure $\overline{\Bbbk}$; e.g. $\overline{\mathscr{V}}_G \coloneqq \mathscr{V}_G \times_\Bbbk \overline{\Bbbk}$. For the $\Bbbk$-algebras we mean the tensor product with $\overline{\Bbbk}$: $\overline{A}_G \coloneqq A_G \otimes_\Bbbk \overline{\Bbbk}$.
Note that the inclusions of $\mathfrak{X}$ and U into $\mathscr{V}_G$ are immersions by assumption, which are stable under base change. Let $P_{d,\overline{\Bbbk}}$ be the subset of $\overline{\mathscr{W}}_d(\overline{\Bbbk})$ corresponding to those polynomials $p \in \overline{A}_G$ for which the induced map $\overline{\alpha}_p \colon \overline{\mathscr{V}}_G \to \overline{\mathscr{V}}_G$ satisfies

$$\overline{\alpha}_p\big(\overline{\mathfrak{X}}(\overline{\Bbbk})\big) \cap \overline{U}(\overline{\Bbbk}) = \emptyset. \tag{3.4}$$

Note: $P_{d,\overline{\Bbbk}}$ is a mere subset of the $\overline{\Bbbk}$-points of $\overline{\mathscr{V}}_G$; it is in no way a subvariety.
Let $P_{d,\Bbbk} \coloneqq P_{d,\overline{\Bbbk}} \cap \overline{\mathscr{W}}_d(\Bbbk)$. To prove the statement, we first show that $P_{d,\Bbbk} \neq \overline{\mathscr{W}}_d(\Bbbk)$; that is, we show the existence of a polynomial in $\overline{\mathscr{W}}_d(\Bbbk)$ not satisfying (3.4). To do this, we first prove that $P_{d,\overline{\Bbbk}}$ is closed in $\overline{\mathscr{W}}_d(\overline{\Bbbk})$. The condition (3.4) is equivalent to $\overline{\alpha}_p\big(\overline{\mathfrak{X}}(\overline{\Bbbk})\big) \subseteq \overline{\mathscr{V}}_G(\overline{\Bbbk}) \setminus \overline{U}(\overline{\Bbbk})$. The latter set is closed, hence is the zero set $\mathcal{Z}(\mathfrak{a}) \subseteq \overline{\Bbbk}^{\#G}$ of some ideal $\mathfrak{a} \subseteq \overline{A}_G$.
Now consider the following polynomial

$$P \coloneqq \sum_{\substack{c_G \in \mathbb{N}_0^{\#G} \\ \sum_{\tau\in G} c_\tau \leq d}} X_{c_G} \prod_{\tau\in G} X_\tau^{c_\tau}. \tag{3.5}$$

If we substitute a point $v \in \overline{\mathscr{V}}_G(\overline{\Bbbk})$ for the variables X_τ, $\tau \in G$, then we get a polynomial $P_v \in \overline{B}_d$. Let $f \in \overline{A}_G$. Consider the polynomial

$$f_v \coloneqq f\left(\sum_{\tau\in G} P_{\tau^{-1}(v)} e_\tau\right);$$

here we mean that $P_{\tau^{-1}(v)}$ is substituted for variable X_τ of $f = f\big(\sum_{\tau\in G} X_\tau e_\tau\big)$. The resulting polynomial f_v belongs to $\overline{B}_d$. For any $p \in \overline{\mathscr{W}}_d(\overline{\Bbbk}) \subseteq \overline{A}_G$ we have the equality

$$f_v(p) = f\left(\sum_{\tau\in G} P_{\tau^{-1}(v)}(p) e_\tau\right) = f\left(\sum_{\tau\in G} P\big(p; \tau^{-1}(v)\big) e_\tau\right) = f\left(\sum_{\tau\in G} p\big(\tau^{-1}(v)\big) e_\tau\right) = f(\overline{\alpha}_p(v)).$$

In the penultimate expression p represents the polynomial in $\overline{A}_G$ corresponding to the point $p \in \overline{\mathscr{W}}_d(\overline{\Bbbk})$; this is obtained by substituting the components of the point p for the variables X_{c_G} of P, as described above.
Now let $\mathfrak{b} \subseteq \overline{B}_d$ be the ideal generated by the f_v for $f \in \mathfrak{a}$ and $v \in \mathcal{Z}(\mathfrak{a})$. Then

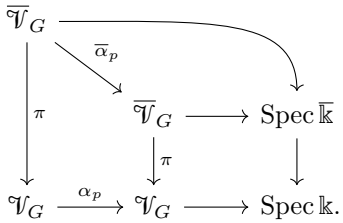
$$\begin{aligned}
p \in P_{d,\overline{\Bbbk}} &\iff \forall v \in \overline{\mathfrak{X}}(\overline{\Bbbk}) \colon \overline{\alpha}_p(v) \in \mathcal{Z}(\mathfrak{a}) \\
&\iff \forall v \in \overline{\mathfrak{X}}(\overline{\Bbbk}), \forall f \in \mathfrak{a} \colon f(\overline{\alpha}_p(v)) = 0 \\
&\iff \forall v \in \overline{\mathfrak{X}}(\overline{\Bbbk}), \forall f \in \mathfrak{a} \colon f_v(p) = 0 \\
&\iff \forall g \in \mathfrak{b} \colon g(p) = 0
\end{aligned}$$

$$\iff p \in \mathcal{Z}(\mathfrak{b}),$$

where $\mathcal{Z}(\mathfrak{b}) \subseteq \overline{\mathcal{W}}_d(\overline{\Bbbk})$. Thus we see that $P_{d,\overline{\Bbbk}} = \mathcal{Z}(\mathfrak{b})$, wherefore it is closed in $\overline{\mathcal{W}}_d(\overline{\Bbbk})$.
The next step is to show that in fact $P_{d,\Bbbk} \neq \overline{\mathcal{W}}_d(\Bbbk)$ for some d, because we need a map on $\Bbbk$-points, not $\overline{\Bbbk}$-points. Suppose instead that $P_{d,\Bbbk} = \overline{\mathcal{W}}_d(\Bbbk)$ for every $d \in \mathbb{N}_0$. Then

$$\overline{\mathcal{W}}_d(\overline{\Bbbk}) \supseteq P_{d,\overline{\Bbbk}} \supseteq P_{d,\Bbbk} = \overline{\mathcal{W}}_d(\Bbbk)$$

Since $\Bbbk$ is infinite, $\overline{\mathcal{W}}_d(\Bbbk)$ lies dense in $\overline{\mathcal{W}}_d(\overline{\Bbbk})$ by Lemma 2.13. Now $P_{d,\overline{\Bbbk}}$ is closed and contains a dense set, which means that $P_{d,\overline{\Bbbk}} = \overline{\mathcal{W}}_d(\overline{\Bbbk})$. However, by Proposition 3.17, there exists a non-empty, open subset of $\overline{\mathfrak{X}}(\overline{\Bbbk})$ on which G acts freely. In particular this means that there is some $v \in \overline{\mathfrak{X}}(\overline{\Bbbk})$ with a full G-orbit. Since $\overline{\mathcal{V}}_G(\overline{\Bbbk})$ lies dense in $\overline{\mathcal{V}}_G$, there is a $\overline{\Bbbk}$-point $w \in \overline{U}$. Then, by (a), there is some polynomial p such that $\bar{\alpha}_p(v) = w$; that is, $\bar{\alpha}_p\big(\overline{\mathfrak{X}}(\overline{\Bbbk})\big) \cap \overline{U}(\overline{\Bbbk}) \neq \emptyset$. Whence $p \in \overline{\mathcal{W}}_d(\overline{\Bbbk}) \setminus P_{d,\overline{\Bbbk}}$ for $d \geq \deg p$. We have thus reached a contradiction with the first part of this proof. This implies that there is a $d \geq 0$ such that $P_{d,\Bbbk} \neq \overline{\mathcal{W}}_d(\Bbbk)$.
For a suitable d we can now pick a $p \in \overline{\mathcal{W}}_d(\Bbbk) \setminus P_{d,\Bbbk}$. Then p has coefficients in $\Bbbk$ and so induces the morphism $\alpha_p \colon \mathcal{V}_G \to \mathcal{V}_G$. Looking at the construction of α_p above and the same construction of $\bar{\alpha}_p \colon \overline{\mathcal{V}}_G \to \overline{\mathcal{V}}_G$ shows that they fit the commutative diagram



Let $\overline{Q} \in \overline{\mathfrak{X}}(\overline{\Bbbk})$ be such that $\bar{\alpha}_p(\overline{Q}) \in \overline{U}(\overline{\Bbbk})$, and $Q \coloneqq \pi(\overline{Q}) \in \mathfrak{X}$. Then

$$\alpha_p(Q) = \alpha_p\big(\pi(\overline{Q})\big) = \pi\big(\bar{\alpha}_p(\overline{Q})\big) \in U,$$

as $\bar{\alpha}_p(\overline{Q}) \in \overline{U}(\overline{\Bbbk})$. Hence $\alpha_p(\mathfrak{X}) \cap U \neq \emptyset$. Thus we take $\beta \coloneqq \alpha_p$ to get the desired morphism. □

The next lemma allows us to utilize $\mathcal{V}_G$. For any faithful G-variety we can find a subvariety of $\mathcal{V}_G$ over which it is defined. The statement comes from [3, Lemma 3.4]. We give a proof that is different from, but inspired by, the one given in [3].

***Lemma* 3.23.** *Let $\mathcal{X}$ be a faithful G-variety. Then there exists a closed, affine G-subvariety $\mathfrak{X} \subseteq \mathcal{V}_G$ over which $\mathcal{X}$ is defined such that* $\operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) = \dim(\mathfrak{X})$.

Proof. By Corollary 3.14, there exists an affine variety $\mathcal{Y} = \operatorname{Spec} B$ over which $\mathcal{X}$ is defined such that $\operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) = \dim(\mathcal{Y})$. Let $\psi \colon \mathcal{X} \dashrightarrow \mathcal{Y}$ be a dominant, rational G-map. Let $E \coloneqq \Bbbk(\mathcal{Y}) = \operatorname{Frac}(B)$. Since E is separable over E^G, there is a primitive element $\alpha \in E$ for the extension E/E^G. As G acts faithfully on E, all ${}_E\tau(\alpha)$ are distinct for different $\tau \in G$.
Let $U \subseteq \mathcal{Y}$ be an affine, open subset, on which G acts, such that ${}_E\tau(\alpha) \in \mathcal{O}_{\mathcal{Y}}(U)$ for every $\tau \in G$. Let $C \coloneqq \mathcal{O}_{\mathcal{Y}}(U)$ so that $U = \operatorname{Spec} C$. Define a $\Bbbk$-algebra homomorphism

$$\begin{aligned} f \colon A_G &\longrightarrow C \\ X_\tau &\longmapsto {}_C\tau^{-1}(\alpha) = {}_E\tau^{-1}(\alpha). \end{aligned}$$

Then for any $\sigma, \tau \in G$:

$$f\big({}_{A_G}\sigma(X_\tau)\big) = f(X_{\sigma^{-1}\tau}) = {}_C\big(\sigma^{-1}\tau\big)^{-1}(\alpha) = {}_C\big(\tau^{-1}\sigma\big)(\alpha) = {}_C\sigma\big({}_C\tau^{-1}(\alpha)\big) = {}_C\sigma(f(X_\tau)).$$

Thus f is G-equivariant. Let $A \coloneqq A_G/\ker f$. We then get the following commutative diagram

$$\begin{array}{ccc} A_G & \xrightarrow{\ f\ } & C \\ {\scriptstyle q}\big\downarrow & \nearrow_{\bar{f}} & \\ A & & \end{array} \tag{3.6}$$

with q the quotient map and $\overline{f}$ the induced map. The group action of G extends to A through q: for $\overline{a} \in A$, the residue class of $a \in A_G$, we set

$$ {}_A\sigma(\overline{a}) \coloneqq \overline{{}_{A_G}\sigma(a)} $$

for every $\sigma \in G$. This action is still faithful, because $\overline{f}$ sends the residue class $\overline{X}_\tau$ of $X_\tau \in A_G$ to ${}_C\tau^{-1}(\alpha)$, which are all different for different τ; each $\overline{X}_\tau$ is therefore different, thus in particular each ${}_A\tau$ acts differently on $\overline{X}_e$.
Let $\mathfrak{X} \coloneqq \operatorname{Spec} A$. The diagram (3.6) induces

$$\begin{array}{ccc} \mathcal{V}_G & \xleftarrow{\varphi} & U \\ {\scriptstyle \operatorname{Spec} q}\uparrow & \swarrow_{\overline{\varphi}} & \\ \mathfrak{X}, & & \end{array}$$

where φ and $\overline{\varphi}$ are the morphisms induced by f and $\overline{f}$, respectively. Since $\overline{f}$ is injective, $\overline{\varphi}$ is dominant, and $\mathfrak{X}$ is geometrically irreducible, because U is too. As q is surjective, $\operatorname{Spec} q$ is a closed immersion, and so we may view $\mathfrak{X}$ as a closed G-subvariety of $\mathcal{V}_G$.
The composition $\overline{\varphi} \circ \psi$ defines a dominant, rational G-map $\mathcal{X} \dashrightarrow \mathfrak{X}$. Since $\mathfrak{X}$ is faithful, this means that $\mathcal{X}$ is defined over $\mathfrak{X}$. Consequently,

$$ \dim(\mathcal{Y}) = \operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) \leq \dim(\mathfrak{X}) \leq \dim(\mathcal{Y}). $$

Thus $\operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) = \dim(\mathfrak{X})$, as desired. □

The following two assertions provide us with a useful trick to turn a rational map to an affine variety into a dominant one to some closed subvariety. The compatibility with a possible G-action is also conveniently preserved.

***Lemma* 3.24.** *Let $\varphi\colon \mathcal{X} \to \mathcal{Y}$ be a morphism of varieties, and assume that $\mathcal{Y}$ is affine. Then the closure $\mathfrak{X}$ of its image in $\mathcal{Y}$ is a variety.*

Proof. By [9, Remark 10.32], $\mathfrak{X}$ can naturally be endowed with the structure of a reduced $\Bbbk$-subscheme of $\mathcal{Y}$. Let $\Bbbk'/\Bbbk$ be an algebraic extension. Let $\varphi'\colon \mathcal{X}_{\Bbbk'} \to \mathcal{Y}_{\Bbbk'}$ be the base change of φ to $\Bbbk'$. The base change morphism $\operatorname{Spec} \Bbbk' \to \operatorname{Spec} \Bbbk$ is flat and, since $\mathcal{Y}$ is affine, φ is quasi-compact. Therefore, [9, Lemma 14.6] asserts that the closure of the image of φ' is precisely $\mathfrak{X}_{\Bbbk'}$. Since $\mathcal{X}_{\Bbbk'}$ is irreducible, the continuous image of an irreducible space is irreducible, and the closure of an irreducible subspace is again irreducible, it follows that $\mathfrak{X}_{\Bbbk'}$ is irreducible as well. Therefore, $\mathfrak{X}$ is geometrically irreducible. We conclude that $\mathfrak{X}$ is a variety. □

***Proposition* 3.25.** *Let $\varphi\colon \mathcal{X} \dashrightarrow \mathcal{Y}$ be a rational map between varieties, and assume that $\mathcal{Y}$ is affine. Then the closure $\mathfrak{X}$ of its image is a well-defined variety, and $\varphi\colon \mathcal{X} \dashrightarrow \mathfrak{X}$ is dominant. Moreover, if $\mathcal{X}$ and $\mathcal{Y}$ are G-varieties, and φ is G-equivariant, then $\mathfrak{X}$ is a G-variety.*

Proof. Let $(U, {}_U\varphi)$ and $(V, {}_V\varphi)$ be representatives of φ. Let $W \subseteq U \cap V$ be a non-empty open such that ${}_U\varphi|_W = {}_V\varphi|_W$. Since W is dense in both U and V, we have in $\mathcal{Y}$

$$ \overline{{}_U\varphi(U)} = \overline{{}_U\varphi(W)} = \overline{{}_V\varphi(W)} = \overline{{}_V\varphi(V)}. $$

Thus the closure of the image of φ can be chosen to be the closure of the image of any of its representatives. Then, by Lemma 3.24, $\mathfrak{X}$ is a variety. Since, by construction, $\mathfrak{X}$ is the closure of the image of any representative, $\varphi\colon \mathcal{X} \dashrightarrow \mathfrak{X}$ is dominant.
Next assume that G acts on $\mathcal{X}$ and $\mathcal{Y}$. Choose a representative $(U, {}_U\varphi)$ of φ such that U is G-invariant. Then for any $\sigma \in G$ and ${}_U\varphi(P) \in \operatorname{im} {}_U\varphi$, we have ${}_{\mathcal{Y}}\sigma({}_U\varphi(P)) = {}_U\varphi({}_{\mathcal{X}}\sigma(P)) \in {}_U\varphi(U)$. Thus ${}_U\varphi(U)$ is G-invariant. Since ${}_{\mathcal{Y}}\sigma^{-1}(\mathfrak{X})$ is closed and contains ${}_U\varphi(U)$, it follows that $\mathfrak{X} \subseteq {}_{\mathcal{Y}}\sigma^{-1}(\mathfrak{X})$, because $\mathfrak{X}$ is the closure of ${}_U\varphi(U)$. Whence ${}_{\mathcal{Y}}\sigma(\mathfrak{X}) \subseteq \mathfrak{X}$. This means that the action of G on $\mathcal{Y}$ restricts to $\mathfrak{X}$. □

Lastly, we prove that the essential dimension of any faithful, linear G-variety is the same and that this forms an upper bound for the essential dimension of all faithful G-varieties.

***Lemma* 3.26.** *Assume that $\Bbbk$ is infinite. Let $\mathcal{W}$ be a faithful, linear G-variety. Then* $\operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{W}) \geq \operatorname{ed}_{\Bbbk}(G \curvearrowright \mathcal{V}_G)$.

Proof. Let $\mathcal{Y}$ be an affine G-variety over which $\mathcal{W}$ is defined such that $\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{W}) = \dim(\mathcal{Y})$. Let $\varphi\colon \mathcal{W} \dashrightarrow \mathcal{Y}$ be a dominant, rational G-map. Let $(U, {}_U\varphi)$ be a representative for φ, with $U \subseteq \mathcal{W}$ a non-empty open on which G acts. Since $\Bbbk$ is infinite, Lemma 2.13 implies that $U(\Bbbk)$ is dense in U. Consequently, ${}_U\varphi(U(\Bbbk))$ is dense in $\operatorname{im} {}_U\varphi$, which in turn is dense in $\mathcal{Y}$. Note that ${}_U\varphi(U(\Bbbk)) \subseteq \mathcal{Y}(\Bbbk)$. Since $\mathcal{Y}$ is faithful and $\Bbbk$-unirational by assumption, Corollary 3.18 asserts that there is a non-empty, open subset $V \subseteq \mathcal{Y}(\Bbbk)$ on which G acts freely. It now follows that ${}_U\varphi(U(\Bbbk)) \cap V \neq \emptyset$, wherefore there exists a $w \in U(\Bbbk)$ such that ${}_U\varphi(w) \in V$. Define a morphism $\psi\colon \mathcal{V}_G \to \mathcal{W}$ by defining on the $\Bbbk$-points

$$\begin{aligned} \mathcal{V}_G(\Bbbk) &\longrightarrow \mathcal{W}(\Bbbk) \\ v &\longmapsto \sum_{\tau \in G} v_\tau \cdot_{\mathcal{W}} \tau(w) \end{aligned}$$

where $v_\tau \in \Bbbk$ is the τ-th component of $v = \sum_{\tau \in G} v_\tau e_\tau$. Then for any $v \in \mathcal{V}_G(\Bbbk)$ and $\sigma \in G$

$$\psi\big({}_{\mathcal{V}_G}\sigma(v)\big) = \sum_{\tau \in G} v_{\sigma^{-1}\tau} \cdot_{\mathcal{W}} \tau(w) = \sum_{\gamma \in G} v_\gamma \cdot_{\mathcal{W}} (\sigma\gamma)(w) = {}_{\mathcal{W}}\sigma\left(\sum_{\gamma \in G} v_\gamma \cdot_{\mathcal{W}} \gamma(w)\right) = {}_{\mathcal{W}}\sigma(\psi(v)).$$

For the second equality we made the substitution $\gamma := \sigma^{-1}\tau$. We now see that ψ is G-equivariant. Moreover, $\psi(e_e) = 1 \cdot_{\mathcal{W}} e(w) = w$. This implies that $\psi^{-1}(U)$ is a non-empty open of $\mathcal{V}_G$. Hence the composition $\varphi \circ \psi\colon \mathcal{V}_G \dashrightarrow \mathcal{Y}$ is a rational G-map.
Now let $\mathfrak{X} \subseteq \mathcal{Y}$ be the closure of the image of this composition. By Proposition 3.25, $\mathfrak{X}$ is a G-variety and $\varphi \circ \psi$ defines a dominant, rational map $\mathcal{V}_G \dashrightarrow \mathfrak{X}$. Now ${}_U\varphi \circ \psi(e_e) = {}_U\varphi(w) \in \mathfrak{X}$. Recall that ${}_U\varphi(w) \in V$ and so ${}_U\varphi(w)$ has a full G-orbit, because G acts freely on V. This means that G acts faithfully on $\mathfrak{X}$, because each $\sigma \in G$ acts differently on ${}_U\varphi(w)$.
We have now found that $\mathfrak{X}$ is a faithful G-variety over which $\mathcal{V}_G$ is defined. Therefore,

$$\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{V}_G) \leq \dim(\mathfrak{X}) \leq \dim(\mathcal{Y}) = \mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{W}). \qquad \square$$

***Proposition* 3.27.** *Assume that $\Bbbk$ is infinite. Let $\mathcal{X}$ be a faithful G-variety. Then we have the inequality* $\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) \leq \mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{V}_G)$.

Proof. Let $\mathcal{Y}$ be an affine variety over which $\mathcal{V}_G$ is defined such that $\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{V}_G) = \dim(\mathcal{Y})$. Let $\varphi\colon \mathcal{V}_G \dashrightarrow \mathcal{Y}$ be a dominant, rational G-map. There exists a non-empty, G-invariant open $V \subseteq \mathcal{Y}$ such that G acts freely on $V(\Bbbk)$, which asserts Proposition 3.17. Let $U \subseteq \mathcal{V}_G$ be an open subset such that there is a representative of φ, whose image lies in V. This exists, because φ is dominant.
Let $\mathfrak{X} \subseteq \mathcal{V}_G$ be an affine, closed subvariety over which $\mathcal{X}$ is defined, satisfying $\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) = \dim(\mathfrak{X})$. This is possible due to Lemma 3.23. Let $\psi\colon \mathcal{X} \dashrightarrow \mathfrak{X}$ be a dominant, rational G-map. Lemma 3.22 provides us with a G-morphism $\beta\colon \mathcal{V}_G \to \mathcal{V}_G$ such that $\beta(\mathfrak{X}) \cap U \neq \emptyset$. Then the composition

$$\varphi \circ \beta \circ \psi\colon \mathcal{X} \dashrightarrow \mathcal{Y}$$

is a rational G-map. Let $\mathcal{Q}$ be the closure of its image in $\mathcal{Y}$. By construction, $\mathcal{Q} \cap V$ is non-empty. Moreover, $\mathcal{Q}$ is $\Bbbk$-unirational, which means that $\mathcal{Q}(\Bbbk)$ is dense in $\mathcal{Q}$. Therefore, $\mathcal{Q} \cap V$ contains a $\Bbbk$-rational point. From the fact that G acts freely on $V(\Bbbk)$ follows that $\mathcal{Q}$ is faithful. Since $\varphi \circ \beta \circ \psi\colon \mathcal{X} \dashrightarrow \mathcal{Q}$ defines a dominant, rational G-map, it follows that $\mathcal{X}$ is defined over $\mathcal{Q}$. Therefore,

$$\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{X}) \leq \dim(\mathcal{Q}) \leq \dim(\mathcal{Y}) = \mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{V}_G). \qquad \square$$

***Theorem* 3.28.** *Assume that $\Bbbk$ is infinite. Let $\mathcal{W}$ be a faithful, linear G-variety. Then* $\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{W}) = \mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{V}_G)$.

Proof. From Proposition 3.27 we obtain that $\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{W}) \leq \mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{V}_G)$, while Lemma 3.26 assures us that $\mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{W}) \geq \mathrm{ed}_{\Bbbk}(G \curvearrowright \mathcal{V}_G)$, as desired. $\square$

Chapter 4

Essential Dimension of a Finite Group

We now fix an infinite field $\Bbbk$. All fields that we will consider are assumed to contain $\Bbbk$, homomorphisms of these fields are $\Bbbk$-linear, and all algebraic varieties are defined over $\Bbbk$, unless stated otherwise. An algebraic closure of $\Bbbk$ will be denoted by $\overline{\Bbbk}$. We also fix a finite group G with neutral element ϵ.

We shall first define the essential dimension of a finite group, and subsequently discover some basic properties of it. We then move on to the relation to Chapter 1, and improve results from that chapter (bar the cases where $\Bbbk$ is finite).

Thanks to Theorem 3.28, the following concept is well-defined.

Definition 4.1 (Essential dimension of a finite group)**.** Let $\mathscr{W}$ be a faithful, linear G-variety. We define the *essential dimension of the finite group G over $\Bbbk$*, denoted by $\operatorname{ed}_\Bbbk(G)$, to be $\operatorname{ed}_\Bbbk(G \circlearrowright \mathscr{W})$. ☆

We start with some basic, but very useful, properties.

***Lemma* 4.2.** *Let H be a subgroup of G. Then* $\operatorname{ed}_\Bbbk(H) \leq \operatorname{ed}_\Bbbk(G)$.

Proof. Let $\mathscr{Y}$ be a G-variety over which $\mathscr{V}_G$ is defined such that $\dim(\mathscr{Y}) = \operatorname{ed}_\Bbbk(G)$. Because of the inclusion $H \hookrightarrow G$, $\mathscr{V}_G$ and $\mathscr{Y}$ are faithful H-varieties, and a dominant, rational G-map $\mathscr{V}_G \dashrightarrow \mathscr{Y}$ is H-equivariant. Thus

$$\operatorname{ed}_\Bbbk(H) = \operatorname{ed}_\Bbbk(H \circlearrowright \mathscr{V}_G) \leq \dim(\mathscr{Y}) = \operatorname{ed}_\Bbbk(G). \qquad \square$$

***Proposition* 4.3.** *If $G = G_1 \times G_2$ for two groups G_1 and G_2, then* $\operatorname{ed}_\Bbbk(G) \leq \operatorname{ed}_\Bbbk(G_1) + \operatorname{ed}_\Bbbk(G_2)$.

Proof. We shall translate the statement to one in the theory of fields. For $i = 1, 2$ consider the purely transcendental extensions $L_i := \Bbbk(\{X_\sigma \mid \sigma \in G_i\})$; note that $L_i = \Bbbk(\mathscr{V}_{G_i}) = \operatorname{Frac}(A_{G_i})$ (recall the construction below Definition 3.19). Let $A := A_{G_1} \otimes_\Bbbk A_{G_2}$. Note that A is just a polynomial ring and that $\operatorname{Spec} A = \mathscr{V}_{G_1} \times_\Bbbk \mathscr{V}_{G_2}$ is a linear variety. We may let G act on A via $(\sigma, \tau) \mapsto {}_{A_{G_1}}\sigma \otimes {}_{A_{G_2}}\tau$. This action is faithful, because the actions of the G_i on A_{G_i} are faithful. Thusly, $\operatorname{Spec} A$ becomes a faithful, linear G-variety. The induced action of G on $L := \Bbbk(\operatorname{Spec} A)$ is also faithful. Now, by definition and Theorem 3.13, $\operatorname{ed}_\Bbbk(G) = \operatorname{ed}_\Bbbk(G \circlearrowright \operatorname{Spec} A) = \operatorname{ed}_\Bbbk(L/L^G)$ and $\operatorname{ed}_\Bbbk(G_i) = \operatorname{ed}_\Bbbk(L_i/L_i^{G_i})$.
For $i = 1, 2$ let E_i be a subfield of L_i on which G_i acts faithfully such that $L_i/L_i^{G_i}$ is defined over $E_i/E_i^{G_i}$ and $\operatorname{ed}_\Bbbk(L_i/L_i^{G_i}) = \operatorname{trdeg}_\Bbbk(E_i)$. This is possible due to Lemma 1.4. Consider the compositum $E_1E_2 \subseteq L$ and observe that G acts faithfully on E_1E_2. Then, upon applying Lemma 1.3, we obtain the desired result:

$$\begin{aligned}\operatorname{ed}_\Bbbk(G) = \operatorname{ed}_\Bbbk(L/L^G) &\leq \operatorname{trdeg}_\Bbbk(E_1E_2) \leq \operatorname{trdeg}_\Bbbk(E_1) + \operatorname{trdeg}_\Bbbk(E_2) \\ &= \operatorname{ed}_\Bbbk(L_1/L_1^{G_1}) + \operatorname{ed}_\Bbbk(L_2/L_2^{G_2}) = \operatorname{ed}_\Bbbk(G_1) + \operatorname{ed}_\Bbbk(G_2). \qquad \square\end{aligned}$$

The following gives a simple lower bound for non-trivial groups (cf. Proposition 1.18). It is [3, Lemma 4.4].

***Proposition* 4.4.** *We have* $\operatorname{ed}_\Bbbk(G) = 0$ *if and only if* $G = \{e\}$.

Proof. Consider $L := \operatorname{Frac}(A_G)$. By Theorem 3.13 and Lemma 1.4, there is a subfield $E \subseteq L$, on which G acts faithfully, such that $\operatorname{ed}_\Bbbk(G) = \operatorname{trdeg}_\Bbbk(E)$. Now $\operatorname{ed}_\Bbbk(G) = 0$ if and only if $E/\Bbbk$ is algebraic. Since L is a purely transcendental extension of $\Bbbk$, it follows that $\Bbbk$ is algebraically closed in L. Thus that $E/\Bbbk$ is algebraic is equivalent to $E = \Bbbk$. Finally, G acts faithfully on $\Bbbk$ if and only if $G = \{e\}$. $\square$

4.1 A Connection to Polynomials

We have finally reached the connection to the essential dimension of a general polynomial that we hinted at in Chapter 1. The following statement makes this concrete.

***Proposition* 4.5.** *Let $n \in \mathbb{N}$ and consider the symmetric group S_n. We have $\mathrm{ed}_{\Bbbk}(\mathrm{S}_n) = \mathrm{d}_{\Bbbk}(n)$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be algebraically independent variables over $\Bbbk$. Consider the monic polynomial

$$p(X) \coloneqq \prod_{i=1}^{n} (X - \alpha_i).$$

Let $a_1, \dots, a_n$ be the elementary symmetric polynomials in the α_i with $\deg a_i = i$. Set $K \coloneqq \Bbbk(a_1, \dots, a_n)$. Then $p \in K[X]$, as its non-leading coefficients are, up to sign, the a_i. Let $A \coloneqq \Bbbk[\alpha_1, \dots, \alpha_n]$ and $L \coloneqq \mathrm{Frac}(A)$. Let S_n act on A as usual: For $\sigma \in \mathrm{S}_n$ set ${}_A\sigma(\alpha_i) \coloneqq \alpha_{\sigma(i)}$. From the theory of symmetric polynomials we know that $L^{\mathrm{S}_n} = K$. Thus $\operatorname{Spec} A$ is a faithful, linear S_n-variety. Hence $\mathrm{ed}_{\Bbbk}(\mathrm{S}_n) = \mathrm{ed}_{\Bbbk}(\mathrm{S}_n \curvearrowright \operatorname{Spec} A) = \mathrm{ed}_{\Bbbk}(L/K)$, where the last equality follows from Theorem 3.13.
Now consider $L' \coloneqq K[X]/(p)$. As defined in Chapter 1, $\mathrm{d}_{\Bbbk}(n) = \mathrm{ed}_{\Bbbk}(L'/K)$. Since the normal closure of L' is L, Lemma 1.5 asserts that $\mathrm{ed}_{\Bbbk}(L/K) = \mathrm{ed}_{\Bbbk}(L'/K)$. Consequently, $\mathrm{ed}_{\Bbbk}(\mathrm{S}_n) = \mathrm{d}_{\Bbbk}(n)$. □

Observe that Proposition 4.5 makes Proposition 4.4 a generalization of Proposition 1.18.

***Corollary* 4.6.** *The sequence $\mathrm{d}_{\Bbbk}(n)$ for $n \in \mathbb{N}$ is non-decreasing.*

Proof. Since S_{n+1} contains S_n as a subgroup, we get $\mathrm{d}_{\Bbbk}(n+1) = \mathrm{ed}_{\Bbbk}(\mathrm{S}_{n+1}) \geq \mathrm{ed}_{\Bbbk}(\mathrm{S}_n) = \mathrm{d}_{\Bbbk}(n)$ by Lemma 4.2 and Proposition 4.5. □

In Chapter 1 we already found some upper bounds for $\mathrm{d}_{\Bbbk}(n)$ with $n \leq 4$, but it turned out be to rather complicated for larger values of n. The following gives an upper bound for all $n \geq 5$. We mostly follow the approach of [17, §3].

***Proposition* 4.7.** *For $n \in \mathbb{N}$ with $n \geq 5$ we have $\mathrm{d}_{\Bbbk}(n) = \mathrm{ed}_{\Bbbk}(\mathrm{S}_n) \leq n - 3$.*

Proof. Consider $L \coloneqq \Bbbk(X_1, \dots, X_n)$ with the usual S_n action. We have seen that $\mathrm{ed}_{\Bbbk}(\mathrm{S}_n) = \mathrm{ed}_{\Bbbk}(L/L^{\mathrm{S}_n})$. Thus it suffices to find a subfield $E \subseteq L$, on which S_n acts faithfully, with $\mathrm{trdeg}_{\Bbbk}(E) = n-3$. For distinct integers $i, j, k, l \in \{1, \dots, n\}$ we define the so-called *cross ratio*

$$[i, j, k, l] \coloneqq \frac{(X_i - X_k)(X_j - X_l)}{(X_i - X_l)(X_j - X_k)},$$

and we let the subfield of L generated by these cross ratios be

$$E \coloneqq \Bbbk(\{[i, j, k, l] \mid i, j, k, l \in \{1, \dots, n\} \text{ all distinct}\}).$$

There are some easy to check equalities between cross ratios:

$$\begin{aligned} [j, i, k, l] &= [i, j, k, l]^{-1} = [i, j, l, k], \\ [i, k, j, l] &= 1 - [i, j, k, l] = [l, j, k, i]. \end{aligned} \tag{4.1}$$

Note that these equalities imply in particular that, if $[i, j, k, l]$ belongs to some field, then so does the cross ratio $[\tau(i), \tau(j), \tau(k), \tau(l)]$ for any permutation $\tau \in \mathrm{S}_4$ of $\{i, j, k, l\}$. Furthermore, for every $\sigma \in \mathrm{S}_n$, we have

$${}_L\sigma([i, j, k, l]) = [\sigma(i), \sigma(j), \sigma(k), \sigma(l)].$$

Thus E is an S_n-invariant subfield of L. We therefore have a group homomorphism $\rho\colon \mathrm{S}_n \to \mathrm{Aut}_{\Bbbk}(E)$. Since $n \geq 5$, the only normal subgroups of S_n are S_n itself, the alternating group A_n, and $\{e\}$; one of these must be the kernel of ρ. From (4.1) we see that in particular $(13)(12) \in \mathrm{A}_n$ satisfies $(13)(12)[1, 2, 3, 4] = 1 - [1, 2, 3, 4]^{-1} \neq [1, 2, 3, 4]$. Thus $(13)(12) \notin \ker \rho$, which implies that ρ is injective, i.e., the action on E is faithful.
It now remains to show that $\mathrm{trdeg}_{\Bbbk}(E) = n - 3$. Let $i \in \{4, \dots, n\}$ and consider the field $F \coloneqq \Bbbk(X_1, X_2, X_3, [1, 2, 3, i]) \subseteq \Bbbk(X_1, X_2, X_3, X_i)$. A direct computation shows that

$$X_i = X_1 - \frac{1}{\frac{[1,2,3,i]}{X_1 - X_3} + \frac{[1,3,2,i]}{X_1 - X_2}} \in F.$$

Thus $F = \Bbbk(X_1, X_2, X_3, X_i)$. Consequently, $L = \Bbbk(X_1, X_2, X_3, [1,2,3,4], \ldots, [1,2,3,n])$, which implies that $E' \coloneqq \Bbbk([1,2,3,4], \ldots, [1,2,3,n])$ is purely transcendental over $\Bbbk$ with transcendence degree $n-3$. To complete the proof we show that $E' = E$. First observe that for distinct $i,j,k,l,m \in \{1,\ldots,n\}$ we have

$$[i,j,m,l] \cdot [j,i,m,k] = \frac{(X_i - X_m)(X_j - X_l)}{(X_i - X_l)(X_j - X_m)} \cdot \frac{(X_j - X_m)(X_i - X_k)}{(X_j - X_k)(X_i - X_m)} = \frac{(X_i - X_k)(X_j - X_l)}{(X_i - X_l)(X_j - X_k)} = [i,j,k,l]. \tag{4.2}$$

Let $i,j,k,l \in \{1,\ldots,n\}$ be distinct. We show that $[i,j,k,l] \in E'$. We consider several cases.

(i) If $\#(\{i,j,k,l\} \cap \{1,2,3\}) = 3$, then $[i,j,k,l]$ is, up to permutation, one of the generators of E'; so $[i,j,k,l] \in E'$.
(ii) Suppose $\#(\{i,j,k,l\} \cap \{1,2,3\}) = 2$. Without loss of generality, suppose that $i,j \in \{1,2,3\}$. Let $m \in \{1,2,3\} \setminus \{i,j\}$. Then $[i,j,m,l], [j,i,m,k] \in E'$ by (i). From (4.2) we find that $[i,j,k,l] = [i,j,m,l] \cdot [j,i,m,k] \in E'$.
(iii) Suppose $\#(\{i,j,k,l\} \cap \{1,2,3\}) = 1$. Without loss of generality, $i \in \{1,2,3\}$. Let $m \in \{1,2,3\} \setminus \{i\}$. By (ii), both $[i,j,m,l]$ and $[j,i,m,k]$ belong to E', hence, by (4.2), so does their product $[i,j,k,l]$.
(iv) Finally, consider the case where $\#(\{i,j,k,l\} \cap \{1,2,3\}) = 0$. Let $m \in \{1,2,3\}$. From (iii) we infer that $[i,j,m,l], [j,i,m,k] \in E'$, wherefore also $[i,j,k,l] \in E'$ by (4.2).

All cases have been exhausted, whence $E' = E$. We conclude that $\mathrm{ed}_\Bbbk(\mathrm{S}_n) \leq \mathrm{trdeg}_\Bbbk(E) = n-3$. □

Next we focus on finding lower bounds of $\mathrm{d}_\Bbbk(n) = \mathrm{ed}_\Bbbk(\mathrm{S}_n)$, which shall also yield some exact values for small n. In order to do this we shall prove a useful special case of Proposition 4.3, where the inequality becomes an equality. This requires that we lay some conditions on G and $\Bbbk$. Subsequently, we apply this to S_n. The next series of assertions aim towards this result, stated in Theorem 4.14. The original proof for the case where $\mathrm{char}\,\Bbbk = 0$ was presented in [3, Theorem 5.3] and related lemmas. A generalization to arbitrary characteristic is proved in [17, Theorems 4.5–4.6] and related lemmas, which is the approach we shall follow closely.

Let R be a discrete valuation $\Bbbk$-algebra with field of fractions K, $\mathfrak{m}$ the maximal ideal of R, and $F \coloneqq R/\mathfrak{m}$ its residue field. Assume that $\Bbbk$ is algebraically closed in F. Suppose that there is a surjective valuation $\mu\colon K \to \mathbb{Z} \cup \{\infty\}$. Let there be a faithful group action of G on K, fixing $\Bbbk$ pointwise, that respects this valuation, i.e., for any $\sigma \in G$ and $\alpha \in K$, $\mu({}_K\sigma(\alpha)) = \mu(\alpha)$.
Observe that the action of G restricts to R and that this action remains faithful: Let $\sigma \in G$ and suppose ${}_K\sigma$ becomes the identity on R. Then for any $\alpha \in K^\times$, either α or α^{-1} belongs to R; either way, since ${}_K\sigma(\alpha)^{-1} = {}_K\sigma(\alpha^{-1})$, ${}_K\sigma$ fixes α. Then $\sigma = \mathrm{e}$, because G acts faithfully on K.
We subsequently get induced actions on F and $\mathfrak{m}/\mathfrak{m}^2$. Define

$$G_0 \coloneqq \{\sigma \in G \mid {}_F\sigma = \mathrm{id}_F\},$$
$$G_1 \coloneqq \left\{\sigma \in G_0 \;\middle|\; {}_{\mathfrak{m}/\mathfrak{m}^2}\sigma = \mathrm{id}_{\mathfrak{m}/\mathfrak{m}^2}\right\}.$$

These are, respectively, the inertia group and the first ramification group of G. The properties, that we show these groups have, can also be found in [27, §§IV.1-2]. Observe that these are normal subgroups of G. Let t be a generator of $\mathfrak{m}$. Let $\sigma \in G$. Since $\mu({}_R\sigma(t)) = \mu(t) = 1$, there is a $\lambda_\sigma \in R^\times$ such that ${}_R\sigma(t) = \lambda_\sigma t$. For the residue class of λ_σ in $R/\mathfrak{m}$ we write $\overline{\lambda}_\sigma$. Define the map

$$\begin{aligned} \Phi\colon G_0 &\longrightarrow F^\times \\ \sigma &\longmapsto \overline{\lambda}_\sigma. \end{aligned}$$

***Lemma* 4.8.** *With the definitions as above, the map Φ is a group homomorphism, whose kernel is G_1, and whose image is a cyclic group.*

Proof. For any $\sigma, \tau \in G_0$ we have

$$\lambda_{\sigma\tau} t = {}_R(\sigma\tau)(t) = {}_R\sigma({}_R\tau(t)) = {}_R\sigma(\lambda_\tau t) = {}_R\sigma(\lambda_\tau)\lambda_\sigma t.$$

Thus $\lambda_{\sigma\tau} = {}_R\sigma(\lambda_\tau)\lambda_\sigma$. Since $\sigma \in G_0$, we have ${}_R\sigma(\lambda_\tau) \equiv \lambda_\tau \bmod \mathfrak{m}$. Therefore,

$$\Phi(\sigma\tau) = \overline{\lambda}_{\sigma\tau} = {}_F\sigma(\overline{\lambda}_\tau)\overline{\lambda}_\sigma = \overline{\lambda}_\tau \overline{\lambda}_\sigma = \Phi(\sigma)\Phi(\tau).$$

Next we show that $\ker\Phi = G_1$. For any $\sigma \in \ker\Phi$ we have $\lambda_\sigma \equiv 1 \bmod \mathfrak{m}$. Thus $\lambda_\sigma = 1 + \alpha t$ for some $\alpha \in R$. Let $\beta t \in \mathfrak{m}$ be arbitrary. Since $\sigma \in G_0$, we have ${}_R\sigma(\beta) = \beta + \beta' t$ for some $\beta' \in R$. Therefore, ${}_R\sigma(\beta t) = {}_R\sigma(\beta)\lambda_\sigma t = (\beta + \beta' t)(1 + \alpha t)t \equiv \beta t \bmod \mathfrak{m}^2$. Thus $\sigma \in G_1$.
Conversely, if $\sigma \in G_1$, then in particular ${}_R\sigma(t) \equiv t \bmod \mathfrak{m}^2$. Thus $\lambda_\sigma t = {}_R\sigma(t) = t + \alpha t^2$ for some $\alpha \in R$. Then $\lambda_\sigma = 1 + \alpha t \equiv 1 \bmod \mathfrak{m}$, which means that $\overline{\lambda}_\sigma = 1$.
Finally, the image of Φ is a finite subgroup of the multiplicative group of a field, which is always cyclic. □

***Corollary* 4.9.** *If q is a prime divisor of $\#(G_0/G_1)$, then $\Bbbk$ contains a primitive q-th root of unity.*

Proof. By Lemma 4.8, $G_0/G_1 \cong \operatorname{im}\Phi$, which is cyclic of finite order. If $q \mid \#(G_0/G_1)$, then there is an element of order q in G_0/G_1, and hence in $\operatorname{im}\Phi \subseteq F$. Thus F contains a primitive q-th root of unity. Since, by assumption, $\Bbbk$ is algebraically closed in F, it follows that this root of unity actually lies in $\Bbbk$. □

***Lemma* 4.10.** *For every $\tau \in G$ and $\sigma \in G_0$ the commutator $\tau\sigma\tau^{-1}\sigma^{-1}$ belongs to G_1.*

Proof. Let $\tau \in G$ and $\sigma \in G_0$; we shall prove that $\tau\sigma\tau^{-1}\sigma^{-1} \in \ker\Phi$. Note that $\tau\sigma\tau^{-1} \in G_0$. Since $\operatorname{im}\Phi$ is cyclic by Lemma 4.8, there is a $\gamma \in F^\times$ that generates $\operatorname{im}\Phi$. This γ has finite order, wherefore it is algebraic over $\Bbbk$. It follows that $\gamma \in \Bbbk$, because $\Bbbk$ is algebraically closed in F by assumption.
First observe that $t = \lambda_{\tau\tau^{-1}}t = {}_R(\tau\tau^{-1})(t) = {}_R\tau({}_{\tau^{-1}})\lambda_\tau t$, wherefore ${}_R\tau({}_{\tau^{-1}})\lambda_\tau = 1$. Let $i \in \mathbb{N}$ such that $\overline{\lambda}_\sigma = \gamma^i$. We have $\lambda_{\tau\sigma\tau^{-1}}t = {}_R(\tau\sigma\tau^{-1})(t) = {}_R\tau({}_R\sigma({}_{\tau^{-1}})\lambda_\sigma)\lambda_\tau t$. Using the fact that $\sigma \in G_0$, we obtain

$$\lambda_{\tau\sigma\tau^{-1}} = {}_R\tau({}_R\sigma({}_{\tau^{-1}})\lambda_\sigma)\lambda_\tau \equiv {}_R\tau({}_{\tau^{-1}}\lambda_\sigma)\lambda_\tau \equiv {}_R\tau({}_{\tau^{-1}})\lambda_\tau\ {}_R\tau(\lambda_\sigma) \equiv {}_R\tau(\lambda_\sigma) \bmod \mathfrak{m}.$$

Since ${}_F\tau$ fixes $\Bbbk$ pointwise, we find $\overline{\lambda}_{\tau\sigma\tau^{-1}} = {}_F\tau(\overline{\lambda}_\sigma) = {}_F\tau(\gamma^i) = \gamma^i$. As Φ is a homomorphism, we obtain

$$\overline{\lambda}_{\tau\sigma\tau^{-1}\sigma^{-1}} = \overline{\lambda}_{\tau\sigma\tau^{-1}} \cdot \overline{\lambda}_{\sigma^{-1}} = \gamma^i \cdot \gamma^{-i} = 1.$$

Thus $\tau\sigma\tau^{-1}\sigma^{-1} \in \ker\Phi = G_1$. □

***Lemma* 4.11.** *If $\operatorname{char}\Bbbk = 0$, then G_1 is trivial; if $\operatorname{char}\Bbbk =: \ell > 0$, then G_1 is an ℓ-subgroup of G.*

Proof. Let $\sigma \in G_1$. Let $r \in \mathbb{N}_0$ and $z \in \mathfrak{m}^r$ (where $\mathfrak{m}^0 = R$). We first prove that ${}_R\sigma(z) - z \in \mathfrak{m}^{r+1}$. Let $\alpha \in R$ such that $z = \alpha t^r$. We have ${}_R\sigma(\alpha) = \alpha + \alpha' t$ for some $\alpha' \in R$, because $\sigma \in G_0$, and $\lambda_\sigma = 1 + \beta t$ for some $\beta \in R$, since $\sigma \in \ker\Phi$. Then

$${}_R\sigma(z) = {}_R\sigma(\alpha)\ {}_R\sigma(t)^r = (\alpha + \alpha' t)(1 + \beta t)^r t^r \equiv \alpha t^r \equiv z \bmod \mathfrak{m}^{r+1}.$$

Thus indeed ${}_R\sigma(z) - z \in \mathfrak{m}^{r+1}$.
Let $n \coloneqq \operatorname{ord}(\sigma)$. Define $m \in \mathbb{N}$ as follows: If $\operatorname{char}\Bbbk = 0$, let $m \coloneqq n$; if $\operatorname{char}\Bbbk = \ell > 0$, let m be such that $n = \ell^s m$ for some $s \in \mathbb{N}_0$ and $\ell \nmid m$. Observe that m is invertible in $\Bbbk$. Set $\tau \coloneqq \sigma^{\frac{n}{m}}$ and note that $\operatorname{ord}(\tau) = m$. We shall show that $m = 1$.
Suppose to the contrary that $m > 1$. Then $\tau \neq e$, and, since G acts faithfully on R, ${}_R\tau \neq \mathrm{id}_R$. Let $x \in R$ such that ${}_R\tau(x) \neq x$. Set $y \coloneqq {}_R\tau(x) - x$. Then $y \neq 0$, and so there is some $r \in \mathbb{N}$ such that $y \in \mathfrak{m}^r \setminus \mathfrak{m}^{r+1}$. We shall use induction to show that for every $i \in \mathbb{N}_0$, ${}_R\tau^i(x) \equiv x + iy \bmod \mathfrak{m}^{r+1}$. The base case where $i = 0$ is trivial. Suppose the assertion holds for some $i \in \mathbb{N}_0$. We have ${}_R\tau^i(y) - y = {}_R\tau^{i+1}(x) - {}_R\tau^i(x) - y$. Since $y \in \mathfrak{m}^r$ and $\tau^i \in G_1$, it follows that ${}_R\tau^i(y) - y \in \mathfrak{m}^{r+1}$ by the argument above. Therefore,

$${}_R\tau^{i+1}(x) \equiv {}_R\tau^i(x) + y \equiv x + (i+1)y \bmod \mathfrak{m}^{r+1},$$

where the last congruence follows from the induction hypothesis. The assertion now holds for all $i \in \mathbb{N}_0$ by induction. In particular, for $i = m$ we have

$$x = {}_R\tau^m(x) \equiv x + my \bmod \mathfrak{m}^{r+1}.$$

Thus $my \in \mathfrak{m}^{r+1}$. Since $y \notin \mathfrak{m}^{r+1}$, we must have that $m \in \mathfrak{m}$. But then $m = 0$ in F, and hence in $\Bbbk$, which contradicts the fact that m is invertible in $\Bbbk$. Consequently, $m > 1$ is false, and so $m = 1$. This means that $\operatorname{ord}(\sigma) = 1$ in characteristic 0, and $\operatorname{ord}(\sigma) = \ell^s$ in characteristic $\ell > 0$. □

***Proposition* 4.12.** *Let p be a prime number such that $\operatorname{char}\Bbbk \neq p$. Assume that $\Bbbk$ contains a primitive p-th root of unity ζ_p. Then $\operatorname{ed}_\Bbbk(\mathbb{Z}/p\mathbb{Z}) = 1$.*

Proof. Let Y be a variable and consider $\Bbbk[Y]$. Let $\mathbb{Z}/p\mathbb{Z}$ act on $\Bbbk[Y]$ by letting $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ send Y to $\zeta_p^n Y$. Observe that this action is faithful. Extend it to $\Bbbk(Y)$. Since $\Bbbk(Y)$ is the function field of $\operatorname{Spec} \Bbbk[Y]$, it follows that $\operatorname{Spec} \Bbbk[Y]$ is a faithful, linear $\mathbb{Z}/p\mathbb{Z}$-variety. Because $\operatorname{trdeg}_{\Bbbk}(\Bbbk(Y)) = 1$ and $\mathbb{Z}/p\mathbb{Z}$ is not the trivial group, we have $\operatorname{ed}_{\Bbbk}(\mathbb{Z}/p\mathbb{Z}) = 1$. □

The following statement is [15, Lemma 8.1.2], which forms a crucial part of the proof of the next theorem. The proof we give is entirely based on the one given in the source.

***Lemma* 4.13.** *Let E be a field of transcendence degree $n \in \mathbb{N}_0$ over $\Bbbk$. Suppose $\mu\colon E \to \mathbb{Z} \cup \{\infty\}$ is a valuation that is trivial on $\Bbbk$. For $i \in \mathbb{N}_0$ write $E_{\geq i} \coloneqq \{\alpha \in E \mid \mu(\alpha) \geq i\}$. Let $F \coloneqq E_{\geq 0}/E_{\geq 1}$ be the residue field of μ. If $\operatorname{trdeg}_{\Bbbk}(F) = \operatorname{trdeg}_{\Bbbk}(E)$, then μ is the trivial valuation on E.*

Proof. Assume that $\operatorname{trdeg}_{\Bbbk}(F) = n$. Let $x_1, \dots, x_n \in E_{\geq 0}$ be such that their residue classes $\overline{x}_1, \dots, \overline{x}_n$ constitute a transcendence basis for F over $\Bbbk$. Then $\{x_1, \dots, x_n\}$ is a transcendence basis for E over $\Bbbk$: If $\{x_1, \dots, x_n\}$ were algebraically dependent over $\Bbbk$, then this would reduce to a non-trivial dependence in F upon quotienting out by $E_{\geq 1}$. This would contradict the algebraic independence of $\{\overline{x}_1, \dots, \overline{x}_n\}$. Note that $\Bbbk[x_1, \dots, x_n] \subseteq E_{\geq 0}$. If $f \in \Bbbk[x_1, \dots, x_n]$ is non-zero, then the residue $\overline{f} \in \Bbbk[\overline{x}_1, \dots, \overline{x}_n] \subseteq F$ is also non-zero by the foregoing argument. This means that $f \notin E_{\geq 1}$, wherefore $\mu(f) = 0$. Then also $\mu(1/f) = 0$, which implies that μ is trivial on $\Bbbk(x_1, \dots, x_n)$.
Now E is algebraic over $\Bbbk(x_1, \dots, x_n)$. Let $\alpha \in E^{\times}$. We show that $\mu(\alpha) = 0$. Since $\mu(\alpha^{-1}) = -\mu(\alpha)$, without loss of generality, $\mu(\alpha) \geq 0$. Let $m \in \mathbb{N}$ be minimal such that for some $a_1, \dots, a_m \in \Bbbk(x_1, \dots, x_n)$ we have $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$ with $a_m \neq 0$. Set $a_0 \coloneqq 1$, and let $j \coloneqq \min\{i \in \mathbb{N} \mid a_{m-i} \neq 0\}$. Then $\alpha^j = \frac{-a_m}{\alpha^{m-j} + \cdots + a_{m-j}}$. Observe that $\mu(a_{m-i}\alpha^{i-j}) = \mu(a_{m-i}) + (i-j)\mu(\alpha) \geq 0$ for each $j \leq i \leq m$. Therefore,

$$\begin{aligned} j\mu(\alpha) &= \mu(-a_m) - \mu(\alpha^{m-j} + \cdots + a_{m-j}) \\ &\leq \mu(-a_m) - \min\{\mu(\alpha^{m-j}), \dots, \mu(a_{m-j})\} \\ &= 0, \end{aligned}$$

because $\mu(a_{m-j}) = 0$. It now follows that $\mu(\alpha) = 0$. Consequently, $\mu(E^{\times}) = \{0\}$, as desired. □

We have now enough material to prove the theorem, which shall provide us with some lower bounds for $\mathrm{d}_{\Bbbk}(n) = \operatorname{ed}_{\Bbbk}(\mathrm{S}_n)$.

***Theorem* 4.14.** *Let p be a prime number with $\operatorname{char} \Bbbk \neq p$. Suppose that $G = G' \times \mathbb{Z}/p\mathbb{Z}$ for some group G'. Let ζ_p be a primitive p-th root of unity, and assume that $\zeta_p \in \Bbbk$. Further assume that either $\operatorname{char} \Bbbk = 0$, or $\operatorname{char} \Bbbk =: \ell > 0$ and G has no non-trivial, normal ℓ-subgroups. Finally, suppose that for all primes $q \neq p$ that satisfy $q \mid \#Z(G')$ we have $\zeta_q \notin \Bbbk$. Then $\operatorname{ed}_{\Bbbk}(G) = \operatorname{ed}_{\Bbbk}(G') + 1$.*

Proof. Firstly, by Propositions 4.3 and 4.12, we have

$$\operatorname{ed}_{\Bbbk}(G) \leq \operatorname{ed}_{\Bbbk}(G') + \operatorname{ed}_{\Bbbk}(\mathbb{Z}/p\mathbb{Z}) = \operatorname{ed}_{\Bbbk}(G') + 1. \tag{4.3}$$

We next prove the converse inequality. Consider $A_{G'}$ and let $K \coloneqq \operatorname{Frac}(A_{G'}) = \Bbbk(\{X_\sigma \mid \sigma \in G'\})$. Let Y be an independent variable over K, and set $L \coloneqq K(Y)$. Let $\mathbb{Z}/p\mathbb{Z}$ act on $A_{G'}[Y]$ letting $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ send Y to $\zeta_p^n Y$. This action is faithful. Thusly, G acts faithfully on L. Then $\operatorname{Spec} A_{G'}[Y]$ is a faithful, linear G-variety, wherefore $\operatorname{ed}_{\Bbbk}(G) = \operatorname{ed}_{\Bbbk}(G \circlearrowright \operatorname{Spec} A_{G'}[Y]) = \operatorname{ed}_{\Bbbk}(L/L^G)$.
The localization $K[Y]_{(Y)}$ of $K[Y]$ at the ideal $(Y) \subset K[Y]$ has field of fractions L, and therefore defines the surjective (Y)-adic valuation $\nu\colon L \to \mathbb{Z} \cup \{\infty\}$. For $i \in \mathbb{Z}$ let $L_{\geq i} \coloneqq \{\alpha \in L \mid \nu(\alpha) \geq i\}$. The residue field $L_{\geq 0}/L_{\geq 1}$ is isomorphic to K. Since every $\sigma \in G$ sends Y to $\zeta_p^n Y$ for some $n \in \mathbb{N}_0$, it follows that for all $\alpha \in L$, $\nu({}_L\sigma(\alpha)) = \nu(\alpha)$.
Let E be a subfield of L, on which G acts faithfully, such that $\operatorname{ed}_{\Bbbk}(G) = \operatorname{trdeg}_{\Bbbk}(E)$. We consider $\nu|_E$. Suppose that $\nu|_E$ is the trivial valuation. Then $E \subseteq L_{\geq 0}$. Thus we get a G-equivariant homomorphism

$$E \hookrightarrow L_{\geq 0} \twoheadrightarrow L_{\geq 0}/L_{\geq 1} \cong K.$$

Since E is a field, this composition is injective, which means we have a G-equivariant embedding of E into K. However, since G acts faithfully on E, this implies that G acts faithfully on K as well. Yet $\mathbb{Z}/p\mathbb{Z}$ acts trivially on K, thus this is a contradiction. Consequently, $\nu|_E$ is not trivial, and so there is some $r \in \mathbb{N}$ such that $\operatorname{im} \nu|_E = r\mathbb{Z}$. Let $\mu \coloneqq \frac{1}{r}\nu$. This defines a surjective valuation on E. Let $F \coloneqq E_{\geq 0}/E_{\geq 1}$. Note that $E_{\geq 0} = L_{\geq 0} \cap E$, because for any $\alpha \in E$, $\mu(\alpha) \geq 0$ if and only if $\nu(\alpha) \geq 0$. In particular, the

action of G on E restricts to a faithful one on $E_{\geq 0}$.
Next observe that $E_{\geq 1} \subseteq L_{\geq 1}$. Therefore, $E_{\geq 1}$ lies in the kernel of the composition

$$E_{\geq 0} \hookrightarrow L_{\geq 0} \twoheadrightarrow L_{\geq 0}/L_{\geq 1} \cong K.$$

Thus there is a G-equivariant embedding of the residue field F into K. This implies that $\Bbbk$ is algebraically closed in F, because $\Bbbk$ is algebraically closed in K, being a purely transcendental extension.
Since μ becomes the trivial valuation on F, but remains non-trivial on E, Lemma 4.13 asserts that $\operatorname{trdeg}_{\Bbbk}(F) < \operatorname{trdeg}_{\Bbbk}(E)$; equivalently,

$$\operatorname{trdeg}_{\Bbbk}(F) \leq \operatorname{trdeg}_{\Bbbk}(E) - 1.$$

We shall show that G' acts faithfully on F. The action of G on E induces an action on $E_{\geq 1}/E_{\geq 2}$. We may therefore consider the ramification groups

$$G_0 \coloneqq \{\sigma \in G \mid {}_F\sigma = \mathrm{id}_F\},$$
$$G_1 \coloneqq \left\{\sigma \in G_0 \;\middle|\; {}_{E_{\geq 1}/E_{\geq 2}}\sigma = \mathrm{id}_{E_{\geq 1}/E_{\geq 2}}\right\}.$$

Observe that, since $F \subset K$ and $\mathbb{Z}/p\mathbb{Z}$ acts trivially on K, we have $\mathbb{Z}/p\mathbb{Z} \leq G_0$. Thus G' acts faithfully on F if and only if $G_0 = \mathbb{Z}/p\mathbb{Z}$.
Lemma 4.11 implies that, if $\operatorname{char}\Bbbk = 0$, then G_1 is trivial, and if $\operatorname{char}\Bbbk = \ell > 0$, then G_1 is an ℓ-subgroup of G. Since G_1 is normal and, by assumption, G has no non-trivial, normal ℓ-subgroups, it follows that G_1 is trivial. Let $\tau \in G$ and $\sigma \in G_0$. Their commutator $\tau\sigma\tau^{-1}\sigma^{-1}$ belongs to G_1 by Lemma 4.10. Since $G_1 = \{e\}$, this implies that $\tau\sigma = \sigma\tau$, and so G_0 lies in the center of G. Therefore, $G_0 = H \times \mathbb{Z}/p\mathbb{Z}$ for some normal subgroup H of G' with $H \leq Z(G')$. We show that H is trivial.
Suppose that $p \mid \#H$. Then $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is a subgroup of $H \times \mathbb{Z}/p\mathbb{Z}$. But from Lemma 4.8 we infer that G_0 is cyclic. Subgroups of cyclic groups are cyclic, whereas $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ is not, wherefore this is a contradiction. Let $q \neq p$ be a prime dividing $\#H$. Then $q \mid \#Z(G')$ and so, by assumption, $\zeta_q \notin \Bbbk$. However, since also $q \mid \#G_0$, Corollary 4.9 shows that $\zeta_q \in \Bbbk$. Thus we have again reached a contradiction. Consequently, $\#H$ has no prime divisors, which means it equals 1. So H is trivial and $G_0 = \mathbb{Z}/p\mathbb{Z}$. Whence G' acts faithfully on F, and therefore

$$\operatorname{ed}_{\Bbbk}(G') \leq \operatorname{trdeg}_{\Bbbk}(F) \leq \operatorname{trdeg}_{\Bbbk}(E) - 1 = \operatorname{ed}_{\Bbbk}(G) - 1,$$

and so $\operatorname{ed}_{\Bbbk}(G) \geq \operatorname{ed}_{\Bbbk}(G') + 1$. Together with (4.3) we conclude that $\operatorname{ed}_{\Bbbk}(G) = \operatorname{ed}_{\Bbbk}(G') + 1$. □

Finally, we extend—for $\Bbbk$ infinite—the results in Table 1.1 from Chapter 1.

***Theorem* 4.15.** *Let* $\operatorname{char}\Bbbk \neq 2$ *and* $n \in \mathbb{N}$. *We have*
(a) $\operatorname{ed}_{\Bbbk}(\mathrm{S}_{n+2}) \geq \operatorname{ed}_{\Bbbk}(\mathrm{S}_n) + 1$;
(b) $\operatorname{ed}_{\Bbbk}(\mathrm{S}_n) \geq \left\lfloor \frac{n}{2} \right\rfloor$;
(c) *the values of* $\mathrm{d}_{\Bbbk}(n) = \operatorname{ed}_{\Bbbk}(\mathrm{S}_n)$ *as shown in Table* 4.1.

n	1	2	3	4	5	6
$\mathrm{d}_{\Bbbk}(n)$	0	1	1	2	2	3

Table 4.1: Essential dimension of S_n for small values of n with $\operatorname{char}\Bbbk \neq 2$.

Proof.
(a) We have an injective group homomorphism $\mathrm{S}_n \times \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{S}_{n+2}$, which includes S_n in S_{n+2} in the usual way, and the non-trivial element of $\mathbb{Z}/2\mathbb{Z}$ is sent to the permutation of S_{n+2} that swaps $n+1$ and $n+2$. Thus $\operatorname{ed}_{\Bbbk}(\mathrm{S}_{n+2}) \geq \operatorname{ed}_{\Bbbk}(\mathrm{S}_n \times \mathbb{Z}/2\mathbb{Z})$ by Lemma 4.2. We subsequently wish to apply Theorem 4.14, so we check the hypotheses. Firstly, we have $p = 2$ and $\operatorname{char}\Bbbk \neq 2$ by assumption; in particular $-1 = \zeta_p \in \Bbbk$. The only possible non-trivial, normal subgroups of S_n are S_n, A_n, and the Klein four-group in case of $n = 4$. If $n \neq 3$, then none of these normal subgroups are ℓ-subgroups for some $\ell \neq 2$; otherwise $\mathrm{A}_3 = \mathbb{Z}/3\mathbb{Z}$ is a 3-group—so the theorem cannot be used when $\operatorname{char}\Bbbk = 3$ and $n = 3$. Finally, for the last condition, the center of S_n is trivial for $n \neq 2$ and its order is divisible only by 2 for $n = 2$. Thus the final condition is vacuously satisfied. Whence, by Theorem 4.14,

$$\operatorname{ed}_{\Bbbk}(\mathrm{S}_{n+2}) \geq \operatorname{ed}_{\Bbbk}(\mathrm{S}_n \times \mathbb{Z}/2\mathbb{Z}) = \operatorname{ed}_{\Bbbk}(\mathrm{S}_n) + 1, \quad n \neq 3.$$

Observe that this implies that $\operatorname{ed}_{\Bbbk}(\mathrm{S}_4) \geq \operatorname{ed}_{\Bbbk}(\mathrm{S}_2) + 1 = 2$. Therefore, $\operatorname{ed}_{\Bbbk}(\mathrm{S}_5) \geq 2 = \operatorname{ed}_{\Bbbk}(\mathrm{S}_3) + 1$ by Table 1.1 and Proposition 4.5. Thus the statement holds also for $n = 3$, and so for all $n \in \mathbb{N}$.

(b) We prove the assertion by induction, making use of (a). The base cases $n = 1$ and $n = 2$ are clear: $\mathrm{ed}_{\Bbbk}(\mathrm{S}_1) = 0 = \left\lfloor \frac{1}{2} \right\rfloor$, and $\mathrm{ed}_{\Bbbk}(\mathrm{S}_2) = 1 = \left\lfloor \frac{2}{2} \right\rfloor$ by Table 1.1. Next assume the assertion holds for all $m \leq n$ for some $n \in \mathbb{N}$. We may assume that $n \geq 2$. We have, by (a),

$$\mathrm{ed}_{\Bbbk}(\mathrm{S}_{n+1}) \geq \mathrm{ed}_{\Bbbk}(\mathrm{S}_{n-1}) + 1 \geq \left\lfloor \tfrac{n-1}{2} \right\rfloor + 1 = \left\lfloor \tfrac{n+1}{2} \right\rfloor,$$

where the second inequality follows from the inductive hypothesis.

(c) We have already seen the value of $\mathrm{ed}_{\Bbbk}(\mathrm{S}_n)$ for $n \leq 3$ in Table 1.1. By (b), we have $\mathrm{ed}_{\Bbbk}(\mathrm{S}_5) \geq \mathrm{ed}_{\Bbbk}(\mathrm{S}_4) \geq 2$ and $\mathrm{ed}_{\Bbbk}(\mathrm{S}_6) \geq 3$. Proposition 4.7 tells us that $\mathrm{ed}_{\Bbbk}(\mathrm{S}_5) \leq 2$ and $\mathrm{ed}_{\Bbbk}(\mathrm{S}_6) \leq 3$, which subsequently show that $\mathrm{ed}_{\Bbbk}(\mathrm{S}_4) = \mathrm{ed}_{\Bbbk}(\mathrm{S}_5) = 2$ and $\mathrm{ed}_{\Bbbk}(\mathrm{S}_6) = 3$. □

A theorem similar to Theorem 4.15 for the case $\operatorname{char} \Bbbk = 2$ requires some more work. We start with a lemma from [24], whose proof we follow closely.

***Proposition* 4.16.** *Let L be a field of finite transcendence degree over $\Bbbk$. Let Y be a variable and $E \subseteq L(Y)$ a subfield. If $\mathrm{trdeg}_{\Bbbk}(E) \leq \mathrm{trdeg}_{\Bbbk}(L)$, then there is an embedding $E \hookrightarrow L$.*

Proof. Let $d \coloneqq \mathrm{trdeg}_{\Bbbk}(E)$. If $d < \mathrm{trdeg}_{\Bbbk}(L)$, then we may choose a set $T \subset L(Y)$ of $\mathrm{trdeg}_{\Bbbk}(L) - d$ elements that are algebraically independent over E. Then $\mathrm{trdeg}_{\Bbbk}(E(T)) = \mathrm{trdeg}_{\Bbbk}(L)$. Proving the assertion for $E(T)$ in place of E is clearly sufficient, hence we may and do assume that $d = \mathrm{trdeg}_{\Bbbk}(L)$.
If $d = 0$, then L is the algebraic closure of $\Bbbk$ inside $L(Y)$. Since E is algebraic over $\Bbbk$, E embeds into L. Thus it remains to prove the case where $d > 0$.
Suppose $L(Y)/E(Y)$ is not algebraic. Then $\mathrm{trdeg}_{E(Y)}(L(Y)) = 1$, hence there is some $t \in L(Y)$ such that $L(Y)/E(Y)(t)$ is algebraic. Then $Y + t$ is transcendental over $E(Y)$, and hence over E, wherefore $L(Y)/E(Y + t)$ is algebraic. Since $L(Y) = L(Y + t)$, we may replace Y with $Y + t$, and henceforth assume that $L(Y)$ is algebraic over $E(Y)$.
Let $\{t_1, \ldots, t_d\}$ be a transcendence basis of L over $\Bbbk$. Each t_i is algebraic over $E(Y)$, so for each $i \in \{1, \ldots, d\}$ there is a polynomial

$$f_i(X) \coloneqq g_{i,m_i}(Y)X^{m_i} + \cdots + g_{i,1}(Y)X + g_{i,0}(Y),$$

where $m_i \coloneqq \deg_X(f_i)$ and $g_{i,j}(Y) \in E[Y]$, such that $f_i(t_i) = 0$. Set $n_{i,j} \coloneqq \deg_Y(g_{i,j})$ and write

$$g_{i,j}(Y) = h_{i,j,n_{i,j}}Y^{n_{i,j}} + \cdots + h_{i,j,1}Y + h_{i,j,0},$$

with $h_{i,j,k} \in E$ for $1 \leq i \leq d$, $0 \leq j \leq m_i$, and $0 \leq k \leq n_{i,j}$. Consider the set of all non-zero $g_{i,j}(Y)$ and $h_{i,j,k}$:

$$U \coloneqq \{g_{i,j}(Y), h_{i,j,k} \mid 1 \leq i \leq d, 0 \leq j \leq m_i, 0 \leq k \leq n_{i,j}\} \setminus \{0\}.$$

For a suitable $\alpha \in L$ we shall consider the $(Y - \alpha)$-adic valuation; i.e., the valuation on $L(Y)$ determined by the ideal $(Y - \alpha) \subset L[Y]$. Let $\nu \colon L(Y) \to \mathbb{Z} \cup \{\infty\}$ denote this valuation, and let $R \subseteq L(Y)$ be its valuation ring with maximal ideal $\mathfrak{m}$. We show that we can choose α such that each element of U has valuation 0 in order that their residue classes be non-zero in the residue field $R/\mathfrak{m}$. Any $\beta \in L(Y)^{\times}$ is of the form $\frac{p(Y)}{q(Y)}$ with $p, q \in L[Y] \setminus \{0\}$. If we choose α such that it is a root of neither p nor q, then $\nu(\beta) = 0$. The set U is finite, hence so is the set of such roots that we should avoid when choosing α. The set $\{t_1, t_1^2, t_1^3, \ldots\}$ is infinite, thus if we set $\alpha \coloneqq t_1^{\ell}$ for sufficiently large $\ell \in \mathbb{N}$, then $\nu(\beta) = 0$ for all $\beta \in U$. We choose such an ℓ with $\ell > m_1$.
Observe that $R/\mathfrak{m} \cong L$; in particular note that $\overline{Y} = \overline{\alpha}$ in $R/\mathfrak{m}$. Let $F \coloneqq (R \cap E)/(\mathfrak{m} \cap E)$ be the residue field of the restriction $\nu|_E$ of ν to E. Since, by construction, the residue class $\overline{\beta} \in F[\overline{\alpha}] \subseteq R/\mathfrak{m}$ of every $\beta \in U$ is non-zero, the equation $f_i(t_i) = 0$ gives a non-trivial equation for $\overline{t}_i$ over $F[\overline{\alpha}]$:

$$\overline{g}_{i,m_i}(\overline{\alpha})\overline{t}_i^{m_i} + \cdots + \overline{g}_{i,0}(\overline{\alpha}) = 0.$$

This shows that each $\overline{t}_i$ is algebraic over $F[\overline{\alpha}]$. Since $L \cong R/\mathfrak{m}$ and L is algebraic over $\Bbbk(t_1, \ldots, t_d)$, it now follows that $R/\mathfrak{m}$ is algebraic over $F[\overline{\alpha}]$. If we expand the $\overline{g}_{1,j}(\overline{\alpha})$ in the equation for $i = 1$ further, then, with $\overline{\alpha} = \overline{t}_1^{\ell}$, we get an equation for $\overline{t}_1$ over F:

$$\left(\overline{h}_{1,m_1,n_{1,m_1}}\left(\overline{t}_1^{\ell}\right)^{n_{1,m_1}} + \cdots + \overline{h}_{1,m_1,0}\right)\overline{t}_1^{m_1} + \cdots + \left(\overline{h}_{1,0,n_{1,0}}\left(\overline{t}_1^{\ell}\right)^{n_{1,0}} + \cdots + \overline{h}_{1,0,0}\right) = 0.$$

Each exponent of $\overline{t}_1$ is of the form $\ell k + j$ with $0 \leq j \leq m_1$ and $0 \leq k \leq n_{1,j}$. We show that the coefficient of $\overline{t}_1^{\ell n_{1,m_1} + m_1}$ is just $\overline{h}_{1,m_1,n_{1,m_1}}$. Say some other exponent $\ell k + j$ equals $\ell n_{1,m_1} + m_1$. Then

$\ell(n_{1,m_1}-k)=m_1-j$. Since $\ell>m_1$ and $0\le m_1-j\le m_1$, it follows that $n_{1,m_1}-k=0$. Whence $m_1=j$ and $k=n_{1,m_1}$. Thus the coefficient is $\bar{h}_{1,m_1,n_{1,m_1}}$, which is non-zero by our choice of α. Consequently, $\bar{t}_1$ is algebraic over F, and hence so is $\bar{\alpha}$.
Since $R/\mathfrak{m}$ is algebraic over $F[\bar{\alpha}]$, we see that $R/\mathfrak{m}$ is algebraic over F. This means that $\operatorname{trdeg}_{\Bbbk}(F)=\operatorname{trdeg}_{\Bbbk}(L)=\operatorname{trdeg}_{\Bbbk}(E)$. Therefore, ν is trivial on E by Lemma 4.13. Whence $E\cong F$ and so E embeds into L. □

***Corollary* 4.17.** *Let E be a subfield of $\Bbbk(X_1,\dots,X_n)$ for some $n\in\mathbb{N}_0$. If $\operatorname{trdeg}_{\Bbbk}(E)\le d$ for some $d\in\mathbb{N}_0$, then E can be embedded into $\Bbbk(X_1,\dots,X_d)$.*

Proof. Consider the fields $F_i\coloneqq\Bbbk(X_1,\dots,X_{n-i})$ for $0\le i\le n-d$. We show that E can be embedded into F_i for each i using induction on i. The base case is true by assumption. Suppose that E can be embedded into F_i for some $0\le i<n-d$. Then $\operatorname{trdeg}_{\Bbbk}(E)\le d\le n-(i+1)=\operatorname{trdeg}_{\Bbbk}(F_{i+1})$. Since $F_i=F_{i+1}(X_{n-i})$, Proposition 4.16 shows that E can be embedded into F_{i+1}. Whence, by induction, there is in particular an embedding of E into $F_{n-d}=\Bbbk(X_1,\dots,X_d)$. □

For the following assertions we generally follow the approach of [17, §5].

***Lemma* 4.18.** *Assume that $\Bbbk$ is algebraically closed and has positive characteristic ℓ. Let $\sigma\in\mathrm{PGL}_2(\Bbbk)$ be an element of finite order. Then either $\ell\nmid\operatorname{ord}(\sigma)$ or $\operatorname{ord}(\sigma)=\ell$.*

Proof. Let $n\coloneqq\operatorname{ord}(\sigma)$. Write I_2 for the 2×2 identity matrix. Let $T\in\mathrm{GL}_2(\Bbbk)$ be a matrix representing σ, and let $\lambda_1,\lambda_2\in\Bbbk^\times$ be its eigenvalues. Let J be the Jordan canonical form of T. Note that for every $m\in\mathbb{N}$ we have: $J^m\in\Bbbk^\times\cdot I_2$ if and only if $T^m\in\Bbbk^\times\cdot I_2$. We consider two cases.
Suppose that $\lambda_1\ne\lambda_2$. Then $J=\left(\begin{smallmatrix}\lambda_1&0\\0&\lambda_2\end{smallmatrix}\right)$. Since σ has order n, we have $\left(\begin{smallmatrix}\lambda_1^n&0\\0&\lambda_2^n\end{smallmatrix}\right)=J^n\in\Bbbk^\times\cdot I_2$. Thus $(\lambda_1/\lambda_2)^n=1$. Observe that $\operatorname{ord}(\lambda_1/\lambda_2)$ in $\Bbbk^\times$ is precisely n, wherefore $\Bbbk$ contains a primitive n-th root of unity. In particular, $\ell\nmid n$.
Next we consider the case where $\lambda_1=\lambda_2$. If J is a diagonal matrix, then $J\in\Bbbk^\times\cdot I_2$, and so $n=1$. Hence $\ell\nmid n$ and we are done. Otherwise, $J=\left(\begin{smallmatrix}\lambda_1&1\\0&\lambda_1\end{smallmatrix}\right)$ and $n>1$. We find $J^\ell=\left(\begin{smallmatrix}\lambda_1^\ell&\ell\lambda_1^{\ell-1}\\0&\lambda_1^\ell\end{smallmatrix}\right)=\left(\begin{smallmatrix}\lambda_1^\ell&0\\0&\lambda_1^\ell\end{smallmatrix}\right)\in\Bbbk^\times\cdot I_2$. This implies that $n\mid\ell$. Since ℓ is prime and $n\ne 1$, it follows that $n=\ell$. □

***Proposition* 4.19.** *Assume that* $\operatorname{char}\Bbbk=2$. *Then* $\mathrm{d}_{\Bbbk}(4)=\operatorname{ed}_{\Bbbk}(\mathrm{S}_4)\ge 2$.

Proof. First, recall Lüroth's Theorem (see [21] or [30, p. 126]), which asserts that, if K is a field, X an independent variable over K, and $K\subset K'\subseteq K(X)$ an intermediate field with $\operatorname{trdeg}_K(K')=1$, then $K'=K(f(X))$ for some rational function $f(X)\in K(X)$.
Suppose to the contrary that $\operatorname{ed}_{\Bbbk}(\mathrm{S}_4)=1$—note that Proposition 4.4 eliminates the case $\operatorname{ed}_{\Bbbk}(\mathrm{S}_4)=0$. By Proposition 1.19, over the algebraic closure we have $\operatorname{ed}_{\overline{\Bbbk}}(\mathrm{S}_4)=1$. Thus there is some subfield E of $\overline{\Bbbk}(X_1,X_2,X_3,X_4)$, on which S_4 acts faithfully, with $\operatorname{trdeg}_{\overline{\Bbbk}}(E)=1$. By Corollary 4.17, E can be embedded into $\overline{\Bbbk}(X_1)$, wherefore Lüroth's Theorem shows that $E=\overline{\Bbbk}(Y)$ for some Y transcendental over $\overline{\Bbbk}$. That S_4 acts faithfully means that there is an injective group homomorphism $\mathrm{S}_4\hookrightarrow\operatorname{Aut}_{\overline{\Bbbk}}\bigl(\overline{\Bbbk}(Y)\bigr)$. The latter group is isomorphic to $\mathrm{PGL}_2(\overline{\Bbbk})$. Lemma 4.18 implies, in particular, that $\mathrm{PGL}_2(\overline{\Bbbk})$ contains no element of order 4, because $\operatorname{char}\overline{\Bbbk}=2$. However, there is an element of order 4 in S_4. We have thus reached a contradiction, wherefrom we conclude that $\operatorname{ed}_{\Bbbk}(\mathrm{S}_4)\ge 2$. □

***Theorem* 4.20.** *Assume that* $\operatorname{char}\Bbbk=2$, *and let $n\in\mathbb{N}$. We have*
(a) $\operatorname{ed}_{\Bbbk}(\mathrm{S}_{n+3})\ge\operatorname{ed}_{\Bbbk}(\mathrm{S}_n)+1$ *for $n\ne 4$, provided that $\Bbbk$ contain a primitive third root of unity;*
(b) $\operatorname{ed}_{\Bbbk}(\mathrm{S}_n)\ge\left\lfloor\frac{n+1}{3}\right\rfloor$;
(c) *the values of* $\mathrm{d}_{\Bbbk}(n)=\operatorname{ed}_{\Bbbk}(\mathrm{S}_n)$ *as shown in Table* 4.2.

n	1	2	3	4	5	6
$\mathrm{d}_{\Bbbk}(n)$	0	1	1	2	2	2 or 3

Table 4.2: Essential dimension of S_n for small values of n with $\operatorname{char}\Bbbk=2$.

Proof.
(a) Assume that $n\ne 4$ and $\Bbbk$ contains a primitive third root of unity. We have an injective group homomorphism $\mathrm{S}_n\times\mathbb{Z}/3\mathbb{Z}\hookrightarrow\mathrm{S}_{n+3}$, where S_n fits inside S_{n+3} as usual, and one of the generators of $\mathbb{Z}/3\mathbb{Z}$ is sent to the cycle $((n+1)(n+2)(n+3))$. Thus $\operatorname{ed}_{\Bbbk}(\mathrm{S}_{n+3})\ge\operatorname{ed}_{\Bbbk}(\mathrm{S}_n\times\mathbb{Z}/3\mathbb{Z})$ by Lemma 4.2. We check the hypotheses for Theorem 4.14. We have $p=3$ and $\zeta_3\in\Bbbk$ by assumption. The only

non-trivial, normal subgroups of S_n are S_n and A_n for $n \neq 4$. For $n \neq 2, 4$ neither of these is a 2-group. Moreover, the center of S_n is trivial for any $n \neq 2$, hence then the last condition is vacuously met. Thus the hypotheses are satisfied for $n \neq 2, 4$, which yields

$$\mathrm{ed}_{\Bbbk}(\mathrm{S}_{n+3}) \geq \mathrm{ed}_{\Bbbk}(\mathrm{S}_n \times \mathbb{Z}/3\mathbb{Z}) = \mathrm{ed}_{\Bbbk}(\mathrm{S}_n) + 1, \quad n \neq 2, 4.$$

In the case of $n = 2$, we have, due to Proposition 4.19, $\mathrm{ed}_{\Bbbk}(\mathrm{S}_5) \geq \mathrm{ed}_{\Bbbk}(\mathrm{S}_4) \geq 2 = \mathrm{ed}_{\Bbbk}(\mathrm{S}_2) + 1$, where the last equality follows from Table 1.1.

(b) We use induction to prove the formula. In order to apply (a), we must check the formula for $n \leq 7$. By Table 1.1, Proposition 4.19, and Lemma 4.2, we find $\mathrm{ed}_{\Bbbk}(\mathrm{S}_1) = 0 \geq \lfloor \frac{2}{3} \rfloor$, $\mathrm{ed}_{\Bbbk}(\mathrm{S}_2) = 1 \geq \lfloor \frac{3}{3} \rfloor$, $\mathrm{ed}_{\Bbbk}(\mathrm{S}_3) = 1 \geq \lfloor \frac{4}{3} \rfloor$, $\mathrm{ed}_{\Bbbk}(\mathrm{S}_4) \geq 2 \geq \lfloor \frac{5}{3} \rfloor$, $\mathrm{ed}_{\Bbbk}(\mathrm{S}_5) \geq 2 \geq \lfloor \frac{6}{3} \rfloor$, $\mathrm{ed}_{\Bbbk}(\mathrm{S}_6) \geq 2 \geq \lfloor \frac{7}{3} \rfloor$, and $\mathrm{ed}_{\Bbbk}(\mathrm{S}_7) \geq 2 \geq \lfloor \frac{8}{3} \rfloor$.
We proceed to the inductive step. Assume the statement holds for all $m \leq n$ for some $n \in \mathbb{N}$. We may assume that $n \geq 7$; in particular, $n - 2 > 4$. Let ζ_3 be a primitive third root of unity, and set $k \coloneqq \Bbbk(\zeta_3)$. By (a),

$$\mathrm{ed}_k(\mathrm{S}_{n+1}) \geq \mathrm{ed}_k(\mathrm{S}_{n-2}) + 1 \geq \lfloor \tfrac{n-1}{3} \rfloor + 1 = \lfloor \tfrac{n+2}{3} \rfloor,$$

where the last inequality holds due to the inductive hypothesis. Since $k/\Bbbk$ is algebraic, Proposition 1.19 asserts that $\mathrm{ed}_{\Bbbk}(\mathrm{S}_{n+1}) \geq \mathrm{ed}_k(\mathrm{S}_{n+1})$. Whence the formula holds for all $n \in \mathbb{N}$ by induction.

(c) From Proposition 4.19 and Proposition 4.7 we find that $2 \leq \mathrm{ed}_{\Bbbk}(\mathrm{S}_4) \leq \mathrm{ed}_{\Bbbk}(\mathrm{S}_5) \leq 2$, which means that $\mathrm{ed}_{\Bbbk}(\mathrm{S}_4) = \mathrm{ed}_{\Bbbk}(\mathrm{S}_5) = 2$. Moreover, $\mathrm{ed}_{\Bbbk}(\mathrm{S}_6) \leq 3$, and so $\mathrm{ed}_{\Bbbk}(\mathrm{S}_6) \in \{2, 3\}$. □

4.2 The Essential Dimension of S_6 in Characteristic 2, a Failed Attempt

We shall use a subscript to indicate assumptions on the characteristic of the field $\Bbbk$; so $\Bbbk_2$ is $\Bbbk$ with the assumption that $\mathrm{char}\,\Bbbk = 2$, and $\Bbbk_{\neq 2}$ means that $\Bbbk$ can have any characteristic bar 2.

With Theorems 4.15 and 4.20 we have almost completely computed $\mathrm{d}_{\Bbbk}(n) = \mathrm{ed}_{\Bbbk}(\mathrm{S}_n)$ for all $1 \leq n \leq 6$ and $\Bbbk$ arbitrary; the missing value being in the last column of Table 4.2. A natural next step is to try and determine whether this value, $\mathrm{ed}_{\Bbbk_2}(\mathrm{S}_6)$, should be 2 or 3. We were primarily inspired by the proof of Proposition 4.19, and wondered whether a similar argument could be made to show that $\mathrm{ed}_{\Bbbk_2}(\mathrm{S}_6) \neq 2$, if this is indeed the case.
Namely, suppose that $\mathrm{ed}_{\Bbbk_2}(\mathrm{S}_6) = 2$. Then, by Proposition 1.19, also $\mathrm{ed}_{\overline{\Bbbk}_2}(\mathrm{S}_6) = 2$. Let $L' \coloneqq \overline{\Bbbk}(X_1, \ldots, X_6)$ be the rational function field in six variables. Let S_6 acts on L' as usual. By assumption, there exists a faithful S_6-invariant subfield $E' \subseteq L'$ of transcendence degree 2 over $\overline{\Bbbk}_2$. The next step would be to show that E' itself is purely transcendental over $\overline{\Bbbk}_2$, so that it is of the form $\overline{\Bbbk}_2(X, Y)$ with X and Y independent variables over $\overline{\Bbbk}_2$. For this we need some generalization of Lüroth's Theorem. This would give an injective group homomorphism $\mathrm{S}_6 \hookrightarrow \mathrm{Aut}_{\overline{\Bbbk}_2}\big(\overline{\Bbbk}_2(X, Y)\big)$. The latter group is also known as the *plane Cremona group over* $\overline{\Bbbk}_2$. Finally, we would need to show that in fact S_6 is not a subgroup of the plane Cremona group to reach a contradiction.
We have the following generalization of Lüroth's Theorem for arbitrary characteristic (see [32]).

***Theorem* 4.21** (Lüroth's Theorem for transcendence degree 2)**.** *Let X and Y be two algebraically independent variables over $\overline{\Bbbk}$. Let $\overline{\Bbbk} \subset E' \subseteq \overline{\Bbbk}(X, Y)$ be an intermediate field of transcendence degree 2. If $\overline{\Bbbk}(X, Y)$ is separable over E', then E' is a purely transcendental extension of $\overline{\Bbbk}$.* □

By Corollary 4.17, the field $E' \subseteq L'$ can be embedded into $\overline{\Bbbk}_2(X_1, X_2)$. This embedding is obtained by repeatedly applying Proposition 4.16. In order to utilize Theorem 4.21 we must show that there is such an embedding $E' \hookrightarrow \overline{\Bbbk}_2(X_1, X_2)$, for which the resulting field extension $\overline{\Bbbk}_2(X_1, X_2)/E'$ is separable. A natural approach would be to try and tweak the proof of Proposition 4.16 in order that it maintain separability. That is, given a field extension L of $\overline{\Bbbk}$, an independent variable Y over L, and a subfield $E \subseteq L(Y)$ with $\mathrm{trdeg}_{\overline{\Bbbk}}(E) \leq \mathrm{trdeg}_{\overline{\Bbbk}}(L)$, if $L(Y)/E$ is separable, can we find an embedding $E \hookrightarrow L$ that is separable? This naturally raises a second question: Can we find a faithful S_6-invariant subfield $E' \subseteq L'$ with $\mathrm{trdeg}_{\overline{\Bbbk}_2}(E') = 2$ such that L'/E' is separable in the first place?
Our approach therefore consists of three steps:

1. Show that the subfield $E' \subseteq L'$ can be chosen such that L'/E' is separable.
2. Prove that if $L(Y)/E$ is separable, then the embedding $\iota\colon E \hookrightarrow L$ obtained from Proposition 4.16 results in a separable extension $L/\iota(E)$.

3. Show that S_6 is not a subgroup of the plane Cremona group.

We will go over what we have attempted for each step individually and describe the complications that arise.

Step 1.
The assumption that $\mathrm{ed}_{\overline{\Bbbk}_2}(\mathrm{S}_6) = 2$ merely provides us with the existence of a subfield $E' \subseteq L'$, on which S_6 acts faithfully, of transcendence degree 2 over $\overline{\Bbbk}_2$. There is no obvious way to construct such a subfield. Thus far we have seen just one such construction, the field of cross ratios in the proof of Proposition 4.7, which was a non-trivial construction. Interestingly, $\Bbbk(X_1, \dots, X_n)$, with $n \geq 4$, is separable over its field of cross ratios, because $\{X_1, X_2, X_3\}$ is a separating transcendence basis. Thus it is not unreasonable to expect that such an $E' \subseteq L'$ exists with L'/E' separable.
Any field extension can be split into a separable extension followed by a purely inseparable one. Let $T \subseteq L'$ be a transcendence basis for L'/E'. Then, by [28, Lemma 9.14.6], there is a field $E'(T) \subseteq E'_{\mathrm{sep}} \subseteq L'$ such that L'/E'_{sep} is purely inseparable, and $E'_{\mathrm{sep}}/E'(T)$ is separable; then E'_{sep} is separable over E', since T is a separating transcendence basis. However, E'_{sep} need not at all be purely transcendental over $\overline{\Bbbk}_2$. It would be sufficient to find a suitable intermediate field $E'(T) \subseteq K' \subseteq E'_{\mathrm{sep}}$ that is purely transcendental over $\overline{\Bbbk}_2$, for then $K'/E'(T)$ is separable, and hence so is K'/E'. This cannot be just any field K'; we require that K' be the rational function field of a faithful, linear S_6-variety, because then $\mathrm{ed}_{\overline{\Bbbk}_2}(\mathrm{S}_6) = \mathrm{ed}_{\overline{\Bbbk}_2}(K'/K'^{\mathrm{S}_6}) = \mathrm{trdeg}_{\overline{\Bbbk}_2}(E')$. For instance, $K' = \overline{\Bbbk}_2(X_1^{2^{n_1}}, \dots, X_6^{2^{n_6}})$ for suitable $n_1, \dots, n_6 \in \mathbb{N}_0$.
Ideally, we would have a subextension $E' \subseteq E'_{\mathrm{insep}} \subseteq L'$ with the reverse property of E'_{sep}: that L'/E'_{insep} is separable and E'_{insep}/E' is purely inseparable. In that case, $\mathrm{Aut}_{\overline{\Bbbk}_2}(E'_{\mathrm{insep}}) = \mathrm{Aut}_{\overline{\Bbbk}_2}(E')$ and E'_{insep}/E' is algebraic, so E'_{insep} is a faithful S_6-invariant subfield of L' of transcendence degree 2 over $\overline{\Bbbk}_2$. Moreover, L'/E'_{insep} is separable. Such subextensions do exist for normal extensions by [28, Lemma 9.27.3], but we are unaware of such a notion with a similar result for transcendental extensions. Thus this does not seem fruitful.

Step 2.
For this step we let $\mathrm{char}\,\Bbbk =: p > 0$. We adopt the notation used in the proof of Proposition 4.16 and further assume that $L(Y)/E$ is separable. There is a separating transcendence basis for $L(Y)/E$, of which we may choose a subset T of $\mathrm{trdeg}_{\Bbbk}(L) - \mathrm{trdeg}_{\Bbbk}(E)$ elements. Then $\mathrm{trdeg}_{\Bbbk}(E(T)) = \mathrm{trdeg}_{\Bbbk}(L)$. Observe that $L(Y)/E(T)$ remains separable, because T is just a subset of a separating transcendence basis of $L(Y)/E$. It now suffices to find an embedding $\iota\colon E(T) \hookrightarrow L$ such that $L/\iota(E(T))$ is separable, because $E(T)/E$ is trivially separable (T is a separating transcendence basis) and $\iota(E(T)) = \iota(E)(\iota(T))$, which is trivially separable over $\iota(E)$. Thus we may assume that $\mathrm{trdeg}_{\Bbbk}(E) = \mathrm{trdeg}_{\Bbbk}(L)$. Subsequently, from the proof of Proposition 4.16 we obtain an $\alpha \in L(Y)$ such that the $(Y - \alpha)$-adic valuation ν on $L(Y)$ is trivial on E. Let $R \subsetneq L(Y)$ be the valuation ring with maximal ideal $\mathfrak{m}$. Let $\widetilde{L} \coloneqq R/\mathfrak{m}$ and $\widetilde{E} \coloneqq (R \cap E)/(\mathfrak{m} \cap E)$. Then $\widetilde{L} \cong L$ and $\widetilde{E} \cong E$, and we want to show that $\widetilde{L}/\widetilde{E}$ is separable.
Since $L(Y)/E$ is separable and transcendental of degree 1, there exists a $t \in L(Y)$ such that $L(Y)/E(t)$ is algebraic and separable. Since $\mathrm{trdeg}_{\Bbbk}(E(t)) > \mathrm{trdeg}_{\Bbbk}(L)$, we see that ν is non-trivial on $E(t)$, for otherwise $E(t) \hookrightarrow \widetilde{L}$, just like E itself. Suppose that $\nu(t) > 0$. Then the residue field $\widetilde{E(t)} \coloneqq (R \cap E(t))/(\mathfrak{m} \cap E(t))$ of $\nu|_{E(t)}$ is precisely $\widetilde{E}$, because $t \in \mathfrak{m} \cap E(t)$.
If $\widetilde{L} = \widetilde{E}$, then we are done, so suppose this is not the case. In particular, $L(Y) \neq E(t)$. We want to apply this in the case where L is a finitely generated extension of $\overline{\Bbbk}$, thus we can simply assume that $L(Y)$ is finitely generated over $\Bbbk$. Then there exists a primitive element θ for $L(Y)/E(t)$, so that $L(Y) = E(t, \theta)$. If $\nu(\theta) \neq 0$, then replacing θ with θ^{-1} assures that $\nu(\theta) > 0$, wherefrom follows that $\nu(\theta + 1) = \min\{\theta, 1\} = 0$, as $\nu(1) = 0 \neq \nu(\theta)$. Thus, by replacing θ with $\theta + 1$, we may assume, without loss of generality, that $\nu(\theta) = 0$. Consider its minimal polynomial $m_{\theta/E(t)}(X) \in E(t)[X]$. Observe that it is separable. Upon scaling with a suitable element, we obtain a polynomial f of the same degree with coefficients in $R \cap E(t)$ with not all of them in $\mathfrak{m} \cap E(t)$. Thus the reduction $\bar{f}$ of f modulo $\mathfrak{m} \cap E(t)$ is non-zero. Since $\bar{\theta} \neq 0$ in $\widetilde{L}$ and $\bar{f}(\bar{\theta}) = 0$, we see that $\bar{f}$ is not constant. Thus $m_{\bar{\theta}/\widetilde{E}} \mid \bar{f}$. As we have $\widetilde{L} = \widetilde{E}(\bar{\theta})$, it suffices to show that $\bar{\theta}$ is separable over $\widetilde{E}$. However, it seems not impossible that the coefficients of f that do not vanish upon reducing to $\bar{f}$ are each at a p-th power of X, making $\bar{f}$ inseparable, whilst f was not.
Even if the above succeeds, we are still not assured that the element t exists with $\nu(t) > 0$. However, there certainly is some irreducible polynomial $g(t) \in E[t]$ with $\nu(g(t)) > 0$. Since ν is non-trivial on $E(t)$, there is some $\frac{g_1(t)}{g_2(t)} \in E(t)$ with non-zero valuation, where $g_1(t), g_2(t) \in E[t]$. Certainly one of

these polynomials has positive valuation. Then one of its irreducible factors $g(t)$ satisfies $\nu(g(t)) > 0$. If g is separable over E, then the extension $E(t)/E(g(t))$ is separable as well by Lemma 4.22 below. Subsequently, $\{g(t)\}$ is a separating transcendence basis for $L(Y)/E$ with $\nu(g(t)) > 0$.

***Lemma* 4.22.** *Let* $\operatorname{char}\Bbbk =: p > 0$ *and* t *a transcendental element over* $\Bbbk$*. Let* $g \in \Bbbk[t]$ *be an irreducible polynomial. Then* g *is separable over* $\Bbbk$ *if and only if the field extension* $\Bbbk(t)/\Bbbk(g(t))$ *is separable.*

Proof. We first prove the direct implication. Let $f(X) \coloneqq g(X) - g(t) \in \Bbbk(g(t))[X]$. In fact, $f(X) \in \Bbbk[g(t)][X] = \Bbbk[X][g(t)]$, and f is linear as a polynomial of $g(t)$. Thus $f(X)$ is irreducible in $\Bbbk[g(t)][X]$, and hence in $\Bbbk(g(t))[X]$. We have $f(t) = 0$, wherefore $\Bbbk(t) \cong \Bbbk(g(t))[X]/(f)$. Finally, since g is separable, $\frac{d}{dX}g(X) \neq 0$, wherefrom follows that $\frac{d}{dX}f(X) = \frac{d}{dX}g(X) \neq 0$. Thus f is separable, and thereby so is the extension $\Bbbk(t)/\Bbbk(g(t))$.
For the converse implication assume that $\Bbbk(t)/\Bbbk(g(t))$ is separable. Then $\Bbbk(t)^p\Bbbk(g(t)) = \Bbbk(t)$ by [19, Corollary 6.10]. Note that $\Bbbk(t^p, g(t)) = \Bbbk(t)^p\Bbbk(g(t))$. If g were not separable, then $g(t) = h(t^p)$ for some $h(t) \in E[t]$. But then $\Bbbk(t) = \Bbbk(h(t^p), t^p) = \Bbbk(t^p)$, which is a contradiction. □

We would like to briefly mention the concept of *formal smoothness*. The precise definition can be found in [28, §15.36]. In particular, a field extension $F/\Bbbk$ is formally smooth if and only if it is separable by [28, Proposition 10.152.9]. Moreover, from [28, Lemma 15.97.5] we obtain that, if the inclusion $R \cap E(t) \hookrightarrow R$ of discrete valuation rings is formally smooth, then the field extension $\widetilde{L}/\widetilde{E}$ of residue fields is separable.

Finally, we point out that the above might require stronger assumptions, because we have the following counter example for smaller transcendence degree, ignoring the group action. Let u be a transcendental element over $\Bbbk$, set $L \coloneqq \Bbbk(u)$, and let $E \coloneqq \Bbbk(Y+u^p) \subset L(Y)$. Take the (Y)-adic valuation on $L(Y)$, which is trivial on E. Observe that $E(u) = \Bbbk(Y + u^p, u) = \Bbbk(Y, u) = L(Y)$, so $L(Y)/E$ is separable. However, for the residue fields we have $\widetilde{L} = \Bbbk(u)$ and $\widetilde{E} = \Bbbk(u^p)$, wherefrom we see that $\widetilde{L}/\widetilde{E}$ is inseparable.

Step 3.
The *Cremona group of order* $n \in \mathbb{N}$ *over* $\Bbbk$, denoted by $\mathrm{Cr}_n(\Bbbk)$, is the group of $\Bbbk$-automorphisms of the field $\Bbbk(X_1, \dots, X_n)$ of rational functions in n variables. It is also the group of birational automorphisms of the projective space $\mathbb{P}^n_\Bbbk$. In particular, $\mathrm{Cr}_2(\Bbbk)$ is called the *plane Cremona group*.
In Proposition 4.19, using Lemma 4.18, we looked at the order of elements to show that $\mathrm{S}_4 \nleq \mathrm{PGL}_2(\overline{\Bbbk}_2) = \mathrm{Cr}_1(\overline{\Bbbk}_2)$. Such an approach will unfortunately not work to show that $\mathrm{S}_6 \nleq \mathrm{Cr}_2(\overline{\Bbbk}_2)$: The elements of S_6 have order at most 6, and it is easy to find elements of orders 2 through 6 in $\mathrm{Cr}_2(\overline{\Bbbk}_2)$, as we now demonstrate. Let us denote by $\varphi_{\alpha,\beta} \in \mathrm{Cr}_2(\overline{\Bbbk}_2)$ the automorphism induced by $X_1 \mapsto \alpha$ and $X_2 \mapsto \beta$ for $\alpha, \beta \in \overline{\Bbbk}_2(X_1, X_2)$. We see that $\varphi_{\zeta_n X_1, X_2}$ has order n for n odd, where ζ_n is a primitive n-th root of unity. Moreover, $\varphi_{X_2^{-1}, X_1}$ has order 4, and $\varphi_{\zeta_3 X_1, X_2^{-1}}$ has order 6.
Due to the above, a different method would have to be considered to show that $\mathrm{S}_6 \nleq \mathrm{Cr}_2(\overline{\Bbbk}_2)$, supposing that this is true. Unfortunately, little is known about the finite subgroups of $\mathrm{Cr}_2(\overline{\Bbbk}_2)$ or the conjugacy classes.

Since some parts of the steps above do not seem very promising, we also take a brief look at the possibility that $\mathrm{ed}_{\Bbbk_2}(\mathrm{S}_6) = 2$.
As $(\mathbb{Z}/2\mathbb{Z})^3$ is a subgroup of S_6, by Lemma 4.2, $\mathrm{ed}_\Bbbk(\mathrm{S}_6) \geq \mathrm{ed}_\Bbbk\big((\mathbb{Z}/2\mathbb{Z})^3\big)$. This prevents $\mathrm{ed}_{\Bbbk_{\neq 2}}(\mathrm{S}_6)$ from being lower than 3, as the following proposition proves.

***Proposition* 4.23.** *Let* p *be prime. Assume that* $\Bbbk$ *contains a primitive* p*-th root of unity—in particular,* $\operatorname{char}\Bbbk \neq p$*. Let* $r \in \mathbb{N}$*. Then* $\mathrm{ed}_\Bbbk((\mathbb{Z}/p\mathbb{Z})^r) = r$.

Proof. We apply induction on r. The base case $\mathrm{ed}_\Bbbk(\mathbb{Z}/p\mathbb{Z}) = 1$ is precisely Proposition 4.12. Suppose the statement holds for some $r \in \mathbb{N}$, we prove it for $r + 1$. Since $\zeta_p \in \Bbbk$, we may apply Theorem 4.14 to $(\mathbb{Z}/p\mathbb{Z})^r \times \mathbb{Z}/p\mathbb{Z}$. This yields

$$\mathrm{ed}_\Bbbk((\mathbb{Z}/p\mathbb{Z})^r \times \mathbb{Z}/p\mathbb{Z}) = \mathrm{ed}_\Bbbk((\mathbb{Z}/p\mathbb{Z})^r) + 1 = r + 1,$$

where the last equality follows from the induction hypothesis. This proves the assertion. □

In particular, for $r = 3$ we have $\mathrm{ed}_{\Bbbk_{\neq 2}}(\mathrm{S}_6) \geq \mathrm{ed}_{\Bbbk_{\neq 2}}\big((\mathbb{Z}/2\mathbb{Z})^3\big) = 3$. However, in characteristic 2 this is no longer the case, due to the following.

***Proposition* 4.24.** *Let* p *be prime,* $\operatorname{char}\Bbbk = p$*, and* $r \in \mathbb{N}$*. Then* $\mathrm{ed}_\Bbbk((\mathbb{Z}/p\mathbb{Z})^r) = 1$.

Proof. Since $\Bbbk$ is infinite, it is an infinite-dimensional vector space over $\mathbb{F}_p$. Whence there exist non-zero elements $\alpha_1, \dots, \alpha_r \in \Bbbk$ linearly independent over $\mathbb{F}_p$. Let $(\overline{\lambda}_1, \dots, \overline{\lambda}_r) \in (\mathbb{Z}/p\mathbb{Z})^r$ act on $\Bbbk[X]$ by $X \mapsto X + \lambda_1\alpha_1 + \cdots + \lambda_r\alpha_r$. This induces a group action, because $\operatorname{char}\Bbbk = p$. By the $\mathbb{F}_p$-linear independence of the α_i, this action is faithful. Thus $\operatorname{Spec}\Bbbk[X]$ is a faithful, linear $(\mathbb{Z}/p\mathbb{Z})^r$-variety. Since $\operatorname{trdeg}_{\Bbbk}(\Bbbk(X)) = 1$, we have $\operatorname{ed}_{\Bbbk}((\mathbb{Z}/p\mathbb{Z})) = 1$. □

We thus see that one 'obstacle' preventing $\operatorname{ed}_{\Bbbk}(\mathrm{S}_6)$ from falling below 3 vanishes in characteristic 2. This is also the case for $\operatorname{ed}_{\Bbbk}(\mathrm{S}_4)$ and $(\mathbb{Z}/2\mathbb{Z})^2$, yet here the obstacle that $\mathrm{PGL}_2(\overline{\Bbbk}_2)$ does not contain an element of order 4 appears instead. In Theorem 4.15 we used the fact that $\mathrm{S}_4 \times \mathbb{Z}/2\mathbb{Z} \leq \mathrm{S}_6$ to show that $\operatorname{ed}_{\Bbbk_{\neq 2}}(\mathrm{S}_6) \geq 3$. Whether $\operatorname{ed}_{\Bbbk_2}(\mathrm{S}_4 \times \mathbb{Z}/2\mathbb{Z})$ equals 2 or 3 we do not know.
Lastly, we know that $\mathrm{A}_6 \leq \mathrm{PGL}_3(\Bbbk_2)$ due to [10, p. 156]. Moreover, $\mathrm{Cr}_2(\overline{\Bbbk})$ is generated by $\mathrm{PGL}_3(\overline{\Bbbk})$ and the standard involution induced by $X_1 \mapsto X_1^{-1}$ and $X_2 \mapsto X_2^{-1}$ by [5, Theorem 2.2]—or see [29]. Since $\mathrm{S}_6 \cong \mathrm{A}_6 \rtimes \mathbb{Z}/2\mathbb{Z}$, this may result in S_6 being a subgroup of $\mathrm{Cr}_2(\overline{\Bbbk})$. However, this would not be sufficient to conclude that $\operatorname{ed}_{\Bbbk_2}(\mathrm{S}_6) = 2$. For instance, we have $\mathrm{S}_6 \leq \mathrm{Cr}_2(\Bbbk_5)$ by [7, Theorem 47(vi)], while $\operatorname{ed}_{\Bbbk_5}(\mathrm{S}_6) = 3$.

In conclusion, the value of $\operatorname{ed}_{\Bbbk_2}(\mathrm{S}_6)$ remains unknown, as far as we are aware. In the case that this value is 2, the three steps proposed above might be helpful to prove this result. However, we do acknowledge that they would require some strong improvements to be actually fruitful. One might also take the final remarks against $\operatorname{ed}_{\Bbbk_2}(\mathrm{S}_6)$ equalling 2 into account when deciding to attempt to prove one or the other.

Bibliography

[1] V. S. Adamchik and D. J. Jeffrey, *Polynomial transformations of Tschirnhaus, Bring and Jerrard*, ACM SIGSAM Bulletin, 37 (2003), pp. 90–94.

[2] N. Bourbaki, *Algebra II: Chapters 4–7*, Springer-Verlag, 2003.

[3] J. P. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Mathematica, 106 (1997), pp. 159–179.

[4] ——, *On Tschirnhaus transformations*, in Topics in Number Theory, S. D. Ahlgren, G. E. Andrews, and K. Ono, eds., no. 467 in Mathematics and Its Applications, Springer-Verlag, 1999, pp. 127–142.

[5] S. Cantat, *The Cremona group in two variables*, European Congress of Mathematics, (2012), pp. 211–225.

[6] D. A. Cox, *Galois Theory*, Pure and Applies Mathematics: A Wiley Series of Texts, Monographs and Tracts, John Wiley & Sons, 2nd ed., 2012.

[7] I. V. Dolgachev and V. A. Iskovskikh, *Finite subgroups of the plane Cremona group*, in Algebra, Arithmetic, and Geometry, vol. 1, Y. Tschinkel and Y. Zarhin, eds., no. 269 in Progress in Mathematics, Birkäuser, 1st ed., 2009, pp. 443–548.

[8] D. Eisenbud, *Commutative Algebra: with a View Toward Algebraic Geometry*, no. 150 in Graduate Texts in Mathematics, Springer-Verlag, 1st ed., 1995.

[9] U. Görtz and T. Wedhorn, *Algebraic Geometry I: Schemes with Examples and Exercises*, Vieweg+Teubner Verlag, 1st ed., 2010.

[10] R. W. Hartley, *Determination of the ternary collineation groups whose coefficients lie in the* GF(2^n), Annals of Mathematics, Second Series, 27 (1925), pp. 140–158.

[11] R. Hartshorne, *Algebraic Geometry*, no. 52 in Graduate Texts in Mathematics, Springer-Verlag, 1977.

[12] C. Hermite, *Sur l'invariant du 18^e ordre des formes du cinquième degré et sur le role qu'il joue dans la résolution de l'équation du cinquième degré, extrait de deux lettres*, Journal für die reine und angewandte Mathematik, 59 (1861), pp. 304–305.

[13] D. Hilbert, *Mathematische Probleme*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, 7 (1900), pp. 253–297.

[14] ——, *Über die Gleichung neunten Grades*, Mathematische Annalen, 97 (1927), pp. 243–250.

[15] C. U. Jensen, A. Ledet, and N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, no. 45 in Mathematical Sciences Research Institute Publications, Cambridge University Press, 2002.

[16] P. Joubert, *Sur l'équation du sixième degré*, Comptes rendus hebdomadaires des séances de l'Académie des science, 64 (1867), pp. 1025–1029.

[17] M. Kang, *Essential dimension of finite groups*, ArXiv e-prints, arXiv:math/0611673v2 (2006).

[18] F. Klein, *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*, Dover Publications, revised 2nd ed., 1956.

[19] S. Lang, *Algebra*, no. 211 in Graduate Texts in Mathematics, Springer-Verlag, revised 3rd ed., 2002.

[20] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, no. 6 in Oxford Graduate Texts in Mathematics, Oxford University Press, 2006.

[21] J. Lüroth, *Beweis eines Satzes über rationale Curven*, Mathematische Annalen, 9 (1875), pp. 163–165.

[22] U. C. Merzbach and C. B. Boyer, *A History of Mathematics*, John Wiley & Sons, 3rd ed., 2011.

[23] P. J. Nahin, *An Imaginary Tale: The Story of* $\sqrt{-1}$, Princeton University Press, 1998.

[24] J. Ohm, *On subfields of rational function fields*, Archiv der Mathematik, 42 (1984), pp. 136–138.

[25] H. W. Richmond, *Note on the invariants of a binary sextic*, The Quarterly Journal of Pure and Applied Mathematics, 31 (1900), pp. 57–59.

[26] J. Salazar, *The repesentability hierarchy and Hilbert's 13th problem.* `https://math.uchicago.edu/~may/REU2016/REUPapers/Salazar.pdf`, 2016.

[27] J.-P. Serre, *Local Fields*, no. 67 in Graduate Texts in Mathematics, Springer-Verlag, 1st ed., 1979.

[28] The Stacks project authors, *The Stacks project.* `https://stacks.math.columbia.edu`, 2018.

[29] C. Urech and S. Zimmermann, *A new presentation of the plane Cremona group*, ArXiv e-prints, arXiv:1802.02735v1 (2018).

[30] B. L. van der Waerden, *Moderne Algebra*, vol. 1, Springer-Verlag, 1930.

[31] E. W. von Tschirnhaus, *A method for removing all intermediate terms from a given equation*, Acta Eruditorum, 2 (1683), pp. 204–207.

[32] O. Zariski, *On Castelnuovo's criterion of rationality* $p_a = p_2 = 0$ *of an algebraic surface*, Illinois Journal of Mathematics, 2 (1958), pp. 303–315.