Abstract

Let K be an algebraically closed field and $\mathbb{A}^n \cong K^n$ affine n-space. It is known that a finite group $\mathfrak{G}$ can only act freely on $\mathbb{A}^n$ if K has characteristic $p > 0$ and $\mathfrak{G}$ is a p-group. In that case the group action is "non-linear" and the ring of regular functions $K[\mathbb{A}^n]$ must be a *trace-surjective* $K - \mathfrak{G}$-algebra.

Now let k be an arbitrary field of characteristic $p > 0$ and let G be a finite p-group. In this paper we study the category $\mathfrak{Ts}$ of all finitely generated trace-surjective $k - G$ algebras. It has been shown in [**13**] that the objects in $\mathfrak{Ts}$ are precisely those finitely generated $k - G$ algebras A such that $A^G \leq A$ is a Galois-extension in the sense of [**7**], with faithful action of G on A. Although $\mathfrak{Ts}$ is not an abelian category it has "s-projective objects", which are analogues of projective modules, and it has (s-projective) categorical generators, which we will describe explicitly. We will show that s-projective objects and their rings of invariants are retracts of polynomial rings and therefore regular UFDs. The category $\mathfrak{Ts}$ also has "weakly initial objects", which are closely related to the essential dimension of G over k. Our results yield a geometric structure theorem for free actions of finite p-groups on affine k-varieties. There are also close connections to open questions on retracts of polynomial rings, to embedding problems in standard modular Galois-theory of p-groups and, potentially, to a new constructive approach to homogeneous invariant theory.

Free actions of p-groups on affine varieties in characteristic p

By Peter Fleischmann, Chris Woodcock

School of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury

(*Received*)

0. *Introduction*

Let k be a field, $\mathfrak{G}$ a finite group and X a k-variety. The following beautiful argument appears in Serre's paper "How to use finite fields for problems concerning infinite fields" ([27]). Unable to express it any better we quote almost verbatim:

" Suppose that $\mathfrak{G}$ acts freely on X. There is a Cartan-Leray spectral sequence (... of étale cohomology...) $H^i(\mathfrak{G}, H^j(X,C)) \Rightarrow H^{i+j}(\mathfrak{G}, H^j(X/\mathfrak{G}, C))$, where C is any finite abelian group. If X is the affine n-space $\mathbb{A}^n$ and $|C|$ is prime to $\mathrm{char}(k)$, then $H^j(X,C) = 0$ for $j > 0$ and $H^0(X,C) = C$. In that case the spectral sequence degenerates and gives $H^i(\mathfrak{G}, C) = H^i(X/\mathfrak{G}, C)$ for every i, i.e. $X/\mathfrak{G}$ has the same cohomology as the classifying space of $\mathfrak{G}$. Take now $C = \mathbb{Z}/\ell\mathbb{Z}$ and suppose that ℓ divides $|\mathfrak{G}|$. It is well known that $H^j(\mathfrak{G}, C)$ is non-zero for infinitely many j's, and that $H^j(X/\mathfrak{G}, C)$ is zero for $j > 2 \cdot \dim X$: contradiction!"

This establishes the following

Theorem 0·1. *The only finite groups which can act freely on $\mathbb{A}^n$ are the p-groups with $p = \mathrm{char}(k)$.*

Serre then poses the *Exercise*: "Let $\mathfrak{G}$ be a finite p-group with $p = \mathrm{char}(k)$. Show that there exists a free action on $\mathbb{A}^n$, provided that n is large enough."

Parts of the current article can be viewed as solving a "generic version" of this exercise. Using results from [13] we obtain the following:

Theorem 0·2. *Let $k = \overline{k}$ be an algebraically closed field of characteristic $p > 0$ and G be a finite group of order p^n. Then the group G acts freely on the affine space $\mathbf{A} \cong k^{|G|-1}$ in such a way that the following hold:*

(i) *The quotient space $\mathbf{A}/G$ is isomorphic to affine space $k^{|G|-1}$.*

(ii) *There is a (non-linear) decomposition $\mathbf{A} = \mathbf{B} \times \mathbf{C}$ such that G acts freely on $\mathbf{B} \cong k^n$ and trivially on $\mathbf{C} \cong k^{|G|-n-1}$.*

(iii) *The quotient space $\mathbf{B}/G$ is isomorphic to affine space k^n.*

Moreover we will show that the varieties $\mathbf{A}$ and $\mathbf{B}$ are *cogenerators* in the category of affine varieties with free G-action. Combining this with a structure theorem in [13] on modular Galois-extensions of finite p-groups, we obtain the following *geometric structure theorem*:

Theorem 0·3. *Let $k = \overline{k}$ be an algebraically closed field of characteristic $p > 0$ and G be a finite group of order p^n and let X be an arbitrary affine variety.*

(i) *There is an affine variety Y with free G-action such that $Y/G \cong X$.*

(ii) *Every such Y is a fibre product of the form $Y \cong X \times_{\mathbf{B}/G} \mathbf{B}$.*

(iii) *For every such Y there is a G-equivariant embedding $Y \hookrightarrow \mathbf{B}^N$ for some $N \in \mathbb{N}$ (which is the "cogenerator property" of $\mathbf{B}$).*

It turns out that free actions of p-groups on affine varieties in characteristic $p > 0$ are dualizations of group actions on affine k-algebras which are Galois ring extensions over the ring of invariants, in the sense of Auslander-Goldmann [1] or Chase-Harrison-Rosenberg [7]. In [13] we showed that for a p-group G acting faithfully on a k-algebra A in characteristic p, the extension $A \geq A^G$ is Galois if and only if the algebra A is *trace-surjective* in the sense of Definition 0·4. We then went on to develop a structure theory for such algebras and their rings of invariants. Using the results obtained there, we will prove Theorems 0·2 and 0·3 by

2010 Mathematics Subject Classification: 13A50,14L24,13B05,20C20,12F12.

studying the category of modular Galois extensions of finitely generated k-algebras, where the Galois group is a fixed finite p-group.

Let $\mathfrak{G}$ be an arbitrary finite group, k a field and A a commutative k-algebra on which $\mathfrak{G}$ acts by k-algebra automorphisms; then we call A a $k-\mathfrak{G}$ algebra. Let $A^{\mathfrak{G}} := \{a \in A \mid ag = a\ \forall g \in \mathfrak{G}\}$ be the *ring of invariants* and let $\mathrm{tr} := \mathrm{tr}_{\mathfrak{G}} :\ A \to A^{\mathfrak{G}},\ a \mapsto \sum_{g\in\mathfrak{G}} ag$ be the *transfer map* or *trace map*. This is obviously a homomorphism of $A^{\mathfrak{G}}$-modules, but not of k-algebras. As a consequence the image $\mathrm{tr}(A) \trianglelefteq A^{\mathfrak{G}}$ is an ideal in $A^{\mathfrak{G}}$.

DEFINITION 0·4. *A $k-\mathfrak{G}$ algebra A such that $\mathrm{tr}(A) = A^{\mathfrak{G}}$ will be called a* **trace-surjective** *$k-\mathfrak{G}$-algebra. With $\mathfrak{Ts} := \mathfrak{Ts}_{\mathfrak{G}}$ we denote the category of all finitely generated trace-surjective $k-\mathfrak{G}$-algebras, with morphisms being $\mathfrak{G}$-equivariant homomorphisms of k-algebras. For $A, B \in \mathfrak{Ts}$ the set of morphisms $\phi :\ A \to B$ will be denoted by $\mathfrak{Ts}(A, B)$.*

We are grateful to an anonymous referee for pointing out to us that there is in fact a deeper analogy between free $\mathfrak{G}$ actions on affine varieties and faithful $\mathfrak{G}$-actions up to birational isomorphism (or, equivalently, finitely generated field extensions K/k with $\mathfrak{G}$-action). The latter can also be organized into a category, $R\mathfrak{G}$ which has been studied by many authors (e.g. see [**24**] (subsection 1.3) or [**25**] (subsection 2.4,2.6).
While the duality between free actions of finite groups on varieties and Galois-extensions of corresponding coordinate rings over their ring of invariants is true for any finite group, the identification with trace-surjective algebras is only valid for finite p-groups. Indeed, if $1 < |G|$ is coprime to $p = \mathrm{char}(k)$, then every linear G-action is trace-surjective, but not free. This special role of p-groups with regard to free group actions was a major motivation for the investigations in this paper. However, some of our results and aspects of the theory developed for p-groups have natural generalizations to arbitrary finite groups, where they lead to the notion of "p-local Galois extensions" or "p-locally free group actions". For initial steps in this direction see [**15**].
The category $\mathfrak{Ts}$ contains *weakly initial* objects $\mathfrak{W} \in \mathfrak{Ts}$ satisfying $\mathfrak{Ts}(\mathfrak{W}, A) \neq \emptyset$ for any $A \in \mathfrak{Ts}$. If G is a finite p-group, then every algebra $A \in \mathfrak{Ts}$ turns out to be an extension by invariants of a quotient of $\mathfrak{W}$ of the form $A^G \otimes_{\mathfrak{W}^G} \mathfrak{W}$. Although the category $R\mathfrak{G}$ does not have weakly initial objects, it contains analogues that some authors call "versal" or "strongly versal", referring to a G-variety X with faithful G-action, which admits a G-equivariant dominant rational map $V \to X$ for some linear action of G on a vector space V. For the notion of "versality" see [**26**] section 5. Strong versality is defined and studied in [**11**], where the term "very versal" is used in place of "strongly versal".

The category $\mathfrak{Ts}$ is not abelian. However, it has finite coproducts given by tensor products of k-algebras. With the help of these one can define analogues of projective modules, which we call "s-projective objects", because projectivity is defined using surjective maps rather than epimorphisms. There are also analogues of generators in module categories and we will give explicit descriptions of s-projective generators. These arise in (homogeneous) modular invariant theory as dehomogenized symmetric algebras of suitable linear representations, such as the regular representation. Let $S \hookrightarrow T$ be an extension of k-algebras, then S is a *retract* of T if $T = S \oplus I$ with *ideal* $I \trianglelefteq T$. We will show that s-projective objects and their rings of invariants are retracts of polynomial rings and therefore regular Unique Factorization Domains (UFDs) (see [**10**] Proposition 1.8).
From now on let k be an arbitrary field of characteristic $p > 0$ and G a finite p-group, whereas $\mathfrak{G}$ will be used to denote a general finite group. We will adopt the following definitions and notations, often used in affine algebraic geometry:

DEFINITION 0·5. *Let R be a k-algebra and $n \in \mathbb{N}$.*
(i) *With $R^{[n]}$ we denote the polynomial ring $R[T_1, \cdots, T_n]$ over R.*
(ii) *Let $\mathbb{P} = k[T_1, \cdots, T_m] \cong k^{[m]}$ and $G \leq \mathrm{Aut}_k(\mathbb{P})$. Then $\mathbb{P}$ is called* **triangular** *(with respect to the chosen generators $T_1, \cdots, T_m$), if for every $g \in G$ and $i = 1, \cdots, m$ there is $f_{g,i}(T_1, \cdots, T_{i-1}) \in k[T_1, \cdots, T_{i-1}]$ such that $(T_i)g = T_i + f_{g,i}(T_1, \cdots, T_{i-1})$.*
(iii) *Let $m \in \mathbb{N}$, then a k-algebra R is called* **(m-) stably polynomial** *if $T := R \otimes_k k^{[m]} \cong R^{[m]} \cong k^{[N]}$ for some $N \in \mathbb{N}$. Assume moreover that R is a $k-G$ algebra and T extends the G-action on R trivially, i.e. $T \cong R \otimes_k F$ with $F = F^G \cong k^{[m]}$. If T is triangular, then we call R* **(m-) stably triangular**.

In order to describe the results of this paper in more detail, we need to refer to some definitions and results obtained in [**13**]:

Let G be a finite group of order p^n with regular representation $V_{reg} \cong kG$ and let D_k be the dehomogenization of the symmetric algebra $\mathrm{Sym}(V_{reg}^*)$, as defined in [**13**] (see also Section 1 shortly after Theorem 1·8). It is known that a graded algebra and its dehomogenizations share many interesting properties (see e.g. [**4**] pg. 38 and the exercises 1.5.26, 2.2.34, 2.2.35 loc. cit.) Clearly the algebra $D_k \in \mathfrak{Ts}$ is a polynomial ring of Krull-dimension $|G| - 1$ with triangular G-action.

The following Theorem was one of the main results of [13]:

THEOREM 0·6 ([13] Theorems 1.1-1.3). *There exists a trace-surjective triangular G-subalgebra $U := U_G \leq D_k$, such that $U \cong k^{[n]}$ is a retract of D_k, i.e. $D_k = U \oplus I$ with a G-stable* ideal *$I \trianglelefteq D_k$. Moreover: $U^G \cong k^{[n]}$ and $D_k^G \cong k^{[|G|-1]}$.*

For any $k-G$-algebra $A \in \mathfrak{Ts}$ and $\ell \in \mathbb{N}$ we define $A^{\otimes \ell} := \coprod_{i=1}^{\ell} A := A \otimes_k \cdots \otimes_k A$ with ℓ copies of A involved. The following are main results of the present paper:

THEOREM 0·7. *Let $\Gamma \cong k^{[d]} \in \mathfrak{Ts}$ with triangular G-action, e.g. $\Gamma \in \{D_k, U\}$. Then*
(i) *Γ is an s-projective generator in the category $\mathfrak{Ts}$.*
(ii) *For any $A \in \mathfrak{Ts}$ there is a G equivariant isomorphism $A \otimes_k \Gamma \cong A \otimes_k k[T_1, \cdots, T_d] \cong A^{[d]}$, which is the identity on A, with*

$$k[T_1, \cdots, T_d] \leq (A \otimes_k \Gamma)^G \cong (A^G)^{[d]}.$$

(iii) *$\Gamma^{\otimes \ell} \cong \Gamma \otimes_k k[s_1, \cdots, s_N]$ with $k^{[N]} \cong k[s_1, \cdots, s_N] \leq (\Gamma^{\otimes \ell})^G$.*
(iv) *For every ℓ the ring of invariants $(\Gamma^{\otimes \ell})^G$ is stably polynomial.*
(v) *If $\Gamma \in \{D_k, U\}$, then $(\Gamma^{\otimes \ell})^G$ is a polynomial ring.*

Proof. (1),(2) and (3): It follows from Proposition 2·9 that Γ is "erasable" (see Definition 2·8), which by Theorem 2·11 implies that Γ is an s-projective generator in $\mathfrak{Ts}$.
(4): This follows from Theorem 2·13.
(5): This follows from Corollary 2·14. □

The above results on rings in $\mathfrak{Ts}$ having polynomial, stably polynomial or retract-polynomial rings of invariants have analogues in the category $R\mathfrak{G}$: they appear in the form of invariant fields being rational, stably rational and retract rational, respectively. In the case where $X \in R\mathfrak{G}$ is strongly versal, retract rationality of $k(X)^{\mathfrak{G}}$ is equivalent to the existence of a "generic polynomial" for $\mathfrak{G}$ (for details, see [17], Section 5.2. e.g. Theorem 5.2.3. pg.99).]

THEOREM 0·8. *Let $\mathcal{P} \in \mathfrak{Ts}$ be s-projective*[1] *then both, $\mathcal{P}$ and $\mathcal{P}^G$ are retracts of polynomial rings over k.*

Proof. See Theorem 2·16. □

It follows from [10] Proposition 1.8 that retracts of a unique factorization domain (UFD) are UFDs as well and from [10] Corollary 1.11 that retracts of regular rings are regular. Hence

COROLLARY 0·9. *Let $\mathcal{P} \in \mathfrak{Ts}$ be s-projective, then both, $\mathcal{P}$ and $\mathcal{P}^G$ are regular UFDs.*

Setting $\mathbf{A} := \max-\operatorname{spec}(D_k)$ and $\mathbf{B} := \max-\operatorname{spec}(U)$ with $\mathbf{A}/G \cong \max-\operatorname{spec}(D_k^G)$ and $\mathbf{B}/G \cong \max-\operatorname{spec}(U^G)$ it is clear now how to obtain Theorems 0·2 and 0·3 (3) from Theorems 0·6 and 0·7. The statements in 0·3 (1) and (2) follow from

THEOREM 0·10 ([13] Theorem 1.2). *Every algebra $A \in \mathfrak{Ts}$ with given ring of invariants $A^G = R$ is of the form*

$$A \cong R[Y_1, \cdots, Y_n]/(\sigma_1(\underline{Y}) - r_1, \cdots, \sigma_n(\underline{Y}) - r_n)$$

with suitable $r_1, \cdots, r_n \in R$, and G-action derived from the action on U.

Let V be a finite dimensional k-vector space, $\mathfrak{G} \leq \mathrm{GL}(V)$ a finite group and $S(V^*) := \mathrm{Sym}(V^*)$ the symmetric algebra over the dual space V^* with induced linear $\mathfrak{G}$-action. One of the main objectives of (homogeneous) invariant theory is the study of the structure of the ring of invariants $S(V^*)^{\mathfrak{G}}$. By a result of Serre ([3]) these rings are regular (and then polynomial, as they are graded rings) only if the group $\mathfrak{G}$ is generated by pseudo-reflections. If $\mathrm{char}(k)$ does not divide $|\mathfrak{G}|$, the converse also holds by the well-known theorem of Chevalley-Shephard-Todd and Serre(see e.g. [9] or [28]). If $\mathfrak{G} = G$ is a p-group in characteristic $p > 0$, all pseudo-reflections are transvections of order p, so if G is not generated by elements of order p the ring $S(V^*)^G$ can never be regular. In this case $S(V^*)^G$ can have a very complicated structure and, in most cases, will not even be Cohen-Macaulay. If $A \in \mathfrak{Ts}$, then obviously $S(V^*) \otimes_k A \in \mathfrak{Ts}$. Using the universal property of polynomial rings one can show that for every k-G-algebra $S \cong k^{[d]}$ with triangular G-action, the k-G algebra $S \otimes_k \mathcal{P}$ is s-projective in $\mathfrak{Ts}$, whenever $\mathcal{P}$ is. In particular $S \otimes_k \mathcal{P}$ and $(S \otimes_k \mathcal{P})^G$ are retracts of polynomial rings and therefore regular UFDs.

[1] see Definition 2·1

In [10], the question was asked whether retracts of polynomial rings are again polynomial rings. Despite some positive answers in low-dimensional special cases (see [29]) this question was unanswered for several decades. Recently S. Gupta ([16]) found a counterexample to the "cancellation problem" in characteristic $p > 0$, which also implies a negative answer in general to Costa's question. Gupta's example yields a non-polynomial retract R of a polynomial ring, which however is still stably polynomial. Using Theorem 0·10 one can easily construct $A \in \mathfrak{Ts}$ with $A^G \cong R$, such that A is s-projective. So there are s-projective objects in $\mathfrak{Ts}$ with non-polynomial invariant rings. If all retracts of polynomial rings were *stably* polynomial, then this would be true for arbitrary s-projective objects in $\mathfrak{Ts}$ and their invariant rings. This is our main reason for the following

QUESTION 0·1. *Are $\mathcal{P}$ and $\mathcal{P}^G$ stably polynomial rings for every s-projective $\mathcal{P} \in \mathfrak{Ts}$?*

For $\mathcal{P} = D_k$ or U this is already contained in Theorem 0·6 and for $\mathcal{P} = S \otimes D_k$ or $\mathcal{P} = S \otimes U$ with triangular $k - G$ algebra $S \cong k^{[d]}$ it follows from 2·10. From this one can derive a result that includes "graded modular rings of invariants", for which we don't know any other reference in the literature:

THEOREM 0·11. *Let $S \cong k^{[d]}$ be a polynomial ring with triangular G-action (e.g. $S = S(V^*)$). Then the ring of invariants S^G is the intersection of two polynomial subrings inside an s-projective polynomial $k-G$-algebra $k^{[N]} \in \mathfrak{Ts}$ of Krull-dimension $N = d + n$ with $n := \log_p |G|$. If moreover $S \in \mathfrak{Ts}$, then $S^G \otimes_k k^{[n]} \cong k^{[n+d]}$, i.e. S^G is n-stably polynomial.*

Proof. See Theorem 2·17. The proof will show that the intersection S^G can be obtained by a procedure of "elimination of variables". □

A special role in the category $\mathfrak{Ts}$ is played by "minimal universal" or "basic" algebras, which are investigated in Sections 3 and 4. They turn out to be integral domains of the same Krull-dimension $d_k(G)$, an invariant depending only on the group G and the field k. The analogues in the category $R\mathfrak{G}$ are the strongly versal varieties of minimal dimension. This minimal dimension is the essential dimension $e_k(\mathfrak{G})$ as defined by Buhler and Reichstein ([5]) and we will see that $d_k(G)$ provides an upper bound for $e_k(G)$.
The following is one of the main results of these sections: (See Section 4 and Theorem 4·4 for details and precise definitions).

THEOREM 0·12. *Let $\mathrm{char}(k) = p > 0$ and G be a group of order p^n. The minimal universal objects $\mathfrak{U} \in \mathfrak{Ts}$ are integral domains of Krull dimension $d_k(G)$, satisfying $e_k(G) \le d_k(G) \le n$. Moreover, "essential G-fields" of transcendence degree $e_k(G)$ appear among the "embedded residue class fields" $k(\wp) \hookrightarrow \mathrm{Quot}(\mathfrak{U})$ of $\mathfrak{U}$ with respect to suitable G-stable prime ideals $\wp \trianglelefteq \mathfrak{U}$.*

The rest of the paper is organized as follows: In *Section one* we describe the connection between free actions of a finite group on affine varieties and Galois extensions of rings. In particular for normal varieties we formulate a freeness-criterion in terms of the Dedekind different (Corollary 1·6). We will also introduce some basic notation and describe results from previous work, which will be needed in the sequel. From there on, k will always be a field of characteristic $p > 0$ and G will be a finite p-group. In *Section two* we introduce and analyze the *universal*, *projective* and *generating* objects in $\mathfrak{Ts}$. We also introduce the notion of *erasable* algebras, which will lead to proofs of the main results, Theorems 0·7, 0·8 and 0·11. In *Section three* we turn our attention to *basic* algebras, which we define as *minimal* universal algebras in $\mathfrak{Ts}$. We classify all basic algebras which are also normal rings, in the case where G is elementary-abelian of rank n and $\dim_{\mathbb{F}_p}(k) \ge n$. They all turn out to be univariate polynomial algebras with explicitly described non-linear G-action. Moreover, in this case the basic normal algebras in $\mathfrak{Ts}$ coincide with the minimal normal generators and minimal normal s-projective objects (see Theorem 3·15). The connection between basic algebras and the essential dimension of G over k and the proof of Theorem 0·12 is the topic of the short *Section four*. Most of the results here are known, at least for fields of characteristic zero or algebraically closed fields. Our contribution consists in some new ways of proving them as well as proposing new models for essential G-fields via basic objects in $\mathfrak{Ts}$ (see Theorem 0·12).
The brief final *Section five* contains an open question and a conjecture.

1. *Free affine actions and Galois-extensions*

Free group actions on affine varieties are closely related to Galois ring extensions, as we will now demonstrate. First let $\mathfrak{G}$ be an arbitrary finite group and A a finitely generated commutative $k - \mathfrak{G}$ algebra. We want to keep flexibility between left and right group actions; therefore in whatever way the "natural side" of the action is chosen, we will use the rule $gf := f \cdot g^{-1}$ to switch freely between left and right actions when convenient. [2]

Set $B := A^{\mathfrak{G}}$ and define $\Delta := \mathfrak{G} \star A = A \star \mathfrak{G} := \oplus_{g\in\mathfrak{G}} d_g A$ to be the crossed product of $\mathfrak{G}$ and A with $d_g d_h = d_{gh}$ and $d_g a = g(a) \cdot d_g = (a)g^{-1} \cdot d_g$ for $g \in \mathfrak{G}$ and $a \in A$. Let ${}_BA$ denote A as left B-module, then there is a homomorphism of rings

$$\rho:\ \Delta \to \mathrm{End}({}_BA),\ ad_g \mapsto \rho(ad_g) = (a' \mapsto a \cdot g(a') = a \cdot (a')g^{-1}).$$

One calls $B \leq A$ a *Galois-extension* with group $\mathfrak{G}$ if ${}_BA$ is finitely generated projective and ρ is an isomorphism of rings. This definition goes back to Auslander and Goldmann [1] (Appendix, pg.396) and generalizes the classical notion of Galois field extensions. It also applies to non-commutative $k - \mathfrak{G}$ algebras, but if A is commutative, this definition of 'Galois-extension' coincides with the one given by Chase-Harrison-Rosenberg in [7], where the extension of commutative rings $A^{\mathfrak{G}} \leq A$ is called a Galois-extension if there are elements $x_1, \cdots, x_n,\ y_1, \cdots, y_n$ in A such that

$$\sum_{i=1}^{n} x_i(y_i)g = \delta_{1,g} := \begin{cases} 1 & \text{if g=1} \\ 0 & \text{otherwise.} \end{cases} \tag{1·1}$$

In [7] the following has been shown:

THEOREM 1·1. *(Chase-Harrison-Rosenberg)*[7] *$A^{\mathfrak{G}} \leq A$ is a Galois extension if and only if for every $1 \neq \sigma \in \mathfrak{G}$ and maximal ideal* p *of A there is $s := s(\mathrm{p}, \sigma) \in A$ with $s - (s)\sigma \notin \mathrm{p}$.*

Now, if X is an affine variety over the algebraically closed field k, with $\mathfrak{G} \leq \mathrm{Aut}(X)$ and $A := k[X]$ (the ring of regular functions), then for every maximal ideal $\mathrm{m} \trianglelefteq A$, $A/\mathrm{m} \cong k$. Hence if $(\mathrm{m})g = \mathrm{m}$, then $a - (a)g \in \mathrm{m}$ for all $a \in A$. Therefore we conclude

THEOREM 1·2. *The finite group $\mathfrak{G}$ acts freely on X if and only if $k[X]^{\mathfrak{G}} \leq k[X]$ is a Galois-extension.*

If $B \leq A$ is a Galois-extension, then it follows from equation (1·1), that $\mathrm{tr}(A) = A^{\mathfrak{G}} = B$ (see [7], Lemma 1.6), so A is a *trace-surjective* $k - \mathfrak{G}$ algebra. It also follows from Theorem 1·1, that for a p-group G and k of characteristic p, the algebra A is trace-surjective if and only if $A \geq A^G = B$ is a Galois-extension (see [13] Corollary 4.4.). Using Theorem 0·1 we obtain

COROLLARY 1·3. *Let k be algebraically closed. Then the finite group $\mathfrak{G}$ acts freely on $X \cong \mathbb{A}^n$ if and only if $\mathfrak{G}$ is a p-group with $p = \mathrm{char}(k)$ and $k[X]$ is a trace-surjective $k - \mathfrak{G}$ algebra.*

Since for p-groups in characteristic p the trace-surjective algebras coincide with Galois-extensions over the invariant ring, we obtain from Theorem 1·2:

COROLLARY 1·4. *If k is an algebraically closed field of characteristic $p > 0$, X an affine k-variety and G a finite p-group, then G acts freely on X if and only if $A = k[X] \in \mathfrak{Ts}$.*

Any finite p-group G can be realized as a subgroup of some $\mathrm{SL}_n(k)$. The left multiplication action of G on $\mathrm{Mat}_n(k)$ induces a homogeneous right regular action on the coordinate ring $k[M] := k[\mathrm{Mat}_n(k)] \cong k[X_{ij} \mid 1 \leq i,j \leq n]$ with $\det := \det(X_{ij}) \in k[M]^G$. It can be shown that $\det \in \sqrt{\mathrm{tr}(k[M])}$, in other words $\mathrm{tr}(f) = (\det)^N$ for some $N \in \mathbb{N}$ and some $f \in k[M]$. It follows that the coordinate ring $k[\mathrm{GL}_n] = k[M][1/\det]$ is a trace-surjective G-algebra. Since epimorphic images of trace-surjective algebras are again trace-surjective (see Theorem 1·8 (iii)), a similar conclusion holds if GL_n is replaced by an arbitrary closed linear algebraic subgroup H containing G (see [13] Corollary 4.5, where this is proved in a different way). In particular, if $H = \mathbf{U}$ is a connected unipotent subgroup with $\mathbf{U} \cong \mathbb{A}^n$, then we obtain the free G-action asked for in Serre's exercise.

In the case of a normal affine variety, associated to an affine $k - \mathfrak{G}$ algebra which is also a normal noetherian domain, there is a nice and useful characterization of Galois-extensions in terms of the Dedekind-different.[3] Set $B := A^{\mathfrak{G}}$ and $A^\vee := \mathrm{Hom}_B({}_BA, B)$. Then $A^\vee$ is an A-module via $a \cdot \lambda(a') = \lambda(a'a)$ for $a, a' \in A$ and $\lambda \in A^\vee$. Moreover $A^\vee$ is an A-submodule of $\mathrm{End}({}_BA)$ and for $\mathfrak{G}^+ := \sum_{g\in\mathfrak{G}} d_g \in \Delta$ we have $\rho(\mathfrak{G}^+ \cdot a)(a') =$

[2] If A is an algebra of k-valued functions on a $\mathfrak{G}$-set X, (e.g. $A = k[X]$, the algebra of regular functions on a variety X with $\mathfrak{G} \leq \mathrm{Aut}(X)$) there is a natural right action of $\mathfrak{G}$ on A given by composition $f \circ g$ for $g \in \mathfrak{G}$. In other situations we might have a given linear left $\mathfrak{G}$-action defined on a k-vector space $\Omega := \sum_{i=1}^m k\omega_i$. This extends to a natural *left* action on the symmetric algebra $\mathrm{Sym}_k(\Omega) = k[\omega_1, \cdots, \omega_m]$ by $g(\omega_1^{e_1} \cdots \omega_m^{e_m}) := (g\omega_1)^{e_1} \cdots (g\omega_m)^{e_m}$.

[3] which in the circumstances considered coincides with E Noether's "homological different".

$\mathrm{tr}(aa') = (a \cdot \mathrm{tr})(a')$, so $\rho(\mathfrak{G}^+ \cdot A) = A \cdot \mathrm{tr} \subseteq A^\vee$. If in addition A is a normal noetherian domain, then we define $\mathcal{D}_{A,B}^{-1} := \{x \in \mathrm{Quot}(A) \mid \mathrm{tr}_{\mathfrak{G}}(xA) \subseteq B\}$, the inverse of the Dedekind-different. In this case the field extension $\mathbb{L} := \mathrm{Quot}(A) \geq \mathbb{K} := \mathrm{Quot}(B) = \mathbb{L}^{\mathfrak{G}}$ is Galois, so normal and separable, and it follows that the map $\theta : \mathcal{D}_{A,B}^{-1} \to A^\vee, \ x \mapsto \mathrm{tr}(x())$ is an isomorphism of (divisorial) A-modules.

PROPOSITION 1·5. *Let A be a noetherian normal domain and $\mathfrak{G} \leq \mathrm{Aut}(A)$ a finite group of ring automorphisms with ring of invariants $B := A^{\mathfrak{G}}$. Then the following are equivalent:*
(i) *$B \leq A$ is a Galois-extension;*
(ii) *${}_BA$ is projective and $A^\vee := \mathrm{Hom}\,({}_BA, {}_BB) = A \cdot \mathrm{tr}_{\mathfrak{G}}$.*
(iii) *${}_BA$ is projective and $\mathcal{D}_{A,B} = A$ (or $\mathcal{D}_{A,B}^{-1} = A$).*

Proof. "(1) ⇒ (2)": By assumption $\rho : \ \Delta \to \mathrm{End}({}_BA)$ is an isomorphism. For any $\lambda \in A^\vee$ we have $\lambda = \rho(d)$ with $d := \sum_{g\in\mathfrak{G}} a_g \cdot d_g \in \Delta$. Then $\lambda(a) = \sum_{g\in\mathfrak{G}} a_g g(a) \in A^{\mathfrak{G}}$, hence for every $h \in \mathfrak{G}$, $\sum_{g\in\mathfrak{G}} h(a_g)hg(a) = \sum_{g\in\mathfrak{G}} a_g g(a)$, which implies

$$\sum_{g\in\mathfrak{G}} h(a_g) d_{hg} = \sum_{g\in\mathfrak{G}} a_g d_g \in \Delta$$

and therefore $h(a_1) = a_h$. We get $d = \sum_{g\in\mathfrak{G}} g(a_1) d_g = \sum_{g\in\mathfrak{G}} d_g \cdot a_1 = \mathfrak{G}^+ \cdot a_1 \in \mathfrak{G}^+ \cdot A$. Hence $A^\vee \subseteq \rho(\mathfrak{G}^+ \cdot A) = A \cdot \mathrm{tr}_{\mathfrak{G}} \subseteq A^\vee$.
"(2) ⇒ (1) ": Since the field extension $\mathbb{L} \geq \mathbb{K} = \mathbb{L}^{\mathfrak{G}}$ is Galois, the map

$$\rho \otimes_B \mathbb{K} : \ \Delta \otimes_B \mathbb{K} \to \mathrm{End}({}_BA) \otimes_B \mathbb{K} = \mathrm{End}({}_{\mathbb{K}}\mathbb{L})$$

is an isomorphism, so ρ is injective. Since ${}_BA$ is finitely generated and projective, the map $\gamma^\vee : \ A \otimes_B A^\vee \to \mathrm{End}({}_BA), \ a \otimes \lambda \mapsto a \cdot \lambda() = (a' \mapsto a \cdot \lambda(a'))$ is surjective (and bijective). Hence $\rho(\Delta) \supseteq \rho(A\mathfrak{G}^+A) = \gamma^\vee(A \otimes_B \mathfrak{G}^+A) = \mathrm{End}({}_BA)$, so ρ is surjective and therefore bijective.
"(2) $\iff$ (3)": Consider the isomorphism $\theta : \ \mathcal{D}_{A,B}^{-1} \to A^\vee, \ x \mapsto \mathrm{tr}(x())$. Then $A^\vee = A \cdot \mathrm{tr}_{\mathfrak{G}}$ if and only if for every $x \in \mathcal{D}_{A,B}^{-1}$ there is $a \in A$ with $\theta(x) = \theta(a)$, i.e. $\mathcal{D}_{A,B}^{-1} \subseteq A$, which is equivalent to $\mathcal{D}_{A,B}^{-1} = A$ (since $A \subseteq \mathcal{D}_{A,B}^{-1}$ is always true) and equivalent to $\mathcal{D}_{A,B} = A$. □

COROLLARY 1·6. *Let k be algebraically closed and X be a normal irreducible k-variety (so $A := k[X]$ is a normal domain). Then the following are equivalent:*
(i) *$\mathfrak{G}$ acts freely on X;*
(ii) *${}_{A^{\mathfrak{G}}}A$ is projective and $\mathcal{D}_{A,A^{\mathfrak{G}}} = A$ (or $\mathcal{D}_{A,A^{\mathfrak{G}}}^{-1} = A$).*

In the rest of this section we will recapitulate notation and results from earlier papers, which will be used in the sequel. For a finitely generated commutative k-algebra A we will denote by $\mathrm{Dim}\,(A)$ the *Krull-dimension* of A. For a k-vector space V we will denote with $\dim\,(V) = \dim_k(V)$ the k-dimension of that space. So $\mathrm{Dim}\,(A) = 0 \iff \dim\,(A) < \infty$.

DEFINITION 1·7. *Let $A \in \mathfrak{Ts}$, then an element $a \in A$ with $\mathrm{tr}(a) = 1$ is called a* **point** *in A.*

In [13] Theorem 4.1 and Proposition 4.2 the following general result has been shown:

THEOREM 1·8. *Let A be trace-surjective and $a \in A$ be a point, then:*
(i) *$A = \oplus_{g\in G} A^G \cdot (a)g$ is a free A^G-module with basis $\{(a)g \mid g \in G\}$ and also a free $A^G[G]$ module of rank one, where $A^G[G]$ denotes the group ring of G over A^G.*
(ii) *If $S := k[(a)g \mid g \in G] \leq A$ is the subalgebra generated by the G-orbit of the point a, then $A = A^G \otimes_{S^G} S$.*

REMARK 1·9. *Note that Theorem 1·8 (2) is a special case of the "no-name lemma" for Galois ring extensions (see e.g.[23], Lemma 9.4.1). If $\mathfrak{G}$ is not a p-group, this statement is false for general trace-surjective algebras as the following example shows:*
Let $\mathfrak{G}$ be the natural semidirect product $\mathfrak{G} = U \rtimes C$ with $U = \mathbb{F}_p$ and $C = \mathbb{F}_p^*$, acting on $A := k[X]$ by $f(X)^{(a,b)} = f(a + bX)$. Then $A^U = k[X^p - X]$ and $A^{\mathfrak{G}} = (A^U)^C = k[(X^p - X)^{p-1}]$. The subalgebra $B := k[X^p] \leq A$ is isomorphic to A in $\mathfrak{Ts}$, $A^{\mathfrak{G}}[B] = k[X^p, (X^p - X)^{p-1}] < A$.

Now let $V = V_{reg}$ and $V^* := \oplus_{g\in G} kX_g \cong kG$, with $X_g = (X_{1_G})g$, be the regular representation of G and set $S_{reg} := \mathrm{Sym}(V^*)$ (note that V^* and V are isomorphic kG-modules). Set $X := \sum_{g\in G} X_g \in S_{reg}^G$, then $V^{*G} = k \cdot X$. Following [13] Definition 2, we set $D_k := D_k(G) := S_{reg}/(\alpha)$ with $\alpha = X - 1$. Then $D_k \cong k[x_g \mid 1 \neq g \in G]$, with $x_g := \overline{X}_g$ and $\mathrm{tr}(x_1) = 1$, is a polynomial ring of Krull dimension $|G| - 1$ and there is an isomorphism of trace-surjective $k-G$-algebras $D_k \cong (S_{reg}[1/X])_0;\ x_g \mapsto X_g/X$. Moreover there is an isomorphism of $\mathbb{Z}$-graded trace-surjective algebras: $D_k[X,1/X] \to \sum_{z\in\mathbb{Z}} D_k X^z = S_{reg}[1/X]$. Taking G-invariants on both sides we obtain an isomorphism of $\mathbb{Z}$-graded k-algebras: $D_k^G[X,1/X] \cong S_{reg}^G[1/X]$. As mentioned in Theorem 0·6, there is a retract $U \le D_k$ with $U \in \mathfrak{Ts}$ such that the rings U, U^G and D_k^G are polynomial rings. We will show that the algebras D_k and U are s-projective [4]objects in $\mathfrak{Ts}$ (see Definition 2·1 and Theorem 2·19). It has been shown in [**13**] Proposition 5.5. that the Krull-dimension $\log_p(|G|)$ of U is the minimal possible number of generators for a trace-surjective subalgebra of D_k, if $k = \mathbb{F}_p$.

REMARK 1·10. *The embedding $U \hookrightarrow D_k = (S_{reg}[1/X])_0 \hookrightarrow S_{reg}[1/X]$ dualizes to a G-equivariant surjective morphism $V_{reg,X} \to \mathbf{B} = \max - \mathrm{spec}(U)$, where $V_{reg,X} \subseteq V_{reg}$ is the fundamental open set of elements not vanishing on X. Hence there is a rational map $V_{reg} \to \mathbf{B}$, which shows that the varieties $\mathbf{B}$ and $\mathbf{B}^N$ are strongly versal in the the category RG, in the sense defined in Section 0.*

2. *Universal, projective and generating objects in the category $\mathfrak{Ts}$*

From now on, unless explicitly stated otherwise, G will denote a *non-trivial* finite p-group.

The category $\mathfrak{Ts}$ is non-abelian but it has finite coproducts, given by tensor products over k. This together with the structure theorem 1·8 gives rise to the concepts of weakly initial, generating, projective and free objects, in analogy to module categories. In particular there are categorical characterizations of D_k and its standard subalgebras in $\mathfrak{Ts}$, as defined in [**13**] Definition 3, comparable to projective generators in module categories, which we are now going to develop. This was announced in [**13**] Remark 5.

Let $\mathfrak{C}$ be an arbitrary category. Then an object $u \in \mathfrak{C}$ is called *weakly initial*, if for every object $c \in \mathfrak{C}$ the set $\mathfrak{C}(u,c) := \mathrm{Mor}_{\mathfrak{C}}(u,c)$ is not empty, i.e. if for every object in $\mathfrak{C}$ there is at least one morphism from u to that object. If moreover $|\mathfrak{C}(u,c)| = 1$ for every $c \in \mathfrak{C}$, then u is called an *initial object* and is uniquely determined up to isomorphism.

An object $m \in \mathfrak{C}$ is called a *generator* in $\mathfrak{C}$, if the covariant morphism - functor $\mathrm{Mor}_{\mathfrak{C}}(m,*)$ is injective on morphism sets. In other words, m is a generator if for any two objects $x, y \in \mathfrak{C}$ and morphisms $f_1,\ f_2 \in \mathfrak{C}(x,y)$, $f_1 \ne f_2$ implies $(f_1)_* \ne (f_2)_*$, i.e. there is $f \in \mathfrak{C}(m,x)$ with $f_1 \circ f \ne f_2 \circ f$. It follows that $\mathfrak{C}(m,x) \ne \emptyset$ whenever $x \in \mathfrak{C}$ has nontrivial automorphisms. So if every object $x \in \mathfrak{C}$ has a nontrivial automorphism, then generators in $\mathfrak{C}$ are weakly initial objects. If $\mathfrak{C} = \mathfrak{Ts}_G$ then right multiplication with any $1 \ne z \in Z(G)$ is a nontrivial automorphism for every $A \in \mathfrak{Ts}$, hence every generator in $\mathfrak{Ts}_G$ is weakly initial.

Recall that in an arbitrary category $\mathfrak{C}$ an object x is called "projective" if the covariant representation functor $\mathfrak{C}(x,?) := \mathrm{Mor}_{\mathfrak{C}}(x,?)$ transforms epimorphisms into surjective maps. If $\mathfrak{C}$ is the module category of a ring, then a morphism is an epimorphism if and only if it is surjective. Therefore a module M can be defined to be projective, if $\mathrm{Mor}_{\mathfrak{C}}(M,?)$ turns surjective morphisms to surjective maps. In the category $\mathfrak{Ts}$, however, there are non-surjective epimorphisms (e.g. $A^p \hookrightarrow A$ for a domain $A \in \mathfrak{Ts}$ over a perfect field k). This leads to the slightly modified notions of "s-generators" and "s-projective objects" in the category $\mathfrak{Ts}$:

DEFINITION 2·1. *Let B be a $k-G$ algebra in $\mathfrak{Ts}$.*

(i) *B is called* **universal**, *if it is a weakly initial object in $\mathfrak{Ts}$.*

(ii) *$\Gamma \in \mathfrak{Ts}$ is an* **s-generator** *if for every $R \in \mathfrak{Ts}$ there is a surjective morphism $\Psi:\ \Gamma^{\otimes \ell} \to R$ for some $\ell \ge 1$.*

(iii) *$A \in \mathfrak{Ts}$ is called* **s-projective**, *if the covariant representation functor $\mathfrak{Ts}(A,*)$ transforms* **surjective morphisms** *into surjective maps.*

Let $a \in A$ be a point, i.e. $\mathrm{tr}(a) = 1$. Then the map $X_g \mapsto (a)g$ for $g \in G$ extends to a k-algebra homomorphism $\mathrm{Sym}(V_{reg}^*) \to A$ with $\alpha \mapsto 0$, hence it defines a unique morphism $\phi:\ D_k \to A$ with $\phi \in \mathfrak{Ts}$, mapping $x_g \mapsto (a)g$. In other words D_k has a "free point" x_e, which can be mapped to any point $a \in A \in \mathfrak{Ts}$ to define a morphism $\phi \in \mathfrak{Ts}(D_k, A)$. It is not hard to see that, due to the existence of these free points x_g, the algebra D_k is s-projective in $\mathfrak{Ts}$. The following generalization has been shown in [**14**]:

THEOREM 2·2 ([**14**] Theorem 2.8). *Let $W \to V$ be an epimorphism of finite dimensional kG-modules, $S := \mathrm{Sym}(V^*) \hookrightarrow T := \mathrm{Sym}(W^*)$ the corresponding embedding of symmetric algebras and $v^* \in (V^*)^G$. Assume that $\bar S := S/(v^*-1)S$ is in $\mathfrak{Ts}$. Then $\bar S$ is a retract of $\bar T := T/(v^*-1)T$ and $\bar T$ and $\bar S$ are s-projective objects in $\mathfrak{Ts}$.*

REMARK 2·3.

(i) *It is easy to see that every s-generator and every s-projective object is also universal.*

(ii) *Every $A \in \mathfrak{Ts}$ with $\mathfrak{Ts}(A,P) \ne \emptyset$ for some s-projective $P \in \mathfrak{Ts}$ is universal. So the universal objects are precisely the objects of $\mathfrak{Ts}$ that map to D_k.*

[4] with respect to surjective functions rather than epimorphisms

(iii) *The commutative artinian "diagonal group ring" $kG := \oplus_{g\in G} ke_g$ with $e_g e_h = \delta_{g,h} e_g$ and regular G-action is a non-universal object in $\mathfrak{Ts}$.*

The following Lemma characterizes universal objects in $\mathfrak{Ts}$ and also indicates the particular significance of this notion in that category:

LEMMA 2·4. *Let $\mathfrak{W} \in \mathfrak{Ts}$, then the following are equivalent:*
(i) *$\mathfrak{W}$ is universal;*
(ii) *$\mathfrak{W}/I \le D_k$ for some G-stable prime ideal $I \le \mathfrak{W}$;*
(iii) *every $A \in \mathfrak{Ts}$ can be written as $A \cong A^G \otimes_{SG} S$ where $S \le A$ is any subalgebra isomorphic to $\mathfrak{W}/I$ for some G-stable ideal $I \trianglelefteq \mathfrak{W}$.*
(iv) *every $A \in \mathfrak{Ts}$ is of the form $A \cong R \otimes_{\mathfrak{W}^G} \mathfrak{W}$ for some k-algebra R with trivial G-action and homomorphism $\mathfrak{W}^G \to R$.*

Proof. (1) $\iff$ (2): This has been shown above.
(1) $\Rightarrow$ (3): Let $\phi \in \mathfrak{Ts}(\mathfrak{W}, A)$ with $S := \phi(\mathfrak{W}) \le A$, then $S \cong \overline{\mathfrak{W}} := \mathfrak{W}/I$ for some G-stable ideal $I \trianglelefteq \mathfrak{W}$ and it follows from Theorem 1·8, that $A \cong A^G \otimes_{\bar{\mathfrak{W}}^G} \bar{\mathfrak{W}}$.
(3) $\Rightarrow$ (1): This follows from "(1) $\iff$ (2)" and choosing $A = D_k$. Finally, (3) and (4) are different ways of expressing the same situation. $\square$

REMARK 2·5. *The property (3) in Lemma 2·4 gives universal objects a special significance in the case of p-groups in characteristic $p > 0$, which is not present for general finite groups:*
If G is a p-group and $\mathfrak{W} \in \mathfrak{Ts}$ is universal, then every object $A \in \mathfrak{Ts}$ can be obtained from $\mathfrak{W}$ as an "extension by invariants" $A \cong R \otimes_{\mathfrak{W}^G} \mathfrak{W}$ with trivial G-action on R. So $\mathfrak{W}$ contains all information on the G-action needed to construct in principle every object in $\mathfrak{Ts}$.
If $p \not| \, |G|$, then the trivial module $k \in \mathfrak{Ts}$ is weakly initial and every finitely generated $k-G$-algebra lies in $\mathfrak{Ts}$. However, $A \cong R \otimes_{kG} k$ with trivial G-action on R can only hold if G acts trivially on A.

Let $R \in \mathfrak{Ts}$ with point $w \in R$, $w_g := (w)g$ for $g \in G$ and $R^G = k[r_1, \cdots, r_n]$, then by Theorem 1·8,

$$R = k[R^G, w_g \mid g \in G] = k[w_g, w_g + r_i \mid g \in G, i = 1, \cdots, n]$$

with $\mathrm{tr}(w_g + r_i) = \mathrm{tr}(w_g) + |G| r_i = 1$ for all $g \in G$ and $i = 1, \cdots, n$ (since $G \ne 1$). So $R = k[v_1, \cdots, v_\ell]$, with points v_i so we conclude:

LEMMA 2·6. *Every object $R \in \mathfrak{Ts}$ is generated by a finite set of points.*

Recall that the finite coproducts in $\mathfrak{Ts}$ are given by the tensor-product over k. A finite tensor product of k-G algebras lies in $\mathfrak{Ts}$ if at least one of the factors does. In particular the category $\mathfrak{Ts}$ also has finite coproducts given by the tensor-product over k. Recall that for an object $A \in \mathfrak{Ts}$ and $\ell \in \mathbb{N}$ we define

$$A^{\otimes \ell} := \coprod_{i=1}^{\ell} A := A \otimes_k A \otimes_k \cdots \otimes_k A$$

with ℓ copies of A involved. This allows for the following partial characterization of *categorical generators* in $\mathfrak{Ts}$:

LEMMA 2·7. *If Γ is an s-generator, then it is a categorical generator in $\mathfrak{Ts}$.*

Proof. Let $\alpha, \beta \in \mathfrak{Ts}(R, S)$ with $\alpha \circ \psi = \beta \circ \psi$ for all $\psi \in \mathfrak{Ts}(\Gamma, R)$. By assumption we have the following commutative diagram

$$\begin{tikzcd}
\Gamma^{\otimes \ell} \arrow[r, two heads, "\Psi"] & R \\
\Gamma \arrow[u, "\tau_i"] \arrow[ur, "\Psi_i"'] &
\end{tikzcd}$$

where τ_i maps $\gamma \in \Gamma$ to $1 \otimes \cdots \otimes \gamma \otimes \cdots \otimes 1$ and Ψ is surjective. Then $\alpha \circ \Psi \circ \tau_i = \beta \circ \Psi \circ \tau_i$ for all i, hence $\alpha \circ \Psi = \beta \circ \Psi$. Since Ψ is surjective it follows that $\alpha = \beta$, so Γ is a generator in $\mathfrak{Ts}$. $\square$

We will now give some definitions that turn out to be useful in finding criteria for s-projectivity and the s-generator property:

DEFINITION 2·8. *Let $\mathcal{E}$ be an k-G-algebra of Krull dimension N.*

(i) *$\mathcal{E}$ is said to be* **erasable**, *if for every $A \in \mathfrak{Ts}$, the tensor product $A \otimes_k \mathcal{E}$ erases the G-action on $\mathcal{E}$ in the sense that*

$$A \otimes_k \mathcal{E} = (A \otimes_k 1)[\lambda_1, \cdots, \lambda_N] \cong A^{[N]},$$

with the isomorphism being the identity on A and $k^{[N]} \cong k[\lambda_1, \cdots, \lambda_N] \subseteq (A \otimes_k \mathcal{E})^G$.

(ii) *If $\mathcal{E} \in \mathfrak{Ts}$ and isomorphism in (1) holds for $A = \mathcal{E}$, then $\mathcal{E}$ is called* **self-erasing**.

PROPOSITION 2·9. *Let $\Gamma \in \mathfrak{Ts}$ be a polynomial ring with triangular G-action. Then Γ is erasable.*

Proof. We assume that $\Gamma = k[T_1, \cdots, T_N] \in \mathfrak{Ts}$ is a polynomial ring such that for each $g \in G$ and $1 \le i \le N$ we have $(T_i)g = T_i + f_{i,g}$ with $f_{i,g} \in k[T_1, \cdots, T_{i-1}]$. Now let $A \in \mathfrak{Ts}$ and $a \in A$ with $\mathrm{tr}(a) = 1$. Then $\mathrm{tr}(aT_i) = \sum_{g \in G}(a)g \cdot (T_i)g = \sum_{g \in G}(a)g \cdot (T_i + f_{i,g}) = \mathrm{tr}(a) \cdot T_i + \sum_{g \in G}(a)g \cdot f_{i,g}$. Hence $T_i - \mathrm{tr}(aT_i) \in A[T_1, \cdots, T_{i-1}]$. Therefore an obvious induction argument shows that

$$A \otimes_k \Gamma = A[T_1, \cdots, T_N] = A[\mathrm{tr}(aT_1), \cdots, \mathrm{tr}(aT_N)],$$

so Γ is erasable. $\square$

PROPOSITION 2·10. *Let $\mathcal{E}$ be an erasable $k - G$-algebra of Krull-dimension e (not necessarily in $\mathfrak{Ts}$) and let $\mathbb{P} \in \mathfrak{Ts}$. Then the following hold:*

(i) *$\mathcal{E}^G = \mathcal{E} \cap (\mathcal{E} \otimes_k \mathbb{P})^G$ with $(\mathcal{E} \otimes_k \mathbb{P})^G \cong (\mathbb{P}^{[e]})^G \cong (\mathbb{P}^G)^{[e]}$.*

(ii) *If $\mathbb{P}^G \cong k^{[m]}$, then $(\mathcal{E} \otimes_k \mathbb{P})^G \cong k^{[e+m]}$.*

(iii) *If $\mathbb{P}$ is s-projective, then so is $\mathcal{E} \otimes_k \mathbb{P}$.*

Proof. (1) and (2): Clearly $\mathcal{E}^G = \mathcal{E} \cap (\mathcal{E} \otimes_k \mathbb{P})^G$. By definition of "erasable", $\mathcal{F} := \mathcal{E} \otimes_k \mathbb{P} \cong \mathbb{P} \otimes_k k[T_1, \cdots, T_n] \cong \mathbb{P}^{[e]}$ with $k[\underline{T}] \le \mathcal{F}^G$, hence $(\mathbb{P}^{[e]})^G \cong (\mathbb{P}^G)^{[e]}$.
(3): Let $\alpha : A \to B \in \mathfrak{Ts}$ be surjective and $\beta : \mathcal{F} = \mathbb{P}[T_1, \cdots, T_e] \to B$ be morphisms in $\mathfrak{Ts}$. Choose $\mathbf{a} := (a_1, \cdots, a_e) \in A^e$ with $\alpha(a_i) = \beta(T_i)$ and $\theta \in \mathfrak{Ts}(\mathbb{P}, A)$ with $\alpha\theta = \beta_{|\mathbb{P}}$. Then θ extends to a map

$$\tilde{\theta} : \mathcal{F} \to A, \sum_{\mu \in \mathbb{N}_0^e} p_\mu \underline{T}^\mu \mapsto \theta(p_\mu) a_1^{\mu_1} \cdots a_e^{\mu_e}$$

with $\alpha \circ \tilde{\theta} = \beta$. Since the T_i are G-invariant, $\tilde{\theta} \in \mathfrak{Ts}(\mathcal{F}, A)$, which shows that $\mathcal{F}$ is s-projective. $\square$

THEOREM 2·11. *Let $\Gamma \in \mathfrak{Ts}$. Then Γ is erasable if and only if Γ is self-erasing and any one of the following equivalent conditions is satisfied:*

(i) *Γ is universal;*

(ii) *Γ is s-projective;*

(iii) *Γ is an s-generator.*

Proof. "Only if": Suppose that Γ is erasable, then clearly Γ is self-erasing (take $A = \Gamma$). Now put $A = D_k$; then $D_k \otimes_k \Gamma = D_k[\lambda_1, \cdots, \lambda_d] =: D_k[\underline{\lambda}]$, where each λ_i is invariant and d is the Krull-dimension of Γ. Now D_k is s-projective and so $D_k[\underline{\lambda}]$ is also s-projective by Proposition 2·10 (3). Further, as D_k is universal, there exists a morphism $D_k \to \Gamma$. Therefore Γ is a direct summand of $D_k[\underline{\lambda}]$ and so is s-projective and hence universal. Finally, as Γ is self-erasing, $\Gamma \otimes_k \Gamma = \Gamma[\underline{\mu}] := \Gamma[\mu_1, \cdots, \mu_d]$ where each μ_i is invariant. Hence, by a simple induction argument, $\Gamma^{\otimes(m+1)} \cong \Gamma[\nu_1, \cdots, \nu_{md}]$ for all $m \ge 1$. Since Γ is universal it follows easily from Lemma 2·6, that every $A \in \mathfrak{Ts}$ is surjective image of some $\Gamma^{\otimes \ell}$, so Γ is also an s-generator.
"If": Note first that if Γ is either s-projective or an s-generator, then Γ is universal. Now suppose that Γ is self-erasing and universal and let $A \in \mathfrak{Ts}$. Then there exists a morphism $\theta : \Gamma \to A$. Now, as above, $\Gamma \otimes_k \Gamma = \Gamma[\underline{\mu}]$ with invariants $\underline{\mu} = (\mu_1, \cdots, \mu_d)$ and further $A \cong A^G \otimes_{\Gamma^G} \Gamma$ where $\Gamma^G \to A^G$ is induced by θ. Hence

$$A \otimes_k \Gamma \cong (A^G \otimes_{\Gamma^G} \Gamma) \otimes_k \Gamma \cong A^G \otimes_{\Gamma^G} (\Gamma \otimes_k \Gamma) \cong A^G \otimes_{\Gamma^G} (\Gamma[\underline{\mu}]) \cong (A^G \otimes_{\Gamma^G} \Gamma)[\underline{\mu}] \cong A[\underline{\mu}]$$

with trivial G-action on $k[\underline{\mu}]$. Thus Γ is erasable. $\square$

COROLLARY 2·12. *The following algebras in $\mathfrak{Ts}$ are triangular polynomial rings and therefore erasable s-projective generators:*

(i) *Every algebra $\bar{S} := S/(v^* - 1)S \in \mathfrak{Ts}$ as in Theorem 2·2.*

(ii) *The algebra D_k and its standard retract U (as in Theorem 0·6).*

Proof. The proof of Theorem 0·6, given in [**13**] shows that U is a polynomial ring on which G acts in a triangular way. All the other algebras are visibly triangular, so the claim follows from Proposition 2·9 and Theorem 2·11. $\square$

THEOREM 2·13. *Let $\Gamma \in \mathfrak{Ts}$ of Krull dimension d and assume that Γ is erasable. Then $\Gamma \cong k^{[d]}$ and $\Gamma^G \otimes_k k^{[n]} \cong k^{[n+d]}$ with $n = \log_p(|G|)$. Moreover*
(i) *Γ is n-stably triangular.*
(ii) *Γ^G is n-stably polynomial.*

Proof. We use notation of the proof of Theorem 2·11. Suppose that $\Gamma \in \mathfrak{Ts}$ is erasable. Then Γ is universal and so there is a morphism $\Gamma \to kG$, the disconnected abelian group algebra from Remark 2·3. Hence Γ has a maximal ideal $\mathfrak{m}$ with $\Gamma/\mathfrak{m} \cong k$. Since Γ is self-erasing, $\Gamma \otimes_k \Gamma = \Gamma[\underline{\mu}]$, therefore $\Gamma \cong k \otimes_k \Gamma = \Gamma/\mathfrak{m} \otimes_k \Gamma = (\Gamma \otimes_k \Gamma)/\mathfrak{m}^e = \Gamma[\underline{\mu}]/\mathfrak{m}^e = \Gamma/\mathfrak{m}[\underline{\mu}] \cong k^{[d]}$ as k-algebras, with $k^{[d]} \cong k[\underline{\mu}] \subseteq (\Gamma \otimes_k \Gamma)^G$. Here $\mathfrak{m}^e$ denotes the extended ideal in $\Gamma \otimes_k \Gamma$.
Now by Proposition 2·9 the algebra $U \cong k^{[n]}$ is erasable, therefore, as before, there are invariants $\underline{\lambda} = (\lambda_1, \cdots, \lambda_d)$ and $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n)$ such that $U[\underline{\lambda}] = U \otimes_k \Gamma \cong \Gamma \otimes_k U \cong \Gamma[\underline{\alpha}]$ is triangular. Hence

$$\Gamma^G[\underline{\alpha}] = (\Gamma[\underline{\alpha}])^G = (U[\underline{\lambda}])^G = U^G[\underline{\lambda}] \cong k^{[n+d]}$$

and so Γ^G is n-stably polynomial. Since U is triangular, Γ is n-stably triangular. □

COROLLARY 2·14. *Let $\Gamma \in \mathfrak{Ts}$ be erasable and assume that $\Gamma^G \cong k^{[d]}$. Then $(\Gamma^{\otimes \ell})^G \cong k^{[d\ell]}$. In particular this is satisfied for $\Gamma \in \{D_k, U\}$.*

Proof. The proof is by induction on ℓ. For $\ell = 1$ the statement is true by the hypothesis. $\Gamma^{\otimes \ell} \cong \Gamma^{\otimes(\ell-1)} \otimes_k \Gamma \cong \Gamma^{\otimes(\ell-1)} \otimes_k k[\lambda_1, \cdots, \lambda_d]$ with $k[\underline{\lambda}] \leq (\Gamma^{\otimes \ell})^G$. Hence

$$(\Gamma^{\otimes \ell})^G \cong (\Gamma^{\otimes(\ell-1)} \otimes_k k[\underline{\lambda}])^G \cong (\Gamma^{\otimes(\ell-1)})^G \otimes_k k[\underline{\lambda}] \cong k^{[d(\ell-1)]} \otimes_k k^{[d]} \cong k^{[d\ell]}.$$

□

As a consequence we see that every stably triangular $k-G$ algebra is a tensor factor of a tensor power of U or of D_k:

COROLLARY 2·15. *Let $X \in \{D_k, U\}$ and let A be a stably triangular $k-G$ algebra. Then there is an erasable algebra $B \in \mathfrak{Ts}$ and an $N \in \mathbb{N}$, such that $A \otimes_k B \cong X^{\otimes N}$. If moreover $A \in \mathfrak{Ts}$, then A^G is stably polynomial.*

Proof. First note that, since U is erasable, we have for every $\ell \in \mathbb{N}$: $U^{\otimes \ell} \cong U \otimes_k U^{\otimes(\ell-1)} \cong U[\lambda_1, \cdots, \lambda_{n(\ell-1)}] \cong U^{[n(\ell-1)]}$ with $k[\lambda_1, \cdots, \lambda_{n(\ell-1)}] \leq (U^{\otimes \ell})^G$. Similarly $D_k^{\otimes \ell} \cong U^{[(|G|-1)\ell - n]}$. Assume now that $A \otimes_k F \cong k^{[N]}$ is triangular with $F = F^G \cong k^{[m]}$. Then $A \otimes_k F$ is erasable by Proposition 2·9. Hence $A \otimes_k F \otimes_k U \cong U \otimes_k k[\underline{\beta}] \cong U^{[N]}$ with $k^{[N]} \cong k[\underline{\beta}] \leq (A \otimes_k F \otimes_k U)^G$. Now let $\ell \in \mathbb{N}$ be minimal with $\ell > N/n + 1$ and set $M := (\ell-1) \cdot n - N > 0$. Then with $B := F \otimes_k U^{[M]}$ we obtain $A \otimes_k B \cong U^{[N]} \otimes_k k^{[M]} \cong U^{[N+M]} \cong U^{[(\ell-1) \cdot n]} \cong U^{\otimes \ell}$. Similarly let $\ell' \in \mathbb{N}$ be minimal with $\ell' > \frac{N+n}{|G|-1}$ and set $M' := \ell'(|G|-1) - n - N > 0$. Then with $B' := F \otimes_k U^{[M']}$ we obtain $A \otimes_k B' \cong U^{[N]} \otimes_k k^{[M']} \cong U^{[N+M']} \cong U^{[\ell'(|G|-1)-n]} \cong D_k^{\otimes \ell'}$. Now assume in addition that $A \in \mathfrak{Ts}$. Since $B \in \mathfrak{Ts}$ is erasable, $A \otimes_k B \cong A \otimes_k k[\underline{\alpha}]$ with $k[\underline{\alpha}] \leq (A \otimes_k B)^G = A^G \otimes_k k[\underline{\alpha}] \cong (U^{\otimes \ell})^G$, which is a polynomial ring by Theorem 0·7. It follows that A^G is stably polynomial. □

We now give a **Proof of Theorem 0·8**:

THEOREM 2·16. *Let $\mathcal{P} \in \mathfrak{Ts}$ be s-projective, then both, $\mathcal{P}$ and $\mathcal{P}^G$ are retracts of polynomial rings over k.*

Proof. Let $\mathcal{P} \in \mathfrak{Ts}$ be s-projective and $\Gamma = U$ or D_k, then there is a surjective morphism $\Gamma^{\otimes \ell} \to \mathcal{P}$, which splits, since $\mathcal{P}$ is s-projective. It follows that $\mathcal{P}$ and $\mathcal{P}^G$ are retracts of $\Gamma^{\otimes \ell}$ and $(\Gamma^{\otimes \ell})^G$, respectively. Both of these rings are polynomial rings over k. □

We now give a **Proof of Theorem 0·11** from the introduction:

THEOREM 2·17. *Let $S \cong k^{[d]}$ be a polynomial ring with triangular G-action (e.g. $S = S(V^*)$). Then the ring of invariants S^G is the intersection of two polynomial subrings inside an s-projective polynomial $k-G$-algebra $k^{[N]} \in \mathfrak{Ts}$ of Krull-dimension $N = d + n$ with $n := \log_p |G|$. If moreover $S \in \mathfrak{Ts}$, then $S^G \otimes_k k^{[n]} \cong k^{[n+d]}$, i.e. S^G is n-stably polynomial.*

Proof. Clearly $S(V^*)$ is a triangular $k-G$-algebra (taking a triangular basis for the vector space V^*) and U is triangular by Theorem 0·6. If follows from Proposition 2·9 that S and U are erasable. Now the first claim follows from Proposition 2·10, taking $\mathbb{P} = U$ with $U^G \cong k^{[n]}$ and $n = \log_p |G|$, by Theorem 0·6.
If in addition $S \in \mathfrak{Ts}$, then $S \otimes_k U \cong S \otimes_k k[\lambda_1, \cdots, \lambda_n]$ with $k^{[n]} \cong k[\lambda_1, \cdots, \lambda_n] \leq (S \otimes_k U)^G$, by Theorem

0·7(2). It follows, switching the roles of U and S, that $S^G \otimes_k k^{[n]} \cong (S \otimes_k U)^G \cong (U \otimes_k S)^G \cong (U^G)^{[d]} \cong k^{[n+d]}$. $\square$

DEFINITION 2·18. *Following* [13] *Definition 3, we call a trace-surjective G-subalgebra $S \leq D_k$* **standard**, *if it is a* retract *of D_k, or in other words, if $D_k = S \oplus J$, where J is some G-stable (prime) ideal. We also call $C \in \mathfrak{Ts}$* **cyclic**, *if $C \cong D_k/I$ with G-stable ideal I. Equivalently, C is generated by one G-orbit of a point $c \in C$.*

In this terminology, U is standard as well as cyclic and s-projective. The next theorem shows that the latter two properties characterize standard subalgebras of D_k:

THEOREM 2·19. *Let $R, S \in \mathfrak{Ts}$, then the following hold:*
(i) *R is s-projective, if and only if it is retract of a tensor product $D_k^{\otimes \ell}$.*
(ii) *S is a standard subalgebra of D_k if and only if $S \in \mathfrak{Ts}$ is cyclic and s-projective.*

Proof. (1): This follows from the fact that every $R \in \mathfrak{Ts}$ is surjective image of some $D_k^{\otimes \ell}$.
(2): By definition every standard subalgebra is cyclic and a retract of D_k. Hence by (1) it is s-projective. Now let $S \in \mathfrak{Ts}$ be cyclic and s-projective. Then there is a surjective morphism $D_k \to S$, which must split, hence S is a standard subalgebra. $\square$

REMARK 2·20. *The statement (1) in Theorem 2·19 shows that the algebra $D_k^{\otimes \ell}$ is the analogue in $\mathfrak{Ts}$ of the free module of rank ℓ in a module category.*

3. *Basic Algebras*

Let $\mathfrak{C}$ be an arbitrary category, then for objects $a, b \in \mathfrak{C}$ one defines $a \prec b$ to mean that there is a monomorphism $a \hookrightarrow b \in \mathfrak{C}$ and $a \approx b$ if $a \prec b$ and $b \prec a$. According to this definition, an object $b \in \mathfrak{C}$ is called *minimal* if $a \prec b$ for $a \in \mathfrak{C}$ implies $b \prec a$ and therefore $a \approx b$. Clearly "$\approx$" is an equivalence relation on the object class of $\mathfrak{C}$. Recall that $A \in \mathfrak{Ts}$ is universal if it is weakly initial, or, equivalently, if it maps to D_k.

DEFINITION 3·1. *The algebra $B \in \mathfrak{Ts}$ is called* **basic** *if it is universal and minimal.*

The following Lemma characterizes types of morphisms in $\mathfrak{Ts}$ by their action on points. The results will then be used to analyze basic objects in $\mathfrak{Ts}$:

LEMMA 3·2. *A morphism $\theta \in \mathfrak{Ts}(R, S)$ is surjective (injective, bijective) if and only if it induces a surjective (injective, bijective) map from the set of points of R to the set of points of S. In particular $\theta \in \mathfrak{Ts}(R, S)$ is a monomorphism if and only if θ is injective.*

Proof. "Surjectivity": Let $s \in S$ with $\mathrm{tr}(s) = 1$ and $r \in R$ with $\theta(r) = s$. Then $r' := \mathrm{tr}(r) - 1 \in \ker(\theta) \cap R^G$. Let $w \in R$ with $\mathrm{tr}(w) = 1$, then $r' = \mathrm{tr}(r'w)$ and $v := r - r'w$ satisfies $\theta(v) = s$ and $\mathrm{tr}(v) = 1$, hence the induced map on points is surjective. On the other hand, since R and S are generated as algebras by points, the reverse conclusion follows.
"Injectivity": We can assume that the induced mapping on points is injective and want to show that θ is injective. Let $w \in R$ be a point and $r, r' \in R^G$ with $\theta(r) = \theta(r')$, then $\mathrm{tr}(r + w) = \mathrm{tr}(w) = 1 = \mathrm{tr}(r' + w)$ and $\theta(r + w) = \theta(r' + w)$, so $r + w = r' + w$ and $r = r'$. Hence the induced map on the rings of invariants is injective. But $R = \oplus_{i=1}^n R^G w_i$, with $n = |G|$ and a G-orbit of points $\{w_1, \cdots, w_n\}$. It follows that $V' := \langle \theta(w_i) \mid i = 1, \cdots, n \rangle \leq S$ is a copy of the regular representation of G, so by 1·8 we have $S = \oplus_{i=1}^n S^G \theta(w_i)$. Let $r = \sum_{i=1}^n r_i w_i, r' = \sum_{i=1}^n r'_i w_i$ with $r_i, r'_i \in R^G$ and $\theta(r) = \theta(r')$, then $\sum_{i=1}^n \theta(r_i - r'_i)\theta(w_i) = 0$ implies $\theta(r_i) = \theta(r'_i)$, so $r_i = r'_i$ for all i and therefore $r = r'$.
For the last claim, it is clear that an injective morphism is a monomorphism, so assume now that θ is a monomorphism. It suffices to show that θ is injective on the points of R, so let $a_1, a_2 \in R$ be points with $\theta(a_1) = \theta(a_2)$. Define $\psi_i : D_k \to R$ as the morphisms determined by the map $D_k \ni x_1 \mapsto a_i$, then $\theta \circ \psi_1 = \theta \circ \psi_2$, hence $\psi_1 = \psi_2$ and $a_1 = a_2$. This finishes the proof. $\square$

Now let A be an object in $\mathfrak{Ts}$, then $\mathrm{Dim}\,(A) = \max\{\mathrm{Dim}\,(A/\mathrm{p}) \mid \mathrm{p} \in \mathrm{Spec}(A)\}$, where $\mathrm{Dim}\,(A/\mathrm{p}) = \mathrm{transc.deg}_k(A/\mathrm{p}) := \mathrm{transc.deg}_k(\mathrm{Quot}(A/\mathrm{p}))$, the transcendence degree over k of the quotient field $\mathrm{Quot}(A/\mathrm{p})$. If $B \prec A$ then

$$\mathrm{Dim}\,(B) = \mathrm{transc.deg}_k(B) \leq \mathrm{transc.deg}_k(A) = \mathrm{Dim}\,(A).$$

This is clear if A is a domain and an easy exercise otherwise. In particular, any two $\approx$-equivalent domains in $\mathfrak{Ts}$ have the same Krull-Dimension.

If $A \in \mathfrak{Ts}$ is universal it maps into D_k with a universal image isomorphic to A/I for some G-invariant prime ideal $I \trianglelefteq A$. So every universal object has a quotient which is a universal integral sub-domain of D_k. Notice also that if $B \prec A$ with universal A, then B is also universal; so if A is minimal among the universal objects, then A is also a minimal object and therefore basic. It is however not completely obvious from the definition that basic objects do exist. This is established as follows, which also shows the existence of basic normal domains:

LEMMA 3·3. *Let $X \in \mathfrak{Ts}$ be a subalgebra of U or of D_k and let $\hat{X}$ denote its normal closure in* $\mathrm{Quot}(X)$. *Then $\hat{X}$ is universal in $\mathfrak{Ts}$. Moreover if X is a subalgebra of minimal Krull-dimension in U or in D_k, then X and $\hat{X}$ are basic domains.*

Proof. The polynomial rings U and D_k are universal domains of Krull-dimension n and $|G| - 1 = p^n - 1$, respectively. Let $X \in \mathfrak{Ts}$, $X \hookrightarrow U$ or D_k, then X is a universal domain. Now suppose that X has minimal Krull-dimension. If $Y \prec X$, then $\mathrm{Dim}\,(Y) = \mathrm{Dim}\,(X)$, but there is $\alpha \in \mathfrak{Ts}(X, Y)$ with $\alpha(X) \prec Y \prec X$. It follows that $\mathrm{Dim}\,(\alpha(X)) = \mathrm{Dim}\,(Y) = \mathrm{Dim}\,(X)$, so $\ker(\alpha) = 0$ and $X \prec Y$. This shows that X is a universal minimal, hence basic, domain.
Since X is a finitely generated k-algebra, so is $\hat{X}$ and, since U and D_k are normal rings, $\hat{X} \le U$ or $\hat{X} \le D_k$, respectively. It follows that $\hat{X}$ is universal, and basic, if X is. □

The next result describes properties of basic objects and shows that they form a single $\approx$-equivalence class consisting of integral domains, all of which have the same Krull-dimension:

PROPOSITION 3·4. *Let $A \in \mathfrak{Ts}$ be universal. Then the following are equivalent:*
- (i) *A is basic;*
- (ii) *A is a basic domain;*
- (iii) *every $\alpha \in \mathrm{End}_{\mathfrak{Ts}}(A)$ is injective;*
- (iv) *$A \prec B$ for every universal $B \in \mathfrak{Ts}$;*
- (v) *$A \approx B$ for one (and therefore every) basic object $B \in \mathfrak{Ts}$;*
- (vi) *no proper quotient of A is universal;*
- (vii) *no proper quotient of A is a subalgebra of A.*

Any two basic objects are $\approx$-equivalent domains of the same Krull-dimension $d_k(G) \le n = \log_p(|G|)$ with $d_k(G) > 0$ if $G \ne 1$. With $\mathfrak{B}$ we denote the $\approx$-equivalence class of basic objects in $\mathfrak{Ts}$.

Proof. Let $X \in \mathfrak{Ts}$ be a basic domain and $\alpha \in \mathrm{End}_{\mathfrak{Ts}}(X)$. Then $\alpha(X) \prec X$, hence $X \prec \alpha(X)$, so $\mathrm{Dim}\,(X) = \mathrm{Dim}\,(\alpha(X))$ and α must be injective.
"(1) ⇒ (2)": There is $\beta \in \mathfrak{Ts}(X, A)$ and $\gamma \in \mathfrak{Ts}(A, X)$, so $\gamma \circ \beta \in \mathrm{End}_{\mathfrak{Ts}}(X)$ is injective, which implies that β is injective and therefore $X \prec A$. It follows that $A \prec X$, hence A is a domain.
"(2) ⇒ (3)": This has already been shown above. (We didn't use the fact that A is universal, there. So every minimal domain in $\mathfrak{Ts}$ satisfies (3)).
"(3) ⇒ (4)": Since A and B are universal there exist morphisms $\alpha \in \mathfrak{Ts}(A, B)$ and $\beta \in \mathfrak{Ts}(B, A)$ with $\beta \circ \alpha$ injective, because A is minimal. Hence $A \prec B$.
"(4) ⇒ (5)": This is clear.
"(5) ⇒ (1)": $B \approx A$ means that $B \hookrightarrow A$ and $A \hookrightarrow B$. In that case A is universal (minimal) if and only if B is universal (minimal). Choosing $B := X$, it follows that A is basic.
"(3)⇒ (6)": Now assume that every $\alpha \in \mathrm{End}_{\mathfrak{Ts}}(B)$ is injective and let B/I be universal for the G-stable ideal $I \trianglelefteq B$. Then there is $\gamma \in \mathfrak{Ts}(B/I, B)$ and the composition with the canonical map $c: B \to B/I$ gives $\gamma \circ c \in \mathrm{End}_{\mathfrak{Ts}}(B)$. It follows that $I = 0$.
"(6) ⇒ (1)": Assume $B \prec A$. Then B is universal and since A is universal, there is $\theta \in \mathfrak{Ts}(A, B)$ with $\theta(A) \le B$ universal. Hence $A \cong \theta(A) \prec B$ and A is basic.
Let $A, B \in \mathfrak{Ts}$ be basic, then $\mathfrak{Ts}(A, B) \ne \emptyset \ne \mathfrak{Ts}(B, A)$ implies that $A \prec B \prec A$, hence $A \approx B$ and $\mathrm{Dim}\,(A) = \mathrm{Dim}\,(B) =: d_k(G) \le n = \log_p(|G|)$ (see Theorem 0·6). Assume that $d_k(G) = 0$. Then X must be a Galois-field extension $K \ge k$ with Galois group G and $K \hookrightarrow D_k$, which implies $K = k$ and $G = 1$.
"(6) ⇒ (7)": This is clear, because a quotient A/I as subalgebra of A would be universal.
"(7) ⇒ (1)": We have $X \prec A$ and there is $\theta \in \mathfrak{Ts}(A, X)$ with $\theta(A) \le X$ universal. It follows that $\theta(A) \prec A$, hence $\ker\theta = 0$ and $\theta(A) \cong A \approx X$, so A is basic. □

COROLLARY 3·5. *Let $A \in \mathfrak{Ts}$ be a universal domain. Then $d_k(G) \le \mathrm{Dim}\,(A)$ and the following are equivalent:*
- (i) *$A \in \mathfrak{B}$;*
- (ii) *$d_k(G) = \mathrm{Dim}\,(A)$;*
- (iii) *If $C \in \mathfrak{Ts}$ with $C \prec A$, then $\mathrm{Dim}\,(C) = \mathrm{Dim}\,(A)$.*

Proof. The first statement and "(1) $\Rightarrow$ (2)" follow immediately from Proposition 3·4.
"(2) $\Rightarrow$ (3)": $C \prec A$ implies that C is a universal domain and $\mathrm{Dim}\,(C) \le \mathrm{Dim}\,(A)$. Hence $\mathrm{Dim}\,(A) = d_k(G) \le \mathrm{Dim}\,(C) \le \mathrm{Dim}\,(A)$.
"(3) $\Rightarrow$ (1)": Suppose A is *not* minimal. Then there is $\alpha \in \mathrm{End}_{\mathfrak{Ts}}(A)$ with $\ker(\alpha) \neq 0$. Hence $A/\ker(\alpha) \cong \alpha(A) =: C \prec A$. Clearly $\mathrm{Dim}\,(C) < \mathrm{Dim}\,(A)$. $\square$

The results in Theorem 2·19 can give useful bounds for $d_k(G)$. Let $S = \mathrm{Sym}(V^*)$ be as in Theorem 2·2; it has been shown in [**14**] Theorem 2.7 that there exists $v^* \in V^{*G}$ such that $S/(v^* - 1)S \in \mathfrak{Ts}$, and so is s-projective and universal, if and only if $\mathcal{X}_V := \langle V^g \mid 1 \neq g \in G,\ g^p = 1\rangle < V$. In this case $d_k(G) \le \dim(V) - 1$. If $k = \mathbb{F}_p$, the condition $\mathcal{X}_V < V$ implies $\dim(V) \ge n+1$ with $n = \log_p(|G|)$ (see [**14**] Proposition 3.3). For certain p-groups (called "CEA-groups" in [**14**]) the condition $\mathcal{X}_V < V$ is satisfied with $\dim(V) = n+1$, which then gives the known bound $d_k(G) \le n$. For extension fields however, one can obtain sharp bounds for d_k and the essential dimension e_k as the following examples show:

EXAMPLES 3·6.
(i) *Let $q := p^n$, $\mathbb{F}_q \le k$ and $(C_p)^n \cong G$ a Sylow p-subgroup of $\mathrm{GL}_2(q)$ consisting of upper triangular matrices. Set $V := k^2 = ke_1 \oplus ke_2$ be the natural kG-module, then $\mathcal{X} = ke_1 < V$ and $\mathrm{Sym}(V^*)/(x_1 - 1) \cong B = k[Z]$ (see Theorem 3·15), proving again that $d_k(G) = 1$.*
(ii) *Now let $\mathbb{F}_{q^2} \le k$ and let G be a Sylow p-subgroup of $\mathrm{SU}_3(q^2)$. Then G can be represented as the group of matrices*

$$g_{a,b} := \begin{pmatrix} 1 & a & b \\ 0 & 1 & -a^q \\ 0 & 0 & 1 \end{pmatrix},\ a, b \in \mathbb{F}_{q^2},\ b + b^q + aa^q = 0.$$

Let $V \cong k^3 = ke_1 \oplus ke_2 \oplus ke_3$ be the natural $\mathrm{SU}_3(q^2)$-representation, then an elementary calculation shows that $\mathcal{X}_V = \langle e_1, e_2\rangle_k < V$, hence $\mathrm{Sym}(V^*)/(x_1 - 1)$ is s-projective and $d_k(G) \le 2$, so $d_k(G) = e_k(G) = 2$ by Corollary 4·9. Note that for $q = p$, G is extraspecial (of exponent p, if $p \ge 3$).

COROLLARY 3·7. *Let $p \ge 3$, $\mathbb{F}_{p^2} \le k$ and G be extraspecial of order p^3 and of exponent p. Then $d_k(G) = e_k(G) = 2$.*

Back again to basic objects; the $\approx$-equivalence class $\mathfrak{B}$ of basic objects contains cyclic domains:

COROLLARY 3·8. *If $B \in \mathfrak{B}$, then $B \approx C$ with C a cyclic domain.*

Proof. Let $\alpha \in \mathfrak{Ts}(D_k, B)$, then $C := \alpha(D_k) \prec B$, hence $B \approx C$ with cyclic domain $C \in \mathfrak{Ts}$. $\square$

In Lemma 2·4 we showed that every object $A \in \mathfrak{Ts}$ arises from extending the quotient of a universal object by a ring with trivial G-action. The class $\mathfrak{B}$ consists of those objects from which all *universal* objects arise by extending invariants:

LEMMA 3·9. *An object $B \in \mathfrak{Ts}$ is basic, if and only if every universal object is of the form $\mathfrak{W} = \mathfrak{W}^G \otimes_{B^G} B$ with embedding $B \hookrightarrow \mathfrak{W}$.*

Proof. If $B \in \mathfrak{Ts}$ has the described property and $X \in \mathfrak{Ts}$ is basic, then $B \prec X$, so $X \approx B$ and B is basic. Now assume that B is basic and $\mathfrak{W}$ is universal. Then by Lemma 2·4, $\mathfrak{W} = \mathfrak{W}^G \otimes_{S^G} S$ with $B/I \cong S \hookrightarrow \mathfrak{W}$. It follows that B/I is universal, hence $I = 0$ and $S \cong B$. $\square$

We are therefore particularly interested in describing basic objects, i.e. minimal subalgebras of D_k which are also in $\mathfrak{Ts}$. However, with regard to minimality the following has to be taken into account: Since D_k is the polynomial ring $k[x_g \mid 1 \neq g \in G]$, we have $D_k^p = k^p[x_g^p \mid g \in G]$ and $\cap_{i \in \mathbb{N}} D_k^{p^i} = \cap_{i \in \mathbb{N}} k^{p^i} = k^{p^\infty}$, where k^{p^∞} denotes the maximal perfect subfield of k. This implies that $C^p < C$ for every subring $C \neq k^{p^\infty} \le D_k$, hence there will be in general no subalgebra of D_k which is minimal with respect to ordinary inclusion of k-subalgebras. (If k is perfect and $C \le D_k$ is trace-surjective, then $C^p < C$ is a proper inclusion of isomorphic objects in $\mathfrak{Ts}$). The result in Corollary 3·8 motivates the following

LEMMA 3·10. *Let $C \in \mathfrak{Ts}$ be basic and cyclic. Then up to isomorphism $C \le D_k$ and there exists $\chi \in \mathrm{End}_{\mathfrak{Ts}}(D_k)$ with $\chi(D_k) = C$ and $\ker(\chi_{|C}) = 0$. Moreover one of the following two situations can occur:*
(i) *$C > \chi(C) > \cdots > \chi^n(C) > \chi^{n+1}(C) \cdots$ is an infinite descending chain of properly contained, isomorphic $k - G$-subalgebras in $\mathfrak{Ts}$.*
(ii) *$C = \chi(C)$ and $D_k = C \oplus I$, where $I = \ker(\chi) \trianglelefteq D_k$ is a G-stable ideal.*

Proof. By Proposition 3·4, $C \prec D_k$, so there is an embedding $\iota: C \hookrightarrow D_k$ and we can assume $C = \iota(C) = k[W] \le D_k$ with $w \in W$ of trace 1 and $W \cong kG$ as kG-module. Then $W = \langle wg \mid g \in G\rangle$ and the map $x_g \mapsto wg$ defines a G-equivariant k-algebra epimorphism $\theta: D_k \to C$. Set $\phi := \theta \circ \iota$ and $\chi := \iota \circ \theta$, then $\phi \in \mathrm{End}_{\mathfrak{Ts}}(C)$ is injective with image $C \cong \phi(C) = \theta(C) \le C$, so $\chi(C) = \iota \circ \theta(\iota(C)) = \phi(C) \le C$. Suppose $\chi^{n+1}(C) = \chi^n(C)$ and let $c \in C$; then $\chi^n(c) = \chi^{n+1}(c')$ for some $c' \in C$, so $c - \chi(c') \in \ker(\chi^n_{|C}) \subseteq \ker(\phi^{n+1}) = 0$. Hence $c = \chi(c')$, $\chi(C) = C = \phi(C)$ and $\phi = \theta \circ \iota$ is an automorphism of C. We conclude $D_k = C \oplus \ker(\chi)$. $\square$

If $k = k^p$, we have already seen that case (1) actually occurs. For general k, the homomorphism $\tilde{F} = k[X_g \mid g \in G] \to \tilde{F}$ defined by $X_g \mapsto X_g^p$ induces a **Frobenius-endomorphism**

$$\Phi: D_k = k[x_g \mid g \in G] \to D_k,\ \alpha(x_1, \cdots, x_g, \cdots) \mapsto \alpha(x_1^p, \cdots, x_g^p, \cdots),$$

which in the case $k = \mathbb{F}_p$ coincides with the ordinary power map $a \mapsto a^p$. It follows that $D_k > \Phi(D_k) > \cdots \Phi^n(D_k) > \Phi^{n+1}(D_k) > \cdots$. Similarly, for every subalgebra $C_0 = \mathbb{F}_p[V] \le D_{\mathbb{F}_p}$ with subspace $1 \in V \cong \mathbb{F}_pG$ we have

$$C_0 > \Phi(C_0) = C_0^p > \cdots > C_0^{p^n} > C_0^{p^{n+1}} > \cdots$$

and therefore the subalgebra $C := k \otimes_{\mathbb{F}_p} C_0 \le D_k$ satisfies

$$C > \Phi(C) > \cdots > \Phi^n(C) > \Phi^{n+1}(C) > \cdots.$$

In the rest of this section, and in fact the paper, we will study the second case of lemma 3·10, which also occurs naturally and, in many respects, is the more interesting situation.

If $S \le D_k$ is standard, then there is a projection morphism $\chi: D_k \to S \hookrightarrow D_k$, which is an idempotent in $\mathrm{End}_{\mathfrak{Ts}}(D_k)$. The following has been shown in [**13**]:

Lemma 3·11. *[[**13**] Lemma 5.1] Let $S \hookrightarrow D_k$ be a trace-surjective G-algebra, then the following are equivalent:*

(i) *S is standard.*
(ii) *$\exists\ \chi = \chi^2 \in (\mathrm{End}_{\mathfrak{Ts}}(D_k)$ with $S = \chi(D_k)$.*
(iii) *$\exists \chi \in (\mathrm{End}_{k-\mathrm{alg}}(D_k))^G$ with $\chi^2(x_1) = \chi(x_1) =: w \in S = k[wg \mid g \in G]$.*
(iv) *$\exists\ w = W(x_1, x_{g_2}, \cdots, x_{g_{|G|}}) \in S$ with $\mathrm{tr}(w) = 1$, $w = W(w, wg_2, \cdots, wg_{|G|})$ and $S = k[wg \mid g \in G] \le D_k$.*

Let $S \le D_k$ be standard. Since D_k is a polynomial k-algebra it follows from [**10**] Corollary 1.11, that S is a regular UFD.

Definition 3·12. *(see [**13**][Definition 4]) A point $w \in D_k$ will be called* **reflexive**, *if*

$$w = W(x_1, \cdots, x_g \cdots) = W(w, \cdots, wg, \cdots) = \theta(w),$$

where $\theta \in (\mathrm{End}_{k-\mathrm{alg}}(D_k))^G$ is defined by $x_g \mapsto w \cdot g\ \forall g \in G$.

By definition a trace-surjective G-algebra is cyclic, if and only if it is generated as an algebra by the G-orbit of one point. Lemma 3·11 shows, that the standard subalgebras of D_k are precisely the subalgebras generated by the G-orbit of a *reflexive* point.

Let G_1, G_2 be two finite p-groups and $A_i \in \mathfrak{Ts}_{G_i}$ with point $a_i \in A_i$ for $i = 1, 2$. Then $a_1 \otimes_k a_2$ is easily seen to be a point of $A_1 \otimes_k A_2 \in \mathfrak{Ts}_{G_1 \times G_2}$. Moreover, $D_k(G_1) \otimes_k D_k(G_2)$ is standard universal, i.e. a retract of $D_k(G_1 \times G_2)$ (see [**13**] Section 5, Example 3). If the A_i's are universal with $\theta_i \in \mathfrak{Ts}_{G_i}(A_i, D_k(G_i))$, then $\theta_1 \otimes \theta_2 \in \mathfrak{Ts}_{G_1 \times G_2}(A_1 \otimes_k A_2, D_k(G_1) \otimes_k D_k(G_2))$, hence $A_1 \otimes_k A_2$ is universal in $\mathfrak{Ts}_{G_1 \times G_2}$. Clearly the polynomial ring $\tilde{D} := D_k(G_1) \otimes_k D_k(G_2)$ can be viewed as an object in $\mathfrak{Ts}_{G_1}$ or $\mathfrak{Ts}_{G_2}$ by restricting the action accordingly. In that way $\tilde{D}_{|G_1} \cong D_k(G_1) \otimes_k k[T_1, \cdots, T_{|G_2|-1}]$ is a polynomial ring over $D_k(G_1)$ with trivial G_1-action on $k[T_1, \cdots, T_{|G_2|-1}]$. Let $R \in \mathfrak{Ts}_{G_1}$ and $\phi \in \mathfrak{Ts}_{G_1}(D_k(G_1), R)$, then any map $T_j \mapsto r_j \in R^{G_1}$ extends ϕ to a morphism $\tilde{\phi} \in \mathfrak{Ts}_{G_1}(\tilde{D}_{|G_1}, R)$, which shows that $\tilde{D}_{|G_i}$ is universal in $\mathfrak{Ts}_{G_i}$.

Suppose that $\phi \in \mathfrak{Ts}_{G_1 \times G_2}(\tilde{A}, \tilde{D})$ for $\tilde{A} := A_1 \otimes_k A_2$ with $i_1 \in \mathfrak{Ts}_{G_1}(A_1, \tilde{A})$ the canonical morphism. Then the composition $\phi_{|G_1} \circ i_1$ is in $\mathfrak{Ts}_{G_1}(A_1, \tilde{D}_{|G_1})$, hence A_1 is universal. We summarize:

Proposition 3·13. *Let G_1 and G_2 be two finite p-groups with $A_i \in \mathfrak{Ts}_{G_i}$ for $i = 1, 2$. Then $A_1 \otimes_k A_2 \in \mathfrak{Ts}_{G_1 \times G_2}$ and the following hold:*

(i) *A_i universal in $\mathfrak{Ts}_{G_i}$ for $i = 1, 2 \iff A_1 \otimes_k A_2$ is universal in $\mathfrak{Ts}_{G_1 \times G_2}$;*
(ii) *A_i standard universal in $\mathfrak{Ts}_{G_i}$ for $i = 1, 2 \Rightarrow A_1 \otimes_k A_2$ is standard universal in $\mathfrak{Ts}_{G_1 \times G_2}$;*
(iii) *$d_k(G_1 \times G_2) \le d_k(G_1) + d_k(G_2)$.*

We close this section by illustrating the above notions in the case of elementary-abelian p-groups. We need some notation and a lemma: Define $\partial_n(T) \in k[X_1, \cdots, X_{n-1}][T]$ to be the following $n \times n$-determinant:

$$\partial_n(T) = \partial_n(\underline{X}, T) := \begin{vmatrix} X_1 & \cdots & X_{n-1} & T \\ X_1^p & \cdots & X_{n-1}^p & T^p \\ \cdots & \cdots & \cdots & \cdots \\ X_1^{p^{n-1}} & \cdots & X_{n-1}^{p^{n-1}} & T^{p^{n-1}} \end{vmatrix},$$

and set $F_{n-1}(T) := \prod_{x \in V}(T - x)$, where $V := \langle X_1, \cdots, X_{n-1}\rangle_{\mathbb{F}_p}$.

LEMMA 3·14. *The following hold:*
 (i) $\partial_n(T) = \partial_{n-1}(X_{n-1}) \cdot F_{n-1}(T)$;
 (ii) *for any* $\alpha_1, \cdots, \alpha_n \in k$, $\partial_n(\alpha_1, \cdots, \alpha_{n-1}, \alpha_n) \neq 0$ *if and only if the set* $\{\alpha_1, \cdots, \alpha_n\}$ *is linearly independent over* $\mathbb{F}_p$.

Proof. (1): For every $x \in V$ we have $\partial_n(x) = 0$, so considering the T-degree we obtain $\partial_n(T) = c \cdot F_{n-1}(T)$ with c being the coefficient of $\partial_n(T)$ at T^{p^n}, hence $c = \partial_{n-1}(X_{n-1})$.
(2): Assume that $\{\alpha_1, \cdots, \alpha_n\} \subseteq k$ is linearly independent over $\mathbb{F}_p$ and set

$$f(T) := \prod_{x \in W}(T - x) \text{ with } W := \langle \alpha_1, \cdots, \alpha_{n-1}\rangle_{\mathbb{F}_p}.$$

Then we have $\partial_n(\alpha_1, \cdots, \alpha_{n-1}, \alpha_n) = \partial_{n-1}(\alpha_1, \cdots, \alpha_{n-2}, \alpha_{n-1}) \cdot f(\alpha_n)$. By induction the first factor is nonzero and $f(\alpha_n) \neq 0$, since $\alpha_n \notin W$; hence $\partial_n(\alpha_1, \cdots, \alpha_{n-1}, \alpha_n) \neq 0$. Conversely, if $\partial_n(\alpha_1, \cdots, \alpha_{n-1}, \alpha_n) \neq 0$, then, again by induction, $\{\alpha_1, \cdots, \alpha_{n-1}\}$ is linearly independent over $\mathbb{F}_p$. Moreover $f(\alpha_n) \neq 0$, so $\alpha_n \notin W$ and $\{\alpha_1, \cdots, \alpha_n\}$ is linearly independent over $\mathbb{F}_p$. □

Let G be an elementary-abelian group of order p^n. We identify G with the additive group $(\mathbb{F}_p^n, +)$ and write an element $g \in G$ as a vector $g = \sum_{i=1}^n g_i e_i$ with $g_i \in \mathbb{F}_p$ and e_i the standard basis vector of $\mathbb{F}_p^n$. Set $\mho := k[Y_1, \cdots, Y_n]$, the polynomial ring in n variables, then G acts on $\mho$ by the rule $(Y_i)g = Y_i - g_i$ for all i, hence $\mho = U_1 \otimes_k U_2 \otimes_k \cdots \otimes_k U_n$, with $U_i = k[Y_i] \in \mathfrak{Ts}_{G_i}$ and $G_i := \langle e_i\rangle$. It follows from [**13**] Proposition 3.2 that every $U_i \in \mathfrak{Ts}_{G_i}$ is a basic and standard subalgebra of $D_k(G_i)$, hence by Proposition 3·13, $\mho$ is a standard universal subalgebra of $D_k(G)$.

Now assume that k contains an n-dimensional $\mathbb{F}_p$-subspace $W := \langle \alpha_1, \cdots, \alpha_n\rangle$; then there is an embedding of abelian groups $\alpha: G \to W \leq k^+, \ g \mapsto \alpha_g := \sum_{i=1}^n g_i\alpha_i$. Consider a univariate polynomial ring $k[Z]$ with (nonlinear) G-action extending the maps $Z \mapsto (Z)g = Z - \alpha_g$ to k-algebra automorphisms. The corresponding $k - G$-algebra will be denoted by B_α. Then the map $Z \mapsto \sum_{i=1}^n \alpha_i Y_i$ extends to a G-equivariant morphism of $k - G$-algebras $\theta: B_\alpha \to \mho$. It follows from Lemma 3·14 that there exists a matrix $(f_{ij})^T := (\alpha_i^{p^{j-1}})^{-1} \in \mathrm{GL}_n(k)$, i.e. such that $\sum_{j=0}^{n-1} f_{ij}\alpha_k^{p^j} = \delta_{ik}$. Set $f_i(Z) := \sum_{j=0}^{n-1} f_{ij}Z^{p^j} \in k[Z]$, then $f_i(\alpha_g) = g_i$ for every $g \in G$. Now define a k-algebra morphism $\psi: \mho \to B_\alpha$ by extending the map $Y_i \mapsto f_i(Z)$. Then $f_i(\mu + \lambda) = f_i(\mu) + f_i(\lambda)$ for $\mu, \lambda \in k$ and $f_i(\lambda) = \lambda_i$, whenever $\lambda = \sum_{i=1}^n \lambda_i\alpha_i$ with $\lambda_i \in \mathbb{F}_p$. Hence $\psi \circ \theta(Z) = h(Z) \in k[Z]$ is a polynomial of degree less than p^n such that $h(\lambda) - \lambda = \sum_{i=1}^n \alpha_i f_i(\lambda) - \lambda = \sum_{i=1}^n \alpha_i\lambda_i - \lambda = 0$ for all $\lambda \in W$. It follows that $h(Z) = Z$. Moreover, for every $g \in G$ we have $\psi((Y_i)g) = \psi(Y_i - g_i) = \psi(Y_i) - g_i = f_i(Z) - f_i(\alpha_g) = f_i(Z - \alpha_g) = f_i((Z)g) = (f_i(Z))g = (\psi(Y_i))g$. This shows that ψ is a G-equivariant retraction. In particular B_α is a trace-surjective retract of $\mho$, hence a standard and basic universal algebra in $\mathfrak{Ts}_G$.
Let $\beta: G \to k^+, \ g \mapsto \beta_g := \sum_{i=1}^n g_i\beta_i$ be a different embedding of abelian groups and define B_β to be the univariate polynomial ring $k[Z]$ with G-action given by $Z \mapsto (Z)g = Z - \beta_g$. Since the set $\{\beta_1, \cdots, \beta_n\}$ is linearly independent over $\mathbb{F}_p$, there are $(\lambda_0, \cdots, \lambda_{n-1}) \in k$ with $\sum_{j=0}^{n-1} \lambda_j \cdot \beta_i^{p^j} = \alpha_i$ for $i = 1, \cdots, n$. Let $L_{\alpha,\beta}: B_\alpha \to B_\beta$ be the algebra homomorphism extending the map $Z \mapsto f_{\alpha,\beta}(Z) := \sum_{j=0}^{n-1} \lambda_j \cdot Z^{p^j}$. Then $L_{\alpha,\beta}$ is injective, because $f_{\alpha,\beta}(Z) \notin k$ and $L_{\alpha,\beta}((Z)g) = L_{\alpha,\beta}(Z - \alpha_g) = L_{\alpha,\beta}(Z) - \alpha_g = f_{\alpha,\beta}(Z) - f_{\alpha,\beta}(\beta_g) = f_{\alpha,\beta}(Z - \beta_g) = (L_{\alpha,\beta}(Z))g$. So $L_{\alpha,\beta}$ is a G-equivariant embedding $B_\alpha \hookrightarrow B_\beta$. In a similar way we see that $L_{\beta,\alpha} \in \mathfrak{Ts}_G(B_\beta, B_\alpha)$ is injective, hence B_β is universal and indeed $B_\alpha \approx B_\beta$.
We summarize

THEOREM 3·15. *Let G be elementary-abelian of order p^n and $\mho := k[Y_1, \cdots, Y_n] \in \mathfrak{Ts}_G$ as described above. Then the polynomial ring $\mho$ is a standard universal subalgebra of $D_k(G)$.*
Assume now that $\dim_{\mathbb{F}_p}(k) \geq n$, *then there is an embedding of abelian groups*

$$\alpha: G \to W := \langle \alpha_1, \cdots, \alpha_n\rangle_{\mathbb{F}_p} \leq k^+, \ g \mapsto \alpha_g := \sum_{i=1}^n g_i\alpha_i$$

and the following hold:

(i) *The univariate polynomial ring $B_\alpha = k[Z]_\alpha$ with G-action as described above is a retract of $\mho$ in $\mathfrak{Ts}_G$ and a standard universal and basic object in $\mathfrak{Ts}_G$. In particular $d_k(G) = 1$.*
(ii) *Every basic object in $\mathfrak{Ts}_G$ which is also a normal ring is of the form B_β for some embedding of abelian groups $\beta:\ G \hookrightarrow k^+$.*
(iii) *Two normal basic algebras $B_\alpha, B_\beta \in \mathfrak{Ts}_G$ are isomorphic if and only if $\alpha = c\cdot\beta$ for some $0 \neq c \in k$. They are conjugate under an outer automorphism of G if and only if $\alpha(G) = c\cdot\beta(G)$ for some $0 \neq c \in k$.*
(iv) *Let $\underline{\alpha} := \alpha^{(1)}, \cdots, \alpha^{(n)}$ be n not necessarily distinct embeddings $G \hookrightarrow k^+$. Then*

$$\mho \cong B_{\underline{\alpha}}^{\otimes n} \cong B_{\alpha^{(1)}} \otimes_k B_{\alpha^{(2)}} \otimes_k \cdots \otimes_k B_{\alpha^{(n)}}.$$

Proof. (1): This has already been shown. (2): Let $N \in \mathfrak{Ts}$ be basic and normal. Then $N \hookrightarrow \mho$ and it follows from [12] that $N \cong k[T]$ is a univariate polynomial algebra. It is clear that the G-action is of the form $(T)g = T - \beta(g)$ with $\beta \in \mathrm{Hom}(G, k^+)$. Since $\ker(\beta) \leq G$ acts trivially on N, which is a faithful kG-module, we must have $\ker(\beta) = 1$, so β is injective and $N \cong B_\beta \in \mathfrak{Ts}$. (3): Let $\eta \in \mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{F}_p)$ and assume that θ is an k-algebra isomorphism $B_\alpha \to (B_\beta)^\eta$. Then $\theta(Z) = c\cdot Z + \mu$ with $c, \mu \in k$ and $c \neq 0$, such that $\theta((Z)g) = \theta(Z - \alpha(g)) = cZ + \mu - \alpha(g) = (\theta(Z))\eta(g) = (cZ+\mu)\eta(g) = c(Z - \beta(\eta(g))) + \mu$. This implies $\alpha(g) = c\cdot\beta(\eta(g))$ for all $g \in G$ and the last statement in (3) follows easily.
(4): As above we define $\theta_s \in \mathfrak{Ts}_G(B_{\alpha^{(s)}}, \mho)$ by $Z \mapsto \sum_{j=1}^n \alpha_j^{(s)} Y_j$. Assume first that $\alpha^{(s)} = (\alpha^{(1)})^{(p^{s-1})}$ with $\alpha_i^{(s)} = (\alpha_i^{(1)})^{p^{s-1}}$. Set $\Gamma := (\gamma_{ij}) = (\alpha_i^{p^{j-1}})^{-1} \in \mathrm{GL}_n(k)$, then $Y_k = \sum_{j=1}^n \gamma_{kj}\theta_j(Z)$, hence the coproduct morphism $\Theta := \coprod_{s=1}^n \theta_s := \theta_1 \otimes \cdots \otimes \theta_n$ is a surjective G-equivariant algebra homomorphism from $\otimes_{i=1}^n B_{\alpha^{(i)}}$ to $\mho$. Since both algebras are polynomial algebras of Krull-dimension n, Θ is an isomorphism. Clearly $\mho$ and each of the $B_{\alpha^{(i)}}$ are triangular and therefore erasable. It follows that $\mho \cong B_{\alpha^{(1)}} \otimes_k k[\lambda_2, \cdots, \lambda_n]$ with $k^{[n-1]} \cong k[\lambda_2, \cdots, \lambda_n] \leq \mho^G$. Now we take $\alpha^{(i)}$ for $i = 2, ..., n$ to be arbitrary embeddings $G \hookrightarrow k^+$. As before we see that $B_{\underline{\alpha}}^{\otimes n} \cong B_{\alpha^{(1)}} \otimes_k k[\mu_2, \cdots, \mu_n]$ with $k^{[n-1]} \cong k[\mu_2, \cdots, \mu_n] \leq (B_{\underline{\alpha}}^{\otimes n})^G$, so $\mho \cong B_{\underline{\alpha}}^{\otimes n}$. This finishes the proof. □

Corollary 3·16. *Let $G \cong \mathbb{F}_{p^n}^+$ and $\mathbb{F}_{p^s} \leq k$ for some $s \leq n$. Then*

$$d_k(G) \leq \begin{cases} n/s & \text{if } s \text{ divides } n \\ \lfloor n/s \rfloor + 1 & \text{otherwise} \end{cases}$$

where $\lfloor x \rfloor$ is the largest integer $\leq x$.

Proof. Let $n = ms + r$ with $0 \leq r < s$. Then Proposition 3·13 and Theorem 3·15 give $d_k((C_p)^n) \leq m\cdot d_k((C_p)^s) + d_k((C_p)^r)$, which is equal to $m = n/s$, if $r = 0$ and equal to $m + 1 = \lfloor n/s \rfloor + 1$ otherwise. □

With the help of Theorem 2·11 we can classify the minimal normal generators and minimal normal s-projective objects of $\mathfrak{Ts}$ in the case where G is elementary-abelian and k is large enough. We will use the notation introduced before Theorem 3·15:

Proposition 3·17. *Let G be elementary-abelian of order p^n and $\dim_{\mathbb{F}_p}(k) \geq n$ and let $\Gamma \in \mathfrak{Ts}$ be a normal ring. Then the following are equivalent:*
(i) *Γ is a generator and minimal in $\mathfrak{Ts}$;*
(ii) *$\Gamma \cong B_\alpha = k[Z]_\alpha$ for some embedding $\alpha:\ G \hookrightarrow k^+$;*
(iii) *Γ is an s-projective and minimal object in $\mathfrak{Ts}$.*

Proof. "(1) or (3) ⇒ (2) ": Since every generator and every s-projective object is universal, this follows from Theorem 3·15. "(2) ⇒ (3) ": This also follows directly from Theorem 3·15. "(2) ⇒ (1) ": Since B_α is basic, it is minimal in $\mathfrak{Ts}$, so it remains to show that B_α is a generator. But $B_\alpha \in \mathfrak{Ts}$ is triangular and therefore erasable, so it follows from Theorem 2·11 that B_α is an s-generator, hence a generator (see Lemma 2·7). □

4. *Basic Algebras and the Essential Dimension of G*

In this section we are going to briefly point out the connections to the notion of "essential dimension" of a group, as defined by Buhler and Reichstein ([5]). Let for the moment k be an arbitrary field and $\mathfrak{G}$ an arbitrary finite group, acting faithfully on the finite-dimensional k-vector space V. Then the essential dimension $e_k(\mathfrak{G})$ is defined to be the minimal transcendence degree over k of a field E with $k \leq E \leq k(V^*) := \mathrm{Quot}(S_k(V^*))$ such that $\mathfrak{G}$ acts faithfully on E. It can be shown, that the value $e_k(\mathfrak{G})$ only depends on the group $\mathfrak{G}$ and the field k, but not on the choice of the faithful representation (see [5] Theorem 3.1., if k has characteristic 0 and

[2] Proposition 7.1 or [6] for arbitrary field k). For an arbitrary field $K \geq k$ together with an embedding of $\mathfrak{G}$ in $\mathrm{Aut}_k(K)$, define

$$e_k(K) := \min\{\mathrm{tr.deg}_k E \mid k \leq E \leq K,\ E \text{ is} \mathfrak{G} - \text{stable with faithful action}\},$$

in other words, $e_k(K)$ is the minimum transcendence degree of a Galois field extension $E/E^{\mathfrak{G}}$ containing k and contained in K.

LEMMA 4·1. $e_k(\mathfrak{G}) = \max_{\substack{k\leq K \\ \mathfrak{G}\leq \mathrm{Aut}_k(K)}} e_k(K) = \max_{\substack{k\leq K \\ \mathfrak{G}\leq \mathrm{Aut}_k(K)}} (\min_{\substack{k\leq E\leq K \\ \mathfrak{G}\leq \mathrm{Aut}_k(E)}} \mathrm{tr.deg}_k E)$.
Moreover, $e_k(\mathfrak{G}) = e_k(L)$ *for any field* $L \leq k(V^*)$ *with* $\mathfrak{G} \leq \mathrm{Aut}_k(L)$.

Proof. Define $\tilde{e}_k(\mathfrak{G}) := \max_{\substack{k\leq K \\ \mathfrak{G}\leq \mathrm{Aut}_k(K)}} e_k(K)$. By definition $e_k(\mathfrak{G}) = e_k(k(V^*)) \leq \tilde{e}_k(\mathfrak{G})$. By [6] Proposition 2.9, $e_k(K) \leq e_k(\mathfrak{G})$ for any field K with $\mathfrak{G} \leq \mathrm{Aut}_k(K)$, hence $\tilde{e}_k(\mathfrak{G}) \leq e_k(\mathfrak{G})$. Now pick any field $L \leq k(V^*)$ with faithful $\mathfrak{G}$-action. Then by the definitions we have $e_k(\mathfrak{G}) \leq e_k(L) \leq \tilde{e}_k(\mathfrak{G})$, which finishes the proof. □

DEFINITION 4·2. *A field extension* $L \geq k$ *with* $\mathfrak{G} \leq \mathrm{Aut}_k(L)$ *will be called a* **$\mathfrak{G}$-field** *(over* k*). If* $\mathrm{tr.deg}_k L = e_k(\mathfrak{G}) = e_k(L)$*, then* L *will be called an* **essential** *$\mathfrak{G}$-field (over* k*).*

Now let k again be of characteristic $p > 0$, let G be a p-group and choose $V := V_{reg}$. Let $B \in \mathfrak{Ts}$ be basic (and cyclic, if we wish), then $B \prec D_k$ with

$$\mathrm{Quot}(B) \leq \mathrm{Quot}(D_k) \leq k(V^*).$$

Clearly G acts faithfully on $\mathrm{Quot}(B)$, so $d_k(G) = \mathrm{Dim}\,(B) \geq e_k(G)$. On the other hand, let $k \leq K$ be essential with $K \leq k(V^*)$, then we can choose a point $a \in K$ and consider the algebra $A := k[a^G] := k[(a)g \mid g \in G] \in \mathfrak{Ts}$. It follows from the definition of $e_k(G)$ that $\mathrm{Dim}\,(A) = e_k(G)$. Moreover, the map $(x_1)g \mapsto (a)g$ extends to a surjective morphism $\phi: D_k \to A$, so $A \cong D_k/\ker(\phi)$ is a cyclic domain in $\mathfrak{Ts}$. If $\mathfrak{U} \leq D_k$ is universal, there is also a morphism $\alpha \in \mathfrak{Ts}(\mathfrak{U}, A)$ and since $\alpha(\mathfrak{U}) \subseteq K$ with faithful G-action on $\alpha(\mathfrak{U})$ it follows again from the definition of $e_k(G)$ that $\mathrm{Dim}\,(A) = \mathrm{Dim}\,(\alpha(\mathfrak{U})) = e_k(G)$. Hence $d_k(G) = \mathrm{Dim}\,(B) \geq \mathrm{Dim}\,(\alpha(\mathfrak{U})) = \mathrm{tr.deg}_k(\mathrm{Quot}(\alpha(\mathfrak{U}))) = e_k(G)$, so $K \geq \mathrm{Quot}(\alpha(\mathfrak{U}))$ is an algebraic extension. Note that $\alpha(\mathfrak{U}) \cong \mathfrak{U}/\mathrm{p}$ for some G-stable prime ideal $\mathrm{p} \trianglelefteq \mathfrak{U}$. Conversely, if $\wp \in \mathrm{Spec}(\mathfrak{U})$ is G-stable such that $k(\wp) := \mathrm{Quot}(\mathfrak{U}/\wp) \leq K$, then K is algebraic over $k(\wp)$, so $k \leq k(\wp)$ is essential. It follows that $e_k(G)$ is the minimum of the transcendence degrees of "embedded residue class fields" $\mathrm{tr.deg}_k k(\wp)$ of those G-stable prime ideals $\wp \trianglelefteq \mathfrak{U}$ that satisfy $k(\wp) \hookrightarrow \mathrm{Quot}(\mathfrak{U})$. This motivates the following

DEFINITION 4·3. *Let* $A \in \mathfrak{Ts}$ *with total ring of quotients* $Q(A) := \mathrm{Quot}(A)$*. With* $\mathrm{Spec}(A)^G$ *we denote the set of* G*-stable prime ideals of* A*. We also define*

$$\mathcal{S}_A := \{k(\wp) \mid \wp \in \mathrm{Spec}(A)^G,\ \exists \text{ a } G-\text{equivariant embedding } k(\wp) \hookrightarrow Q(A)\},$$

the set of all "embedded residue class fields" of G*-stable prime ideals of* A*.*

Note that if $A \in \mathfrak{Ts}$ is a domain, then $Q(A) = k(0) \in \mathcal{S}_A$. We can now summarize

PROPOSITION 4·4. *Let* k *be a field of characteristic* $p > 0$*,* G *a group of order* p^n *and* $\mathfrak{U} \leq D_k$ *a universal trace-surjective algebra (e.g. any basic algebra). Set* $d_{\mathrm{dom},k}(G) := \min\{\mathrm{Dim}\,(C) \mid C \in \mathfrak{Ts} \mid C \text{ (cyclic) domain}\}$*, then*

$$n \geq d_k(G) \geq e_k(G) \geq d_{\mathrm{dom},k}(G).$$

Moreover $e_k(G) = e_k(Q(\mathfrak{U})) = \min\{\mathrm{tr.deg}_k k(\wp) \mid k(\wp) \in \mathcal{S}_{\mathfrak{U}}\}$ *and every essential* G*-field* $K \geq k$ *is algebraic over an essential* G*-field of the form* $k \leq k(\wp) \in \mathcal{S}_{\mathfrak{U}}$*.*

Note that we can choose $\mathfrak{U}$ to be, for example, the polynomial algebra $U = k[Y_1, \cdots, Y_n]$ mentioned in Theorem 0·6. So, at the expense of replacing a faithful linear action of G on $S(V^*)$ by a nonlinear action on U, one can reduce the dimensions of rings from which to construct essential G-fields. If for example G is cyclic of order p^n, the smallest faithful representation has dimension $p^{n-1}+1$, whereas U has Krull-dimension n. Since every *basic* algebra $B \in \mathfrak{B}$ is embedded into D_k, we have the following "intrinsic description" of the essential dimension:

COROLLARY 4·5. *Let* B *be any basic algebra in* $\mathfrak{Ts}$*, then*

$$e_k(G) = e_k(Q(B)) = \min\{\mathrm{tr.deg}_k k(\wp) \mid k(\wp) \in \mathcal{S}_B\}.$$

In Proposition 3·4 (7) we proved that a universal algebra $A \in \mathfrak{Ts}$ is basic if and only if it does not have any "embedded" trace-surjective proper factor rings. The following is a criterion in a similar spirit for the situation where $d_k(G) = e_k(G)$:

Lemma 4·6. *For any universal domain $A \in \mathfrak{Ts}$ the following are equivalent:*
(i) $\mathcal{S}_A = \{Q(A)\}$;
(ii) *A is basic and $d_k(G) = e_k(G)$;*
(iii) $e_k(G) = \mathrm{Dim}\,(A)$.
If these hold, $Q(A)$ is an essential G-field and all the others are algebraic extensions thereof.

Proof. (1) $\Rightarrow$ (2): It follows from Proposition 3·4 (7) that A is basic, hence by Corollary 4·5, $e_k(G) = \mathrm{tr.deg}_k k(\wp)$ for some $k(\wp) \in \mathcal{S}_A$. So $k(\wp) = Q(A)$, $\wp = 0$ and $d_k(G) = \mathrm{Dim}\,(A) = e_k(G)$.
(2) $\Rightarrow$ (3): This is obvious, since $\mathrm{Dim}\,(A) = d_k(G)$.
(3) $\Rightarrow$ (1): Since A is universal, Corollary 3·5 yields $\mathrm{Dim}\,(A) = e_k(G) \leq d_k(G) \leq \mathrm{Dim}\,(A)$, so A is basic. Now assume $k(\wp) \in \mathcal{S}_A$; then, $k(\wp) \leq Q(A)$ and by Corollary 4·5, $e_k(G) = e_k(Q(A)) \leq \mathrm{tr.deg}_k k(\wp) = \mathrm{Dim}\,(A/\wp) \leq \mathrm{Dim}\,(A) = e_k(G)$, so $\wp = 0$. $\square$

If k is algebraically closed, then the numerical invariant $d_k(G)$ is similar in nature to the "covariant dimension", defined and analyzed in [20] and [19] for finite groups acting on varieties in characteristic zero. The analogue for arbitrary fields would be to define $\mathrm{covdim}_k(\mathfrak{G})$ as the minimum Krull dimension of a faithful subalgebra of some $S(V^*)$, in contrast to $d_k(G)$, which is the minimum Krull dimension of a trace-surjective subalgebra of $D_k(G)$. Using arguments of [20] one can see that $e_k(\mathfrak{G}) \leq \mathrm{covdim}_k(\mathfrak{G}) \leq e_k(\mathfrak{G}) + 1$ for arbitrary field k. The fact that $D_k(G) < S(V_{reg})[1/X]$ implies the inequalities $d_k(G) \geq e_k(G)$ and $d_k(G) + 1 \geq \mathrm{covdim}_k(G)$.
Let $T := k(x_1, \cdots, x_n)$ be a purely transcendental field extension and $L \leq T$ a subfield of transcendence degree $m \leq n-1$. Then it follows from a result of Roquette and Ohm (see Proposition 8.8.1. [17]) that L can be embedded into $k(x_1, \cdots, x_{n-1})$. An obvious induction shows that, indeed, L can be embedded into $k(x_1, \cdots, x_m)$. This can be used to obtain the following result:

Proposition 4·7. *Let $A \in \mathfrak{Ts}$ with $A \leq D_k$ and assume that G is not isomorphic to a subgroup of $\mathrm{Aut}_k(L)$ for any intermediate field $k < L \leq k(x_1, \cdots, x_{m-1})$ with $L = k(\wp) \in \mathcal{S}_A$. Then $m \leq e_k(G)$.*

Proof. By Proposition 4·4 there is an essential G-field $k(\wp) \in \mathcal{S}_A$ with $k(\wp) \leq Q(A) \leq Q(D_k) \cong k(x_1, \cdots, x_{|G|-1})$. Assume $e_k(G) < m$, then $k(\wp)$ can be embedded into $k(x_1, \cdots, x_{m-1})$ and $G \leq \mathrm{Aut}(k(\wp))$. This contradiction finishes the proof. $\square$

By Lüroth's theorem, any intermediate field $k < L \leq k(x_1)$ is rational, i.e. isomorphic to $k(x_1)$ and therefore $\mathrm{Aut}_k(L) \cong \mathrm{PGL}_2(k)$. From this we obtain:

Proposition 4·8. *Let k be a field of characteristic $p > 0$ and $1 \neq G$ a finite p-group. Then the following are equivalent:*
(i) $d_k(G) = 1$;
(ii) $e_k(G) = 1$;
(iii) $G \cong \mathbb{F}_{p^n}^+ \leq k$;
(iv) *G is isomorphic to a subgroup of $\mathrm{GL}_2(k)$.*

Proof. "(3) $\iff$ (4)" is clear, since the finite p-groups of $\mathrm{GL}_2(k)$ are isomorphic to subgroups of the additive group $\mathbf{G}_a = (k, +)$.
"(1)$\Rightarrow$ (2)" is clear, because $e_k(G) = 0 \iff G = 1 \iff d_k(G) = 0$.
"(2)$\Rightarrow$ (4)": If G is not isomorphic to a subgroup of $\mathrm{PGL}_2(k)$ we take $A := D_k$ and $m = 2$ in Proposition 4·7. By Lüroth's theorem $\mathrm{Aut}_k(L) \cong \mathrm{PGL}_2(k)$ for any intermediate field $k < L \leq k(x_1)$, hence $2 \leq e_k(G)$.
"(3)$\Rightarrow$ (1)": This follows from Theorem 3·15. $\square$

Corollary 4·9. *Let k be a field of characteristic $p > 0$ and G a finite p-group, then $d_k(G) = 2$ if and only if $e_k(G) = 2$.*

Corollary 4·10. *Let $G \in \{C_p \times C_p, C_{p^2}\}$; assume moreover that k is the prime field $\mathbb{F}_p$ in the case $G = C_p \times C_p$. Then $d_k(C_{p^2}) = e_k(C_{p^2}) = 2 = d_{\mathbb{F}_p}(C_p \times C_p) = e_{\mathbb{F}_p}(C_p \times C_p)$.*

Proof. Note that G is not isomorphic to a subgroup of $\mathrm{PGL}_2(k)$, hence $2 \leq e_k(G) \leq d_k(G) \leq 2$, by Proposition 4·4. $\square$

Proposition 4·11. *Let G be elementary-abelian of order p^n with $n \geq 3$ and k be any field of characteristic p. Then $e_k(G) \leq 2$.*

Proof. We can assume $k = \mathbb{F}_p$. We use the description of G and further notation from Theorem 3·15 and the arguments immediately before that. In particular $U = k[Y_1, \cdots, Y_n]$ with G-action given by $(Y_j)g_i = Y_j - \delta_{ij}$. Let $b \in U^G \backslash k$, so that b is transcendental over k and put $A = k[b, bY_1 + b^2Y_2 + b^3Y_3 + \ldots + b^nY_n] < U$.

Clearly A is a polynomial subalgebra of U with only two generators on which G acts faithfully. Note that for $Z := \sum_{i=1}^n b^i Y_i$ and $\underline{b} := (b, b^2, \cdots, b^n)$, we have $k(b) \otimes_k A \cong k(b)[Z]_{\bar{b}}$, in the notation of Theorem 3·15. It follows that $\mathrm{Quot}(A) < \mathrm{Quot}(U)$, contains a trace-surjective algebra which is a quotient of U of Krull dimension 2. In particular $e_{F_p}(G) \le 2$. □

REMARK 4·12.

(i) *In the case where k is a field of characteristic different from p, containing a primitive p-th root of unity and G is a finite p-group, $e_k(G)$ is equal to the least dimension of a faithful linear representation of G over k (see* [**18**]*).*

(ii) *The result in Proposition 4·8 has been obtained in* [**21**] *for arbitrary finite groups and infinite fields k, together with the consequence that $e_k(C_p \times C_p) = 1$. The result of Proposition 4·8, that $e_k(G) = 1$ for G being elementary abelian and $|G| \le |k|$ has also been obtained with a different method in* [**22**] *Lemma 2. In* [**8**] *the groups with essential dimension one were classified for all fields k. We are not aware that the general bound in Proposition 4·11, which is independent of k, already appears in the literature.*

(iii) *The results in Corollaries 4·9, 4·10, Proposition 4·11 and Theorem 3·15 show that the group invariants $d_k(G)$ and $e_k(G)$ depend crucially on the choice of the ground field k.*

(iv) *Set $A := k[x, y]$, the polynomial ring in two variables, and $G := \langle g \rangle \cong C_{p^2}$, then there is a G-action on A defined by $(x)g = x + y^{p-1}$ and $(y)g = y - 1$. Using* [**13**] *Lemma 5.2. one can show that $A \in \mathfrak{T}\mathfrak{s}$ is standard universal (i.e. a retract of D_k). Then it follows from 4·10, that A is a basic object in $\mathfrak{T}\mathfrak{s}$, $Q(A)$ is an essential G-field and all essential G-fields are algebraic extensions of $Q(A)$.*

5. *Concluding Remarks*

We conclude this article with a couple of open questions:

- In all cases where we know $d_k(G)$, there exists a basic algebra which is an erasable polynomial ring. Is there always an erasable basic algebra? Its ring of G-invariants would be stably polynomial.
- If $k = \mathbb{F}_p$ we dare to conjecture that $d_k(G) = n = \log_p(|G|)$. This would follow from a positive answer to the first question and Proposition 5.5 in [**13**].
- Does every erasable algebra in $\mathfrak{T}\mathfrak{s}$ have a polynomial invariant ring?

REFERENCES

[**1**] M. Auslander and O. Goldmann. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, 97:367–409, 1960.

[**2**] G Berhuy and G Favi. Essential Dimension: A functorial point of view (after A Merkurjev). *Documenta Mathematica*, 8:270–330, 2003.

[**3**] Nicolas Bourbaki. *Groupes et algèbres de Lie, Chap. IV, V, VI.* Herman, Paris, 1968.

[**4**] W. Bruns and J. Herzog. *Cohen - Macaulay Rings.* Cambridge University Press, 1993.

[**5**] Joe Buhler and Zinovy Reichstein. On the essential dimension of a finite group. *Compos. Math.*, 106:159–179, 1997.

[**6**] Ming chang Kang. Essential dimensions of finite groups. *arXiv.math*, 0611673v2:1 – 24, 2006.

[**7**] S U Chase, D K Harrison, and A Rosenberg. Galois theory and Galois cohomology of commutative rings. *Memoirs of the AMS*, 52:15–33, 1965.

[**8**] H. Chu, S. J. Hu, M. C. Kang, and J. Zhang. Groups with essential dimension one. *Asian. Journal of Mathematics*, 12((2)):177–191, 2008.

[**9**] D.J.Benson. *Polynomial Invariants of Finite Groups.* Cambridge University Press, 1993.

[**10**] D.L.Costa. Retracts of polynomial rings. *J. of Algebra*, 44:492–502, 1975.

[**11**] A Duncan and Z. Reichstein. Versality of algebraic group actions and rational points on twisted varieties. with an appendix containing a letter from j.-p. serre. *J. Algebraic Geom.*, 3:499–530, 2015.

[**12**] P. Eakin. A note on finite dimensional subrings of polynomial rings. *Proc. Amer. Math. Soc.*, 31(1):75–80, 1972.

[**13**] P. Fleischmann and C.F. Woodcock. Non-linear group actions with polynomial invariant rings and a structure theorem for modular Galois extensions. *Proc. LMS*, 103(5):826–846, November 2011.

[**14**] P. Fleischmann and C.F. Woodcock. Universal Galois Algebras and Cohomology of p-groups. *Journal of Pure and Applied Algebra*, 217(3):530–545, 2013.

[**15**] P. Fleischmann and C.F. Woodcock. Modular group actions on algebras and p-local Galois extensions for finite groups. *Journal of Algebra*, 442:316–353, 2015.

[**16**] N Gupta. On the cancellation problem for the affine space $\mathbb{A}^3$ in characteristic p. *arXiv:1208.0483v2*, pages 1–9, 2013.

[**17**] C U Jensen, A Ledet, and N Yui. *Generic Polynomials.* Cambridge University Press, 2002.

[**18**] N. A. Karpenko and A. S. Merkurjev. Essential dimension of finite p-groups. *Invent.Math.*, 172((3)):491–508, 2008.
[**19**] H. Kraft, R. Lötscher, and G.W. Schwarz. Compression of finnite group actions and covariant dimension II. *J. Algebra*, 322:94–107, 2009.
[**20**] H. Kraft and G.W. Schwarz. Compression of finnite group actions and covariant dimension. *J. Algebra*, 313:268–291, 2007.
[**21**] A Ledet. Finite groups of essential dimension one. *J. of Algebra*, 311:31–37, 2007.
[**22**] Arne Ledet. On the essential dimension of p-groups. In *Galois theory and modular forms*, number 11 in Dev. Math., pages 159–172. Kluwer, 2003.
[**23**] M Lorenz. *Multiplicative Invariant Theory.* Springer, 2005.
[**24**] Vladimir L. Popov. *Sections in Invariant Theory.* Scand. Univ. Press, Oslo, 1994.
[**25**] Z. Reichstein. On the notion of essential dimension for algebraic groups. *Transform. Groups*, 5:265–304, 2000.
[**26**] J P Serre. Cohomological invariants, witt invariants, and trace forms. In *Cohomological invariants in Galois cohomology*, pages 1–100. Amer. Math. Soc., 2003.
[**27**] Jean-Pierre Serre. How to use finite fields for problems concerning infinite fields. *arXiv:0903.0517v2*, pages 1–12, 2009.
[**28**] L. Smith. *Polynomial Invariants of Finite Groups.* A K Peters, 1995.
[**29**] V.Shpilrain and Jie-Tai Yu. Polynomial retracts and the Jacobian conjecture. *Trans. of AMS*, 352(1):477–484, 1999.

Author's current addresses:
P. Fleischmann, School of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury, CT2 7NF, UK
e-mail: `P.Fleischmann@kent.ac.uk`

C.F.Woodcock, School of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury, CT2 7NF, UK
e-mail: `C.F.Wooodcock@kent.ac.uk`