Article:
Bavula, V.V. (2024) Isomorphism problems and groups of automorphisms for ore extensions K[x][y; fd/dx] (prime characteristic). Algebras and Representation Theory, 27. pp. 2389-2422. ISSN: 1386-923X

https://doi.org/10.1007/s10468-024-10301-w

Algebras and Representation Theory (2024) 27:2389–2422
https://doi.org/10.1007/s10468-024-10301-w

Isomorphism Problems and Groups of Automorphisms for Ore Extensions $K[x][y; f\frac{d}{dx}]$ (Prime Characteristic)

V. V. Bavula[1]

Received: 15 March 2023 / Accepted: 16 November 2024 / Published online: 4 December 2024

Abstract
Let $\Lambda(f) = K[x][y; f\frac{d}{dx}]$ be an Ore extension of a polynomial algebra $K[x]$ over an arbitrary field K of characteristic $p > 0$ where $f \in K[x]$. For each polynomial f, the automorphism group of the algebras $\Lambda(f)$ is explicitly described. The automorphism group $\mathrm{Aut}_K(\Lambda(f)) = \mathbb{S} \rtimes G_f$ is a semidirect product of two explicit groups where G_f is the *eigengroup* of the polynomial f (the set of all automorphisms of $K[x]$ such that f is their common eigenvector). For each polynomial f, the eigengroup G_f is explicitly described. It is proven that every subgroup of $\mathrm{Aut}_K(K[x])$ is the eigengroup of a polynomial. It is proven that the Krull and global dimensions of the algebra $\Lambda(f)$ are 2. The prime, completely prime, primitive and maximal ideals of the algebra $\Lambda(f)$ are classified.

Keywords A skew polynomial ring · Automorphism · The eigengroup of a polynomial · A prime ideal · A completely prime ideal · A primitive ideal · A maximal ideal · Simple module · The Krull dimension · The global dimension · The centre · Localization · A left denominator set · An Ore set · A normal element

Mathematics Subject Classification (2010) 16D60 · 13N10 · 16S32 · 16P90 · 16U20

1 Introduction

In this paper, module means a left module, K is a field of characteristic $p > 0$ and $\overline{K}$ is its algebraic closure, $K^\times := K\backslash\{0\}$, $K[x]$ be a polynomial algebra in the variable x over K, $\mathrm{Der}_K(K[x]) = K[x]\frac{d}{dx}$ is the set of all K-derivations of the algebra $K[x]$,

$$\Lambda := \Lambda(f) := K[x][y; \delta := f\frac{d}{dx}] = K\langle x, y \mid yx - xy = f\rangle = \bigoplus_{i\geq 0} K[x]y^i$$

is an Ore extension of the algebra $K[x]$ where $f = f(x) \in K[x]$. Given an algebra D and its derivation δ, the *Ore extension* of D, denoted $D[y; \delta]$, is an algebra generated by the algebra

Presented by: K Goodearl

✉ V. V. Bavula
v.bavula@sheffield.ac.uk

1 Department of Pure Mathematics, University of Sheffield, Hicks Building, S3 7RH Sheffield, UK

D and y subject to the defining relations $yd - dy = \delta(d)$ for all $d \in D$. The algebra Λ is a Noetherian domain of Gelfand-Kirillov dimension 2.

The aim of the paper is for each polynomial f to give an explicit description of the automorphism group $\mathrm{Aut}_K(\Lambda(f))$ of the algebra $\Lambda(f)$.

We can assume that the polynomial f is *monic*, i.e. its leading coefficient is 1 provided $f \neq 0$ (by changing the generators from (x, y) to $(x, l^{-1}y)$ where l is the leading coefficient of the polynomial f). Then the algebras $\{\Lambda(f) \mid f \in K[x]\}$ as a class is a disjoint union of four subclasses: $f = 0$, $f = 1$, the polynomial f has only a *single* root in $\overline{K}$ and the polynomial f has at least two *distinct* roots in $\overline{K}$.

If $f = 0$ then the algebra $\Lambda(0) = K[x, y]$ is a polynomial algebra in two variables and its group of automorphisms is well-known [16]: The group $\mathrm{Aut}_K(K[x, y])$ is generated by the automorphisms:

$$\begin{aligned} t_\mu &: x \mapsto \mu x, & y &\mapsto y,\\ \Phi_{n,\lambda} &: x \mapsto x + \lambda y^n, & y &\mapsto y,\\ \Phi'_{n,\lambda} &: x \mapsto x, & y &\mapsto y + \lambda x^n, \end{aligned}$$

where $n \geq 0$, $\mu \in K^\times$, and and $\lambda \in K$.

If $f = 1$ then the algebra $\Lambda(1)$ is the (first) *Weyl algebra*

$$A_1 = K\langle x, \partial \mid \partial x - x\partial = 1\rangle \simeq K[x][y; \frac{d}{dx}].$$

In characteristic zero Dixmier [10], and in prime characteristic Makar-Limanov [13], gave an explicit set of generators for the automorphism group $\mathrm{Aut}_K(A_1)$ (see also [4] for more results on $\mathrm{Aut}_K(A_1)$): The group $\mathrm{Aut}_K(A_1)$ is generated by the automorphisms:

$$\begin{aligned} \Phi_{n,\lambda} &: x \mapsto x + \lambda y^n, & y &\mapsto y,\\ \Phi'_{n,\lambda} &: x \mapsto x, & y &\mapsto y + \lambda x^n, \end{aligned}$$

where $n \geq 0$ and $\lambda \in K$.

The first Weyl algebra A_1 belongs to a wide class of algebras - the class of generalized Weyl algebras. In [3], Bavula and Jordan found explicit generators for generalized Weyl algebras over a polynomial algebra in a single variable over a field of characteristic zero. Alev and Dumas [1] initiated the study of automorphisms of Ore extensions $\Lambda(f)$ in characteristic zero case. Their results were extended also to prime characteristic by Benkart, Lopes and Ondrus [6]. The algebra $\Lambda(x^2)$ (the Jordan plane) was studied by Shirikov [14], Cibils, Lauve, and [9], and Iyudu [11]. The example of the enveloping algebra of the nonabelian Lie algebra of dimension 2 studied by Martha K. Smith [15, Corollary 18]. Gadis [8] studied isomorphism problems for algebras on two generators that satisfy a single quadratic relation.

Isomorphism problems for the algebras $\Lambda(f)$. Theorem 1.1 is an isomorphism criterion for the algebras Λ.

Theorem 1.1 *Let $f, g \in K[x]$ be polynomials. Then $\Lambda(f) \simeq \Lambda(g)$ iff $g(x) = \lambda f(\alpha x + \beta)$ for some elements $\lambda, \alpha \in K^\times$ and $\beta \in K$.*

In characteristic zero, Theorem 1.1 was proven by Alev and Dumas [1, Proposition 3.6] (1997) and in prime characteristic – by Benkart, Lopes and Ondrus [6, Theorem 8.2] (2015).

Benkart, Lopes and Ondrus [6, Theorems 8.3 and 8.6] gave a description of the *set* of automorphisms groups of algebras $\Lambda(f)$ over arbitrary fields and if the automorphism group of $\Lambda(f)$ is *given* they presented information on the type of the polynomial f, [6, Corollary

8.7] (in general, if one fixes the type of the polynomial then the automorphism group is *larger* than the one which is naively expected). In this paper, we proceed in the opposite direction: if the polynomial f is *given* then the automorphism group $\mathrm{Aut}_K\,\Lambda(f)$ is explicitly described.

The eigengroup $G_f(K)$ of a polynomial $f \in K[x]$. Recall that $\mathrm{Aut}_K(K[x]) = \{\sigma_{\lambda,\mu} \mid \lambda \in K^\times, \mu \in K\}$ where $\sigma_{\lambda,\mu}(x) = \lambda x + \mu$.

Definition 1.2 [5] For a polynomial $f \in K[x]$,

$$G_f = G_f(K) := \{\sigma \in \mathrm{Aut}_K(K[x]) \mid \sigma(f) = \lambda_\sigma f \ \text{ for some } \ \lambda_\sigma \in K^\times\} \qquad (1)$$

is called the *eigengroup* of the polynomial *f*.

Clearly, the set $G_f(K)$ is a subgroup of $\mathrm{Aut}_K(K[x])$, it is the largest subgroup of $\mathrm{Aut}_K(K[x])$ such that the polynomial *f* is their common eigenvector. For all scalars $\mu \in K$, $G_\mu = \mathrm{Aut}_K(K[x])$. For all scalars $\nu \in K^\times$, $G_f = G_{\nu f}$. So, in order to describe the eigengroup $G_f(K)$ we can assume that the polynomial *f* is a monic polynomial. It is proven that every subgroup of $\mathrm{Aut}_K(K[x])$ is the eigengroup of a polynomial (Theorem 4.35). For each subgroup G of $\mathrm{Aut}_K(K[x])$ all the polynomials $f \in K[x]$ with $G_f = G$ are explicitly described in the case when the field K is algebraically closed. The most interesting and difficult case is when the group G is a finite group. There are three types of finite subgroups in $\mathrm{Aut}_K(K[x])$ that are not the identity group. For each such group G, the polynomial f with $G_f = G$ has a unique form/presentation the, so-called, *eigenform* of *f*.

The eigengroup G_f has an isomorphic copy in the automorphism group $\mathrm{Aut}_K(\Lambda(f))$: The map

$$G_f(K) \to \mathrm{Aut}_K(\Lambda(f)), \sigma_{\lambda,\mu} \mapsto \sigma_{\lambda,\mu} : x \mapsto \lambda x + \mu, \quad y \mapsto \lambda^{\deg(f)-1} y \qquad (2)$$

is a group monomorphism where $\deg(f)$ is the degree of the polynomial f. We identify the group $G_f(K)$ with its image in $\mathrm{Aut}_K(\Lambda(f))$. The group $G_f(K)$ is the most important/difficult part of the group $\mathrm{Aut}_K(\Lambda(f))$. Approximately half of the paper is about how to find it. If the group $G_f(K)$ is a finite group it is a semidirect product of two subgroups, $G_f(K) = \widetilde{G}_f(K) \rtimes \overline{G}_f(K)$ (Theorem 4.4).

There are four distinguish cases:

1. $\widetilde{G}_f \neq \{e\}$, $\overline{G}_f \neq \{e\}$,
2. $\widetilde{G}_f \neq \{e\}$, $\overline{G}_f = \{e\}$,
3. $\widetilde{G}_f = \{e\}$, $\overline{G}_f \neq \{e\}$,
4. $\widetilde{G}_f = \{e\}$, $\overline{G}_f = \{e\}$.

In the case when $K = \overline{K}$, Theorem 4.24, 4.27, 4.30 and 4.32 are criteria for each case to hold, respectively (see also Proposition 4.10). These four theorems are also explicit descriptions of the eigengroup $G_f(K)$. They also show that in each of four cases the polynomial *f* admits a *unique* presentation – *the eigenform* of *f* (introduced in the paper).

At the end of Section 4, a finite algorithm is given of finding the eigengroups $G_f(\overline{K})$ and $G_f(K)$, and the eigenform of *f*.

In the case when $K \neq \overline{K}$, similar results are obtained, see Theorem 4.33. Proposition 4.34 gives criteria for the groups $\widetilde{G}_f(K)$, $\overline{G}_f(K)$ and $G_f(K)$ to be $\{e\}$.

The group of automorphisms of the algebra $\Lambda(f)$. Given a group G, a normal subgroup N and a subgroup H. The group G is called the *semidirect product* of N and H, written $G = N \rtimes H$, if $G = NH := \{nh \mid n \in N, h \in H\}$ and $N \cap H = \{e\}$ where e is the identity of the group G.

The automorphism group $\mathrm{Aut}_K(\Lambda(f))$ of the algebra $\Lambda(f)$ contains an obvious subgroup

$$\mathbb{S} := \mathbb{S}(K) := \{s_p \mid p \in K[x]\} \simeq (K[x], +), \ s_p \mapsto p \ \text{ where } \ s_p(x) = x \text{ and } s_p(y) = y + p. \tag{3}$$

Theorem 1.3 *Suppose that $f \in K[x]$ is a monic non-scalar polynomial. Then*

$$\mathrm{Aut}_K(\Lambda(f)) = \mathbb{S}(K) \rtimes G_f(K).$$

The Krull and global dimensions of the algebra $\Lambda(f)$. It it proven that the Krull and global dimensions of the algebra $\Lambda(f)$ are 2 (Theorem 2.5).

Classifications of prime, completely prime, primitive and maximal ideals of the algebra $\Lambda(f)$. Theorem 2.3 classifies prime, completely prime, primitive and maximal ideals of the algebra $\Lambda(f)$. The height 1 prime ideals were classified in [6, Theorem 7.6]. It is proven that every nonzero ideal of the algebra $\Lambda(f)$ meets the centre of $\Lambda(f)$ (Corollary 2.2).

Classifications of simple $\Lambda(f)$-modules. In [2], simple modules were classified for all Ore extensions $A = D[x; \sigma, \partial]$ where D is a Dedekind domain, $\sigma \in$ is an automorphism of D and ∂ is a σ-derivation of D (for all $a, b \in D$, $\partial(ab) = \partial(a)b + \sigma(a)\partial(b)$). Recall that the ring A is generated by D and x subject to the defining relations: For all elements $d \in D$, $xd = \sigma(d)x + \partial(d)$. The algebras $\Lambda(f)$ is a a very special case of the rings A.

Theorem 2.4 classifies simple *left* $\Lambda(f)$-modules, see also [7]. For each simple left $\Lambda(f)$-module an explicit K-basis is given and the actions of the canonical generators x and y of the algebra $\Lambda(f)$ on the basis is explicitly described.

A classification of simple *right* $\Lambda(f)$-modules is obtained at once from the classification of simple left $\Lambda(f)$-modules by using the fact that the opposite algebra $\Lambda(f)^{op}$ of the algebra $\Lambda(f)$ is isomorphic to

$$\Lambda(f)^{op} \simeq \Lambda(-f). \tag{4}$$

Recall that the *opposite algebra* A^{op} of an algebra A coincides with the algebra A as vector space but the multiplication in A^{op} is given by the rule $a \cdot b = ba$. Every right A-module is a left A^{op}-module and vice versa.

2 Spectra, the Centre, the Krull and Global Dimensions of the Algebra Λ

In this section, K is a field of characteristic $p > 0$ (not necessarily algebraically closed) and $f = p_1^{n_1} \cdots p_s^{n_s}$ is a non-scalar polynomial of $K[x]$ where $p_1, \ldots, p_s$ are irreducible, co-prime divisors of f (i.e. $K[x]p_i + K[x]p_j = K[x]$ for all $i \neq j$). The aim of this section is to find the centre of the algebra $\Lambda(f)$; to classify simple $\Lambda(f)$-modules; to classify prime, completely prime, primitive and maximal ideals of the algebra $\Lambda(f)$; and to prove that the Krull and global dimension of the algebra $\Lambda(f)$ is 2.

The centre of the algebra $\Lambda(f)$. It follows from the direct sum

$$A_1 = \bigoplus_{i,j=0}^{p-1} K[x^p, \partial^p]x^i\partial^j$$

and the commutation relation $[\partial, x] = 1$, that the centre $Z(A_1)$ of the Weyl algebra is equal to $K[x^p, \partial^p]$, a polynomial algebra in two variables. Let $K(x^p, \partial^p)$ be the field of fractions of the polynomial algebra $K[x^p, \partial^p]$. The localization $\mathcal{A}_1$ of the Weyl algebra A_1 by the Ore set $K[x^p, \partial^p]\backslash\{0\}$ is a simple p^2-dimensional algebra

$$\mathcal{A}_1 = \bigoplus_{i,j=0}^{p-1} K(x^p, \partial^p)x^i\partial^j.$$

This follows from the relation $[\partial, x] = 1$. So, $Z(\mathcal{A}_1) = K(x^p, \partial^p)$. Hence, *every nonzero ideal of the Weyl algebra A_1 meets the centre of A_1.*

The polynomial algebra $K[x]$ is a left A_1-module where ∂ acts as the derivation $\frac{d}{dx}$. Furthermore, the kernel of the corresponding algebra homomorphism

$$A_1 \to \mathrm{End}_K(K[x]), \quad x \mapsto x, \quad \partial \mapsto \frac{d}{dx} \tag{5}$$

is generated by the central element ∂^p. So, $A_1/(\partial^p) = \bigoplus_{i=0}^{p-1} K[x]\partial^i \subseteq \mathrm{End}_K(K[x])$. The factor algebra $A_1/(\partial^p)$ is a subalgebra of the algebra $\mathcal{D}(K[x])$ of differential operators on the polynomial algebra $K[x]$ and the Weyl algebra A_1 is not. This is in sharp contrast with the characteristic zero case where $A_1 = \mathcal{D}(K[x])$.

The algebra $\Lambda = \Lambda(f)$ can be identified with a subalgebra of the Weyl algebra A_1 by the monomorphism:

$$\Lambda \to A_1, \quad x \mapsto x, \quad y \mapsto f\partial. \tag{6}$$

So, $\Lambda = K\langle x, y = f\partial\rangle \subset A_1$. Theorem 2.1 describes the centre of the algebra $\Lambda(f)$. It also gives explicit expressions for the p'th power of various elements of the algebras $\Lambda(f)$ and A_1 that are key facts in finding the centre of $\Lambda(f)$.

The fact that the centre of the algebra $\Lambda(f)$ is equal to $K[x^p, y^p - (\delta^{p-2}(f))'y]$ was proven by Benkart, Lopes and Ondrus, [6, Theorem 5.3,(2)]. Here we present a short proof of this fact.

Theorem 2.1 *Let $\delta = f\frac{d}{dx} \in \mathrm{Der}_K(K[x])$ where $f \in K[x]\backslash\{0\}$, and $g' := \frac{dg}{dx}$ where $g \in K[x]$. Then:*

1. $\delta^p = (\delta^{p-2}(f))'\delta \in \mathrm{Der}_K(K[x])$.
2. *In the algebra $\Lambda(f)$, $y^p = f^p\partial^p + (\delta^{p-2}(f))'y$. In particular, in the Weyl algebra A_1, $(f\partial)^p = f^p\partial^p + (\delta^{p-2}(f))'f\partial$.*
3. *The centre $Z(\Lambda(f))$ of the algebra $\Lambda(f)$ is the polynomial algebra*

$$K[x^p, y^p - (\delta^{p-2}(f))'y] = K[x^p, f^p\partial^p]$$

and $f^p\partial^p = y^p - (\delta^{p-2}(f))'y$.

4. *The algebra $\Lambda(f) = \bigoplus_{i,j=0}^{p-1} Z(\Lambda(f))x^iy^j$ is a free $Z(\Lambda(f))$-module of rank p^2.*
5. *The localization of the algebra $\Lambda(f)$ at the Ore set $Z(\Lambda(f))\backslash\{0\}$ is $\mathcal{A}_1$.*

Proof 1. Since $\delta^p \in \mathrm{Der}_K(K[x])$, we have that $\delta^p = g\frac{d}{dx}$ where $g = \delta^p(x) = \delta^{p-1}(f) = (\delta^{p-2}(f))'f$. Therefore,

$$\delta^p = (\delta^{p-2}(f))'f\frac{d}{dx} = (\delta^{p-2}(f))'\delta.$$

2. Notice that $y^p = (f\partial)^p = f^p\partial^p + \sum_{i=1}^{p-1} a_i\partial^i$ for some elements $a_i \in K[x]$. Recall that $A_1/(\partial^p) = \bigoplus_{i=0}^{p-1} K[x]\partial^i \subseteq \mathrm{End}_K(K[x])$. By statement 1,

$$(f\partial)^p \equiv \sum_{i=1}^{p-1} a_i\partial^i \equiv (\delta^{p-2}(f))'\delta \equiv (\delta^{p-2}(f))'f\partial \equiv (\delta^{p-2}(f))'y \mod (\partial^p),$$

and so $a_1 = (\delta^{p-2}(f))' f$ and $a_2 = \cdots = a_{p-1} = 0$.

3–5. By statement 2, $f^p \partial^p = y^p - (\delta^{p-2}(f))' y \in Z(\Lambda(f))$. Hence,

$$Z' := K[x^p, y^p - (\delta^{p-2}(f))' y] = K[x^p, f^p \partial^p] \subseteq Z(\Lambda(f))$$

and $\Lambda(f) = \bigoplus_{i,j=0}^{p-1} Z' x^i y^j$. Now,

$$(Z' \backslash \{0\})^{-1} \Lambda(f) = \bigoplus_{i,j=0}^{p-1} K(x^p, \partial^p) x^i y^j = \bigoplus_{i,j=0}^{p-1} K(x^p, \partial^p) x^i \partial^j = \mathcal{A}_1,$$

and so statement 5 is obvious and statements 3–4 follow. □

Let A be an algebra and $a \in A$. The map $\mathrm{ad}_a = [a, -] : A \to A$, $b \mapsto [a, b] := ab - ba$ is a derivation of the algebra A which is called the *inner derivation* of A associated with the element a.

Corollary 2.2 *Every nonzero ideal of the algebra $\Lambda(f)$ meets the centre of $\Lambda(f)$.*

Proof Let I be a nonzero ideal of the algebra $\Lambda(f)$. Fix a nonzero element of I, say $a = \sum_{i,j=0}^{p-1} z_{ij} x^i \partial^j$ for some elements $z_{ij} \in Z(\Lambda(f))$, by Theorem 2.1.(4). Then applying several times the inner derivation $\mathrm{ad}_x := [x, -]$ of the algebra $\Lambda(f)$, we obtain a nonzero element, say $b \in I \cap Z(\Lambda(f))[x]$. Then $0 \neq b^p \in I \cap Z(\Lambda(f))$. □

The prime, completely prime, primitive and maximal spectra of the algebra Λ. An ideal $\mathfrak{p}$ of a ring R is called a *completely prime ideal* if the factor ring $R/\mathfrak{p}$ is a domain. A completely prime ideal is a prime ideal. The sets of prime and completely prime ideals of the ring R are denoted by $\mathrm{Spec}(R)$ and $\mathrm{Spec}_c(R)$, respectively. The annihilator of a simple R-module is called a *primitive idea*l of R. Every primitive ideal is a prime ideal of R. The set of all primitive ideals is denoted by $\mathrm{Prim}(R)$. The set of all maximal ideals of R is denoted by $\mathrm{Max}(R)$. Clearly, $\mathrm{Max}(R) \subseteq \mathrm{Prim}(R) \subseteq \mathrm{Spec}(R)$.

An element a of an algebra A is called a *normal element* of A if $Aa = aA$. An element a of an algebra A is called a *regular element* if it is not a zero divisor. The set of all regular elements of the algebra A is denoted by $\mathcal{C}_A$. Each regular normal element a of the algebra A determines an automorphism of the algebra A given by the rule:

$$\omega_a : A \to A, \quad b \mapsto \omega_a(b) \ \text{ where } \ ab = \omega_a(b) a. \tag{7}$$

The elements $p_1, \ldots, p_s$ are regular normal elements of the algebra $\Lambda = \Lambda(f)$ (recall that $f = \prod_{i=1}^s p_i^{n_i}$) since

$$y p_i = p_i (y - p_i^{-1} f) \ \text{ and } \ x p_i = p_i x.$$

Therefore, $\omega_{p_i}(x) = x$ and $\omega_{p_i}(y) = y + p_i^{-1} f$.

For an ideal $\mathfrak{a}$ of an algebra A, we denote by $V(\mathfrak{a})$ the set of all prime ideals of A that contain the ideal $\mathfrak{a}$. Let $\min \mathfrak{a}$ be the *set of minimal primes* of $\mathfrak{a}$. These are the minimal elements of the set $V(\mathfrak{a})$ with respect to inclusion. Suppose that the set $S_a := \{a^i \mid i \geq 0\}$ is a left Ore set of a domain A. The algebra $A_a := S_a^{-1} A = \{a^{-i} b \mid i \geq 0, b \in A\}$ is called the localization of A at the powers of the element a.

For a commutative algebra C and a non-nilpotent element $s \in C$, the map

$$\mathrm{Spec}(C) \backslash V(s) \to \mathrm{Spec}(C_s), \quad \mathfrak{p} \mapsto S_s^{-1} \mathfrak{p}$$

is a bijection with the inverse map $\mathfrak{q} \mapsto C \cap \mathfrak{q}$. We identify the sets $\mathrm{Spec}(C)\backslash V(s)$ and $\mathrm{Spec}(C_s)$ via the bijection above, i.e. $\mathrm{Spec}(C)\backslash V(s) = \mathrm{Spec}(C_s)$.

Recall that the centre of the Weyl algebra $A_1 = K[x][\partial; \frac{d}{dx}]$ is the polynomial algebra $K[x^p, \partial^p]$ (the result is well-known). Then

$$f^p \in K[x^p] \subseteq Z(\Lambda(f)) = K[x^p, f^p\partial^p] \subseteq K[x^p, \partial^p] = Z(A_1)$$

and

$$\begin{aligned} L = \Lambda(f) \subseteq L_f = A_{1,f} = L_{f^p} = A_{1,f^p} &= \bigoplus_{i,j=0}^{p-1} Z(L)_{f^p} x^i y^i \\ &= \bigoplus_{i,j=0}^{p-1} Z(A_1)_{f^p} x^i \partial^i = \bigoplus_{i,j=0}^{p-1} K[x^p, \partial^p]_{f^p} x^i \partial^i. \end{aligned} \tag{8}$$

In particular, $Z(L)_{f^p} = Z(A_1)_{f^p} = K[x^p, \partial^p]_{f^p}$, and so we can write

$$\begin{aligned} \mathrm{Spec}(Z(L))\backslash V(f^p) &= \mathrm{Spec}(Z(L)_{f^p}) = \mathrm{Spec}(Z(A_1)_{f^p}) = \mathrm{Spec}(K[x^p, \partial^p]_{f^p}) \\ &= \mathrm{Spec}(Z(A_1))\backslash V(f^p) = \mathrm{Spec}(K[x^p, \partial^p])\backslash V(f^p). \end{aligned}$$

Theorem 2.3 gives explicit descriptions of the sets of prime, completely prime, primitive and maximal ideals of the algebra Λ. Let $\mathrm{Spec}_c(\Lambda, \mathrm{ht} = 1)$ be the set of completely prime ideals of height 1 of the algebra $\Lambda(f)$.

Theorem 2.3 *Let K be a field of characteristic $p > 0$, $\Lambda = K[x][y; \delta := f\frac{d}{dx}]$ where $f \in K[x]\backslash K$. Let $f = p_1^{n_1} \cdots p_s^{n_s}$ be a unique (up to permutation) product of irreducible polynomials of $K[x]$. Then:*

1. *The elements $p_1, \ldots, p_s$ are regular normal elements of the algebra Λ (i.e. p_i is a non-zero-divisor of Λ and $p_i\Lambda = \Lambda p_i$).*
2. $\min(f) = \{(p_1), \ldots, (p_s)\}$.
3. $\mathrm{Spec}_c(\Lambda) = \{0, \Lambda p_i, (p_i, q_i) \,|\, i = 1, \ldots, s;\ q_i \in \mathrm{Irr}_m(F_i[y])\}$ *where $F_i := K[x]/(p_i)$ is a field and $\mathrm{Irr}_m(F_i[y])$ is the set of monic irreducible polynomials of the polynomial algebra $F_i[y]$ over the field F_i in the variable y. If, in addition, $K = \overline{K}$ and $\lambda_1, \ldots, \lambda_s$ are the roots of the polynomial f then* $\mathrm{Spec}_c(\Lambda) = \{0, \Lambda(x - \lambda_i), (x - \lambda_i, y - \mu) \,|\, i = 1, \ldots, s;\ \mu \in K\}$.
4. $\mathrm{Spec}(\Lambda) = \mathrm{Spec}_c(\Lambda) \coprod \{\Lambda\mathfrak{p} \,|\, \mathfrak{p} \in \mathrm{Spec}(Z(\Lambda))\backslash\{(0), V(f^p)\}$.
5. *For all* $\mathfrak{p} \in \mathrm{Spec}(Z(\Lambda))\backslash V(f^p)$,

$$k(\mathfrak{p}) \otimes_{Z(\Lambda)} \Lambda/(\mathfrak{p}) \simeq \bigoplus_{i,j=0}^{p-1} k(\mathfrak{p}) x^i y^i = \bigoplus_{i,j=0}^{p-1} k(\mathfrak{p}) x^i \partial^i \simeq M_p(k(\mathfrak{p})),$$

the algebra of $p \times p$ matrices over the field of fractions $k(\mathfrak{p})$ of the domain $Z(\Lambda)/\mathfrak{p}$.

6. $\mathrm{Max}(\Lambda) = \mathrm{Prim}(\Lambda) = \{(p_i, q_i), \Lambda\mathfrak{m} \,|\, i = 1, \ldots, s;\ q_i \in \mathrm{Irr}_m(F_i[y]), \mathfrak{m} \in \mathrm{Max}(Z(\Lambda))\backslash V(f^p)\}$.
7. $\mathrm{Spec}_c(\Lambda, \mathrm{ht} = 1) = \{(p_1), \ldots, (p_s)\}$. *If, in addition $K = \overline{K}$, then* $\mathrm{Spec}_c(\Lambda, \mathrm{ht} = 1) = \{(x - \lambda_1), \ldots, (x - \lambda_t)\}$ *where $\{\lambda_1, \ldots, \lambda_t\}$ is the set of roots of the polynomial f.*

Proof 1. Statement 1 is proven above.

2. Since

$$\Lambda/\Lambda p_i \simeq F_i[y] \tag{9}$$

is a polynomial algebra with coefficients in the field F_i (since $yx - xy = f \in \Lambda p_i$), the ideal Λp_i is a completely prime ideal of Λ. Now, statement 2 follows from the equality of ideals $(f) = (p_1)^{n_1} \cdots (p_s)^{n_s}$.

5. Since $\mathfrak{p} \in \mathrm{Spec}(Z(\Lambda))\backslash V(f^p)$, the element f^p is a unit in the field $k(\mathfrak{p})$. Now, the first isomorphism and the equality in statement 5 follows from Eq. 8. Then using the equalities,

$$[y, x^i] = ix^{i-1} \text{ and } [y^i, x] = iy^{i-1},$$

and the fact that $k(\mathfrak{p})$ is a field, we see that the algebra $\bigoplus_{i,j=0}^{p-1} k(\mathfrak{p})x^i\partial^i$ is a simple, central $k(\mathfrak{p})$-algebra of dimension p^2 over the field $k(\mathfrak{p})$. Therefore, it is isomorphic to the matrix algebra $M_p(k(\mathfrak{p}))$.

3-4. The algebra Λ is a domain, hence $0 \in \mathrm{Spec}_c(\Lambda)$. We have seen in the proof of statement 2 that the ideals $(p_1), \dots, (p_s)$ of the algebra Λ are completely prime ideals. By Eq. 9,

$$V(f) = \{\Lambda p_i, (p_i, q_i) \mid i = 1, \dots, s;\ q_i \in \mathrm{Irr}_m(F_i[y])\} \subseteq \mathrm{Spec}_c(\Lambda).$$

Given a nonzero prime ideal P of Λ such that $P \notin V(f) = V(f^p)$. Then P_f is a nonzero prime ideal of the algebra $\Lambda_{f^p} = A_{1,f^p}$. By Corollary 2.2, the intersection $\mathfrak{p} := P \cap Z(\Lambda)$ is a nonzero prime ideal of the centre $Z(\Lambda)$ of the algebra Λ. By Theorem 2.1.(4), $\Lambda = \bigoplus_{i,j=0}^{p-1} Z(\Lambda)x^iy^i$. Now, by statement 5, $\Lambda\mathfrak{p} \in \mathrm{Spec}(\Lambda)\backslash V(f)$ and the prime ideal $\Lambda\mathfrak{p}$ is not completely prime. Now, statements 3 and 4 follows from statement 5.

6. Statement 6 follows from statement 4.

7. Statement 7 follows from statement 3. □

Classification of simple $\Lambda(f)$-modules For a Λ-module M, we denote by $\mathrm{ann}_\Lambda(M)$ the annihilator of the Λ-module M. For an algebra A, we denote by $\widehat{A}$, the set of isomorphism classes of (left) simple A-modules. An isomorphism class of a simple A-modules M is denoted by $[M]$. Let elements $a_1, \dots, a_n \in A$ be generators for a left ideal I of the algebra A. Then we write $I = A(a_1, \dots, a_n)$. Theorem 2.4 is a classification of simple $\Lambda(f)$-modules.

Theorem 2.4 *Let K be a field of characteristic $p > 0$, $\Lambda = K[x][y; \delta := f\frac{d}{dx}]$ where $f \in K[x]\backslash K$. Let $f = p_1^{n_1} \cdots p_s^{n_s}$ be a unique (up to permutation) product of irreducible polynomials of $K[x]$. Then:*

1. *The map*
$$\mathrm{Max}(\Lambda) \to \widehat{\Lambda}, \quad \mathfrak{m} \mapsto L(\mathfrak{m})$$
is a bijection with inverse $[M] \mapsto \mathrm{ann}_\Lambda(M)$ where $L(\mathfrak{m})$ is a unique (up to isomorphism) simple direct summand/submodule/factor module of the (simple) matrix algebra $\Lambda/\mathfrak{m}$. In particular, for all $\mathfrak{m} \in \mathrm{Max}(\Lambda)\backslash V(f^p)$, $\dim_K(L(\Lambda\mathfrak{m})) = p \cdot \dim_K(Z(\Lambda)/\mathfrak{m}) < \infty$.
2. *For each maximal ideal (p_i, q_i) of Λ, where $i = 1, \dots, s$ and $q_i \in \mathrm{Irr}_m(F_i[y])\}$,*
$$L(p_i, q_i) = \Lambda/(p_i, q_i) \simeq K[y]/(q_i)$$
and $\dim_K(L(p_i, q_i)) = \dim_K(K[y]/(q_i)) = \deg_y(q_i) < \infty$.
3. *Suppose that $K = \overline{K}$. For each maximal ideal $\Lambda\mathfrak{m}$ of Λ, where $\mathfrak{m} \in \mathrm{Max}(Z(\Lambda))\backslash V(f^p)$,*
$$L(\Lambda\mathfrak{m}) \simeq \Lambda/\Lambda(\mathfrak{m}, x - \sqrt[p]{\xi}) = \bigoplus_{i,j=0}^{p-1} Ky^i\bar{1}$$
$$\simeq A_{1,f^p}/A_{1,f^p}(\mathfrak{m}, x - \sqrt[p]{\xi}) = \bigoplus_{i,j=0}^{p-1} K\partial^i\hat{1},$$

where $x^p - \xi \in \mathfrak{m}$ *for a unique element* $\xi \in K$, $\bar{1} = 1 + \Lambda(\mathfrak{m}, x - \sqrt[p]{\xi})$ *and* $\hat{1} = 1 + A_{1,f^p}(\mathfrak{m}, x - \sqrt[p]{\xi})$, $\dim_K L(\Lambda\mathfrak{m}) = p < \infty$.

Proof 1. Statements 1 follows at once from Theorem 2.3.(5,6).

2. Statement 2 is obvious.

3. Notice that $(x - \sqrt[p]{\xi}))^p = x^p - \xi \in \mathfrak{m}$.

By Theorem 2.1.(4) and the choice of the ideal $\mathfrak{m}$, we have that

$$\Lambda/\Lambda\mathfrak{m} = \bigoplus_{i=0}^{p-1} Ky^i \otimes K[x]/(x^p - \xi) = \bigoplus_{i=0}^{p-1} Ky^i \otimes K[x]/((x - \sqrt[p]{\xi})^p),$$

direct sums of tensor products of vector spaces. Hence,

$$\Lambda/\Lambda(\mathfrak{m}, x - \sqrt[p]{\xi}) \simeq \bigoplus_{i=0}^{p-1} Ky^i \otimes K[x]/(x - \sqrt[p]{\xi}) \simeq \bigoplus_{i,j=0}^{p-1} Ky^i\bar{1}$$

is a p-dimensional Λ-module that is annihilated by the maximal ideal $\mathfrak{m}$. By statement 1, it must be $L(\Lambda\mathfrak{m})$. Since $\mathfrak{m} \notin V(f^p)$, the central element f^p acts as a bijection on the module $L(\Lambda\mathfrak{m})$. Therefore,

$$L(\Lambda\mathfrak{m}) = L(\Lambda\mathfrak{m})_{f^p} = \Lambda_{f^p}/\Lambda_{f^p}(\mathfrak{m}, x - \sqrt[p]{\xi}) \simeq A_{1,f^p}/A_{1,f^p}(\mathfrak{m}, x - \sqrt[p]{\xi}) = \bigoplus_{i,j=0}^{p-1} K\partial^i\hat{1}.$$

□

The action of the elements x and y on the K-basis $\{y\bar{1} \mid i = 0, \dots, p-1\}$ of the $\Lambda(f)$-module $L(\Lambda\mathfrak{m})$ of Theorem 2.4.(3) is given below:

$$x \cdot \bar{1} = \xi^{\frac{1}{p}}\bar{1},$$

$$x \cdot y^i\bar{1} = \xi^{\frac{1}{p}} y^i\bar{1} + \sum_{j=0}^{i-1} \binom{i}{j} \xi_{ij} y^j\bar{1} \quad \text{where} \quad \xi_{ij} = (-1)^{i-j}\phi_{ij}(\xi^{\frac{1}{p}}), \quad \phi_{ij} = \delta^{i-j-1}(f) \in K[x],$$

$$y \cdot y^i\bar{1} = y^{i+1}\bar{1} \quad \text{where} \quad 0 \le i \le p-2,$$

$$y \cdot y^{p-1}\bar{1} = \rho\bar{1} \quad \text{where} \quad y^p - \rho \in \mathfrak{m} \quad \text{for a unique element} \quad \rho \in K.$$

The Krull and global dimensions of the algebra $\Lambda(f)$**.**

Theorem 2.5 *Let* K *be a field of characteristic* $p > 0$, $\Lambda = K[x][y; \delta := f\frac{d}{dx}]$ *where* $f \in K[x]\backslash K$. *Then:*

1. *The Krull dimension of* Λ *is* $\mathrm{K.dim}\,(\Lambda) = 2$.
2. *The global dimension of* Λ *is* $\mathrm{gldim}(\Lambda) = 2$.

Proof Let $\Lambda = \Lambda(f)$.

1. By Theorem 2.1.(4), the algebra Λ is a finitely generated $Z(\Lambda)$-module. Therefore, the Krull dimension of the algebra Λ is equal to the Krull dimension of the polynomial algebra $Z(\Lambda)$ in two variables (Theorem 2.1.(3)), and statement 1 follows.

2. By [12, Theorem 7.5.3.(i)], $\mathrm{gldim}(\Lambda) \le \mathrm{gldim}(K[X]) + 1 = 1 + 1 = 2$.

Let $f = p_1^{n_1} \cdots p_s^{n_s}$ be a unique (up to permutation) product of irreducible polynomials of $K[x]$. By Eq. 9, $\mathrm{gldim}(\Lambda/\Lambda p_i) = \mathrm{gldim}(F_i[Y]) = 1 < \infty$. Now, by [12, Theorem 7.3.5.(i)],

$$\mathrm{gldim}(\Lambda) \ge \mathrm{gldim}(\Lambda/\Lambda p_i) + 1 \overset{(9)}{=} \mathrm{gldim}(F_i[Y]) + 1 = 1 + 1 = 2.$$

Therefore, $\mathrm{gldim}(\Lambda) = 2$. □

3 Isomorphism Problems and Groups of Automorphisms for Ore Extensions $K[x][y; f\frac{d}{dx}]$

In this section, a proof Theorem 1.3 is given. It can be deduced from Theorem 1.1 but we give a different proof.

Let $K(x)$ be the field of rational functions in the variable x. Then the Ore extension $B_1 := K(x)[\partial; \frac{d}{dx}]$ is the localization $B_1 = S^{-1}A_1$ of the Weyl algebra A_1 at the Ore set $S = K[x]\backslash\{0\}$ of A_1. The multiplicative set S is an Ore set of the algebra Λ such that $B_1 = S^{-1}\Lambda$, by Eq. 6.

Notice that

$$\mathbb{S}(K) \rtimes G_f(K) = \{\sigma_{\lambda,\mu,p} \mid \lambda \in K^\times, \mu \in K, p \in K[x]\} \tag{10}$$

where

$$\sigma_{\lambda,\mu,p}(x) = \lambda x + \mu \;\text{ and }\; \sigma_{\lambda,\mu,p}(y) = \lambda^{d-1}y + p$$

since $\sigma_{\lambda,\mu,p} = s_{\lambda^{-d+1}p}\sigma_{\lambda,\mu}$ where $d = \deg(f)$.

Proof of Theorem 1.3 Let σ be an automorphism of the K-algebra $\Lambda = \Lambda(f)$. It can be uniquely extended to a $\overline{K}$-automorphism, say σ, of the algebra $\overline{K} \otimes_K \Lambda$. Let $\lambda_1, \ldots, \lambda_t$ be the roots of the polynomial f in $\overline{K}$. By Theorem 2.3.(7), the automorphism σ permutes the set

$$\mathrm{Spec}_c(\overline{K} \otimes_K \Lambda, \mathrm{ht} = 1) = \{(x - \lambda_1), \ldots, (x - \lambda_t)\}$$

of height 1 completely prime ideals of the algebra $\overline{K} \otimes_K \Lambda$ that are generated by regular normal elements $x - \lambda_1, \ldots, x - \lambda_t$ of the domain $\overline{K} \otimes_K \Lambda$ and the set $\overline{K}^\times$ is the group of units of the algebra $\overline{K} \otimes_K \Lambda$. So, we must have that

$$\sigma(x) = \lambda x + \mu$$

for some elements $\lambda \in \overline{K}^\times$ and $\mu \in \overline{K}$. Since $K[x] = \Lambda \cap \overline{K}[x]$, we must have that

$$\sigma(x) \in \sigma(\Lambda) \cap \sigma(\overline{K}[x]) = \Lambda \cap \overline{K}[x] = K[x],$$

and so $\lambda \in K^\times$ and $\mu \in K$. So, the automorphism σ respects the polynomial algebra $K[x]$. In particular, it respects the Ore set $S = K[x]\backslash\{0\}$ of the algebra Λ. The automorphism σ can be uniquely extended to an automorphism of the algebra $B_1 = S^{-1}\Lambda$. Then $\sigma(\partial) = \lambda^{-1}\partial + q$ for some element $q \in K(x)$. In particular,

$$\sigma(y) = \sigma(f\partial) = \sigma(f)(\lambda^{-1}\partial + q) = \lambda^{-1}\frac{\sigma(f)}{f}y + p \;\text{ where }\; p := \sigma(f)q \in K[x]$$

and $\sigma(f) = \gamma f$ for some element $\gamma \in K^\times$. Clearly, $\gamma = \lambda^d$ where $d = \deg(f)$ is the degree of the polynomial f (since $\sigma(x) = \lambda x + \mu$). So,

$$\sigma(x) = \lambda x + \mu \;\text{ and }\; \sigma(y) = \lambda^{d-1}y + p,$$

i.e. $\sigma \in \mathbb{S}(K) \rtimes G_f(K)$, as required. □.

By Theorem 1.3,

$$G_f(K) = \mathbb{S}(K) \rtimes G_f(K) = \{\sigma_{\lambda,\mu,p} \mid \lambda \in K^\times, \mu \in K, p \in K[x]\} \tag{11}$$

where the multiplication and the inversion in the group $G_f(K)$ are given by the rule (where $d = \deg(f)$):

$$\sigma_{\lambda_1,\mu_1,p_1}\sigma_{\lambda_2,\mu_2,p_2} = \sigma_{\lambda_1\lambda_2,\lambda_2\mu_1+\mu_2,\lambda_2^{d-1}p_1+p_2},$$
$$\sigma_{\lambda,\mu,p}^{-1} = \sigma_{\lambda^{-1},-\lambda^{-1}\mu,-\lambda^{-d+1}p}.$$

The algebra B_1 and its automorphism group The element *f* is a regular normal element of Λ (i.e. $\Lambda f = f\Lambda$) since

$$fy = yf - f'f = (y - f')f \quad \text{where} \quad f' = \frac{df}{dx}.$$

It determines the K-automorphism ω_f of the algebra Λ:

$$fu = \omega_f(u)f, \quad u \in \Lambda,$$
$$\omega_f : x \mapsto x, \quad y \mapsto y - f'.$$

We denote by Λ_f and $A_{1,f}$ the localizations of the algebras Λ and A_1 at the powers of the element *f*, i.e.

$$\Lambda_f = S_f^{-1}\Lambda \quad \text{and} \quad A_{1,f} = S_f^{-1}A_1 \quad \text{where} \quad S_f = \{f^i\}_{i\geq 0}.$$

By Eq. 6,

$$\Lambda \subset A_1 \subset \Lambda_f = A_{1,f} = K[x, f^{-1}][\partial; \frac{d}{dx}] \subset B_1. \tag{12}$$

Recall that $\mathrm{Aut}_K(K[x]) = \{\sigma_{\lambda,\mu} \mid \lambda \in K^\times, \mu \in K\}$, $\sigma_{\lambda,\mu}(x) = \lambda x + \mu$ and

$$\mathrm{Aut}_K(K(x)) = \{\sigma_M \mid M \in \mathrm{PGL}_2(K)\} \simeq \mathrm{PGL}_2(K), \ \sigma_M \to M \text{ where } \sigma_M(x) = \frac{ax+b}{cx+d},$$
$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(K) := \mathrm{GL}_2(K)/K^\times E \text{ and } E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The maps

$$\mathrm{Aut}_K(K[x]) \to \mathrm{Aut}_K(A_1), \quad \sigma_{\lambda,\mu} \mapsto \sigma_{\lambda,\mu} : x \mapsto \lambda x + \mu, \quad \partial \mapsto \lambda^{-1}\partial,$$
$$\mathrm{Aut}_K(K(x)) \to \mathrm{Aut}_K(B_1), \quad \sigma_M \mapsto \sigma_M : x \mapsto \frac{ax+b}{cx+d}, \quad \partial \mapsto \frac{1}{\sigma_M(x)'}\partial,$$

are group monomorphisms where $g' = \frac{dg}{dx}$ for $g \in K(x)$. We identify these groups with their images, i.e.

$$\mathrm{Aut}_K(K[x]) \subseteq \mathrm{Aut}_K(A_1) \quad \text{and} \quad \mathrm{Aut}_K(K(x)) \subseteq \mathrm{Aut}_K(B_1).$$

Notice that $\sigma_M(y) = \sigma_M(f\partial) = \frac{\sigma_M(f)}{f\sigma_M(x)'}f\partial = \frac{\sigma_M(f)}{f\sigma_M(x)'}y$. The automorphism group $\mathrm{Aut}_K(B_1)$ acts in the obvious way on the algebra B_1. Let

$$\mathbb{S}_1 := \mathrm{St}_{\mathrm{Aut}_K(B_1)}(x) := \{\sigma \in \mathrm{Aut}_K(B_1) \mid \sigma(x) = x\},$$

the stabilizer of the element $x \in B_1$ in $\mathrm{Aut}_K(B_1)$. Clearly,

$$\mathbb{S}_1 = \{s_q : \mid q \in K(x)\} \simeq (K(x), +), \quad s_q \mapsto q$$

where $s_q(x) = x$ and $s_q(\partial) = \partial + q$.

Lemma 3.1 *1.* $\mathrm{Aut}_K(B_1) = \mathbb{S}_1 \rtimes \mathrm{Aut}_K(K(x)) = \{\sigma_{M,q} := s_q\sigma_M \mid M \in \mathrm{PGL}_2(K), q \in K(x)\}$.

2. $\mathrm{Aut}_K(B_1, K[x]) := \{\sigma \in \mathrm{Aut}_K(B_1) \,|\, \sigma(K[x]) = K[x]\} = \mathbb{S}_1 \rtimes \mathrm{Aut}_K(K[x]) = \{\sigma_{l,\mu,q} \,|\, \lambda \in K^\times, \mu \in K, q \in K(x)\}$ *where* $\sigma_{l,\mu,q}(x) = \lambda x + \mu$ *and* $\sigma_{\lambda,\mu,q}(\partial) = \lambda^{-1}\partial + q$.

Proof 1. Since $\mathbb{S}_1 := \mathrm{St}_{\mathrm{Aut}_K(B_1)}(x)$, we must have $\mathbb{S}_1 \cap \mathrm{Aut}_K(B_1) = \{e\}$ and $\sigma \mathbb{S}_1 \sigma^{-1} \subseteq \mathbb{S}_1$ for all automorphisms $\sigma \in \mathrm{Aut}_K(B_1)$. Hence, $\mathrm{Aut}_K(B_1) \supseteq \mathbb{S}_1 \rtimes \mathrm{Aut}_K(K(x))$.

To prove that the reverse inclusion holds we have to show that every element $\sigma \in \mathrm{Aut}_K(K(x))$ belongs to the group $\mathbb{S}_1 \rtimes \mathrm{Aut}_K(K(x))$. The group of units $K(x)^\times := K(x)\backslash\{0\}$ of the algebra B_1 is a σ-invariant set, i.e. $\sigma(K(x)^\times) = K(x)^\times$. Hence so is the field $K(x)$. Let τ be the restriction of the automorphism σ to the field $K(x)$. Then $\sigma_1 := \tau^{-1}\sigma \in \mathbb{S}_1$, and so $\sigma = \tau\sigma_1 \in \mathbb{S}_1 \rtimes \mathrm{Aut}_K(K(x))$, as required.

2. Statement 2 follows from statement 1. □

Below is a different proof of Theorem 1.1 is given.

Proof of Theorem 1.1 Let $\sigma : \Lambda(f) \to \Lambda(g)$ be an isomorphism of the K-algebras. It can be uniquely extended to a $\overline{K}$-isomorphism $\sigma : \overline{K} \otimes_K \Lambda(f) \to \overline{K} \otimes_K \Lambda(g)$. Let $\lambda_1, \dots, \lambda_s$ (resp., $\lambda'_1, \dots, \lambda'_t$) be the roots of the polynomial f (resp., g) in $\overline{K}$. By Theorem 2.3.(7), the automorphism σ maps bijectively the set $\{(x-\lambda_1), \dots, (x-\lambda_s)\}$ of height 1 completely prime ideals of the algebra $\overline{K} \otimes_K \Lambda(f)$ to the set $\{(x-\lambda'_1), \dots, (x-\lambda'_t)\}$ of height 1 completely prime ideals of the algebra $\overline{K} \otimes_K \Lambda(g)$. Therefore, $s = t$. Since the elements $x-\lambda'_1, \dots, x-\lambda'_t$ are regular normal elements of the domain $\overline{K} \otimes_K \Lambda(g)$ and the set $\overline{K}^\times$ is the group of units of the algebra $\Lambda(g)$, we must have that

$$\sigma(x) = \lambda x + \mu$$

for some elements $\lambda \in \overline{K}^\times$ and $\mu \in \overline{K}$. Since $K[x] = \Lambda(g) \cap \overline{K}[x]$, we must have that $\sigma(x) \in \sigma(\Lambda(f)) \cap \sigma(\overline{K}[x]) = \Lambda(g) \cap \overline{K}[x] = K[x]$, and so $\lambda \in K^\times$ and $\mu \in K$. So, the isomorphism σ respects the polynomial algebra $K[x]$ of the algebras $\Lambda(f)$ and $\Lambda(g)$. In particular, it respects the Ore sets $S = K[x]\backslash\{0\}$ of the algebras $\Lambda(f)$ and $\Lambda(g)$, i.e. $\sigma(S) = S$. The isomorphism σ can be uniquely extended to an isomorphism

$$\sigma : B_1 = S^{-1}\Lambda(f) \to B_1 = S^{-1}\Lambda(g).$$

Then $\sigma(\partial) = \lambda^{-1}\partial + q$ for some element $q \in K[x]$. In particular,

$$\sigma(y) = \sigma(f\partial) = \sigma(f)(\lambda^{-1}\partial + q) = \lambda^{-1}\frac{\sigma(f)}{g}y + p \quad \text{where} \quad p := \sigma(f)q \in K[x]$$

and $\sigma(f) = \gamma g$ for some element $0 \neq \gamma \in K[x]$. Applying the same argument for the isomorphism $\sigma^{-1} : \Lambda(g) \to \Lambda(f)$, we have that $\sigma^{-1}(g) = \gamma_1 f$ for some element $0 \neq \gamma_1 \in K[x]$. Therefore,

$$f = \sigma^{-1}\sigma(f) = \sigma^{-1}(\gamma g) = \sigma^{-1}(\gamma)\gamma_1 f,$$

and so $\gamma, \gamma_1 \in K^\times$, and $\gamma_1 = \gamma^{-1}$. Clearly, $\gamma = \lambda^d$ where $d = \deg(f)$ is the degree of the polynomial f (since $\sigma(x) = \lambda x + \mu$), and the theorem follows. Furthermore,

$$\sigma(x) = \lambda x + \mu \quad \text{and} \quad \sigma(y) = \lambda^{d-1}y + p.$$

□

4 The Eigengroup G_f of a Polynomial f

For each non-scalar monic polynomial $f(x)$, Proposition 4.10, Theorem 4.24, 4.27, 4.30 and 4.32 are explicit descriptions of the eigengroup $G_f(K)$ in the case when the field K is algebraically closed. The case of an arbitrary field is obtained from these results, Theorem 4.33. The aim of this section is to prove these results.

The eigengroup $G_U(K)$

Definition 4.1 [5] Given a group, a G-module V over a field K and a non-empty subset U of V. The *eigengroup* of the set U in G, denoted by $G_U(K)$, is the set of all elements of the group G such that the elements of the set U are eigenvectors of them with eigenvalues in the field K. Clearly, the eigengroup is a subgroup of G.

Clearly,

$$G_U = \bigcap_{u \in U} G_u$$

where $G_u := G_{\{u\}} = \{g \in G \mid gu = \lambda(g)u \text{ for some } \lambda(g) \in K\}$. If K is a subfield of a field K' then $G_U(K) \subseteq G_U(K')$ where U is a subset of the G-module $K' \otimes_K V$ over the field K'.

Finite subgroups of $\mathrm{Aut}_K(K[x])$ Let K be a field of prime characteristic $p > 0$, $\mathbb{F}_p = \mathbf{Z}/\mathbf{Z}p$ is the field that contains p elements, for each $n \geq 1$, $\mathbb{F}_{p^n}$ is the finite field that contains p^n elements, $\overline{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ is the algebraic closure of the field $\mathbb{F}_p$. Clearly, $\overline{\mathbb{F}}_p \subseteq \overline{K}$ and group of roots of 1 in the field $\overline{K}$ is $\overline{\mathbb{F}}_p^\times := \overline{\mathbb{F}}_p \backslash \{0\}$. The group $\mathrm{Aut}_K(K[x]) = \{\sigma_{\lambda,\mu} \mid \lambda \in K^\times, \mu \in K\}$ where $\sigma_{\lambda,\mu}(x) = \lambda x + \mu$ and

$$\mathrm{Aut}_K(K[x]) \simeq \mathrm{Sh}(K) \rtimes \mathbb{T} \simeq K \rtimes K^\times$$

where $\mathrm{Sh}(K) := \{\sigma_{1,\mu} \mid \mu \in K\} \simeq (K, +)$, $\sigma_{1,\mu} \mapsto \mu$ and $\mathbb{T} := \{\sigma_\lambda, 0\} \mid \lambda \in K^\times\} \simeq K^\times$, $\sigma_{\lambda,0} \mapsto \lambda$ is the the algebraic 1-dimensional torus.

The set $\mathbb{U} = \mathbb{U}(K) = K \cap \overline{\mathbb{F}}_p^\times$ is the group of roots of 1 of the field K. The map $\mathbb{U} \to \mathbb{T}$, $\lambda \mapsto \sigma_{\lambda,0}$ is a group monomorphism and we identify the group $\mathbb{U}$ with its image, i.e. $\mathbb{U} = \{\sigma_{\lambda,0} \mid \lambda \in \mathbb{U}\}$. Let $\mathrm{or}(g)$ be the *order* of an element g of a group G.

Lemma 4.2 *The group* $\mathrm{Sh}(K) \rtimes \mathbb{U}(K) = \{\sigma_{u,\mu} \mid u \in \mathbb{U}(K), \mu \in K\}$ *is the set of all finite order automorphisms of the group* $\mathrm{Aut}_K(K[x])$. *The order of the element* $\sigma_{u,\mu} = \sigma_{u,0}\sigma_{1,\mu}$ *is*

$$\mathrm{or}(\sigma_{\lambda,\mu}) = \begin{cases} \mathrm{or}(\lambda) & \text{if } \lambda \neq 1, \\ p & \text{if } \lambda = 1, \mu \neq 0, \\ 1 & \text{if } \lambda = 1, \mu = 0. \end{cases}$$

Proof For all $\lambda \in K^\times \backslash \{1\}$ and $\mu \in K$, $\sigma_{1,\mu}^i = \sigma_{1,i\mu}$ and $\sigma_{\lambda,\mu}^i = \sigma_{\lambda^i, \frac{1-\lambda^i}{1-\lambda}\mu}$, and statement 1 follows. □

By Lemma 4.2,

$$1 \to \mathrm{Sh}(K) \to \mathrm{Sh}(K) \rtimes \mathbb{U}(K) \stackrel{\varphi}{\to} \mathbb{U}(K) \to 1, \quad \text{where} \quad \varphi(\sigma_{\lambda,\mu}) = \lambda, \tag{13}$$

is a short exact sequence of group homomorphisms.

Lemma 4.3 *If an element* $\lambda \in \mathbb{U}(\overline{K})$ *is a primitive* n*'th root of unity then* $\mathbb{F}_p(\lambda) = \mathbb{F}_{p^m}$ *where* $m = \min\{k \geq 1 \mid n | (p^k - 1)\}$ = *the degree of the minimal polynomial of* λ *over the field* $\mathbb{F}_p$.

Proof The element λ is algebraic over the field $\mathbb{F}_p$. Let φ be its minimal polynomial over $\mathbb{F}_p$. Then the field $\mathbb{F}_p(\lambda) \simeq \mathbb{F}_p[x]/(\varphi)$ is a finite field, and so $\mathbb{F}_p(\lambda) = \mathbb{F}_{p^m}$ for some $m \geq 1$. Now,

$$\deg(\varphi) = [\mathbb{F}_p(\lambda) : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_p] = m.$$

Notice that the order of the group $\langle\lambda\rangle$, which is n (since λ is a primitive n'th root of unity) divides the order of the group $\mathbb{F}_{p^m}^{\times}$, which is $p^m - 1$. Clearly, $m \geq m' := \min\{k, \mid n | (p^k - 1)\}$. We claim that $m = m'$. Suppose that $m > m'$, wee seek a contradiction. Then $\lambda^{p^{m'}} = \lambda$, and so $\lambda \in \mathbb{F}_{p^{m'}}$, hence $F_{p^m} = \mathbb{F}_p(\lambda) \subseteq \mathbb{F}_{p^{m'}}$. Therefore, $m|m'$, a contradiction. $\square$

The next theorem is a classification of all the finite subgroups of the automorphism group $\mathrm{Aut}_K(K[x])$.

Theorem 4.4 *Let G be a finite subgroup of $\mathrm{Aut}_K(K[x])$. Then:*

1. *$G = \widetilde{G} \rtimes \overline{G}$ where $\widetilde{G} = G \cap \mathrm{Sh}(K) = \{\sigma_{1,\mu} \mid \mu \in V\}$, $V \subseteq K$ is a finite dimensional $\mathbb{F}_p(\lambda_n)$-subspace of K and $\overline{G} = \langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ is a cyclic group of order n where λ_n is a primitive n'th root of 1 and $\nu \in K$.*
   In particular, the order of the group G is np^l where $l = \dim_{\mathbb{F}_p}(V)$ such that $m|l$ where $\mathbb{F}_p(\lambda_n) = \mathbb{F}_{p^m}$ for some $m \geq 1$ (Lemma 4.3).
2. *Conversely, given a finite dimensional $\mathbb{F}_p(\lambda_n)$-subspace V of K, an automorphism $\sigma_{\lambda_n,(1-\lambda_n)\nu}$ where $\lambda_n \in K$ is a primitive n'th root of unity and $\nu \in K$. Let $\widetilde{G} := \{\sigma_{1,\mu} \mid \mu \in V\}$ and $\overline{G} := \langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$. Then:*
   - *(a) The semidirect product $\widetilde{G} \rtimes \overline{G}$ is a finite subgroup of $\mathrm{Aut}_K(K[x])$ of order np^l where $l = \dim_{\mathbb{F}_p}(V)$ such that $m|l$.*
   - *(b) The element $\nu \in K$ is unique up to adding an arbitrary element of V, i.e.*

$$\widetilde{G} \rtimes \langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle \simeq \widetilde{G} \rtimes \langle\sigma_{\lambda_n,(1-\lambda_n)\nu'}\rangle \ \text{ iff } \ \nu' - \nu \in V.$$

Furthermore, $G = \{\sigma^i_{\lambda_n,(1-\lambda_n)\nu}\sigma_{1,v} \mid 0 \leq i \leq n-1, v \in V\}$ and

$$\sigma^i_{\lambda_n,(1-\lambda_n)\nu}\sigma_{1,v} = \sigma_{\lambda_n^i,(1-\lambda_n^i)\nu}\sigma_{1,v} : x \mapsto \lambda_n^i x + (1-\lambda_n^i)\nu + v.$$

Proof Let G be a finite subgroup of $\mathrm{Aut}_K(K[x])$. Then, by (13), the group $\varphi(G)$ is a finite subgroup of $\mathbb{U}(K)$ of order n, hence $\varphi(G) = \langle\lambda_n\rangle$ where λ_n is a primitive n'th root of 1. Fix an element, say $\sigma_{\lambda_n,(1-\lambda_n)\nu} \in G$ where $\nu \in K$, such that $\varphi(\sigma_{\lambda_n,(1-\lambda_n)\nu}) = \lambda_n$. Then $\overline{G} = \langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ is a cyclic group of order $n = |\overline{G}|$ since $\sigma^i_{\lambda_n,(1-\lambda_n)\nu} = \sigma_{\lambda_n^i,(1-\lambda_n^i)\nu}$ for all $i \geq 1$. Therefore,

$$G = \widetilde{G} \rtimes \overline{G} \ \text{ where } \ \widetilde{G} := G \cap \mathrm{Sh}(K) = \{\sigma_{1,\mu} \mid \mu \in V\},$$

$V \subseteq K$ is a finite dimensional $\mathbb{F}_p$-subspace of K since $\sigma^i_{1,\mu} = \sigma_{1,i\mu}$ for all $i \geq 0$. Furthermore, $\lambda_n V \subseteq V$, i.e. the $\mathbb{F}_p$-vector space V is a $\mathbb{F}_p(\lambda)$-module since

$$\sigma^{-1}_{\lambda_n,(1-\lambda_n)\nu}\sigma_{1,\mu}\sigma_{\lambda_n,(1-\lambda_n)\nu} = \sigma_{1,\lambda\mu}.$$

Clearly, $|G| = |\widetilde{G}||\overline{G}| = p^l n$ and $m|l$ since V is a $\mathbb{F}_{p^m}$-module and $\dim_{\mathbb{F}_{p^m}}(V) = \frac{l}{m}$. The converse, is obvious.

Clearly, $\widetilde{G} \rtimes \langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle \simeq \widetilde{G} \rtimes \langle\sigma_{\lambda_n,(1-\lambda_n)\nu'}\rangle$ iff there is natural number i such that $1 \leq i \leq n-1$ and a vector $v \in V$ such that

$$\sigma_{\lambda_n,(1-\lambda_n)\nu'} = \sigma^i_{\lambda_n,(1-\lambda_n)\nu}\sigma_{1,v} = \sigma_{\lambda_n^i,(1-\lambda_n^i)(\nu+(1-\lambda_n^i)^{-1}v)}$$

iff $i = 1$ and $\nu' = \nu + (1-\lambda_n^i)^{-1}v \in V$ iff $\nu' - \nu \in V$ since $(1-\lambda_n^i)^{-1}V = V$. $\square$

The automorphism group $\mathrm{Aut}_K(K[x])$ acts on the set $\mathrm{Max}(K[x])$ of maximal ideals of $K[x]$ in the obvious way. If $K = \overline{K}$ then $\mathrm{Max}(K[x]) = \{(x-\gamma) \mid \gamma \in K\}$ and the action takes the form: For all $\sigma \in \mathrm{Aut}_K(K[x])$ and $\gamma \in K$,

$$\sigma((x-\gamma)) = (x - \sigma^{-1}(\gamma)) \text{ where } \sigma^{-1}(\gamma) := \sigma^{-1}(x)|_{x=\gamma}. \tag{14}$$

Let us identify the set $\mathrm{Max}(K[x])$ with K via $(x-\gamma) \mapsto \gamma$. Then the action of the group $\mathrm{Aut}_K(K[x])$ on $\mathrm{Max}(K[x]) = K$ is given below:

$$\mathrm{Aut}_K(K[x]) \times K \to K, \quad (\sigma, \gamma) \mapsto \sigma * \gamma := \sigma^{-1}(\gamma) = \sigma^{-1}(x)|_{x=\gamma}. \tag{15}$$

If $\sigma = \sigma_{\lambda,\mu}$ then $\sigma_{\lambda,\mu}^{-1} = \sigma_{\lambda^{-1},-\lambda^{-1}\mu}$ and $\sigma_{\lambda,\mu} * \gamma = \sigma_{\lambda,\mu}^{-1}(\gamma) = \sigma_{\lambda^{-1},-\lambda^{-1}\mu}(\gamma) = \lambda^{-1}\gamma - \lambda^{-1}\mu$.

Every automorphism $\sigma_{\lambda,\mu} \in \mathrm{Aut}_K(K[x])$ with $\lambda \neq 1$ can be uniquely written in the form $\sigma_{\lambda,(1-\lambda)\nu}$ where $\nu = (1-\lambda)^{-1}\mu$. Notice that

$$\sigma_{\lambda,(1-\lambda)\nu} * (\nu) = \nu.$$

Furthermore, the set $\{\nu\}$ is the only 1-element orbit in K of the cyclic group $\langle \sigma_{\lambda,(1-\lambda)\nu} \rangle$ generated by the automorphism $\sigma_{\lambda,(1-\lambda)\nu}$. The number of elements in any other orbit is equal to the order of the group $\langle \sigma_{\lambda,(1-\lambda)\nu} \rangle$ which is the order of the element λ in the group $(K^\times, \cdot)$.

Suppose that $K = \overline{K}$. Let $f \in K[x]$ be a non-scalar monic polynomial that has at least two distinct roots in $K = \overline{K}$. Recall that $\mathcal{R}(f)$ is the set of all roots of the polynomial f counted with multiplicity and $\mathcal{R}_d(f)$ be the set of all *distinct* roots of f (i.e. each root has multiplicity 1). Example. For $f = (x-1)^2(x-2)^3$, $\mathcal{R}(f) = \{1, 1, 2, 2, 2\}$ and $\mathcal{R}(f) = \{1, 2\}$.

The group G_f permutes the roots in $\mathcal{R}(f)$ and $\mathcal{R}_d(f)$ via the action Eq. 14. Let us stress that the action of G_f on $\mathcal{R}(f)$ respects the multiplicity. If the group G_f is finite then $G_f = \widetilde{G}_f \rtimes \overline{G}_f$ and $\widetilde{G}_f = \mathrm{Sh}_V$ is a normal subgroup of G_f. For a set $\mathcal{R} = \mathcal{R}(f), \mathcal{R}_d(f)$ and a group $G = G_f, \widetilde{G}_f, \overline{G}_f$, we denote by $\mathcal{R}/G$ the set of G-orbits in $\mathcal{R}$.

Invariants and eigenalgebras of finite subgroups of $\mathrm{Aut}_K(K[x])$ Notice that

$$x^p - x = \prod_{i \in \mathbb{F}_p} (x - i). \tag{16}$$

For each element $\mu \in K^\times$, let

$$f_\mu(x) := \prod_{i=0}^{p-1} \sigma_{1,\mu}^i(x) = \prod_{i=0}^{p-1} (x - i\mu) = \prod_{i \in \mathbb{F}_p} (x - i\mu) = x^p - \mu^{p-1}x. \tag{17}$$

The equality above follows at once from (16): $f_\mu(x) = \prod_{i=0}^{p-1}(x - i\mu) = \mu^p \prod_{i=0}^{p-1}(\mu^{-1} x - i) = \mu^p((\mu^{-1}x)^p - \mu^{-1}x) = x^p - \mu^{p-1}x$. For all $\alpha, \beta \in \mathbb{F}_p$:

$$f_\mu(\alpha x + \beta x') = \alpha f_\mu(x) + \beta f_\mu(x')$$

since $\gamma^p = \gamma$ for all $\gamma \in \mathbb{F}_p$. In particular, the map $K \to K, \lambda \mapsto f(\lambda)$ is a $\mathbb{F}_p$-linear map. Hence for all elements $\lambda \in K$,

$$\begin{aligned} x^p - \mu^{p-1}x - (\lambda^p - \mu^{p-1}\lambda) &= f_\mu(x) - f_\mu(\lambda) = f_\mu(x - \lambda) \\ &= \prod_{i=0}^{p-1}(x - \lambda - i\mu) = \prod_{i \in \mathbb{F}_p}(x - \lambda - i\mu). \end{aligned} \tag{18}$$

Given a K-algebra A, and a subgroup G of the automorphism group $\mathrm{Aut}_K(A)$. A group homomorphism $\chi : G \to K^\times$ is called a *character* of the group G in $K^\times$. Let $\widehat{G}(K)$ be the (multiplicative) *group of characters* of the group G in $K^\times$. The multiplication in the group $\widehat{G}(K)$ is given by the rule: For all $\chi, \psi \in \widehat{G}(K)$, $(\chi\psi)(g) = \chi(g)\psi(g)$ for all elements $g \in G$.

Definition 4.5 The direct sum of G-eigenspaces,

$$\mathbb{E}(A) = \mathbb{E}(A, G) := \bigoplus_{\chi \in \widehat{G}(K)} A^\chi, \quad \text{where} \quad A^\chi := \{a \in A \mid g(a) = \chi(g)a \text{ for all } g \in G\},$$

is called the *G-eigenalgebra* of A. The direct sum is a $\widehat{G}(K)$-graded algebra since $A^\chi A^\psi \subseteq A^{\chi\psi}$ for all $\chi, \psi \in \widehat{G}(K)$.

If e is the identity element of the character group $\widehat{G}(K)$ then $A^e = A^G$ is the *algebra of G-invariants*. In particular $A^G \subseteq \mathbb{E}(A, G)$.

The set $\mathrm{Supp}(A, G) := \{\chi \in \widehat{G}(K) \mid A^\chi \neq 0\}$ is called the *support* of G in A. For each character $\chi \in \mathrm{Supp}(A, G)$, the vector space A^χ is called the *χ-weight/eigenvalue subspace* of the algebra A. If the algebra $\mathbb{E}(A, G)$ is a domain (eg, the algebra A is a domain) then the support $\mathrm{Supp}(A, G)$ is a submonoid of $\widehat{G}(K)$ and the algebra $\mathbb{E}(A, G)$ is a $\mathrm{Supp}(A, G)$-graded algebra. If the algebra A is a commutative algebra then the *Frobenius* endomorphism $\mathrm{Fr} : A \to A, a \mapsto a^p$ is a $\mathbb{F}_p$-algebra endomorphism of A. It is a monomorphism if the algebra A is a domain. By the very definition, the Frobenius endomorphism commute with all endomorphisms of the ring A.

Lemma 4.6 *Let A be a commutative K-algebra and G be a subgroup of the automorphism group* $\mathrm{Aut}_K(A)$.

1. *The algebras $\mathbb{E}(A, G)$ and A^G are* Fr*-stable (that is* $\mathrm{Fr}(\mathbb{E}(A, G)) \subseteq \mathbb{E}(A, G)$ *and* $\mathrm{Fr}(A^G) \subseteq A^G$*).*
2. *Suppose that the algebra A is reduced and* $\mathrm{Fr}(K) = K$*. If* $g(\mathrm{Fr}(a)) = \chi(g)\mathrm{Fr}(a)$ *for all $g \in G$ then $g(a) = (\chi(g))^{\frac{1}{p}} a$. In particular,* $\mathrm{Fr} \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{E}(A, G))$ *and* $\mathrm{Fr} \in \mathrm{Aut}_{\mathbb{F}_p}(A^G)$.

Proof 1. The Frobenius endomorphism commutes with all endomorphisms of the ring A, and statement 1 follows.

2. The equality $\mathrm{Fr}(K) = K$ implies that $\mathrm{Fr} \in \mathrm{Aut}_{\mathbb{F}_p}(K)$. Since the algebra A is reduced the Frobenius endomorphism A is a monomorphism. If $g(\mathrm{Fr}(a)) = \chi(g)\mathrm{Fr}(a)$ for all $g \in G$ then $(g(a) - (\chi(g))^{\frac{1}{p}} a)^p = 0$, and so $g(a) = (\chi(g))^{\frac{1}{p}} a$ for all $g \in G$, and statement 2 follows. □

Let $V \subseteq K$ be a $\mathbb{F}_{p^m}$-subspace of K. The subgroup $\mathrm{Sh}_V := \{\sigma_{1,v} \mid v \in V\}$ of $\mathrm{Aut}_K(K[x])$ is called the *shift group* that is determined by the $\mathbb{F}_{p^m}$-subspace V. Proposition 4.7 describes the algebra of invariants and the eigenalgebra of the shift group Sh_V.

Proposition 4.7 *Let $V \subseteq K$ be a nonzero $\mathbb{F}_{p^m}$-subspace of K. Then* $\mathbb{E}(K[x], \mathrm{Sh}_V) = K[x]^{\mathrm{Sh}_V}$.

1. *If* $\dim_{\mathbb{F}_{p^m}}(V) = \infty$ *then* $K[x]^{\mathrm{Sh}_V} = K$.
2. *If* $l = \dim_{\mathbb{F}_{p^m}}(V) < \infty$ *and* $\{\mu_1, \ldots, \mu_l\}$ *is a basis of the vector space V over* $\mathbb{F}_{p^m}$ *then*
   (a) *the fixed algebra* $K[x]^{\mathrm{Sh}_V} = K[f_V]$ *is a polynomial algebra in* $f_V := \prod_{v \in V}(x - v)$*, the polynomial f_V is divisible by the polynomial* $\prod_{i=1}^{l} f_{\mu_i}$,

(b) *for all elements* $\alpha, \beta \in \mathbb{F}_{p^m}$ *and* $\lambda \in K$, $f_V(\alpha x + \beta\lambda) = \alpha f_V(x) + \beta f_V(\lambda)$. *In particular, the map* $K \to K$, $\lambda \mapsto f_V(\lambda)$ *is a* $\mathbb{F}_{p^m}$*-linear map,*

(c) *If* $V \subset V'$ *are distinct* $\mathbb{F}_{p^m}$*-subspaces of K then* $f_V | f_{V'}$ *and* $f_V \neq f_{V'}$,

(d) $\frac{df_V}{dx} \neq 0$.

3. *In particular, for all elements* $\mu \in K^\times$, $K[x]^{\sigma_{1,\mu}} = K[f_\mu]$.

Proof For all elements $\mu \in K$, the map

$$\sigma_{1,\mu} - 1 : K[x] \to K[x], \quad \psi(x) \mapsto \psi(x+\mu) - \psi(x)$$

is locally nilpotent map. Therefore, the element 1 is the only eigenvalue for the map $\sigma_{1,\mu}$, and so $\mathbb{E}(K[x], \mathrm{Sh}_V) = K[x]^{\mathrm{Sh}_V}$.

1. Statement 1 follows from statement 2. Let $\{\mu_i\}_{i\in\mathbb{N}}$ be a family of $\mathbb{F}_{p^m}$-linearly independent elements of the vector space V and $V_i = \bigoplus_{j=1}^{i} \mathbb{F}_{p^m}\mu_i$. Then $V_1 \subset V_2 \subset \cdots \subset V_\infty := \bigoplus_{i\geq 1} \mathbb{F}_{p^m}\mu_i \subseteq V$. Hence,

$$K[x]^{\mathrm{Sh}_{V_1}} \supseteq K[x]^{\mathrm{Sh}_{V_2}} \supseteq \cdots \supseteq K[x]^{\mathrm{Sh}_{V_\infty}} = \bigcap_{i\geq 1} K[x]^{\mathrm{Sh}_{V_i}} = \bigcap_{i\geq 1} K[f_{V_i}] = K \supseteq K[x]^{\mathrm{Sh}_V} \supseteq K,$$

and so $K[x]^{\mathrm{Sh}_V} = K$.

2. (a,b). For all elements $v' \in V$,

$$\sigma_{1,v'}(f_V) = \prod_{v\in V}(x - v' - v) = f_V.$$

Therefore, $K[x]^{\mathrm{Sh}_V} \supseteq K[f_V]$. By Eq. 17, the polynomial $\prod_{i=1}^{l}\prod_{u\in\mathbb{F}_p}(x - u\mu_i) = \prod_{i=1}^{l} f_{\mu_i}$ is a divisor of the polynomial f_V. In particular, $f_V(0) = 0$.

First, we prove that the statements (a) and (b) hold in the case when $K = \overline{K}$ and then we deduce that the statements (a) and (b) hold for an arbitrary field K.

So, suppose that $K = \overline{K}$. Let $g(x) \in K[x]^{\mathrm{Sh}_V}$ be a non-scalar monic polynomial. Let γ be a root of $g(x)$. Then for all elements $v \in V$, the element $\gamma + v$ is also a root of the polynomial $g(x)$. So, the set of all roots of the polynomial $g(x)$ is a disjoint union of the sets $\coprod_{i=1}^{s}\{\gamma_i + V\}$ for some roots γ_i of $g(x)$.

Therefore, the polynomial

$$g(x) = \prod_{i=1}^{s}\prod_{v\in V}(x - \gamma_i - v) = \prod_{i=1}^{s} f_V(x - \gamma_i)$$

is a product of Sh_V-invariant polynomials $f_V(x - \gamma_i)$ of the same degree p^{lm}. In particular, every non-scalar Sh_V-invariant polynomial has degree at least p^{lm}. Therefore, for all elements $\lambda, \mu \in K$, the difference

$$c_{\lambda,\mu} := f_V(x+\lambda) - f_V(x+\mu)$$

of two monic Sh_V-invariant polynomials of degree p^{lm} must be a constant which is equal to $f_V(\lambda) - f_V(\mu)$. Therefore,

$$f_V(x+\lambda) - f_V(\lambda) = f_V(x+\mu) - f_V(\mu).$$

When $\mu = 0$, we have that

$$f_V(x+\lambda) = f_V(x) + f_V(\lambda) - f_V(0) = f_V(x) + f_V(\lambda)$$

since $f_V(0)=0$. Since for all elements $u\in \mathbb{F}_{p^m}^{\times}$,

$$f_V(ux)=u^{p^{lm}}\prod_{v\in V}(x-u^{-1}v)=u\prod_{v\in V}(x-v)=uf_V(x),$$

and $f_V(0x)=0=0f_V(x)$, we see that for all elements $\xi\in\mathbb{F}_{p^m}$, $f_V(\xi x)=\xi f_V(x)$. Now, the statement (b) follows.

Now, the polynomial

$$g(x)=\prod_{i=1}^{s}f_V(x-\gamma_i)=\prod_{i=1}^{s}(f_V(x)-f_V(\gamma_i))\in K[f_V(x)]$$

and the statement (a) follows.

Suppose that K is not necessarily algebraically closed field and $g(x)\in K[x]^{\mathrm{Sh}_V}$ be a non-scalar monic polynomial. Then $g(x)\in \overline{K}[f_V(x)]$. Since the $\overline{K}=K\oplus W$ for some K-subspace W of K and $f_V(x)\in K[x]$, we must have that $g(x)\in K[f_V(x)]$ since

$$\overline{K}[f_V(x)]=K[f_V(x)]\oplus\bigoplus_{i\geq 0}Wf_V(x)^i\subseteq K[x]\oplus\bigoplus_{i\geq 0}Wf_V(x)^i.$$

Now, the statements (a) and (b) hold for the field K.

(c) The statement (c) follows from the statement (a).

(d) WLOG we may assume that $K=\overline{K}$. Suppose that $\frac{df_V}{dx}=0$. Then $f_V=g^p$ for some polynomial g. This is not possible as every root of f has multiplicity 1.

3. Statement 3 is a particular case of statement 2. □

Notice that for all natural numbers $m\geq 1$,

$$x^{p^m}-x=\prod_{i\in\mathbb{F}_{p^m}}(x-i). \tag{19}$$

By Eq. 19, for each element $\mu\in K^{\times}$, let

$$f_{p^m,\mu}(x):=f_{\mathbb{F}_{p^m}\mu}(x)=\prod_{i\in\mathbb{F}_{p^m}}(x-i\mu)=x^{p^m}-\mu^{p^m-1}x. \tag{20}$$

For all $\alpha,\beta\in\mathbb{F}_{p^m}$:

$$f_{p^m,\mu}(\alpha x+\beta x')=\alpha f_{p^m,\mu}(x)+\beta f_{p^m,\mu}(x') \tag{21}$$

since $\gamma^{p^m}=\gamma$ for all $\gamma\in\mathbb{F}_{p^m}$. In particular, the map $K\to K$, $\lambda\mapsto f_{p^m,\mu}(\lambda)$ is a $\mathbb{F}_{p^m}$-linear map. Hence, for all elements $\lambda\in K$,

$$x^{p^m}-\mu^{p^m-1}x-(\lambda^{p^m}-\mu^{p^m-1}\lambda)=f_{p^m,\mu}(x)-f_{p^m,\mu}(\lambda)=f_{p^m,\mu}(x-\lambda)=\prod_{i\in\mathbb{F}_{p^m}}(x-\lambda-i\mu). \tag{22}$$

Theorem 4.8 describes the algebra of invariants and the eigenalgebra of a 'generic' finite subgroup of $\mathrm{Aut}_K(K[x])$.

Theorem 4.8 *Let* $G=\widetilde{G}\rtimes\overline{G}$ *be a finite subgroup of* $\mathrm{Aut}_K(K[x])$ (Theorem 4.4) *where* $\overline{G}:=\langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ *and* $\widetilde{G}:=\{\sigma_{1,\mu}\,|\,\mu\in V\}$, *$\lambda_n\in K$ is a primitive n'th root of unity, $n\geq 2$ and $\nu\in K$, V is a nonzero finite dimensional $\mathbb{F}_p(\lambda_n)$-subspace of K, and $\mathbb{F}_p(\lambda_n)=\mathbb{F}_{p^m}$ for some* $m\geq 1$ (Lemma 4.3). *Then:*

1. $\sigma_{\lambda_n,(1-\lambda_n)\nu}(f_V(x-\nu))=\lambda_nf_V(x-\nu)$.

2. $K[x]^G = K[f_V^n(x-\nu)]$ *is a polynomial algebra in* $f_V^n(x-\nu) := \Big(f_V(x-\nu)\Big)^n$.
3. *The* G*-eigenvalue subalgebra of* $K[x]$ *is* $\mathbb{E}(K[x], G) = \bigoplus_{i=0}^{n-1} f_V^i(x-\nu)K[x]^G$, *a direct sum of distinct* G*-eigenspaces.*

Proof 1. Let $\sigma = \sigma_{\lambda_n,(1-\lambda_n)\nu}$. Suppose that $l = \dim_{\mathbb{F}_{p^m}}(V)$. Then $\deg(f_V(x)) = p^{lm}$. Now, by Proposition 4.7.(2b),

$$\sigma(f_V(x-\nu)) = f_V(\sigma(x-\nu)) = f_V(\lambda_n(x-\nu)) = \lambda_n f_V(x-\nu)$$

since $\lambda_n \in K(\lambda_n) = \mathbb{F}_{p^m}$.

2 and 3. By Proposition 4.7.(2b), the $\widetilde{G}$-eigenvalue subalgebra of $K[x]$ is the fixed algebra $K[x]^{\widetilde{G}} = K[f_V(x)] = K[f_V(x-\nu)]$ since

$$f_V(x) = f_V(x-\nu+\nu) = f_V(x-\nu) + f_V(\nu).$$

By statement 1, $\sigma(f_V(x-\nu)) = \lambda_n f_V(x-\nu)$, hence the $\widetilde{G}$-eigenvalue subalgebra of $K[x]$, $K[f_V(x-\nu)]$, is σ-invariant, and statements 2 and 3 follow. □

Proposition 4.9 describes the algebra of invariants and the eigenalgebra of the subgroup $G = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ of $\mathrm{Aut}_K(K[x])$ where $\lambda_n \in K$ is a primitive n'th root of unity, $n \geq 2$ and $\nu \in K$.

Proposition 4.9 *Let* $G = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ *be a finite subgroup of* $\mathrm{Aut}_K(K[x])$ *where* $\lambda_n \in K$ *is a primitive* n*'th root of unity,* $n \geq 2$ *and* $\nu \in K$. *Then:*

1. $\sigma_{\lambda_n,(1-\lambda_n)\nu}(x-\nu) = \lambda_n(x-\nu)$.
2. $K[x]^G = K[(x-\nu)^n]$ *is a polynomial algebra in* $(x-\nu)^n$.
3. $\mathbb{E}(K[x], G) = K[x] = \bigoplus_{i=0}^{n-1}(x-\nu)^i K[x]^G$ *is a direct sum of distinct* G*-eigenspaces.*

Proof 1. Statement 1 is obvious.

2. Statement 2 follows from statement 1 and the fact that λ_n is a primitive n'th root of unity.

3. Statement 3 follows from statement 2. □

The eigengroup $G_f(K)$ of a polynomial $f \in K[x]$ that has single root in $\overline{K}$ For an element $\nu \in K$, the subset

$$\mathbb{T}_\nu(K) := \{\sigma_{\lambda,(1-\lambda)\nu} \mid \lambda \in K^\times\} \tag{23}$$

of $\mathrm{Aut}_K(K[x])$ is a subgroup which is isomorphic to the algebraic torus $\mathbb{T} = (K^\times, \cdot)$ via

$$\mathbb{T}_\nu(K) \to \mathbb{T}, \quad \sigma_{\lambda,(1-\lambda)\nu} \mapsto \lambda$$

since $\sigma_{\lambda,(1-\lambda)\nu}\sigma_{\lambda',(1-\lambda')\nu} = \sigma_{\lambda\lambda',(1-\lambda\lambda')\nu}$ for all $\lambda, \lambda' \in K^\times$.

Suppose that a monic non-scalar polynomial $f \in \overline{K}[x]$ of degree d has single root, say $\nu \in \overline{K}$. Then $d = p^r d_1$ where for unique natural numbers r and d_1 such that $p \nmid d_1$. Then

$$f = (x-\nu)^d = (x-\nu)^{p^r d_1} = (x^{p^r} - \nu^{p^r})^{d_1} = x^{p^r d_1} - d_1\nu^{p^r}x^{p^r(d_1-1)} + \cdots. \tag{24}$$

Therefore, $f = (x-\nu)^d \in K[x]$ iff $\nu^{p^r} \in K$ (since $p \nmid d_1$).

The next proposition describes all the monic polynomial $f \in K[x]$ such that $G_f(K) = \mathbb{T}_\nu(K)$ for some $\nu \in K$. Furthermore, it describes the group G_f for all polynomial $f \in K[x]$ that has a single root in $\overline{K}$.

Proposition 4.10 *1. Let $f(x) \in \overline{K}[x]$ be a monic non-scalar polynomial of degree d. Then $f(x) = (x-\nu)^d$ for some $\nu \in \overline{K}$ iff $G_f(\overline{K}) = \mathbb{T}_\nu(\overline{K})$.*

2. Let $f(x) \in K[x]$ be a monic non-scalar polynomial of degree d that has a single root $\nu \in \overline{K}$. Then $G_f(K) = \begin{cases} \mathbb{T}_\nu(K) & \text{if } \nu \in K, \\ \{e\} & \text{if } \nu \notin K. \end{cases}$

3. Let $f(x) \in K[x]$ be a monic non-scalar polynomial of degree d that has a single root $\nu \in \overline{K}$. Then $f(x) = (x-\nu)^d$ for some $\nu \in K$ iff $G_f(K) = \mathbb{T}_\nu(K)$.

Proof 1. ($\Rightarrow$) Suppose that $f = (x-\nu)^d$. An automorphism $\sigma \in \mathrm{Aut}_K(K[x])$ belongs to the group $G_f(\overline{K})$ iff $\sigma(x-\nu) = \lambda(x-\nu)$ for some element $\lambda \in \overline{K}^\times$. The last equality is equivalent to the equality $\sigma = \sigma_{\lambda,(1-\lambda)\nu}$, or equivalently, $G_f = \mathbb{T}_\nu(\overline{K})$.

($\Leftarrow$) Suppose that $G_f = \mathbb{T}_\nu(\overline{K})$. Then $K[x] = \bigoplus_{i\geq 0} K(x-\nu)^i$ is a direct sum of the eigenspaces of the group $\mathbb{T}_\nu(\overline{K})$. Therefore, $f(x) = (x-\nu)^d$ for some $d \geq 1$.

2. Clearly, $G_f(K) = G_f(\overline{K}) \cap \mathrm{Aut}_K(K[x]) = \mathbb{T}_\nu(\overline{K}) \cap \mathrm{Aut}_K(K[x])$. By statement 1, $G_f(K) \neq \{e\}$ iff $e \neq \sigma_{\lambda,(1-\lambda)\nu} \in \mathbb{T}_\nu(\overline{K}) \cap \mathrm{Aut}_K(K[x])$ where $1 \neq \lambda \in K^\times$ and (necessarily) $\nu \in K^\times$ iff $G_f(K) = \mathbb{T}_\nu(K)$.

3. Statement 3 follows from statement 2. □

The eigengroup $G_f(K)$ of a polynomial $f \in K[x]$ that has at least two distinct roots in $\overline{K}$ For each non-scalar monic polynomial $f(x)$, Theorems 4.24, 4.27, 4.30 and 4.32 (resp., Theorem 4.33) are explicit descriptions of the eigengroup $G_f(K)$ in the case when the field K is algebraically closed (resp., in general case).

Lemma 4.11 is an explicit description of the roots of the polynomials of the type $g(f_V^n(x-\nu))$.

Lemma 4.11 *Suppose that $\lambda_n \in K$ is a primitive n'th root of unity, $n \geq 2$ and $\nu \in K$, V is a nonzero finite dimensional $\mathbb{F}_p(\lambda_n)$-subspace of K, and $K(\lambda_n) = \mathbb{F}_{p^m}$ for some $m \geq 1$* (Lemma 4.3). *Then:*

1. For all elements $\rho \in K$,

$$f_V^n(x-\nu) - f_V^n(\rho) = \prod_{i=0}^{n-1}\prod_{v\in V}(x-\nu-\lambda_n^i\rho - v).$$

2. Let $g(x) = \prod_{j=1}^k (x-\xi_j) \in \overline{K}[x]$ where $\mathcal{R}(g) = \{\xi_1, \ldots, \xi_k\}$ is the set of roots of the polynomial $g(x)$ counted with multiplicity. Then $\xi_j = f_V^n(\rho_j)$ for some element $\rho_j \in \overline{K}$ and

$$g(f_V^n(x-\nu)) = \prod_{j=1}^{k}\prod_{i=0}^{n-1}\prod_{v\in V}(x-\nu-\lambda_n^i\rho_j - v).$$

Proof 1. By Proposition 4.7.(2b), the map f_V is a $K(\lambda_n)$-linear map (since $K(\lambda_n) = \mathbb{F}_{p^m}$), and the result follows:

$$\begin{aligned} f_V^n(x-\nu) - f_V^n(\rho) &= \prod_{i=0}^{n-1}(f_V(x-\nu) - \lambda_n^i f_V(\rho)) = \prod_{i=0}^{n-1} f_V(x-\nu-\lambda_n^i\rho) \\ &= \prod_{i=0}^{n-1}\prod_{v\in V}(x-\nu-\lambda_n^i\rho - v). \end{aligned}$$

2. Notice that $g(x) = \prod_{j=1}^k (f_V^n(x-\nu) - f_V^n(\rho_j))$, and statement 2 follows from statement 1. □

Theorem 4.12 *Suppose that a monic polynomial $f(x) \in K[x]$ has at least two distinct roots in $\overline{K}$. Then the group $G_f(K)$ is a finite group, $G_f(K) = \widetilde{G}_f(K) \rtimes \overline{G}_f(K)$ where $\overline{G}_f(K) = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ and $\widetilde{G}_f(K) = \mathrm{Sh}_V(K)$, $\lambda_n \in K$ is a primitive n'th root of unity, $\nu \in K$, V is a finite dimensional $\mathbb{F}_p(\lambda_n)$-subspace of K, and $\mathbb{F}_p(\lambda_n) = \mathbb{F}_{p^m}$ for some $m \geq 1$* (Lemma 4.3).

Proof Since $G_f(K) = G_f(\overline{K}) \cap \mathrm{Aut}_K(K[x])$, it suffices to prove the theorem in the case when the field K is an algebraically closed field. So, we assume that $K = \overline{K}$. Recall that $\mathcal{R}_d$ be the set of *distinct* roots of the polynomial f. The subgroup $\widetilde{G}_f = G_f \cap \mathrm{Sh}(K)$ is equal to a group Sh_V where V is a finite dimensional vector space over the field $\mathbb{F}_p$ since $|V| \leq |\mathcal{R}_d|$ (as $\mathcal{R}_d + V \subseteq \mathcal{R}_d$).

If G is a finite subgroup of G_f that contains the group Sh_V then $G = \mathrm{Sh}_V \rtimes \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ where λ_n is a primitive n'th root of unity and $\nu \in K$. The cyclic group $\langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ of order n acts on the field K and on the set $\mathcal{R}_d$, see Eq. 14. The point ν is the only fixed point of the action and the orbit of every element $\lambda \neq \nu$ contains precisely n elements. The polynomial f contains at least two distinct roots. Therefore $n \leq |\mathcal{R}_d|$. Then, by Eq. 13, the group $\varphi(G_f)$ is equal to $\langle \sigma_{\lambda_{n'},(1-\lambda_{n'})\nu'} \rangle$ where $\lambda_{n'}$ is a primitive n''th root of unity and $\nu' \in K$. By Theorem 4.4, $G_f = \mathrm{Sh}_V \rtimes \langle \sigma_{\lambda_{n'},(1-\lambda_{n'})\nu'} \rangle$ is a finite group. □

Corollary 4.13 is a criterion for the group G_f to be an infinite group.

Corollary 4.13 *Let $f(x) \in K[x]$ be a non-scalar monic polynomial. Then the following statement are equivalent:*

1. *The group G_f is an infinite group.*
2. *$f(x) = (x - \nu)^d$ for some $\nu \in K$.*
3. *$G_f(K) = \mathbb{T}_\nu(K)$ (see Eq. 23 for the definition of the group $\mathbb{T}_\nu(K)$).*

Proof The corollary follows from Proposition 4.10.(3) and Theorem 4.12. □

Recall that the field K is an algebraically closed field, $f(x) \in K[x]$ is a monic polynomial that has at least two distinct roots, and $\mathcal{R}(f)$ is the set of all roots of f counted with multiplicity. Recall that (Theorems 4.12 and 4.4) the group $G_f = \widetilde{G}_f \rtimes \overline{G}_f$ is a finite subgroup of $\mathrm{Aut}_K(K[x])$ where $\overline{G}_f := \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ provided $\overline{G}_f \neq \{e\}$ and $\widetilde{G}_f := \{\sigma_{1,\mu} \mid \mu \in V\}$, $\lambda_n \in K$ is a primitive n'th root of unity, $\nu \in K$, V is a finite dimensional $\mathbb{F}_p(\lambda_n)$-subspace of K, and $\mathbb{F}_p(\lambda_n) = \mathbb{F}_{p^m}$ for some $m \geq 1$ (Lemma 4.3).

There are four distinguish cases:

1. $\widetilde{G}_f \neq \{e\}$, $\overline{G}_f \neq \{e\}$,
2. $\widetilde{G}_f \neq \{e\}$, $\overline{G}_f = \{e\}$,
3. $\widetilde{G}_f = \{e\}$, $\overline{G}_f \neq \{e\}$,
4. $\widetilde{G}_f = \{e\}$, $\overline{G}_f = \{e\}$.

Below, in the case of $K = \overline{K}$, for the polynomial f criteria are given in terms of its roots for each case to hold.

A description of the group $\widetilde{G}_f(K)$ and a criterion for $\widetilde{G}_f(K) \neq \{e\}$.

Definition 4.14 Let $f(x) \in K[x]$ be a non-scalar polynomial. Two distinct roots $\lambda, \lambda' \in \overline{K}$ of the polynomial $f(x)$ are called a *K-shift pair* of $f(x)$ if

$$\lambda - \lambda' \in K \quad \text{and} \quad \mathbb{F}_p(\lambda - \lambda') + \mathcal{R}(f) \subseteq \mathcal{R}(f) \tag{25}$$

where $\mathcal{R}(f)$ is the set of all roots in $\overline{K}$ of the polynomial $F(x)$ counted with multiplicity.

The set of all K-shift pairs of the polynomial $f(x)$ is denoted by $\mathrm{SP}(f, K)$. The vector space over K,

$$V(f,K) = \begin{cases} \sum_{\{\lambda,\lambda'\}\in \mathrm{SP}(f,K)} \mathbb{F}_p(\lambda-\lambda') & \text{if } \mathrm{SP}(f,K)\neq\emptyset, \\ 0 & \text{if } \mathrm{SP}(f,K)=\emptyset. \end{cases} \tag{26}$$

is called the *K-shift vector space* of the polynomial $f(x)$.

For fields $K \subseteq L \subseteq \overline{K}$, we have $\mathrm{SP}(f, K) \subseteq \mathrm{SP}(f, L) \subseteq \mathrm{SP}(f, \overline{K})$ and $V(f, K) \subseteq V(f, L) \subseteq V(f, \overline{K})$.

Proposition 4.15 gives an explicit description of the group $\widetilde{G}_f(K)$ and a criterion for $\widetilde{G}_f(K) \neq \{e\}$.

Proposition 4.15 *Let $f(x) \in K[x]$ be a non-scalar monic polynomial. Then:*

1. $\widetilde{G}_f(K) = \mathrm{Sh}_V$ *where $V = V(f, K)$ is the K-shift vector space of f.*
2. $\widetilde{G}_f(K) = \{e\}$ *iff* $\mathrm{SP}(f, K) = \emptyset$ *iff for all distinct roots $\lambda, \lambda' \in \overline{K}$ of the polynomial f such that $\lambda - \lambda' \in K$ (if they exist), $\mathbb{F}_p(\lambda-\lambda') + \mathcal{R}(f) \nsubseteq \mathcal{R}(f)$.*
3. $\widetilde{G}_f(\overline{K}) = \{e\}$ *iff* $\mathrm{SP}(f, \overline{K}) = \emptyset$ *iff for all distinct roots $\lambda, \lambda' \in \overline{K}$ of the polynomial f, $\mathbb{F}_p(\lambda-\lambda') + \mathcal{R}(f) \nsubseteq \mathcal{R}(f)$.*

Proof 1. It follows from the description of the group $\widetilde{G}_f(K)$ as a shift group, $\widetilde{G}_f(K) = \mathrm{Sh}_V$, that $V = V(f, K)$.

2 and 3. Statement 2 follows from statement 1 and statement 3 is a particular case of statement 2. □

Definition 4.16 Let V be a nonzero finite dimensional $\mathbb{F}_p$-subspace of K. The largest finite field, denoted $\mathbb{F}_{p^e}$, where $e = e(V) \geq 1$, such that $\mathbb{F}_{p^e}V \subseteq V$ is called the *multiplier field* of V. The natural number $e = e(V)$ is called the *p-exponent* of V.

The multiplier field $\mathbb{F}_{p^e}$ is the composite of all finite fields $\mathbb{F}_{p^m}$ such that $\mathbb{F}_{p^m}V \subseteq V$. If $\dim_{\mathbb{F}_p}(V) = n$ then $p^m \leq |V| = p^n$, and so $m \leq n$.

Let λ_{p^e-1} be a primitive $p^e - 1$'st root of unity (a generator of the cyclic group $\mathbb{F}_{p^e}^{\times}$). Since $\lambda_{p^e-1} \in \mathbb{F}_{p^e}$ and $\mathbb{F}_{p^e}V \subseteq V$, we have that $\lambda_{p^e-1}V \subseteq V$.

For each finite dimensional $\mathbb{F}_p$-subspace V of the field K, Lemma 4.17 describes all the roots of unity λ_n such that $\lambda_n V \subseteq V$.

Lemma 4.17 *Let V be a nonzero finite dimensional $\mathbb{F}_p$-subspace of the field K, $\mathbb{F}_{p^e}$ be its multiplier field.*

1. *Suppose that λ_n is a primitive n'th root of unity. Then $\lambda_n V \subseteq V$ iff $n | p^e - 1$.*
2. $|\mathbb{F}_{p^e}^{\times}| = 1$ *iff $(p, e) = (2, 1)$ iff $\lambda_n V \subseteq V$ (where λ_n is a primitive n'th root of unity) implies $\lambda_n = 1$.*

Proof 1. $\lambda_n V \subseteq V$ iff $\lambda_n \in \mathbb{F}_{p^e}^{\times}$ iff $n || \mathbb{F}_{p^e}^{\times}|$ iff $n | p^e - 1$.

2. Statement 2 follows from statement 1. □

Classification of subgroups G of $\mathrm{Aut}_K(K[x])$ which are maximal satisfying the property $G \cap \mathrm{Sh}(K) = \mathrm{Sh}_V$.

Corollary 4.18 *Let V be a nonzero finite dimensional $\mathbb{F}_p$-subspace of the field K, $\mathbb{F}_{p^e}$ be its multiplier field and λ_{p^e-1} be a primitive $p^e - 1$'st root of unity. Then the finite groups $G_{V,\nu} := \mathrm{Sh}_V \rtimes \langle \sigma_{\lambda_{p^e-1},(1-\lambda_{p^e-1})\nu}\rangle$, where $\nu \in K/V$, are the maximal subgroups G of the group $\mathrm{Aut}_K(K[x])$ that satisfy the property that $G \cap \mathrm{Sh}(K) = \mathrm{Sh}_V$.*

Proof Recall that for all elements $\lambda \in K^\times$ and $\mu, v \in K$, $\sigma_{\lambda,\mu}\sigma_{1,v}\sigma_{\lambda,\mu}^{-1} = \sigma_{1,\lambda^{-1}v}$. Hence the groups $G_{V,\nu}$ are well defined and every subgroup H of $\mathrm{Aut}_K(K[x])$ such that $H \cap \mathrm{Sh}(K) = \mathrm{Sh}_V$ is a finite group.

Given a finite subgroup G' of $\mathrm{Aut}_K(K[x])$ such that $G' \cap \mathrm{Sh}(K) = \mathrm{Sh}_V$. By Theorem 4.4, $G' = \mathrm{Sh}_V \rtimes \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ for some $\nu \in K$ and a primitive n'th root of unity λ_n such that $n | p^e - 1$, by Lemma 4.17.(1), and so $G' \subseteq G_{V,\nu}$. Since the groups $\{G_{V,\nu}\}_{\nu \in K}$ are distinct, the corollary follows ($G_{V,\nu} = G_{V,\nu'}$ iff $\sigma_{\lambda,(1-\lambda)\nu'} = \sigma^i_{\lambda,(1-\lambda)\nu}\sigma_{1,v}$ for some natural number i such that $1 \leq i < p$ and $\gcd(i, p) = 1$ and an element $v \in V$ where $\lambda = \lambda_{p^e-1}$ iff $\nu' = \nu + (1-\lambda^i)^{-1}v$ since $\sigma^i_{\lambda,(1-\lambda)\nu}\sigma_{1,v} = \sigma_{\lambda^i,(1-\lambda^i)(\nu+(1-\lambda^i)^{-1}v)}$ iff $\nu' \equiv \nu \mod V$ since $\mathbb{F}_p(\lambda)V = \mathbb{F}_{p^e}V = V$). □

Criterion for $\widetilde{G}_f \neq \{e\}$ and $\overline{G}_f \neq \{e\}$.

Lemma 4.19 *Suppose that K is an algebraically closed field, $f(x) \in K[x]$ is monic non-scalar polynomial that has at least two distinct roots, $\widetilde{G}_f = \mathrm{Sh}_V \neq \{e\}$ and $\overline{G}_f = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle \neq \{e\}$ where V is a nonzero $\mathbb{F}_p(\lambda_n)$-subspace of the field K and λ_n is primitive n'th root of unity. Then:*

1. *$\lambda_n \in \mathbb{F}_{p^e}$ where $\mathbb{F}_{p^e}$ is the multiplier field of the $\mathbb{F}_p$-subspace V of K, or, equivalently, $n|p^e - 1$.*
2. *The group $G_f = \mathrm{Sh}_V \rtimes \overline{G}_f$ is a subgroup of $\mathrm{Sh}_V \rtimes \langle \sigma_{\lambda,(1-\lambda)\nu} \rangle$ where λ is a cyclic generator of the group $\mathbb{F}^\times_{p^e}$, i.e. $\lambda = \lambda_{p^e-1}$ is primitive $p^e - 1$'st root of unity.*

Proof 1. Since $\lambda_n V \subseteq V$, $\lambda_n \in \mathbb{F}_{p^e}$ and the lemma follows from Corollary 4.18. □

Definition 4.20 Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in \overline{K}[x]$ be a monic polynomial of degree $d \geq 1$ where $a_i \in \overline{K}$ are the coefficients of the polynomial $f(x)$. Then the natural number

$$\gcd(f(x)) := \gcd\{i \geq 1 \mid a_i \neq 0\}$$

is called the *exponent* of $f(x)$.

Clearly, the exponent of $f(x)$ is the largest natural number $m \geq 0$ such that $f(x) = g(x^m)$ for some polynomial $g(x) \in K[x]$.

Definition 4.21 For a non-scalar polynomial $f \in K[x]$, we have the unique product

$$\gcd(f) = p^s \gcd_p(f) \quad \text{where} \quad s \geq 0, \quad \gcd_p(f) \in \mathbb{N} \quad \text{and} \quad p \nmid \gcd_p(f). \tag{27}$$

Proposition 4.22 *Suppose that $f(x) = f^i_V(x - \nu)$ for some nonzero finite dimensional $\mathbb{F}_p$-subspace V of K, $\nu \in K$ and a natural number $i \geq 1$ (i.e. $\mathcal{R}_d(f) = \nu + V$ and each root of $f(x)$ has multiplicity i). Let $\mathbb{F}_{p^e}$ be the multiplier field of V, $\mathbb{F}^\times_{p^e} = \langle \lambda_n \rangle$ where $n = p^e - 1$. Then*

$$G_f = \begin{cases} \mathrm{Sh}_V \rtimes \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle \neq \mathrm{Sh}_V & \textit{if } (p, e) \neq (2, 1), \\ \mathrm{Sh}_V & \textit{if } (p, e) = (2, 1). \end{cases}$$

Proof Since $|\mathcal{R}_d(f)| = |\nu + V| = |V| \geq 2$, the group $G_f = \widetilde{G}_f \rtimes \overline{G}_f$ is a finite group. Clearly, $\mathrm{Sh}_V \subseteq \widetilde{G}_f$. In fact, $\mathrm{Sh}_V = \widetilde{G}_f$ since $\mathcal{R}_d(f) = \nu + V$.

Suppose that $(p, e) \neq (2, 1)$. Recall that $n = p^e - 1 > 1$ and $\mathbb{F}^\times_{p^e} = \langle \lambda_n \rangle$, the multiplier field of V. In particular, $\lambda_n V \subseteq V$. Therefore, $\overline{G}_f = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$, by Lemma 4.17.(1).

The case $(p, e) = (2, 1)$ is obvious, see Lemma 4.17.(2). □

Lemma 4.23 *Suppose that* $\mathrm{Fr}(K) = K$ *(where* $\mathrm{Fr}(a) = a^p$*, the Frobenius endomorphism). Then* $G_{f^{p^n}}(K) = G_f(K)$ *for all polynomials* $f \in K[x]$ *and all natural numbers* $n \geq 1$.

Proof (i) $G_{f^{p^n}}(K) \supseteq G_f(K)$: If $\sigma \in G_f(K)$ then $\sigma(f) = \lambda f$ for some $\lambda \in K$, and so $\sigma(f^{p^n}) = \lambda^{p^n} f^{p^n}$. This means that $\sigma \in G_{f^{p^n}}(K)$.

(ii) $G_{f^{p^n}}(K) \subseteq G_f(K)$: If $\tau \in G_{f^{p^n}}(K)$ then $\tau(f^{p^n}) = \mu f^{p^n}$ for some $\mu \in K$, and so $(\tau(f) - \mu^{\frac{1}{p^n}} f)^{p^n} = 0$, i.e. $\tau(f) = \mu^{\frac{1}{p^n}} f$. This means that $\tau \in G_f(K)$. □

Let $f(x) = \sum a_i x^i \in K[x]$ be a monic non-scalar polynomial and $\gcd(f) = p^s \gcd_p(f)$. Suppose that $K = \overline{K}$. Then there is a unique monic non-scalar polynomial $f_1(x) \in K[x]$ such that

$$f(x) = f_1^{p^s}(x). \tag{28}$$

Clearly, $\gcd(f_1) = \gcd_p(f)$, $\deg(f) = p^s \deg(f_1)$ and $f_1' \neq 0$ (the derivative of f_1).

Theorem 4.24 is a criterion for the group $G_f = \widetilde{G}_f \rtimes \overline{G}_f$ to have nontrivial subgroups $\widetilde{G}_f$ and $\overline{G}_f$, it also gives an explicit description of the group G_f.

Theorem 4.24 *Suppose that the field* K *is an algebraically closed field and* $f(x) \in K[x]$ *is a monic polynomial that has at least two distinct roots,* $gcd(f) = p^s \gcd_p(f)$ *and* $f(x) = f_1^{p^s}(x)$ *for a unique monic non-scalar polynomial* $f_1(x) \in K[x]$*, see* Eq. 28. *Suppose that* $V \neq 0$ *is a finite dimensional* $\mathbb{F}_p$*-subspace of* K *and* $\mathbb{F}_{p^e}$ *is the multiplier field of* V. *Then the following statements are equivalent:*

1. $\widetilde{G}_f = \mathrm{Sh}_V \neq \{e\}$ *and* $\overline{G}_f = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle \neq \{e\}$.
2. *There is a primitive* n*'th root of unity* $\lambda_n \neq 1$ *(in particular,* $n \geq 2$*) such that* $\lambda_n V \subseteq V$*, and an element* $\nu \in K$ *such that either* $f(x) = f_V^i(x - \nu)$ *for some natural number* $i \geq 1$ *and* $n = p^e - 1$ *(in this case,* $(p, e) \neq (2, 1)$*,* $\widetilde{G}_f = \mathrm{Sh}_V$ *and* $\overline{G}_f = \langle \sigma_{\lambda_{p^e-1},(1-\lambda_{p^e-1})\nu} \rangle$ *where* $\mathbb{F}_{p^e}^{\times} = \langle \lambda_{p^e-1} \rangle$*) or otherwise* $f(x) = f_V^i(x - \nu) g(f_V^n(x - \nu))$ *for some natural number* $i \geq 0$ *and a monic nonn-scalar polynomial* $g(x) \in K[x]$ *such that* $g(0) \neq 0$*, and the following two conditions hold:*
   - *(a)* $n \geq 2$ *and* $\gcd(\frac{p^e-1}{n}, \gcd_p(g)) = 1$*, and*
   - *(b)* $\mathcal{R}(f) + \mathbb{F}_p(\lambda_n)(\lambda - \lambda') \nsubseteq \mathcal{R}(f)$ *for all distinct roots* λ *and* λ' *of the polynomial* f *such that* $\lambda - \lambda' \notin V$.

Suppose that statement 1 holds. Then:

- *the natural number* i *and the polynomial* $g(x)$ *in statement 2 are unique,*
- *the element* ν *is unique up to adding an arbitrary element of* V *(i.e.* ν *can be replaced by* $\nu + \upsilon$ *for any element* $\upsilon \in V$*),*
- *the equality* $f(x) = f_V^i(x - \nu) g(f_V^n(x - \nu))$ *is unique (since* $f_V(x - \nu - \upsilon) = f_V(x - \nu)$ *for all* $\upsilon \in V$*). Furthermore,* $\sigma_{\lambda_n,(1-\lambda_n)\nu}(f) = \lambda_n^i f$*, and* $f \in K[x]^{G_f}$ *iff* $n|i$.
- *In the second case, i.e.* $f(x) = f_V^i(x - \nu) g(f_V^n(x - \nu))$*,*

  $$n = \gcd(p^e - 1, \gcd_p(h)$$

  where $h(x) \in K[x]$ *is a unique polynomial such that* $f(x) = f_V^i(x - \nu) h(f_V(x - \nu))$ *(i.e.* $h(x) = g(x^n)$*), and either* ν *is a root of* $f(x)$ *(i.e.* $i \geq 1$*) or otherwise (i.e.* $i = 0$*)* ν *is a root of* $f_1'(x)$ *(the derivative of* $f_1(x)$*).*

Proof (1 $\Rightarrow$ 2) Suppose that statement 1 holds. By Theorem 4.12, $\widetilde{G}_f = \mathrm{Sh}_V$ and $\overline{G}_f = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ for a nonzero $\mathbb{F}_p$-subspace V of K, a primitive n'th root of unity $\lambda_n \neq 1$ (in particular, $n \geq 2$) such that $\lambda_n V \subseteq V$ and an element $\nu \in K$. Then, by Theorem 4.8.(3), either $f(x) = f_V^i(x-\nu)$ for some natural number $i \geq 1$ or otherwise

$$f(x) = f_V^i(x-\nu) g(f_V^n(x-\nu))$$

for some natural number $i \geq 0$, $n \geq 2$, and a monic non-scalar polynomial $g(x) \in K[x]$ such that $g(0) \neq 0$.

In the first case, by Proposition 4.22, $\widetilde{G}_f = \mathrm{Sh}_V \neq \{e\}$ and $\overline{G}_f = \langle \sigma_{\lambda_{p^e-1},(1-\lambda_{p^e-1})\nu} \rangle \neq \{e\}$.

Now let us consider the second case. By Lemma 4.17, $n | p^e - 1$ (since $\lambda_n \in \mathbb{F}_{p^e}$). Suppose that $l := \gcd(\frac{p^e-1}{n}, \gcd_p(g)) > 1$. Then $\sigma_{\lambda_{ln},(1-\lambda_{ln})\nu} \in \overline{G}_f = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ where λ_{ln} is a primitive ln'th root of unity, a contradiction (since the order of the element $\sigma_{\lambda_{ln},(1-\lambda_{ln})\nu}$ is $ln > n = |\overline{G}_f|$). Therefore, the statement (a) holds.

Suppose that the condition (b) does not holds, i.e. there are two distinct roots λ and λ' of the polynomial $f(x)$ such that $v' := \lambda - \lambda' \notin V$ and $\mathcal{R}(f) + \mathbb{F}_p(\lambda_n)(\lambda - \lambda') \subseteq \mathcal{R}(f)$. Then

$$V' := V + \mathbb{F}_p(\lambda_n)v'$$

is a $\mathbb{F}_p(\lambda_n)$-submodule of K that properly contains the $\mathbb{F}_p(\lambda_n)$-module V. Then $\mathrm{Sh}_{V'} \subsetneq \mathrm{Sh}_V$, a contradiction.

(2 $\Rightarrow$ 1) In the first case, i.e. $f(x) = f_V^i(x-\nu)$, the implication follows from Proposition 4.22. In the second case, i.e. $f(x) = f_V^i(x-\nu)g(f_V^n(x-\nu))$,

$$\overline{G}_f \supseteq \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle \neq \{e\} \;\; \text{and} \;\; \widetilde{G_f} \supseteq \{\sigma_{1,\mu} \,|\, \mu \in V\} \neq \{e\}.$$

The conditions (a) and (b) imply that the inclusions above are equalities, see the proof of the implication (1 $\Rightarrow$ 2).

Suppose that statement 1 holds. Then statement 2 holds and vice versa. So, we have the equality

$$f(x) = f_V^i(x-\nu) g(f_V^n(x-\nu))$$

in statement 2 (the case $g = 1$ corresponds to the first case). The polynomial $f_V(x-\nu)$ is $\widetilde{G}_f$-invariant, i.e. for all elements $v \in V$, $f_V(x-\nu) = \sigma_{1,-v}(f_V(x-\nu)) = f_V(x-(\nu+v))$. Therefore, for all elements $v \in V$,

$$f(x) = f_V^i(x-(\nu+v)) g(f_V^n(x-(\nu+v))),$$

i.e. the element ν can be replaced by the element $\nu + v$ for any element $v \in V$. This is the only freedom for the choice of the element ν. Indeed, $G_f = \{\sigma^j_{\lambda_n,(1-\lambda_n)\nu}\sigma_{1,v} \,|\, 0 \leq j \leq n-1, v \in V\}$. Since

$$\sigma^j_{\lambda_n,(1-\lambda_n)\nu}\sigma_{1,v} = \sigma_{\lambda_n^j,(1-\lambda_n^j)\nu}\sigma_{1,v} = \sigma_{\lambda_n^j,(1-\lambda_n^j)(\nu+(1-\lambda_n^j)^{-1}v)} \;\; \text{for} \;\; 1 \leq j \leq n-1,$$

it follows that the only freedom in choosing the generator $\sigma_{\lambda_n,(1-\lambda_n)\nu}$ in Theorem 4.8 is an element of the type

$$\sigma_{\lambda_n^j,(1-\lambda_n^j)(\nu+(1-\lambda_n^j)^{-1}v)}$$

where j is a natural number such that $1 \leq j \leq n-1$, $\gcd(j,n) = 1$ and v is an arbitrary element of V. Now, by Theorem 4.8, ν is a unique (up to addition) element of V, and the elements i and $g(x)$ are unique.

Clearly, $\sigma_{\lambda_n,(1-\lambda_n)\nu}(f)=\lambda_n^i f$ (Theorem 4.8.(1)), and so $f\in K[x]^{G_f}$ iff $n|i$ (Theorem 4.8.(2,3)).

Suppose that $g(x)\neq 1$. Clearly, ν is a root of $f(x)$ iff $i\geq 1$. Suppose that ν is not a root of $f(x)$, i.e. $i=0$ and $f(x)=g(f_V^n(x-\nu))$. Recall that $f(x)=f_1^{p^s}(x)$ and $G_f=G_{f_1}$, by Lemma 4.23. Then ν is not a root of $f_1(x)$, i.e. $f_1(x)=g_1(f_V^n(x-\nu))$ for a unique polynomial $g_1(x)\in K[x]$ such that $g=g_1^{p^s}$. Hence, ν is a root of the polynomial $f_1(x)$ since

$$0\neq f_1'(x)=nf_V^{n-1}(x-\nu)f_V'(x-\nu)g_1'(f_V^n(x-\nu)),$$

$n\geq 2$ and $f_V(0)=0$.

In the second case, i.e. $f(x)=f_V^i(x-\nu)g(f_V^n(x-\nu))$, $n=\mathrm{gcd}(p^e-1,\mathrm{gcd}_p(h)$, by the statement (a). $\square$

Definition 4.25 The unique presentation of the polynomial $f(x)$,

$$f(x)=f_V^i(x-\nu)\ \text{ or }\ f(x)=f_V^i(x-\nu)g(f_V^n(x-\nu)),$$

in Theorem 4.24.(2) is called the *eigenform* or the *eigenpresentation* of the polynomial $f(x)$. The scalars $\nu+V$ and the natural number $i\geq 0$ are called the *eigenroots* of $f(x)$ and their *multiplicity*, respectively. The natural number $n\geq 2$ and the monic polynomial $g(x)$ are called the *eigenorder* and the *eigenfactor* of $f(x)$. In the second case, the eigenroots may not be roots of the polynomial $f(x)$. They are iff $i\neq 0$.

Corollary 4.26 *Suppose that the field K is an algebraically closed field and $f(x)\in K[x]$ is a monic polynomial that has at least two distinct roots, $gcd(f)=p^s\,\mathrm{gcd}_p(f)$ and $f(x)=f_1^{p^s}(x)$ for a unique monic non-scalar polynomial $f_1(x)\in K[x]$. Suppose that the polynomial f satisfies the assumption of* Theorem 4.24, *and $f_1(x)=f_V^j(x-\nu)$ or $f_1(x)=f_V^j(x-\nu)g_1(f_V^n(x-\nu))$, is the eigenform of the polynomial $f_1(x)$. Then $f(x)=f_V^{p^sj}(x-\nu)$ or $f(x)=f_V^{p^sj}(x-\nu)g_1^{p^s}(f_V^n(x-\nu))$, is the eigenform of the polynomial $f_1(x)$.*

Proof The statement follows from the facts that $f(x)=f_1^{p^s}(x)$, $G_f=G_{f_1}$ (Lemma 4.23) and the uniqueness of the eigenform (Theorem 4.24). $\square$

Criterion for $\widetilde{G}_f=\{e\}$ and $\overline{G}_f\neq\{e\}$. Theorem 4.27 is a criterion for the group $G_f=\widetilde{G}_f\rtimes\overline{G}_f$ to be equal to $\overline{G}_f\neq\{e\}$.

Theorem 4.27 *Suppose that the field K is an algebraically closed field, $f(x)\in K[x]$ is a monic polynomial that has at least two distinct roots, $gcd(f)=p^s\,\mathrm{gcd}_p(f)$ and $f(x)=f_1^{p^s}(x)$ for a unique monic non-scalar polynomial $f_1(x)\in K[x]$, see* Eq. 28. *Then the following statements are equivalent:*

1. *$\widetilde{G}_f=\{e\}$ and $\overline{G}_f=\langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle\neq\{e\}$ where λ_n is a primitive n'th root of unity and $\nu\in K$.*
2. *$f(x)=(x-\nu)^ig((x-\nu)^n)$ for some natural number $i\geq 0$ and a monic non-scalar polynomial $g(x)\in K[x]$ such that $g(0)\neq 0$,*
   (a) $n\geq 2$, $p\nmid n$ and $\mathrm{gcd}_p(g(x))=1$, and
   (b) $\mathcal{R}(f)+\mathbb{F}_p(\lambda-\lambda')\nsubseteq\mathcal{R}(f)$ for all distinct roots λ and λ' of the polynomial f.

Suppose that statement 1 holds. Then:

- *The presentation* $f(x) = (x-\nu)^i g((x-\nu)^n)$ *is unique, i.e. the triple* $(\nu, i, g(x))$ *is unique.*
- *Either* ν *is a root of* $f(x)$ *(i.e.* $i \geq 1$*) or otherwise (i.e.* $i = 0$*)* ν *is a root of* $f_1'(x)$ *(the derivative of* $f_1(x)$*).*
- *If* ν *is a root of* $f(x)$ *then* $n = \gcd_p(x^{-i} f(x+\nu))$.
- *If* ν *is not a root of* $f(x)$ *then* $n = \gcd_p(f(x+\nu))$.
- $\sigma_{\lambda_n,(1-\lambda_n)\nu}(f) = \lambda_n^i f$*, and* $f \in K[x]^{G_f}$ *iff* $n|i$.

Proof By Proposition 4.15.(3), $\widetilde{G}_f = \{e\}$ iff the condition (b) holds.

$(1 \Rightarrow 2)$ Suppose that statement 1 holds. Then, by Theorem 4.9.(2,3),

$$f(x) = (x-\nu)^i g((x-\nu)^n)$$

for some natural number $i \geq 0$ and a monic *non-scalar* polynomial $g(x) \in K[x]$ such that $g(0) \neq 0$ (since $|\mathcal{R}_d(f)| \geq 2$). Clearly, $n \geq 2$ and $p \nmid n$.

Suppose that $l := \gcd_p(g(x)) > 1$. Then $\sigma_{\lambda_{ln},(1-\lambda_{ln})\nu} \in \overline{G}_f = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ where λ_{ln} is a primitive ln'th root of unity, a contradiction (since the order of the element $\sigma_{\lambda_{ln},(1-\lambda_{ln})\nu}$ is $ln > n = |\overline{G}_f|$). Therefore, the statement (a) holds.

$(2 \Rightarrow 1)$ By the statement (b), $\widetilde{G}_f = \{e\}$. Since $f(x) = (x-\nu)^i g((x-\nu)^n)$ for some natural number $i \geq 0$, $n \geq 2$, $p \nmid n$ and a monic non-scalar polynomial $g(x) \in K[x]$ such that $g(0) \neq 0$,

$$\overline{G}_f \supseteq \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle \neq \{e\}.$$

The condition (a) implies that the inclusion above is the equality, see the proof of the implication $(1 \Rightarrow 2)$.

Suppose that statement 1 holds. Then statement 2 holds and vice versa. So, we have the equality $f(x) = (x-\nu)^i g((x-\nu)^n)$ as in statement 2. To prove uniqueness of this presentation it suffices to show that the element ν is unique. The set of cyclic generators for the group $G_f = \overline{G}_f = \langle \sigma_{\lambda_n,(1-\lambda_n)\nu} \rangle$ is equal to $\{\sigma^j_{\lambda_n,(1-\lambda_n)\nu} \mid 1 \leq j \leq n-1, \gcd(j,n) = 1\}$. Since $\sigma^j_{\lambda_n,(1-\lambda_n)\nu} = \sigma_{\lambda_n^j,(1-\lambda_n^j)\nu}$, the element ν is unique.

Clearly, ν is a root of $f(x)$ iff $i \geq 1$. Suppose that ν is not a root of $f(x)$, i.e. $i = 0$ and $f(x) = g((x-\nu)^n)$, then $f_1(x) = h((x-\nu)^n)$ for a unique monic non-scalar polynomial $h(x) := g^{\frac{1}{p^s}}(x) \in K[x]$ (since $p \nmid n$). Hence, ν is a root of the polynomial $f_1(x)$ since

$$0 \neq f_1'(x) = n(x-\nu)^{n-1} h'((x-\nu)^n)$$

and $n \geq 2$.

If ν is a root of $f(x)$ then $n = \gcd_p(x^{-i} f(x+\nu))$ (since $f(x+\nu) = x^i g(x^n)$). If ν is not a root of $f(x)$ then $n = \gcd_p(f(x+\nu))$ (since $f(x+\nu) = g(x^n)$).

Clearly, $\sigma_{\lambda_n,(1-\lambda_n)\nu}(f) = \lambda_n^i f$, and so $f \in K[x]^{G_f}$ iff $n|i$. □

Definition 4.28 The unique presentation of the polynomial $f(x)$,

$$f(x) = (x-\nu)^i g((x-\nu)^n),$$

in Theorem 4.27.(2) is called the *eigenform* or the *eigenpresentation* of the polynomial $f(x)$. The scalar ν and the natural number $i \geq 0$ are called the *eigenroot* of $f(x)$ and its *multiplicity*, respectively. The natural number $n \geq 2$ and the monic polynomial $g(x)$ are called the *eigenorder* and the *eigenfactor* of $f(x)$. In general, the eigenroot may not be a root of the polynomial $f(x)$. It is iff $i \neq 1$.

Criterion for $\widetilde{G}_f \neq \{e\}$ **and** $\overline{G}_f = \{e\}$**.**

Lemma 4.29 *Let $g(x) \in K[x]$ be a monic non-scalar polynomial such that $g' \neq 0$ (the derivative of g), and V be an $\mathbb{F}_p$-subspace of K and $\mathbb{F}_{p^e}$ be its multiplier field (for $V = 0$, $f_V(x) = x$). Then:*

1. *$g(f_V(x))' \neq 0$.*
2. *For each $\nu \in K$, $g(f_V(x)) = f_V^{i(\nu)}(x-\nu)g_\nu(f_V(x-\nu))$ for a unique natural number $i(\nu) \geq 0$ and a unique monic polynomial $g_\nu(x) \in K[x]$ such that $g_\nu(0) \neq 0$; $i(\nu) \neq 0$ iff ν is a root of the polynomial $g(f_V(x))$. If $n = \gcd(p^e - 1, \gcd_p(g_\nu(x))) \geq 2$ then $e \neq \sigma_{\lambda_n,(1-\lambda_n)\nu} \in \overline{G}_{g(f_V(x))}(\overline{K})$ where $\lambda_n \in \overline{K}$ is a primitive n'th root of unity. If, in addition, $\lambda_n \in K$ then $e \neq \sigma_{\lambda_n,(1-\lambda_n)\nu} \in \overline{G}_{g(f_V(x))}(K)$.*
3. *Suppose that ν is not a root of the polynomial $g(f_V(x))$, i.e. $i(\nu) = 0$ and $g(f_V(x)) = g_\nu(f_V(x-\nu))$, and $\gcd_p(g_\nu(x)) \neq 1$ then ν is a root of the derivative $g(f_V(x))'$ of the polynomial $g(f_V(x))$.*

Proof 1. $g(f_V(x))' = g'(f_V(x))f_V'(x) \neq 0$, by Proposition 4.7.(2d).

2. $g(f_V(x)) = g(f_V(x-\nu+\nu)) = g(f_V(x-\nu)+f_V(\nu)) = f_V^{i(\nu)}(x-\nu)g_\nu(f_V(x-\nu))$ for a unique natural number $i(\nu) \geq 0$ and a unique monic polynomial $g_\nu(x) \in K[x]$ such that $g_\nu(0) \neq 0$. Since $f_V(0) = 0$ and $g_\nu(0) \neq 0$, we see that $i(\nu) \neq 0$ iff ν is a root of the polynomial $g(f_V(x))$.

If $n \geq 2$ then $e \neq \sigma_{\lambda_n,(1-\lambda_n)\nu} \in \overline{G}_{g(f_V(x))}(\overline{K})$, by Theorem 4.8.(1). If, in addition, $\lambda_n \in K$ then $e \neq \sigma_{\lambda_n,(1-\lambda_n)\nu} \in \overline{G}_{g(f_V(x))}(K)$.

3. Suppose that ν is not a root of the polynomial $g(f_V(x))$ and $m = \gcd_p(g_\nu(x)) \neq 1$, i.e. $g(f_V(x)) = g_\nu(f_V(x-\nu)) = h_\nu(f_V^m(x-\nu))$ for some monic non-scalar polynomial $h_\nu(x) \in K[x]$. Then

$$g(f_V(x))' = h_\nu(f_V^m(x-\nu))' = mf_V^{m-1}(x-\nu)f_V'(x-\nu)h_\nu'(f_V^m(x-\nu)),$$

and so ν is a root of the polynomial $g(f_V(x))'$. □

Given monic non-scalar polynomials $f(x), h(x) \in K[x]$. *If $f(x) = g(h(x))$ for some polynomial $g(x) \in K[x]$ then the polynomial $g(x)$ is unique and necessarily monic.* (Proof. If $f(x) = g(h(x))$ then the polynomial $g(x)$ is monic, $\deg(f) = \deg(g)\deg(h)$, $K[h] \ni f_1 := f - h^{\deg(g)}$ and $\deg(f_1) < \deg(f)$. Now, the induction on $\deg(f)$ completes the proof).

Theorem 4.30 is a criterion for the group $G_f = \widetilde{G}_f \rtimes \overline{G}_f$ to be equal to $\widetilde{G}_f \neq \{e\}$.

Theorem 4.30 *Suppose that the field K is an algebraically closed field, $f(x) \in K[x]$ is a monic non-scalar polynomial that has at least two distinct roots, $gcd(f) = p^s \gcd_p(f)$ and $f(x) = f_1^{p^s}(x)$ for a unique monic non-scalar polynomial $f_1(x) \in K[x]$. Suppose that $V \neq 0$ is a finite dimensional $\mathbb{F}_p$-subspace of K and $\mathbb{F}_{p^e}$ is the multiplier field of V. Then the following statements are equivalent:*

1. *$\widetilde{G}_f = \mathrm{Sh}_V \neq \{e\}$ and $\overline{G}_f = \{e\}$.*
2. *$f_1(x) = g(f_V(x))$ for a (unique) monic polynomial $g(x) \in K[x]$ such that*
   - *(a) either $|\mathcal{R}_d(g)| = 1$ and $(p, e) = (2, 1)$ or otherwise $|\mathcal{R}_d(g)| \geq 2$ and $\gcd(p^e - 1, \gcd_p(g_\nu(x))) = 1$ for all roots $\nu \in \mathcal{R}_d(f_1(x)) \cup \mathcal{R}_d(f_1(x)')$ where g_ν is as in Lemma 4.29.(2) (i.e. $f_1(x) = f_V^{i(\nu)}(x-\nu)g_\nu(f_V(x-\nu))$), and*
   - *(b) $\mathcal{R}(f_1) + \mathbb{F}_p(\lambda - \lambda') \nsubseteq \mathcal{R}(f_1)$ for all distinct roots λ and λ' of the polynomial f_1 such that $\lambda - \lambda' \notin V$ ($\Leftrightarrow \mathcal{R}(f) + \mathbb{F}_p(\lambda - \lambda') \nsubseteq \mathcal{R}(f)$ for all distinct roots λ and λ' of the polynomial f such that $\lambda - \lambda' \notin V$).*

Suppose that statement 1 holds. Then $f, f_1 \in K[x]^{G_f} = K[x]^{G_{f_1}}$.

Remark By Lemma 4.23, $G_f = G_{f_1^{p^s}} = G_{f_1}$. This explains why statement 2 is given via properties of the polynomial f_1 rather than f.

Proof By Proposition 4.7 and Proposition 4.15.(1), $\widetilde{G}_f = \widetilde{G}_{f_1} = \mathrm{Sh}_V(\neq \{e\})$ iff $f_1(x) = g(f_V(x))$ for a (unique) monic non-scalar polynomial $g(x) \in K[x]$ such that the condition 2(b) holds.

Suppose that $|\mathcal{R}_d(g)| = 1$, i.e. $\mathcal{R}_d(g) = \{\rho\}$ and let $i(\rho)$ be the multiplicity of the root ρ. Fix an element $\nu' \in K = \overline{K}$ such that $f_V(\nu') = \rho$. Then $f_1(x) = (f_V(x) - f_V(\nu'))^{i(\rho)} = f_V^{i(\rho)}(x - \nu')$, by Proposition 4.7.(2b). By Proposition 4.22, $G_{f_1} = \widetilde{G}_{f_1} = \mathrm{Sh}_V$ iff $(p, e) = (2, 1)$.

Suppose that $|\mathcal{R}_d(g)| \geq 2$. By Lemma 4.29.(2),

$$f_1(x) = g(f_V(x)) = f_V^{i(\nu)}(x - \nu) g_\nu(f_V(x - \nu))$$

for a unique monic *non-scalar* polynomial $g_\nu(x) \in K[x]$ such that $g_\nu(0) \neq 0$ where $i(\nu) \geq 0$ is the multiplicity of the root ν (if $g_\nu(x) = 1$ then $f_1(x) = g(f_V(x)) = f_V^{i(\nu)}(x - \nu) = (f_V(x) - f_V(\nu))^{i(\nu)}$, and so $|\mathcal{R}_d(g)| = 1$, a contradiction).

By Theorem 4.8 and Lemma 4.29.(2), $\overline{G}_{f_1} = \{e\}$ iff $\gcd(p^e - 1, \gcd_p(g_\nu(x))) = 1$ for all $\nu \in K$ iff $\gcd(p^e - 1, \gcd_p(g_\nu(x))) = 1$ for all $\nu \in \mathcal{R}_d(f_1(x)) \cup \mathcal{R}_d(f_1(x)')$, Lemma 4.29.(2,3).

Clearly, $f, f_1 \in K[x]^{G_f} = K[x]^{G_{f_1}}$ (Proposition 4.7 and Lemma 4.23). □

Definition 4.31 The unique presentation $f(x) = g^{p^s}(f_V(x))$ in Theorem 4.30 (where $\gcd(f) = p^s \gcd_p(f)$) is called the *eigenform* or *eigenpresentation* of the polynomial $f(x)$ and the polynomial $g(x)$ is called the *eigenfactor* of $f(x)$.

Criterion for $G_f = \{e\}$**.** Given a monic non-scalar polynomial $g(x) \in K[x]$ with $g'(x) \neq 0$. By Lemma 4.29.(2) (where $V = 0$), for each $\nu \in K$,

$$g(x) = (x - \nu)^{i(\nu)} g_\nu(x - \nu) \tag{29}$$

for a natural number $i(\nu) \geq 0$ and a unique monic polynomial $g_\nu(x) \in K[x]$ such that $g_\nu(0) \neq 0$. Clearly, $i(\nu) \neq 0$ iff ν is a root of the polynomial $g(x)$.

Theorem 4.32 is a criterion for $G_f = \{e\}$.

Theorem 4.32 *Suppose that the field K is an algebraically closed field, $f(x) \in K[x]$ is a monic polynomial that has at least two distinct roots,* $\gcd(f) = p^s \gcd_p(f)$ *and* $f(x) = g^{p^s}(x)$ *for a unique monic non-scalar polynomial $g(x) \in K[x]$, see* Eq. 28. *The following statements are equivalent:*

1. $G_f = \{e\}$.
2. (a) *For each root ν of the polynomial $g(x)$,* $\gcd_p(g_\nu(x)) = 1$ *where the polynomial $g_\nu(x)$ is defined in* Eq. 29,
   (b) *for each root ν' of the derivative $g'(x)$ of the polynomial $g(x)$ such that $g(\nu') \neq 0$,* $\gcd_p(g_\nu(x)) = 1$, *and*
   (c) $\mathcal{R}(g) + \mathbb{F}_p(\lambda - \lambda') \nsubseteq \mathcal{R}(g)$ *for all distinct roots λ and λ' of the polynomial g ($\Leftrightarrow$ $\mathcal{R}(f) + \mathbb{F}_p(\lambda - \lambda') \nsubseteq \mathcal{R}(f)$ for all distinct roots λ and λ' of the polynomial f).*

Proof Notice that $G_f = G_{g^{p^s}} = G_g$. The condition (c) is equivalent to the condition that $\widetilde{G}_g = \{e\}$ (Proposition 4.15.(3)). It remains to show that provided $\widetilde{G}_g = \{e\}$ the condition

$\overline{G}_g = \{e\}$ is equivalent to the conditions (a) and (b). Equivalently, $\widetilde{G}_g = \{e\}$ and $\overline{G}_g \neq \{e\}$ iff one of the conditions (a) or (b) does not hold and the condition (c) holds. This follows from Theorem 4.27. Indeed, by Theorem 4.27, $\widetilde{G}_g = \{e\}$ and $\overline{G}_g \neq \{e\}$ iff the condition (c) holds and $g(x) = (x-\nu)^i g_\nu(x-\nu)$ for a unique $\nu \in K$, a natural number $i \geq 0$ and a monic non-scalar polynomial $g_\nu(x)$ such that $g_\nu(0) \neq 0$ (since $|\mathcal{R}_d(f)| \geq 2$) and $\gcd_p(g_\nu(x)) \geq 2$. We have two options either ν is a root of the polynomial $g(x)$ or not. If ν is not a root of the polynomial $g(x)$, i.e. $i = 0$, then $g(x) = g_\nu(x-\nu)$, and so ν is a root of $g'(x)$ since $\gcd_p(g_\nu(x)) \geq 2$. Now, it follows that statements 1 and 2 are equivalent. □

Theorem 4.33 describes the group $G_f(K)$ in terms of the group $G_f(\overline{K})$.

Theorem 4.33 *Suppose that the field K is not necessarily algebraically closed and $f(x) \in K[x]$ is a monic polynomial that has at least two distinct roots in $\overline{K}$. Recall that (*Theorems 4.12 and 4.4*) the group $G_f(\overline{K}) = \widetilde{G}_f(\overline{K}) \rtimes \overline{G}_f(\overline{K})$ where $\overline{G}_f(\overline{K}) := \langle \sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ and $\widetilde{G}_f(\overline{K}) := \{\sigma_{1,\mu} \mid \mu \in \overline{V}\}$, $\lambda_n \in \overline{K}$ is a primitive n'th root of unity provided $\overline{G}_f(\overline{K}) \neq \{e\}$, $\nu \in \overline{K}$, $\overline{V}$ is a finite dimensional $\mathbb{F}_p(\lambda_n)$-subspace of $\overline{K}$, and $\mathbb{F}_p(\lambda_n) = \mathbb{F}_{p^m}$ for some $m \geq 1$* (Lemma 4.3)*. Then*

$$G_f(K) = \widetilde{G}_f(K) \rtimes \overline{G}_f(K) = \mathrm{Aut}_K(K[x]) \cap G_f(\overline{K}), \quad \widetilde{G}_f(K) = \mathrm{Sh}_V$$

where $V := K \cap \overline{V}$ and if $\overline{G}_f(K) \neq \{e\}$ then $\overline{G}_f(K) = \langle \sigma_{\lambda_n^i,(1-\lambda_n^i)\nu+\overline{v}}\rangle$ where $i = \min\{i' = 1, \ldots, n-1 \mid i'|n, \lambda_n^{i'} \in K, (1-\lambda_n^{i'})\nu \in \overline{V} + K\}$ and $\overline{v} \in \overline{V}$ is any (fixed) element such that $(1-\lambda_n^i)\nu + \overline{v} \in K$.

Proof It is obvious that $G_f(K) = \mathrm{Aut}_K(K[x]) \cap G_f(\overline{K})$. By Theorem 4.4, $G_f(K) = \widetilde{G}_f(K) \rtimes \overline{G}_f(K)$. It is obvious that $\widetilde{G}_f(K) = \mathrm{Sh}_V$ where $V := K \cap \overline{V}$. By Theorem 4.4, $\overline{G}_f(K) = \langle \sigma_{\lambda_{n'},(1-\lambda_{n'})\nu'}\rangle$ where $\lambda_{n'} \in K$ is a primitive n''th root of unity and $\nu' \in K$ provided $\overline{G}_f(K) \neq \{e\}$. Notice that

$$\sigma_{\lambda_{n'},(1-\lambda_{n'})\nu'} = \sigma^i_{\lambda_n,(1-\lambda_n)\nu}\sigma_{1,\overline{v}} = \sigma_{\lambda_n^i,(1-\lambda_n^i)\nu}\sigma_{1,\overline{v}} = \sigma_{\lambda_n^i,(1-\lambda_n^i)\nu+\overline{v}}$$

for unique elements i and $\overline{v} \in \overline{V}$ such that $0 \leq i \leq n-1$. So, the elements i can be chosen such that

$$\begin{aligned} i &= \min\{i' = 1, \ldots, n-1 \mid i'|n,\ \lambda_n^{i'} \in K,\ (1-\lambda_n^{i'})\nu + \overline{v} \in K \ \text{ for some element } \ \overline{v} \in \overline{V}\} \\ &= \min\{i' = 1, \ldots, n-1 \mid i'|n,\ \lambda_n^{i'} \in K,\ (1-\lambda_n^{i'})\nu \in \overline{V} + K\} \end{aligned}$$

and $\overline{v} \in \overline{V}$ is any (fixed) element such that $(1-\lambda_n^i)\nu + \overline{v} \in K$. □

Proposition 4.34 gives criteria for the groups $\widetilde{G}_f(K)$, $\overline{G}_f(K)$ and $G_f(K)$ to be $\{e\}$.

Proposition 4.34 *Suppose that the field K is not necessarily algebraically closed and $f(x) \in K[x]$ is a monic polynomial that has at least two distinct roots in $\overline{K}$. Recall that* (Theorems 4.12 and 4.4) *the group $G_f(\overline{K}) = \widetilde{G}_f(\overline{K}) \rtimes \overline{G}_f(\overline{K})$ where $\overline{G}_f(\overline{K}) := \langle \sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ and $\widetilde{G}_f(\overline{K}) := \{\sigma_{1,\mu} \mid \mu \in \overline{V}\}$, $\lambda_n \in \overline{K}$ is a primitive n'th root of unity provided $\overline{G}_f(\overline{K}) \neq \{e\}$, $\nu \in \overline{K}$, $\overline{V}$ is a finite dimensional $\mathbb{F}_p(\lambda_n)$-subspace of $\overline{K}$, and $\mathbb{F}_p(\lambda_n) = \mathbb{F}_{p^m}$ for some $m \geq 1$* (Lemma 4.3)*. Then:*

1. *$\widetilde{G}_f(K) = \{e\}$ iff $\overline{V} \cap K = 0$.*
2. *$\overline{G}_f(K) = \{e\}$ iff $\overline{G}_f(\overline{K}) = \{e\}$ or otherwise $\overline{G}_f(\overline{K}) := \langle \sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ and there is no a natural number i' such that $1 \leq i' \leq n-1$ such that $i'|n$, $\lambda_n^{i'} \in K$ and $(1-\lambda_n^{i'})\nu \in \overline{V} + K$.*

3. *$G_f(K)=\{e\}$ iff $G_f(\overline{K})=\{e\}$ or otherwise $\overline{V}\cap K=0$, $\overline{G}_f(\overline{K}):=\langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ and there is no a natural number i' such that $1\leq i'\leq n-1$, $i'|n$, $\lambda_n^{i'}\in K$ and $(1-\lambda_n^{i'})\nu\in\overline{V}+K$.*

Proof Statements 1 and 2 follow at once from Theorem 4.33. Then statement 3 follows from statements 1 and 2. □

Every subgroup of $\mathrm{Aut}_K(K[x])$ **is of type** G_f**.** Theorem 4.35 shows that all subgroups of $\mathrm{Aut}_K(K[x])$ are eigengroups of polynomials.

Theorem 4.35 *Let K be an arbitrary field of characteristic $p>0$. Then for each subgroup H of $\mathrm{Aut}_K(K[x])$ there is a monic polynomial f_H such that $G_{f_H}=H$:*

1. *For $H=\{e\}$, $f_H=x(x+1)^2$.*
2. *For $H=\langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ where $\lambda_n\in K$ is a primitive n'th root of unity and $\nu\in K$, $f_H=(x-\nu)^n-1$.*
3. *For $H=\mathrm{Sh}_V$ where V is a nonzero $\mathbb{F}_p$-subspace of K,*
   - *(a) if $K=\mathbb{F}_{p^n}$ then $f_H(x)=f_V(x-\nu)-\rho$ where ρ is any element of $\mathbb{F}_{p^n}$ that does not belong to the image of the map $f_V(x-\nu):\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$, $x\mapsto f_V(x-\nu)$ (the map $f_V(x-\nu)$ is not a surjection since the set $\nu+V$ is mapped to 0).*
   - *(b) If $|K|=\infty$ then $f_H(x)=f_V(x)f_V^2(x-\nu)$ where $\nu\in K\backslash V$.*
4. *For $H=\mathrm{Sh}_V\rtimes\langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ where V is a nonzero $\mathbb{F}_p$-subspace of K, $\mathbb{F}_{p^e}$ is its multiplier field, and λ_n is primitive n'th root of unity such that $\lambda_nV\subseteq V$, $f_H(x)=\begin{cases}f_V(x-\nu) & \text{if } n=p^e-1,\\ f_V^n(x-\nu)+1 & \text{if } n<p^e-1.\end{cases}$*
5. *For $H=\mathbb{T}_\nu(K)=\{\sigma_{\lambda,(1-\lambda)\nu}\,|\,\lambda\in K^\times\}$, $f_H=x-\nu$.*
6. *For $H=\mathrm{Aut}_K(K[x])$, $f_H=\begin{cases}1 & \text{if } |K|=\infty,\\ x^{p^n}-x & \text{if } K=\mathbb{F}_{p^n}.\end{cases}$*

Proof 1. If $\sigma\in G_{f_H}$ then the maximal ideals (x) and $(x+1)$ of $K[x]$ are σ-stable, hence $\sigma=e$.

2. Clearly, $G_{f_H}\supseteq H$.

(i) $\widetilde{G}_{f_H}=\{e\}$: The polynomial f_H has n distinct roots, namely, $\{\nu+\lambda_n^i\,|\,i=0,1,\dots,n-1\}$, and $p\nmid n$. Suppose that $\widetilde{G}_{f_H}=\mathrm{Sh}_V\neq\{e\}$ for some nonzero $\mathbb{F}_p$-subspace V of K. Then $p||V|$. Since $V+\mathcal{R}(f)\subseteq\mathcal{R}(f)$, we must have $|V|||\mathcal{R}(f)|$, i.e. $|V||n$, and so $p|n$, a contradiction.

(ii) $G_{f_H}=H$: Let $\sigma=\sigma_{\lambda_n,(1-\lambda_n)\nu}$. By the statement (i), $G_{f_H}=\overline{G}_{f_H}=\langle\sigma'\rangle$ where $\sigma=\sigma_{\lambda_m,(1-\lambda_m)\nu'}$ for some primitive m'th root of unity λ_m and $\nu'\in K$. Since $H\subseteq\overline{G}_{f_H}$, we must have $\nu'=\nu$ and $n|m$ (since $(x-\nu')$ is the only $\langle\sigma'\rangle$-invariant maximal ideal of $K[x]$, $(x-\nu)$ is the only $\langle\sigma\rangle$-invariant maximal ideal of $K[x]$ and $\langle\sigma\rangle\subseteq\langle\sigma'\rangle$).

The polynomial f_H is an eigenvector for the automorphism σ' with (necessarily) eigenvalue λ_m^n since $n=\deg(f_H)$. Now,

$$\lambda_m^nf_H=\lambda_m^n((x-\nu)^n-1)=\sigma'(f_H)=\lambda_m^n(x-\nu)^n-1.$$

Therefore, $\lambda_m^n=1$, and so $\langle\sigma\rangle=\langle\sigma'\rangle$. This means that $\overline{G}_{f_H}=H$, and the statement (ii) follows from the statement (i).

3(a). Clearly, $G_{f_H}\supseteq H=\mathrm{Sh}_V$.

(i) $\widetilde{G}_{f_H} = H$: The statement follows at once from the fact that the polynomial f_H has $|V|$ distinct roots in $\overline{K}$ (if $\widetilde{G}_{f_H} = \text{Sh}_{V'}$ for some $\mathbb{F}_p$-subspace V' of K that properly contains V then the polynomial f_H contains at least $|V'|$ distinct roots in $\overline{K}$, a contradiction).

(ii) $\overline{G}_{f_H} = \{e\}$: Suppose that $\overline{G}_{f_H} \neq \{e\}$. Then $\overline{G}_{f_H} = \langle\sigma\rangle$ where $\sigma = \sigma_{\lambda_n,(1-\lambda_n)\nu'}$, $1 \neq \lambda_n \in K$ is a primitive n'th root of unity such that $\lambda_n V \subseteq V$ and $\nu' \in K$. Notice that $\sigma(f_H) = \lambda_n^{|V|} f_H$ and

$$f_H(x) = f_V(x-\nu'-(\nu-\nu'))-\rho = f_V(x-\nu')-f_V(\nu-\nu')-\rho = f_V(x-\nu')+f_V(\nu'-\nu)-\rho.$$

By Theorem 4.8.(1), $\sigma(f_V(x-\nu')) = \lambda_n f_V(x-\nu')$. Let $a = f_V(\nu'-\nu)-\rho$. Now,

$$\lambda_n^{|V|}(f_V(x-\nu')+a) = \lambda_n^{|V|} f_H = \sigma(f_H) = \sigma(f_V(x-\nu')+a) = \lambda_n f_V(x-\nu')+a.$$

Hence, $\lambda_n^{|V|} = \lambda_n \neq 1$ and $(\lambda_n - 1)a = 0$, i.e. $a = 0$. The last equality implies that $\rho \in \text{im}\, f_V(x-\nu)$, a contradiction, and the statement (ii) follows.

(b). Clearly, $G_{f_H} \supseteq H = \text{Sh}_V$.

(i) $\widetilde{G}_{f_H} = H$: The statement follows at once from the fact that $\mathcal{R}(f) = V \coprod (\nu+V)^2$ where the upper index '2' means that the multiplicity of each root in $\nu + V$ is 2.

(ii) $\overline{G}_{f_H} = \{e\}$: Suppose that $e \neq \sigma \in \overline{G}_{f_H}$. Then $\sigma \in \overline{G}_{f_V(x)} \cap \overline{G}_{f_V(x-\nu)}$. Notice that $\overline{G}_{f_V(x-\nu)} = \langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ for some primitive n'th root of unity λ_n such that $\mathbb{F}_p(\lambda_n)V \subseteq V$. Then there is a natural number i such that $\sigma = \sigma^i_{\lambda_n,(1-\lambda_n)\nu} = \sigma_{\lambda_n^i,(1-\lambda_n^i)\nu} \in \overline{G}_{f_V(x)}$. In particular, $V \ni \sigma^{-1} * (0) = (1-\lambda_n^i)\nu$, and so $\nu \in (1-\lambda_n^i)^{-1}V = V$, a contradiction ($1-\lambda_n^i \neq 0$ since $\sigma \neq e$).

4. Statement 4 follows from Theorem 4.24.

5 and 6. Statements 5 and 6 are obvious. □

Algorithm of finding the eigengroup $G_f(\overline{K})$ and the eigenform of f. The algorithm consists of finitely many steps and is based on Prpoposition 4.10, Theorems 4.24, 4.27, 4.30 and 4.32. We assume that $K = \overline{K}$.

Step 1. If $|\mathcal{R}_d(f)| = 1$ then apply Proposition 4.10 to find G_f.

From this moment on we assume that $|\mathcal{R}_d(f)| \geq 2$.

Step 2. Use Theorem 4.32 to check whether $G_f = \{e\}$ or $G_f \neq \{e\}$.

From this moment on we assume that $G_f \neq \{e\}$.

Step 3. By Proposition 4.15.(1), the group $\widetilde{G}_f = \text{Sh}_V$ can be found.

Step 4. Suppose that $\widetilde{G}_f = \{e\}$. Then necessarily $\overline{G}_f \neq \{e\}$, and using Theorem 4.27 the group $\overline{G}_f$ is found. In more detail, we know that $\overline{G}_f = \langle\sigma_{\lambda_n,(1-\lambda_n)\nu}\rangle$ and that $f(x) = (x-\nu)^i g((x-\nu)^n)$ for a unique $\nu \in \mathcal{R}_d(f) \cup \mathcal{R}_d(f_1')$ and $n \geq 2$ such that if ν is a root of $f(x)$ then $n = \text{gcd}_p(x^{-i} f(x+\nu))$, and if ν is not a root of $f(x)$ then $n = \text{gcd}_p(f(x+\nu))$.

From this moment on we assume that $\widetilde{G}_f = \text{Sh}_V \neq \{e\}$, the $\mathbb{F}_p$-subspace V of the field K is non-zero. Let $\mathbb{F}_{p^e}$ be the multiplier field of V. It can be easily found since the multiplier field $\mathbb{F}_{p^e}$ is the largest among finite fields $\mathbb{F}_{p^m}$ such that $\mathbb{F}_{p^m} V \subseteq V$ and $m \leq \dim_{\mathbb{F}_p}(V)$.

Step 5. Now, we check whether the conditions of Theorem 4.30 hold or not. If they do then $\overline{G}_f = \{e\}$.

If they do not then necessarily $\overline{G}_f \neq \{e\}$ and hence the conditions of Theorem 4.24 hold. Using Theorem 4.24 the group $\overline{G}_f$ and the eigenform of f are found in finitely many steps. □

Algorithm of finding the eigengroup $G_f(K)$ where $K \neq \overline{K}$.

Step 1. Using the algorithm above the group $G_f(\overline{K})$ is found.

Step 2. The group $G_f(K)$ is found by using Theorem 4.33. □

Acknowledgements The author would like to thank the anonymous Referee for valuable comments.

Author Contributions I did all the work.

Funding None.

Availability of data and materials Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

Ethical Approval Non-applicable.

References

1. Alev, J., Dumas, F.: Invariants du corps de Weyl sous l'action de groupes finis. Comm. Algebra **25**, 1655–1672 (1997)
2. Bavula, V.V.: The simple modules of the Ore extensions with coefficients from a Dedekind ring. Comm. Algebra **27**(6), 2665–2699 (1999)
3. Bavula, V.V., Jordan, D.A.: Isomorphism problems and groups of automorphisms for generalized Weyl algebras. Trans. Amer. Math. Soc. **353**(2), 769–794 (2001)
4. Bavula, V.V.: The group of automorphisms of the first Weyl algebra in prime characteristic and the restriction map. Glasgow Math. J. **51**, 263–274 (2009)
5. Bavula, V.V.: Isomorphism problems and groups of automorphisms for Ore extensions $K[x][y;\delta]$. Proc. Amer. Math. Soc. **151**(6), 2417–2428 (2023). arXiv:2107.09401
6. Benkart, G., Lopes, S.A., Ondrus, M.: A parametric family of subalgebras of the Weyl algebra I Structure and automorphisms. Trans. Amer. Math. Soc. **3673**, 1993–2021 (2015)
7. Benkart, G., Lopes, S. A., Ondrus, M. : A parametric family of subalgebras of the Weyl algebra II. Irreducible modules. Recent developments in algebraic and combinatorial aspects of representation theory. Contemp. Math. **602**, 73–98, 2013. Amer. Math. Soc., Providence, RI,
8. Gaddis, J.: Two-generated algebras and standard-form congruence. Comm. Algebra **43**(4), 1668–1686 (2015)
9. Cibils, C., Lauve, A., Witherspoon, S.: Hopf quivers and Nichols algebras in positive characteristic. Proc. Amer. Math. Soc. **137**(12), 4029–4041 (2009)
10. Dixmier, J.: Sur les algèbres de Weyl. Bull. Soc. Math. France **96**, 209–242 (1968)
11. Iyudu, N.K.: Representation spaces of the Jordan plane. Comm. Algebra **42**(8), 3507–3540 (2014)
12. J. C. McConnell and J. C. Robson, *Noncommutative Noetherian rings*. With the cooperation of L. W. Small. Revised edition. Graduate Studies in Mathematics, 30. American Mathematical Society, Providence, RI, 2001
13. Makar-Limanov, L.: On automorphisms of Weyl algebra. Bull. Soc. Math. France **112**(3), 359–363 (1984)
14. Shirikov, E.N.: Two-generated graded algebras. Algebra. Discrete Math. **3**, 60–84 (2005)
15. Smith, M.K.: Automorphisms of enveloping algebras. Comm. Algebra **16**, 1769–1802 (1983)

16. van der Kulk, W.: On polynomial rings in two variables. Nieuw Arch. Wiskunde **1**, 33–41 (1953)