TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 345, Number 2, October 1994

HILBERT 90 THEOREMS OVER DIVISION RINGS

T. Y. LAM AND A. LEROY

ABSTRACT. Hilbert's Satz 90 is well-known for cyclic extensions of fields, but attempts at generalizations to the case of division rings have only been partly successful. Jacobson's criterion for logarithmic derivatives for fields equipped with derivations is formally an analogue of Satz 90, but the exact relationship between the two was apparently not known. In this paper, we study triples (K, S, D) where S is an endomorphism of the division ring K, and D is an S-derivation. Using the technique of Ore extensions $K[t, S, D]$, we characterize the notion of (S, D)-algebraicity for elements $a \in K$, and give an effective criterion for two elements $a, b \in K$ to be (S, D)-conjugate, in the case when the (S, D)-conjugacy class of a is algebraic. This criterion amounts to a general Hilbert 90 Theorem for division rings in the (K, S, D)-setting, subsuming and extending all known forms of Hilbert 90 in the literature, including the aforementioned Jacobson Criterion. Two of the working tools used in the paper, the Conjugation Theorem (2.2) and the Composite Function Theorem (2.3), are of independent interest in the theory of Ore extensions.

1. INTRODUCTION

Few theorems in mathematics are universally known by a number: Hilbert's celebrated Theorem 90 enjoys this almost unique distinction. "90", however, is a pure numerological accident, for Hilbert's theorem on cyclic extensions got its name for no better reason than that it appeared between Satz 89 and Satz 91 in his *Zahlbericht* [H], a report on the state-of-the-art of algebraic number theory to the Deutsche Mathematikervereinigung, c. 1897. Anyway, the number "90" has since stuck with this little gem of a theorem, which has come to be viewed by many as exemplary of the quality of Hilbert's creative contributions in *Zahlbericht* (cf. [Re, p. 55]).

For a finite cyclic field extension K/F with Galois group $\langle S\rangle$, Hilbert's Satz 90 states the following:

(1.1) *An element $b \in K$ has norm 1 (with respect to the extension K/F) iff $b = S(c)c^{-1}$ for some $c \in K^*$.*

In view of the multiplicativity of the norm, one has also the following equivalent formulation:

(1.2) *Two elements $a, b \in K$ have the same norm iff $b = S(c)ac^{-1}$ for some $c \in K^*$.*

Received by the editors January 24, 1992 and, in revised form, September 11, 1992.
1991 *Mathematics Subject Classification*. Primary 16A05, 16A39; Secondary 16A72.
Both authors supported in part by NSF.

Here, of course, the norm of an element $b \in K$ is just $N_{K/F}(b) := S^{k-1}(b) \cdots S(b)b \in F$, where $k = |\langle S\rangle| = [K : F]$. One usually thinks of (1.1) as giving a characterization of the elements of norm 1 in the field K, but one may equally well think of it as giving a description of the elements in K expressible in the form $S(c)c^{-1}$ for some $c \in K^*$. Similarly, one may interpret (1.2) as giving an effective description, in terms of the norm, of the equivalence relation " $\sim$ " on K given by $a \sim b \Leftrightarrow b = S(c)ac^{-1}$ for some $c \in K^*$.

Some generalizations and analogues of the Hilbert 90 Theorem are known in the literature. One natural generalization is to try to replace fields by division rings. Consider a division ring K and an automorphism S of K such that $S^k = I$ and none of $S, S^2, \dots, S^{k-1}$ is an inner automorphism of K. Then, for $F = K^S$ (the division subring consisting of fixed points of S), K/F is an "outer cyclic extension" with Galois group $\langle S\rangle$. In this case, Jacobson has shown [J$_3$, Corollary, p. 47] that (1.1) still holds, if we understand by $N_{K/F}(b)$ the expression $S^{k-1}(b) \cdots S(b)b$. Since K need not be commutative, however, the norm function may fail to be multiplicative, so it is no longer possible to derive (1.2) (which we might call the "strong form" of Hilbert 90) from the "weak form" (1.1). The only "strong form" known in the literature seems to be Jacobson's Theorem 27 in [J$_3$]. But, in proving this "strong form", Jacobson had to assume that the norm of a is a central element in K fixed by S. Also, nothing seems to be known if the automorphism S has infinite (instead of finite) order.

Another interesting analogue of the Hilbert 90 Theorem in the setting of derivations on fields was obtained by Jacobson in [J$_1$]. Let D be a derivation on a field K of characteristic $p > 0$, and let K_D be the subfield of constants of D. It is well-known that $[K : K_D] < \infty$ iff D is an algebraic derivation, and if this is the case, then the minimal polynomial of D has the special form $g(t) = \sum_{i=0}^{m} d_t t^{p^i}$ where $d_m = 1$ and $d_i \in K_D$. In this setting, Jacobson has obtained an analogue of the Hilbert 90 Theorem by giving a characterization for the set of "logarithmic derivatives" $\{D(c)c^{-1} : c \in K^*\}$ in K, as follows [J$_1$, Theorem 15], [J$_2$, p. 191]):

(1.3) *An element* $b \in K$ *is a logarithmic derivative with respect to* D *iff* $\sum d_i b^{[p^i]} = 0$, *where*

$$b^{[p^i]} := b^{p^i} + (D^{p-1}(b))^{p^{i-1}} + (D^{p^2-1}(b))^{p^{i-2}} + \cdots + D^{p^i-1}(b).$$

For instance, in the simplest case when $g(t) = t^p$ (i.e. when D is a nilpotent derivation with index of nilpotency p), $b \in K$ is a logarithmic derivative iff $0 = b^{[p]} = b^p + D^{p-1}(b)$. Notice that, although the derivation setting here looks different from the cyclic extension setting of (1.1), there are some strong analogies. First, it is known that D is cyclic as a K_D-linear operator on K [J$_1$, §3]. Secondly, since $D(a^p) = pa^{p-1}D(a) = 0$ for every $a \in K$, we have $K^p \subseteq K_D$, so K/K_D is a purely inseparable field extension of exponent ≤ 1. In this case, there exists a good substitute for a Galois theory for K/K_D, in which the role of the Galois group in the classical theory is taken by the restricted Lie algebra of derivations on K which are constant on K_D (see [J$_1$], [J$_2$, Chapter 4, §8]). In view of these analogies, it seems reasonable to think of (1.3) as a result of the same genre as (1.1).

In this paper, we seek a uniform generalization of the Hilbert 90 Theorem to division rings which will, in particular, subsume and strengthen all the versions mentioned above. This generalization is inspired by Ore's formation [O] of the skew polynomial ring (or Ore extension) $K[t, S, D]$. Here, K is an arbitrary division ring, S is an endomorphism of K, and D is an S-derivation of K, that is, $D: K \to K$ is an additive map such that $D(ab) = S(a)D(b) + D(a)b$ for all $a, b \in K$. By definition, $K[t, S, D]$ consists of left polynomials $\sum b_i t^i$ ($b_i \in K$) which are added in the usual way and multiplied according to the rule $ta = S(a)t + D(a)$ for all $a \in K$. By working with the polynomials in the ring $R := K[t, S, D]$, we have an effective means of analyzing the triple (K, S, D). In particular, when $D = 0$, we will be dealing with the pair (K, S), and when $S = I$, we will be dealing with the pair (K, D).

Given the triple (K, S, D), there is a natural notion of (S, D)-conjugacy, defined as follows. For $a \in K$ and $c \in K^*$, we write $a^c := S(c)ac^{-1} + D(c)c^{-1}$, and we say that $b \in K$ is (S, D)-conjugate to a if $b = a^c$ for some $c \in K^*$. A direct calculation shows that $(a^c)^d = a^{dc}$, and this implies easily that *(S, D)-conjugacy is an equivalence relation on K*. More conceptually, one can check that b is (S, D)-conjugate to a iff the left R-modules $R/R(t-a)$ and $R/R(t-b)$ are isomorphic. Assuming this, of course, the fact that (S, D)-conjugacy is an equivalence relation becomes obvious. In this general context, a Hilbert 90 Theorem (in the "strong form") will be simply any effective criterion for the (S, D)-conjugacy of a pair of elements $a, b \in K$. In this paper, we shall formulate such a theorem, in the case when the (S, D)-conjugacy class $\Delta^{S,D}(a) := \{a^c : c \in K^*\}$ is algebraic, in a sense to be explained below.

In our earlier work [L₁], we have introduced the basic technique of "evaluating" a skew polynomial $f(t) = \sum b_i t^i \in R$ at the constants $a \in K$. Conceptually, $f(a)$ is the unique constant ("remainder") $r \in K$ such that $f(t) = q(t)(t-a) + r$ for some $q(t) \in K[t, S, D]$. Computationally, $f(a)$ is given by $\sum b_i N_i(a)$, where the "power functions" N_i are defined inductively as follows: $N_0(a) = 1$, $N_{i+1}(a) = S(N_i(a))a + D(N_i(a))$. With these definitions of $f(a)$, we can define the notion of *algebraic subsets* of K [L₂]: a set $\Delta \subseteq K$ is said to be (S, D)-algebraic if $f(\Delta) = 0$ for some nonzero $f \in K[t, S, D]$. In this case the monic f of the least degree with $f(\Delta) = 0$ is called the *minimal polynomial* of Δ, and $\deg f$ is called the *rank* of Δ. The most important case for studying the notion of algebraicity is the case when Δ is the (S, D)-conjugacy class $\Delta^{S,D}(a)$ of some element $a \in K$. In the classical case when $S = I$ and $D = 0$, $\Delta^{I,0}(a)$ is just the usual conjugacy class $\{cac^{-1} : c \in K^*\}$ of a, and, as is well-known (see e.g. [La, p. 207]), this is $(I, 0)$-algebraic in the above sense iff a is an algebraic element over $Z(K)$, the center of K. Therefore, the notion of algebraicity of $\Delta^{S,D}(a)$ is in direct generalization of the notion of algebraic elements over the center of a division ring.

Another tool needed from our recent work [L₄] is the notion of a "change-of-variable" polynomial (or a cv-polynomial for short). Let $R = K[t, S, D]$ and $R' = K[t', S', D']$ be two Ore extensions of K. By definition, $p(t) \in R$ is a cv-polynomial with respect to (S', D') if $p(t)a = S'(a)p(t) + D'(a)$ for every $a \in K$. Such a polynomial $p(t)$ determines a unique K-homomorphism $\phi: R' \to R$ by $\phi(t') = p(t)$. For $g(t') = \sum c_i t'^i \in R'$, the image $\phi(g) = \sum c_i p(t)^i \in R$ is the "composite function" $g(p(t))$, which will also be denoted by $(g \circ p)(t)$. Following [L₄], we shall say that $p(t) \in R$ is a cv-polynomial if it is a cv-polynomial with respect to some pair (S', D'). The basic theory of cv-polynomials and their applications to the study of homomorphisms between Ore extensions are given in [L4]. We shall not need the deeper results of [L4] here; however, the idea of using a change of variables to "transfer" information from one Ore extension to another turns out to be crucial for this work.

Let us now give a summary of the results in this paper. In §2, we prove two basic formulas for cv-polynomials, in the form of the "Conjugation Theorem" and the "Composite Function Theorem". The detailed statements are given in (2.2) and (2.3) below. These theorems are easy to prove once they are put in the right context, and they provide the computational basis for the rest of this work. In §3, we study the "λ-transform" associated to a polynomial $h(t) \in R$ and an element $a \in K$. This is a self-map $\lambda_{h,a}$ from K to K defined by: $\lambda_{h,a}(0) = 0$ and $\lambda_{h,a}(c) = h(a^c)c$ for $c \in K^*$. The significance of $\lambda_{h,a}$ lies in the fact that it amounts to the action of a certain "differential operator" on K. In §3, we study the "exponential space" $E(h, a) := \ker(\lambda_{h,a})$ and the "co-exponential space" $\overline{E}(h, a) := \operatorname{coker}(\lambda_{h,a})$, and the relationship between these. This gives information on the solutions of both polynomial equations and differential equations on K, continuing the earlier work of Amitsur [A1]. In general, $E(h, a)$ is a right vector space over the (S, D)-centralizer $C^{S,D}(a) := \{0\} \cup \{c \in K^* : a^c = a\}$, of dimension $\leq \deg h(t)$. One of the main results in §3 is (3.19) which characterizes the polynomials $h(t)$ for which the upper bound above becomes an actual equality. Aside from their applications to the rest of the paper, the results in §3 should be of interest in their own right in the study of polynomial and differential equations over division rings.

With the tools developed in §2–§3 at our disposal, we proceed in §4 to study the behavior of algebraic sets and conjugacy classes under a change of variables. This study results in certain general transfer principles relating (S, D)-algebraicity and conjugacy to (S', D')-algebraicity and conjugacy, as follows. Let $p(t)$ be a nonconstant cv-polynomial with respect to (S', D') and let $\phi: K[t', S', D'] \to K[t, S, D]$ be the K-homomorphism associated with $p(t)$ (defined by $\phi(t') = p(t)$). Then we have:

(1.4) *A subset $\Delta \subseteq K$ is (S, D)-algebraic iff $p(\Delta)$ is (S', D')-algebraic.*

(1.5) *Let $\Delta^{S,D}(a)$ be an algebraic class, and assume that its minimal polynomial lies in $\operatorname{im}(\phi)$. Then an element $b \in K$ is (S, D)-conjugate to a iff $p(b)$ is (S', D')-conjugate to $p(a)$.*

All of the above results come to a head in §5, where we try to find the general criterion for (S, D)-algebraicity and (S, D)-conjugacy. To accomplish this goal, we just need one more idea from the standard theory of division rings, namely, the criterion for usual conjugacy and the algebraicity of an ordinary conjugacy class, as given in the classical Wedderburn-Dickson Theorem. According to this theorem (see, e.g. [La, p. 207]), a class $\Delta(a) = \{cac^{-1} : c \in K^*\}$ is algebraic iff a is algebraic over $Z(K)$ (the center of K), and in this case, $b \in K$ is conjugate to a iff a, b have the same minimal polynomial over $Z(K)$. In the case of a general triple (K, S, D), we proceed as follows. First we can easily dispose of the case when no (positive) power of S is an inner automorphism: in this case there is at most one (S, D)-algebraic class, and this class is easily described (see (5.3)). The more interesting case is then when

S has finite "inner order" (i.e. some power of S is an inner automorphism). Also, we may restrict ourselves to the case when $R = K[t, S, D]$ is not a simple ring (for otherwise there will not be any algebraic classes). Under these assumptions, it is easy to see that R has nonconstant polynomials commuting with all scalars, i.e. cv-polynomials with respect to $(I, 0)$. By choosing such a polynomial $p(t)$ suitably, we can then apply the general results (1.4), (1.5) with $(S', D') = (I, 0)$. The net effect of this is that we can transfer questions concerning (S, D)-algebraicity and (S, D)-conjugacy back to similar questions in the classical case. By applying the Wedderburn-Dickson Theorem in the classical case, we then obtain the Hilbert 90 Theorem we want, with the polynomial $p(t)$ mentioned above playing the role of the "norm". The detailed statement of this theorem is given in (5.4).

In the final section (§6) of the paper, we make the necessary notational translations to show that the general Hilbert 90 Theorem derived in (5.4) subsumes (and extends) all known forms of the theorem in the literature. For instance, in the case $D = 0$, we obtain a strengthening of the aforementioned Theorem 27 of Jacobson [J_3, p. 47], with considerably relaxed hypotheses on the elements a, b and on the automorphism S (see (6.2)(B)). Similarly, Jacobson's "Hilbert 90" results in [J_1, Theorem 15], [J_2, p. 191] are extended from usual derivations to S-derivations, and from fields to division rings. Note, however, that the criterion given for (S, D)-conjugacy in (5.4) is valid only for an *algebraic* (S, D)-class. Counterexamples are given in §6 to show that this criterion may fail to guarantee (S, D)-conjugacy in general.

Throughout this paper, the notations and terminology introduced above will remain in force. At this point, let us also recall a few other standard notations. If $D = 0$, we write $K[t, S]$ for $K[t, S, 0]$, and if $S = I$, we write $K[t, D]$ for $K[t, I, D]$. The same conventions shall be used for (S, D)-conjugacy classes and (S, D)-centralizers. For $u \in K^*$, I_u denotes the inner automorphism of K associated with u, defined by $I_u(x) = uxu^{-1}$. An S-derivation D is said to be *S-inner* if $D = D_{c,S}$ for some $c \in K$, where $D_{c,S}(x) := cx - S(x)c$ for all $x \in K$. On the other hand, D is said to be *algebraic* if $g(D) = 0$ for some nonzero polynomial $g(t) = \sum d_i t^i \in K[t, S, D]$. (Note that, although the evaluation of $g(t)$ at elements of K has to be defined in a nontrivial way, $g(D)$ here is simply defined to be the differential operator $\sum d_i D^i$.) For an algebraic S-derivation D, the *minimal polynomial* of D is the monic polynomial $g(t)$ of the least degree such that $g(D) = 0$. In the same vein, an endomorphism S of K is said to be *algebraic* if $g(S) = 0$ for some nonzero polynomial g, and the minimal polynomial of S is defined accordingly. A polynomial $f(t) \in K[t, S, D]$ is said to be *right invariant*[1] if $f(t)K[t, S, D] \subseteq K[t, S, D]f(t)$, and *right-semi-invariant*[2] if $f(t)K \subseteq Kf(t)$. These polynomials arise naturally in the study of the ideals of $K[t, S, D]$, the minimal polynomials of (S, D)-conjugacy classes of K, and the algebraicity of D and S (see [A_2, Ca, Le, L_2 and L_3]). (Note that semi-invariant polynomials are exactly the cv-polynomials with respect to $(S', 0)$ for some S'.) Other standard ring-theoretic notations and terminology follow [Co, Mc and Ro].

[1] To simplify language, we shall suppress the adjective "right" in the following and simply speak of invariant and semi-invariant polynomials.

[2] See footnote 1.

The work on this paper was done in part while the second author visited the University of California at Berkeley in the Spring Semester of 1990. Funding support from NSF and FNRS for this visit is gratefully acknowledged.

2. The main formulas

The two main results in this section are: the Conjugation Theorem (2.2) and the Composite Function Theorem (2.3). Before we come to these theorems, let us first recall a key fact from [L1] about the evaluation of a product of two (skew) polynomials. Throughout this paper, R denotes the Ore extension $K[t, S, D]$, and R' denotes another Ore extension $K[t', S', D']$.

Product Theorem 2.1. *Let $f(t), g(t) \in R$ and $a \in K$. If $g(a) = 0$, then $(fg)(a) = 0$. If $g(a) \neq 0$, then $(fg)(a) = f(a^{g(a)})g(a)$.*

Here, "exponentiation" is the notation used for (S, D)-conjugacy: for $a \in K$ and $c \in K^*$, the (S, D)-conjugate of a by c is by definition $a^c := S(c)ac^{-1} + D(c)c^{-1}$. Note that, with this notation, $(a^c)^d = a^{dc}$ for any $a \in K$ and $c, d \in K^*$. In this case when we are dealing with two pairs (S, D) and (S', D') simultaneously, we have to be a bit careful in using the exponential notation, since it could mean (S', D')-conjugation as well as (S, D)-conjugation. We would need to specify which conjugation is intended if this is not entirely clear from the context.

Concerning the evaluation of skew polynomials, we should also make the following remark on the composite function notation. For any homomorphism $\phi: R' = K[t', S', D'] \to R = K[t, S, D]$ defined by the cv-polynomial $\phi(t') = p(t) \in R$, we have agreed to write $g(p(t))$ (or $(g \circ p)(t)$) for the image of $g \in R'$ under the map ϕ. In the special case when $p(t)$ is actually a constant, say a, we need to be a little careful with this notation, since $g(a)$ has already a meaning, namely, the evaluation of the (S', D')-polynomial $g(t')$ at $a \in K$. Fortunately, there is no conflict between the two notations. To see this, we need to verify that, if $p(t) = a \in K$, then for any $g(t') = \sum b_i t'^i \in R'$, $\phi(g)$ is indeed $g(a)$. Now $\phi(g) = \phi(\sum b_i t'^i) = \sum b_i \phi(t')^i = \sum b_i a^i$. Therefore, it suffices to show that $N_i'(a) = a^i$, where N_i' is the ith power function with respect to (S', D'), for then $\phi(g) = \sum b_i N_i'(a) = g(a)$. To see this, we induct on i, the case $i = 1$ being automatic. Assume that $N_i'(a) = a^i$. Then, since $p(t) = a$ is a cv-polynomial with respect to (S', D'), we have $ac = S'(c)a + D'(c)$ for all c. For $c = N_i'(a) = a^i$, we have in particular $a^{i+1} = S'(N_i'(a))a + D'(N_i'(a)) = N_{i+1}'(a)$, as desired.

Conjugation Theorem 2.2. *Let $p(t) \in R = K[t, S, D]$ be a cv-polynomial with respect to (S', D'). Then, for any $a \in K$ and $c \in K^*$, we have $p(a^c) = p(a)^c$. Here, on the LHS, the conjugation of a by c is with respect to (S, D), while on the RHS, the conjugation of $p(a)$ by c is with respect to (S', D'). In other words, the following diagram commutes:*

$$\begin{tikzcd}
K \arrow[r, "(S, D)\text{-conjug. by } c"] \arrow[d, "p"'] & K \arrow[d, "p"] \\
K \arrow[r, "(S', D')\text{-conjug. by } c"] & K
\end{tikzcd}$$

where the two vertical maps are given by evaluation of the polynomial $p(t)$.

Proof. Since $p(t)$ is a cv-polynomial with respect to (S', D'), we have $p(t)c = S'(c)p(t) + D'(c)$ for every $c \in K$. Evaluating the two sides of this equation on a and applying the Product Theorem, we get $p(a^c)c = S'(c)p(a) + D'(c)$, where a^c denotes (S, D)-conjugation. Right multiplying by c^{-1}, we get $p(a^c) = S'(c)p(a)c^{-1} + D'(c)c^{-1} = p(a)^c$ ((S', D')-conjugation), as desired. Q.E.D.

Composite Function Theorem 2.3. *Let* $p(t) \in R$ *be a cv-polynomial with respect to* (S', D'). *For any polynomial* $g(t') \in R' = K[t', S', D']$ *and any* $a \in K$, *we have* $(g \circ p)(a) = g(p(a))$. *(Here, the LHS denotes the evaluation of the composite polynomial* $g \circ p \in R$ *on* a, *while the RHS denotes the evaluation of the* (S', D')*-polynomial* $g(t')$ *on* $p(a)$.) *In other words, the following diagram commutes:*

$$\begin{tikzcd} R' \arrow[rr] \arrow[dr, "E_{p(a)}"'] & & R \arrow[dl, "E_a"] \\ & K & \end{tikzcd}$$

where the horizontal map is the K*-homomorphism defined by* $t' \mapsto p(t)$, *and* $E_{p(a)}$ *and* E_a *are the evaluation maps at* $p(a)$ *and* a *respectively.*

Proof. There are two possible ways of proving this fundamental result. The first way is to prove, by induction on i (and using (2.1), (2.2)), that the evaluation of $p(t)^i$ at a is given by $N_i'(p(a))$, where N_i' denotes the ith power function with respect to (S', D'). This implies that, if $g(t') = \sum b_i t'^i$, then $(g \circ p)(a) = \sum b_i N_i'(p(a)) = g(p(a))$. We shall leave the details of this inductive proof to the reader, and present instead a more conceptual proof based on the characterization of the evaluation of a polynomial at a as the remainder of its division by $t - a$ (see [L$_1$, (2.4)]). Using this characterization, we can write $p(t) = q_1(t)(t - a) + p(a)$ for some $q_1(t) \in R$ and $g(t') = q_2(t')(t' - p(a)) + g(p(a))$ for some $q_2(t') \in R'$. Applying to the latter the K-homomorphism $\phi \colon R' \to R$ defined by $\phi(t') = p(t)$, we have

$$\begin{aligned}(g \circ p)(t) &= q_2(p(t))(p(t) - p(a)) + g(p(a)) \\ &= q_2(p(t))q_1(t)(t - a) + g(p(a)).\end{aligned}$$

This implies immediately that $(g \circ p)(a) = g(p(a))$. Q.E.D.

At this point, it is convenient to recall a result from [L$_2$] relating the evaluation of polynomials at constants and evaluation of polynomials at derivations. Let $g(t')$ be any polynomial in $R' = K[t', S', D']$, and $b \in K$ be any constant. Under the isomorphism $R' \to K[\tilde{t}, S', D' - D_{b,S'}]$ defined by $t' \mapsto \tilde{t} + b$, g maps to the polynomial $\tilde{g}(\tilde{t}) := g(\tilde{t} + b)$. According to [L$_2$, (5.8)], we have the relation

$$\tilde{g}(D' - D_{b,S'})(c) = g(b^c)c \quad (\forall c \in K^*), \tag{2.4}$$

where b^c denotes (of course) (S', D')-conjugation. It turns out that we can combine the three basic formulas (2.2), (2.3) and (2.4) into a single formula. For, if $p(t) \in R$ is any cv-polynomial with respect to (S', D'), then, letting $b = p(a)$, the RHS of (2.4) is $g(p(a)^c)c = g(p(a^c))c$ by (2.2), and this is in turn $(g \circ p)(a^c)c$ by (2.3). Therefore, we have proved ($\forall a \in K$):

$$\tilde{g}(D' - D_{p(a),S'})(c) = (g \circ p)(a^c)c, \tag{2.5}$$

where a^c denotes (S, D)-conjugation. Conversely, it can be seen easily that (2.5) subsumes the three formulas (2.2), (2.3) and (2.4). In fact:

(1) Letting $p(t) = t$, we get back (2.4).

(2) Letting $c = 1$, we get back (2.3), since in this case $\tilde{g}(D' - D_{p(a),S'})(c)$ is just $\tilde{g}(0) = g(p(a))$.

(3) Letting $g(t') = t'$, we get back (2.2), since in this case $\tilde{g}(D' - D_{p(a),S'})(c)$ is just $(D' - D_{p(a),S'})(c) + p(a)c = D'(c) + S'(c)p(a) = p(a)^c c$.

In passing, it is worth observing a special case of (2.5) which is much easier to remember. Namely, if we assume that $p(a) = 0$, then $\tilde{g}$ is just the same polynomial as g, and (2.5) takes on the much simpler form:

$$(2.5') \qquad g(D')(c) = (g \circ p)(a^c)c \quad (\forall a \in K,\ c \in K^*).$$

3. The λ-transform and exponential spaces

In this section, we shall focus our attention on a single (S, D)-conjugacy class $\Delta^{S,D}(a) = \{a^c \colon c \in K^*\}$, where a is a fixed element of K. In order to study the set of roots of a polynomial $h(t) \in R = K[t, S, D]$ in $\Delta^{S,D}(a)$, we introduce the following important self-map of K called the λ-transform (associated with the pair (h, a)).

Definition 3.1. For $h \in R$ and $a \in K$, we define $\lambda_{h,a} \colon K \to K$ by: $\lambda_{h,a}(0) = 0$, and $\lambda_{h,a}(c) = h(a^c)c$ for every $c \in K^*$.

Using the formula (2.4) (in the (S, D)-setting), we see that $\lambda_{h,a}$ may be thought of as a "differential operator" on K, namely, $\tilde{h}(D - D_{a,S})$, where $\tilde{h} \in K[\tilde{t}, S, D - D_{a,S}]$ is defined by $\tilde{h}(\tilde{t}) = h(\tilde{t} + a)$. (For instance, $\lambda_{h,0}$ is just the operator $h(D)$.) In particular, $\lambda_{h,a}$ is an additive endomorphism[3] of K. The zeros of the differential operator constitute exactly the kernel of $\lambda_{h,a}$, which we shall denote by

$$(3.2) \qquad E(h, a) := \{0\} \cup \{c \in K^* \colon h(a^c) = 0\}.$$

This has been called the "exponential space" in our earlier work [L₁, (4.2)]; [L₂, (4.1)]. The cokernel of $\lambda_{h,a}$ is also of interest; we shall call it the co-exponential space, and denote it by $\overline{E}(h, a)$.

Recall that $C^{S,D}(a) := \{0\} \cup \{c \in K^* \colon a^c = a\}$ is a subdivision ring of K. (For instance, $C^{S,D}(0)$ is just K_D, the subdivision ring of constants of the derivation D. If $(S, D) = (I, 0)$, $C^{S,D}(a)$ is just the usual centralizer $C_K(a)$ of a.) For any $c \in K^*$ and any nonzero $c_0 \in C^{S,D}(a)$, we have

$$\lambda_{h,a}(cc_0) = h(a^{cc_0})cc_0 = h((a^{c_0})^c)cc_0 = h(a^c)cc_0 = \lambda_{h,a}(c)c_0,$$

so $\lambda_{h,a}$ is a right $C^{S,D}(a)$-vector space endomorphism of K. In particular, $E(h, a)$ and $\overline{E}(h, a)$ are both right vector spaces over $C^{S,D}(a)$.

Examples 3.3. (1) In the classical case when $(S, D) = (I, 0)$, for the polynomial $h(t) = \sum b_i t^i$, $\lambda_{h,a}$ is simply the map $c \mapsto \sum b_i c a^i$. The fact that $\lambda_{h,a}$ is right linear over $C_K(a)$ is particularly clear from this representation.

[3] The additivity of $\lambda_{h,a}$ can also be seen more directly by using the formula (2.9)(1) from [L₁].

(2) If h is a constant polynomial $h(t) = b$, $\lambda_{h,a}$ is just left multiplication by b (independently of a). If $b \neq 0$, then $\lambda_{h,a}$ is an isomorphism, so $E(h, a) = \overline{E}(h, a) = 0$.

(3) If $h(t) = t - b$, the map $\lambda_{h,a}$ sends c to $D(c) + S(c)a - bc$. If $b \notin \Delta^{S,D}(a)$, then $E(h, a) = 0$; if $b \in \Delta^{S,D}(a)$, say $b = a^d$, then $E(h, a) = d \cdot C^{S,D}(a)$.

(4) In general, $\lambda_{h,a}$ is injective iff $h(t)$ has no root in $\Delta^{S,D}(a)$.

(5) In the case when $D = 0$, there is also another interpretation of $\lambda_{h,a}$. In fact, if we let $S' := I_{a^{-1}} \circ S$, and $h'(t') := h(at') \in K[t', S']$, then, according to [L₂, (5.16)], $\lambda_{h,a}(c) = h(a^c)c = h'(S')(c)$ for every $c \in K^*$, so $\lambda_{h,a}$ is given by the operator $h'(S')$. In particular, in the case $a = 1$, $\lambda_{h,1}$ is just the operator $h(S)$.

If $h(t) \in R$ happens to be a cv-polynomial with respect to (S', D'), then using the conventions of (2.2) we have $h(a^c)c = h(a)^c c = S'(c)h(a) + D'(c)$ ($\forall c \in K^*$), so $\lambda_{h,a}$ has the explicit form: $\lambda_{h,a}(c) = S'(c)h(a) + D'(c)$ for every $c \in K$. In particular, if $h(t)$ is a semi-invariant polynomial, we have the following interpretation for the exponential and co-exponential spaces to be zero.

Proposition 3.4. *Let $h(t)$ be a semi-invariant polynomial with degree $n \geq 1$ and let $a \in K$. Then $E(h, a) = 0$ iff $h(a) \neq 0$, and $\overline{E}(h, a) = 0$ iff $h(a) \neq 0$ and S is an automorphism.*

Proof. Let b be the leading coefficient of h. Then h is a cv-polynomial with respect to $(S', 0)$ where $S'(c) = bS^n(c)b^{-1}$ for every $c \in K$. By the remark preceding the proposition, we have then $\lambda_{h,a}(c) = bS^n(c)b^{-1}h(a)$ for every c. If $h(a) = 0$, $\lambda_{h,a}$ is the zero map, and therefore neither injective nor surjective. If $h(a) \neq 0$, then $\lambda_{h,a}$ is clearly injective, and is surjective iff S is surjective. Q.E.D.

Some more properties of the maps $\lambda_{h,a}$ are obtained in the theorem below. The properties in (2) are especially crucial in understanding the behavior of the exponential and co-exponential spaces.

Theorem 3.5. (1) *$\rho_d \circ \lambda_{h,a^d} = \lambda_{h,a} \circ \rho_d$, where ρ_d denotes right multiplication by d on K. In particular, for any $d \in K^*$, ρ_d induces additive group isomorphisms $E(h, a^d) \xrightarrow{\cong} E(h, a)$, and $\overline{E}(h, a^d) \xrightarrow{\cong} \overline{E}(h, a)$.*

(2) *For any $h, h' \in R$, we have $\lambda_{h'h,a} = \lambda_{h',a} \circ \lambda_{h,a}$, and there is a long exact sequence of right vector spaces over the division ring $C := C^{S,D}(a)$:*

$$0 \to E(h, a) \to E(h'h, a) \to E(h', a) \to \overline{E}(h, a) \to \overline{E}(h'h, a) \to \overline{E}(h', a) \to 0.$$

In particular, we have the following cardinal inequalities for the right dimensions:

$$[E(h'h, a) : C]_r \leq [E(h', a) : C]_r + [E(h, a) : C]_r; \tag{3.6}$$

$$[\overline{E}(h'h, a) : C]_r \leq [\overline{E}(h', a) : C]_r + [\overline{E}(h, a) : C]_r. \tag{3.7}$$

Proof. (1) For any $c \in K^*$, we have

$$(\rho_d \circ \lambda_{h,a^d})(c) = \rho_d(h((a^d)^c)c) = h(a^{cd})cd = \lambda_{h,a}(cd) = \lambda_{h,a}\rho_d(c).$$

This proves the first equation in (1). From the commutative diagram of additive endomorphisms of K associated with this equation, it follows that ρ_d

induces additive isomorphisms from $E(h, a^d)$ to $E(h, a)$, and from $\overline{E}(h, a^d)$ to $\overline{E}(h, a)$.

(2) It suffices to show that $\lambda_{h'h,a}(c) = \lambda_{h',a}(\lambda_{h,a}(c))$ for every $c \in K^*$. We may assume that $h(a^c) \neq 0$, for otherwise both sides are zero. Under this assumption, we have by the Product Theorem (2.1):

$$\begin{aligned}\lambda_{h'h,a}(c) &= (h'h)(a^c)c = h'((a^c)^{h(a^c)})h(a^c)c \\ &= h'(a^{h(a^c)c}h(a^c)c = \lambda_{h',a}(h(a^c)c) = \lambda_{h',a}(\lambda_{h,a}(c)),\end{aligned}$$

as desired. Now from the commutative triangle:

$$\begin{tikzcd}
& K \arrow[dr, "\lambda_{h',a}"] & \\
K \arrow[ur, "\lambda_{h,a}"] \arrow[rr, "\lambda_{h'h,a}"] & & K
\end{tikzcd}$$

we derive by a standard argument the kernel-cokernel exact sequence for the three maps $\lambda_{h',a}$, $\lambda_{h',a}$ and $\lambda_{h,a}$ [Ba, p. 25], and this translates into the long exact sequence in (2). The two cardinal inequalities (3.6), (3.7) now follow immediately from this long exact sequence. Q.E.D.

Remark 3.8. If the calculation in the proof of (2) above looks a bit mysterious, we can give a perfectly good explanation for its *raison d'être*. For a given $a \in K$, consider the left simple R-module $M = R/R \cdot (t - a)$, which we shall identify with K using the correspondence $\overline{f(t)} \mapsto f(a)$. Under this identification, the action of a polynomial $h(t) \in R$ on an element $c \in K^*$ is given by $h(t)\#c = h(a^c)c$ (see [L$_2$, (5.21)]). Therefore, the map $\lambda_{h,a}: K \to K$ is exactly the action of $h(t)$ on the R-module $M = K$ (and $E(h, a)$ is just the annihilator of $h(t)$ on this module). From this perspective, the calculation in (2) above simply amounts to the module law $(h'h)\#c = h'\#(h\#c)$ in $M = K$. Note that since $\lambda_{h,a}$ is right C-linear for any h, $M = K$ is an (R, C)-bimodule.[4] In particular, the R-action on the left of $M = K$ gives a ring homomorphism form R to $\mathrm{End}(K_C)$ sending each $h \in R$ to $\lambda_{h,a}$.

Corollary 3.9. (1) *If $\lambda_{h,a}$ is an isomorphism, then $E(h'h, a) \cong E(h', a)$.*[5] (2) *If $\lambda_{h'h,a}$ is an isomorphism, then $E(h', a) \cong \overline{E}(h, a)$.* (3) *If $\lambda_{h',a}$ is an isomorphism, then $\overline{E}(h, a) \cong \overline{E}(h'h, a)$.*

For the rest of this section, we shall continue to write $C = C^{S,D}(a)$, for a fixed element $a \in K$.

Corollary 3.10. *Suppose $h(t)$ has no root in $\Delta^{S,D}(a)$. Then $f(t) := (t-a)h(t)$ has at most one root in $\Delta^{S,D}(a)$.*

Proof. By (3.6), (3.3)(3) and (3.3)(4), we have

$$\dim_C E(f, a) \leq \dim_C E(t-a, a) + \dim_C E(h, a) = 1.$$

Let $a^d, a^{d'}$ be roots of $f(t)$ in $\Delta^{S,D}(a)$. Then $d, d' \in E(f, a)\backslash\{0\}$, so we must have $d' = dc$ for some nonzero $c \in C$. But then $a^{d'} = a^{dc} = (a^c)^d = a^d$. Q.E.D.

[4] In fact, as we have pointed out in the paragraph after [L$_2$, (5.23)], C is naturally isomorphic to $\mathrm{End}_R M$. Here, R-homomorphisms of M are composed on the right.

[5] For instance, this conclusion would hold if S is an automorphism and h is a semi-invariant polynomial not vanishing on a (see (3.4)). Similar remarks can be made about cases (2) and (3).

Theorem 3.11. *For any nonzero $h \in R$, $[E(h, a) : C]_r \leq \deg h(t)$. If the class $\Delta^{S,D}(a)$ is (S, D)-algebraic with minimal polynomial $f(t)$, then $[E(h, a) : C]_r = [\overline{E}(h, a) : C]_r \leq \deg h_0(t)$, where $h_0(t)$ is the remainder of $h(t)$ upon right division by $f(t)$.*

Proof. The first part of the theorem has appeared before in [L$_1$, (4.2)]. Here we offer a shorter, and perhaps also more natural proof, by induction on $\deg h(t)$. If this degree is zero, the desired conclusion follows from (3.3)(2). In the general case, we may assume the existence of a nonzero element $d \in E(h, a)$ (for otherwise $[E(h, a) : C]_r = 0$). Then $h(a^d) = 0$, so we have a factorization $h(t) = q(t)(t - a^d)$, where $q(t) \in R$ has degree $= \deg h(t) - 1$. By (3.6), (3.3)(3) and the inductive hypothesis (in that order), we have

$$\begin{aligned}[E(h, a) : C]_r &\leq [E(t - a^d, a) : C]_r + [E(q, a) : C]_r \\ &= 1 + [E(q, a) : C]_r \\ &\leq 1 + \deg q(t) \\ &= \deg h(t),\end{aligned}$$

as desired. If $\Delta^{S,D}(a)$ happens to be algebraic, then K is finite dimensional as a right C-vector space [L$_2$, (5.10)]. Taking C-dimensions of the spaces in the exact sequence

$$0 \to E(h, a) \to K \to K \to \overline{E}(h, a) \to 0,$$

we see immediately that $[E(h, a) : C]_r = [\overline{E}(h, a) : C]_r$. Since any left multiple of $f(t)$ vanishes on $\Delta^{S,D}(a)$, we have $h(a^c) = h_0(a^c)$ for any $c \in K^*$, and hence $\lambda_{h,a} = \lambda_{h_0,a}$. From this, it follows that

$$[E(h, a) : C]_r = [E(h_0, a) : C]_r \leq \deg h_0(t). \quad \text{Q.E.D.}$$

To illustrate the meaning of the second part of the theorem, let us re-state it in more explicit terms in the special case when $h(t)$ is a linear polynomial $t - b$. Using the computation of $E(h, a)$ in (3.3)(3) in this case, we arrive at the following statement:

Corollary 3.12. *Let $\Delta^{S,D}(a)$ be an algebraic class, and let $b \in K$.*

(1) *If $b \notin \Delta^{S,D}(a)$, then the additive endomorphism of K sending $c \in K$ to $D(c) + S(c)a - bc \in K$ is an isomorphism. In other words, for every $d \in K$, there exists a unique $c \in K$ solving the equation $D(c) + S(c)a - bc = d$.*

(2) *If $b \in \Delta^{S,D}(a)$, then the image of the above additive endomorphism of K is a right $C^{S,D}(a)$-subspace of codimension 1 in K.*

In the classical case when $(S, D) = (I, 0)$, for instance, (1) above says the following: If $a \in K$ is algebraic over the center of K, and b is not a conjugate of a, then for any $d \in K$, there is a unique $c \in K$ solving the equation $ca - bc = d$. But if b is conjugate to a, then there exists $d \in K$ for which $ca - bc = d$ is unsolvable in K. These statements are to be compared with similar ones made by P. M. Cohn in [Co, p. 222].

Some more useful consequences of (3.5) and (3.11) are noted below.

Corollary 3.13. *Let $\Delta^{S,D}(a)$ be an algebraic conjugacy class, and let $h, h' \in R$. If h has no root in $\Delta^{S,D}(a)$, then $\lambda_{h,a}$ is an isomorphism, and $\dim_C E(h'h, a)$*

$= \dim_C E(h', a)$. (*Similar statements can be made in the cases when h' or $h'h$ has no root in $\Delta^{S,D}(a)$; see* (3.9).)

Proof. The assumption on h means that $E(h, a) = 0$, and by (3.11) this implies that $\overline{E}(h, a) = 0$, so $\lambda_{h,a}$ is an isomorphism. From (3.9)(1), we deduce that $E(h'h, a) \cong E(h', a)$, so these spaces have the same dimension over C. Q.E.D.

Corollary 3.14. *Suppose S is not an automorphism, and $\Delta^{S,D}(a)$ is an algebraic class. Then every nonconstant semi-invariant polynomial $h(t) \in R$ vanishes on $\Delta^{S,D}(a)$.*

Proof. Since $\Delta^{S,D}(a^d) = \Delta^{S,D}(a)$, it is sufficient to show that $h(a) = 0$. But if $h(a) \neq 0$, then $E(h, a) = 0$ by (3.4), and so $\overline{E}(h, a) = 0$ by (3.11). By (3.4) again, S must be an automorphism, contradicting the hypothesis. Q.E.D.

Although we have used parallel notation for the exponential and co-exponential spaces, in general they have considerably different behavior. For instance, unlike $E(h, a)$, $\overline{E}(h, a)$ may have *infinite* right dimension over $C = C^{S,D}(a)$ (necessarily in the case when $\Delta^{S,D}(a)$ is not algebraic). We shall give two examples below in which $\dim_C E(h, a) \leq 1$, but $\dim_C \overline{E}(h, a) = \infty$. In both examples, K is a field and $D = 0$; in such a situation, the *a priori* condition that $\Delta^{S,D}(a)$ is not algebraic boils down simply to S not being an algebraic endomorphism, independently of a (see [L_2, (5.17)]). In fact, the endomorphisms S used below are among the simplest examples of nonalgebraic endomorphisms of fields.

Examples 3.15. (A) Let K be a rational function field $k(x)$ over a field k, $D = 0$, and S be the k-endomorphism of K with $S(x) = x^2$. For $a := x$, it is easy to see that $C := C^S(a) = k$. For the invariant polynomial $h(t) := t$, we have $\lambda_{h,a}(c) = S(c)a$ for every $c \in K$, so $E(h, a) = 0$; however, $\overline{E}(h, a) = K/S(K)a = k(x)/k(x^2)x \cong k(x^2)$ is clearly infinite dimensional over $C = k$.

(B) One might think that the above example is pathological since S there is not an automorphism of K. However, a slight variation of the construction will yield a new example in which S is an automorphism. Let $K = k(x)$ as before, where k is a field of characteristic zero; let $D = 0$, and let S be the k-automorphism of K defined by $S(x) = x + 1$. Here, we let $a := 1$, and $h(t) = t - 1$. For these choices, $C := C^S(a)$ is the fixed field $K^S = k$, and by (3.3)(5), $\lambda_{h,a} = h(S) = S - I$. Therefore, $E(h, a) = K^S$ has C-dimension 1, and $\operatorname{im}\lambda_{h,a}$ consists of functions $f(x + 1) - f(x)$, where f ranges over $k(x)$. Using the unique factorization of polynomials in $k[x]$, and the fact that $\operatorname{char} k = 0$, it is not difficult to show that no nontrivial k-linear combination of $\{x^{-1}, x^{-2}, \ldots\}$ can be expressed in the form $f(x + 1) - f(x)$. This shows that the set $\{x^{-1}, x^{-2}, \ldots\}$ is k-linearly independent over $\operatorname{im}\lambda_{h,a}$, and therefore $\dim_C \overline{E}(h, a) = \infty$.[6] Note that the assumption $\operatorname{char} k = 0$ is essential for this example, for if $\operatorname{char} k = p > 0$, then $S^p = I$, so S is an algebraic automorphism. In the case, K is a cyclic extension of degree p over $C := C^S(1) = K^S = k(x^p - x)$, and Theorem 3.11 would apply to show that $\operatorname{im}\lambda_{h,1} = \{f(x + 1) - f(x) \colon f \in k(x)\}$ has C-codimension 1 in K.

[6] This is all the more remarkable in view of the (easily established) fact that the restriction $\lambda_{h,1} \colon k[x] \to k[x]$ is actually onto.

Concerning the question of finite dimensionality of $\overline{E}(h, a)$, we can only offer some partial results, because of the difficulties suggested by the above examples. First of all, for a product of two polynomials, we do have the following:

$$(3.16) \quad \dim_C \overline{E}(h'h, a) < \infty \Leftrightarrow \dim_C \overline{E}(h, a) < \infty \text{ and } \dim_C \overline{E}(h', a) < \infty.$$

To obtain a more quantitative result, we shall need more assumptions.

Proposition 3.17. *Assume that S is an automorphism, and that $f = h'h$ is a nonconstant semi-invariant polynomial. Then* $\dim_C \overline{E}(h, a)$ *and* $\overline{E}(h', a)$ *are both bounded by* $m := \max\{\deg h(t), \deg h'(t)\}$. *If, moreover, $h'h = hh'$, then* $\dim_C \overline{E}(h, a) \leq \deg h(t)$, *and* $\dim_C \overline{E}(h', a) \leq \deg h'(t)$.

Proof. We go into the following two cases.

Case (i). $f(a) = 0$. By the proof of (3.4), we have in fact $f(\Delta^{S,D}(a)) = 0$, so $\Delta^{S,D}(a)$ is algebraic. In this case, (3.11) gives $\dim_C \overline{E}(g, a) = \dim_C E(g, a) \leq \deg g(t)$ for every $g(t)$, so all desired conclusions follow.

Case (ii). $f(a) \neq 0$. Since S is an automorphism, (3.4) implies that $\lambda_{f,a}$ is an isomorphism. By (3.9)(2), we have $E(h', a) \cong \overline{E}(h, a)$, so $\dim_C \overline{E}(h, a) = \dim_C E(h', a) \leq \deg h'(t) \leq m$. Also, by (3.5) there is a surjection from $\overline{E}(f, a)$ to $\overline{E}(h', a)$, so we have $\overline{E}(h', a) = 0$ in this case. If $h'h = hh'$, then we will have $\overline{E}(h, a) = 0$ as well. Q.E.D.

Now let us return to the study of exponential spaces. In general, the inequality $[E(h, a) : C]_r \leq \deg h(t)$ in (3.11) may be strict, so it is useful to introduce the following definition: We say that a nonzero polynomial $h(t) \in R$ is *full* at $a \in K$ if $[E(h, a) : C]_r = \deg h(t)$. For instance, if $\Delta^{S,D}(a)$ happens to be (S, D)-algebraic, then its minimal polynomial (the monic polynomial in R of the least degree vanishing on $\Delta^{S,D}(a)$) is full at a [L$_2$, §4]. An interesting consequence of (3.6) is the following:

Proposition 3.18. *Let $f = h'h \in R$. If f is full at a, then h' and h are both full at a.*

Proof. By the fullness of f at a and by (3.6), we have

$$\begin{aligned} \deg f &= [E(f, a) : C]_r = [E(h'h, a) : C]_r \\ &\leq [E(h', a) : C]_r + [E(h, a) : C]_r \\ &\leq \deg h' + \deg h \\ &= \deg f. \end{aligned}$$

Therefore, we must have $[E(h', a) : C]_r = \deg h'$, and $[E(h, a) : C]_r = \deg h$. Q.E.D.

With the help of this corollary, some alternative characterizations of the fullness property are given in the proposition below.

Proposition 3.19. *Let $\Delta = \Delta^{S,D}(a)$ and let h be a nonconstant polynomial in R. Then the following are equivalent:*

(1) *$h(t)$ is full at a;*

(2) *$h(t)$ is, up to a left scalar multiple, the minimal polynomial of some (S, D)-algebraic subset Δ_0 of Δ.*

If Δ is (S, D)-algebraic, these conditions are also equivalent to:

(3) *$h(t)$ is a right divisor of f_Δ, the minimal polynomial of Δ.*

Proof. To facilitate the proof, we shall use freely the basic properties of P-dependence, P-basic, rank and minimal polynomial of (S, D)-algebraic sets, as developed in [La] and [L$_1$]. Let $n := \deg h(t)$. If $h(t)$ is full at a, let $\{c_1, \dots, c_n\}$ be a right C-basis for $E(h, a)$. By [L$_2$, §4], $\Delta_0 := \{a^{c_1}, \dots, a^{c_n}\}$ are P-independent in Δ, so $\operatorname{rank}\Delta_0 = n$. Since $h(t)$ vanishes on Δ_0, and $\deg h(t) = \operatorname{rank}\Delta_0$, $h(t)$ must be, up to a left K-multiple, the minimal polynomial of Δ_0. Conversely, suppose $h(t)$ is a left K-multiple of the minimal polynomial of an (S, D)-algebraic subset $\Delta_0 \subseteq \Delta$. Then $\operatorname{rank}\Delta_0 = \deg h(t) = n$, so Δ_0 has a P-basis of n elements, say $\{a^{c_1}, \dots, a^{c_n}\}$. By [L$_2$, §4], $\{c_1, \dots, c_n\} \subseteq E(h, a)$ are right linearly independent over C. Since $[E(h, a) : C]_r \le \deg h(t) = n$, it follows that $\{c_1, \dots, c_n\}$ form a C-basis for $E(h, a)$, so $h(t)$ is full at a. We have now completed the proof of (1) $\Leftrightarrow$ (2).

Now suppose Δ is (S, D)-algebraic, with minimal polynomial f_Δ. If $h(t) = b \cdot h_0(t)$ where h_0 is the minimal polynomial of some (S, D)-algebraic subset $\Delta_0 \subseteq \Delta$, then, since f_Δ vanishes on Δ_0, it is a left multiple of h_0, and hence also of h. Conversely, if f_Δ is a left multiple of h, then, since f_Δ is full at a, (3.18) implies that h is also full at a. Q.E.D.

Now let us consider two Ore extensions

$$R = K[t, S, D] \quad \text{and} \quad R' = K[t', S', D'],$$

connected by a K-homomorphism $\phi: R' \to R$. The map ϕ is determined by $p(t) := \phi(t')$, which is a cv-polynomial in R with respect to (S', D'). For a polynomial $g(t') \in K[t', S', D']$ and any $b \in K$, let us denote the associated λ-transform on K by $\lambda'_{g,b}$, and the corresponding exponential and co-exponential spaces by $E'(g, b)$ and $\overline{E}'(g, b)$. As a natural consequence of the Conjugation Theorem and the Composite Function Theorem, we have the following result.

Proposition 3.20. *For any $g(t') \in R'$ and any $a \in K$, we have $\lambda_{g \circ p, a} = \lambda'_{g, p(a)}$. In particular, $E(g \circ p, a) = E'(g, p(a))$, and $\overline{E}(g \circ p, a) = \overline{E}'(g, p(a))$.*

Proof. For any $c \in K^*$, (2.2) and (2.3) give the following

$$\lambda_{g \circ p, a}(c) = (g \circ p)(a^c)c = g(p(a^c))c = g(p(a)^c)c = \lambda'_{g, p(a)}(c),$$

where the conjugation notations follow the conventions in (2.2). This gives the equation for the λ-transforms, and the rest follows by taking kernels and cokernels of these. Q.E.D.

In the above proposition, of course, $\lambda_{g \circ p, a}$ is linear over $C^{S,D}(a)$, while $\lambda'_{g, p(a)}$ is linear over $C^{S', D'}(p(a))$. This fact is reconciled by (1) in the proposition below.

Proposition 3.21. *For the cv-polynomial $p(t)$ as above, and for any $a \in K$, we have*:

(1) $C^{S,D}(a) \subseteq C^{S', D'}(p(a))$;

(2) $C^{S', D'}(p(a)) = E(p - p(a), a)$;

(3) *The right dimension* $[C^{S',D'}(p(a)) : C^{S,D}(a)]_r$ *is bounded by* $\deg p(t)$.

Proof. (1) Let $c \in C^{S,D}(a)\backslash\{0\}$. Then $a^c = a$, and hence $p(a) = p(a^c) = p(a)^c$ (using the conventions in (2.2)). Since the last conjugation here is an (S', D')-conjugation, we see that $c \in C^{S',D'}(p(a))$. For (2), note that c belongs to $E(p - p(a), a)\backslash\{0\}$ iff $0 = (p - p(a))(a^c) = p(a^c) - p(a)$. By (2.2), this means that $p(a)^c = p(a)$, i.e. $c \in C^{S',D'}(p(a))$. This proves (2). Using this, it follows that $[C^{S',D'}(p(a)) : C^{S,D}(a)]_r$ is the right $C^{S,D}(a)$-dimension of $E(p - p(a), a)$, so by (3.11) it is bounded by $\deg(p(t) - p(a)) = \deg p(t)$. Q.E.D.

The above proposition leads to some special properties of the exponential spaces of cv-polynomials. We record these properties in the following corollary.

Corollary 3.22. *Let* $a \in K$, *and* $p(t)$ *be a cv-polynomial as above.*

(1) *If* $E(p, a) \neq \{0\}$, *then it is a one-dimensional left vector space over* $K_{D'}$, *the subdivision ring of constants of the derivation* D'.

(2) *If* $E(p, a_1) \cap E(p, a_2) \neq \{0\}$, *then* $E(p, a_1) = E(p, a_2)$.

(3) *For any nonzero* $d \in E(p, a)$, *we have* $dC^{S,D}(a)d^{-1} \subseteq K_{D'}$.

Proof. Fix a nonzero element $d \in E(p, a)$, so $p(a^d) = 0$. Replacing a in (3.21)(2) by a^d, we get $C^{S',D'}(0) = E(p, a^d)$. By (3.5)(1), this gives $K_{D'} = E(p, a) \cdot d^{-1}$. Therefore, $E(p, a) = K_{D'} \cdot d$. This proves (1), and (2) follows immediately from (1). For (3), we use the fact that $E(p, a)$ is a right vector space over $C^{S,D}(a)$. For any nonzero d as above, we have $dC^{S,D}(a) \subseteq E(p, a) = K_{D'} \cdot d$, so $dC^{S,D}(a)d^{-1} \subseteq K_{D'}$. Q.E.D.

Lastly, putting our results together, we derive a characterization for a composite function to be full at a given point.

Proposition 3.23. *Let* $p(t)$ *be as above,* $a \in K$, *and* $g(t') \in R'$. *Then* $g \circ p$ *is full at* a *iff* $p - p(a)$ *is full at* a *and* g *is full at* $p(a)$.

Proof. We start with the formula $E(g \circ p, a) = E'(g, p(a))$ in (3.20), and let $C = C^{S,D}(a)$, $C' = C^{S',D'}(p(a))$. Taking right dimensions and using the transitivity formula, we have

$$\begin{aligned}
[E(g \circ p, a) : C]_r &= [E'(g, p(a)) : C]_r \\
&= [E'(g, p(a)) : C']_r \cdot [C' : C]_r \\
&= [E'(g, p(a)) : C']_r \cdot [E(p - p(a), a) : C]_r \\
&\leq \deg g(t') \cdot \deg p(t) \\
&= \deg(g \circ p).
\end{aligned}$$

Now, $g \circ p$ is full at a iff we have equality above, and this can happen iff $p - p(a)$ is full at a and g is full at $p(a)$. Q.E.D.

4. Preservation of algebraic subsets

In this section, we shall apply the results obtained in §2 and §3 to the study of self-maps on K induced by cv-polynomials. The first part of this section (all material before (4.10)) is independent of §3, and can therefore be read immediately after §2. Again, the notations $R = K[t, S, D]$ and $R' = K[t', S', D']$ will remain in force.

Proposition 4.1. *Let $p(t) \in R$ be a cv-polynomial with respect to (S', D'). If $a \in K$ is P-dependent on a set $\Delta \subseteq K$ with respect to (S, D), then $p(a)$ is P-dependent on $p(\Delta)$ with respect to (S', D').*

Proof. For any polynomial $g(t') \in R'$ such that $g(p(\Delta)) = 0$, we must show that $g(p(a)) = 0$. By (2.3) (the Composite Function Theorem), $g(p(\Delta)) = 0$ implies that $(g \circ p)(\Delta) = 0$. Since a is P-dependent on Δ with respect to (S, D), the latter implies that $(g \circ p)(a) = 0$. Applying the Composite Function Theorem one more time, we conclude that $g(p(a)) = 0$. Q.E.D.

The converse of this proposition is, of course, not true in general. For instance, in the case when $(S, D) = (I, 0)$, $\{1\}$ is to P-dependent on $\{0\}$; yet for the cv-polynomial $p(t) = t(t-1)$, we have $p(1) = p(0) = 0$, so $\{p(1)\}$ is P-dependent on $\{p(0)\}$. Nevertheless we have in general the following result on the preservation of algebraic sets under the map $a \mapsto p(a)$ for any (nonconstant) cv-polynomial $p(t)$.

Theorem 4.2. *Let $p(t) \in R$ be a nonconstant cv-polynomial with respect to (S', D'), and let $\Delta \subseteq K$. Then Δ is (S, D)-algebraic iff $p(\Delta)$ is (S', D')-algebraic. Moreover, in this case,*

$$\text{(4.3)} \qquad \operatorname{rank} p(\Delta) \leq \operatorname{rank} \Delta \leq \deg p(t) \cdot \operatorname{rank} p(\Delta).$$

The second inequality here is an equality iff f_Δ (the minimal polynomial of Δ) belongs to $K[p(t)]$ (the subring of R generated by $p(t)$ over K).

Proof. Step I. First assume that Δ is (S, D)-algebraic. We fix a finite P-basis for Δ, say $\{a_1, \ldots, a_n\}$. By [L₁, (2.10)], we know there exists a nonzero polynomial $q(t') \in K[t', S', D']$ vanishing on $\{p(a_1), \ldots, p(a_n)\}$, with $\deg q(t') \leq n$. Then, by (2.3), $(q \circ p)(a_i) = q(p(a_i)) = 0$ for $i = 1, \ldots, n$. Since $\{a_1, \ldots, a_n\}$ form a P-basis for Δ, this implies that $q \circ p$ vanishes on Δ. By (2.3) again, we see that $q(p(\Delta)) = 0$, so $p(\Delta)$ is (S', D')-algebraic, with $\operatorname{rank} p(\Delta) \leq \deg q(t') \leq n = \operatorname{rank} \Delta$.

Step II. Next, assume that $p(\Delta)$ is (S', D')-algebraic, and let $g(t') \in R'$ be its (monic) minimal polynomial. Then $g(p(a)) = 0$ for every $a \in \Delta$, and so by (2.3) $g \circ p$ vanishes on Δ. Since $g \circ p \neq 0$ (the fact that $p(t)$ is nonconstant is needed here), this implies that Δ is (S, D)-algebraic, with

$$\text{(4.4)} \qquad \operatorname{rank} \Delta \leq \deg(g \circ p)(t) = \deg p(t) \cdot \deg g(t') = \deg p(t) \cdot \operatorname{rank} p(\Delta).$$

Step III. If $\operatorname{rank} \Delta = \deg p(t) \cdot \operatorname{rank} p(\Delta)$, then, in Step II above, $g \circ p$ must already be a left K-multiple of the minimal polynomial f_Δ of Δ. Therefore, $f_\Delta \in K \cdot g(p(t)) \subseteq K[p(t)]$.

Step IV. Assume that $f_\Delta \in K[p(t)]$, say $f_\Delta = h(p(t))$, where $h(t') \in R'$. Arguing by the Composite Function Theorem as before, we see that $h(t')$ vanishes on $p(\Delta)$, so $\deg h(t') \geq \operatorname{rank} p(\Delta)$. Then we have

$$\text{(4.5)} \qquad \operatorname{rank} \Delta = \deg f_\Delta = \deg p(t) \cdot \deg h(t') \geq \deg p(t) \cdot \operatorname{rank} p(\Delta).$$

Combining this with (4.4), we must have equality in (4.5). Q.E.D.

In some cases, the condition that $f_\Delta \in K[p(t)]$ may hold automatically. In such a situation, we will always get equality in (4.5). to be more specific, we record the following corollary of (4.2)

Corollary 4.6. *Assume that $K[p(t)]$ above is the largest Ore subextension of R in the sense of* [L$_4$, *Definition* 5.15], *and that $\Delta \subseteq K$ is a nonsingleton (S, D)-algebraic set closed under (S, D)-conjugation. Then $p(\Delta)$ is (S', D')-algebraic, and* $\operatorname{rank}\Delta = \deg p(t) \cdot \operatorname{rank} p(\Delta)$. (*In particular,* $\operatorname{rank}\Delta$ *must be divisible by* $\deg p(t)$.)

Proof. By [L$_2$, (5.2)], f_Δ is an invariant polynomial; in particular, it is a cv-polynomial. Since Δ is not a singleton set, we have $\deg f_\Delta \geq 2$. The fact that $K[p(t)]$ is the largest Ore subextension of R then implies that $f_\Delta \in K[p(t)]$. Therefore, the last part of the above theorem applies. Q.E.D.

In general, of course, the equality $\operatorname{rank}\Delta = \deg p(t) \cdot \operatorname{rank} p(\Delta)$ need not hold. In fact, we may not even have the divisibility relation $\operatorname{rank} p(\Delta) | \operatorname{rank}\Delta$ or $\deg p(t) | \operatorname{rank}\Delta$. For instance, again in the simple case when $(S, D) = (I, 0)$, if K is a field with three different elements a, b, c, then $\Delta = \{a, b, c\}$ has rank 3, but for the quadratic cv-polynomial $p(t) = (t-a)(t-b)$, $p(\Delta) = \{0, (c-a)(c-b)\}$ has rank 2. In this example, both of the inequalities in (4.3) are strict inequalities. We shall see, however, that the divisibility relation $\operatorname{rank} p(\Delta) | \operatorname{rank}\Delta$ does hold in a special case, namely, when Δ is a single (S, D)-conjugacy class $\Delta^{S,D}(a)$ of some element $a \in K$ (cf. (4.10) below). Let us now specialize to this important case.

Theorem 4.7. *Let $p(t)$ be as in* (4.2). *For any $a \in K$, we have $p(\Delta^{S,D}(a)) = \Delta^{S',D'}(p(a))$, and the following statements are equivalent:*

(1) *$\Delta^{S,D}(a)$ is (S, D)-algebraic;*

(2) *The S-derivation $D - D_{a,S}$ is algebraic;*

(3) *$\Delta^{S',D'}(p(a))$ is (S', D')-algebraic;*

(4) *The S'-derivation $D' - D_{p(a),S'}$ is algebraic.*

If any of these conditions holds, then we have

$$\text{(4.8)} \qquad \operatorname{rank}\Delta^{S',D'}(p(a)) \leq \operatorname{rank}\Delta^{S,D}(a) \leq \deg(t) \cdot \operatorname{rank}\Delta^{S',D'}(p(a)).$$

Proof. Let $\Delta = \Delta^{S,D}(a)$. Then $p(\Delta)$ consists of $p(a^c)$, where c ranges over K^*. Since $p(a^c) = p(a)^c$ (in the sense of (2.2)), we see that $p(\Delta)$ consists of all (S', D')-conjugates of $p(a)$, that is, $p(\Delta^{S,D}(a)) = \Delta^{S',D'}(p(a))$. In view of this equation, (1) $\Leftrightarrow$ (3) follows from (4.2), and (1) $\Leftrightarrow$ (2) and (3) $\Leftrightarrow$ (4) both follow from (2.4). Finally, (4.8) follows from (4.3). Q.E.D.

Remark 4.9. The equivalences (1) $\Leftrightarrow$ (2) and (3) $\Leftrightarrow$ (4) have appeared before in [L$_2$, (5.10)], with essentially the same proofs (using the identity (2.4)). (2) $\Leftrightarrow$ (4) has also appeared in [L$_4$, (5.13)]; however, the proof given here is substantially different from that in [L$_4$].

Next, we shall bring to bear the basic results on exponential spaces obtained in §3. These results lead to a much more precise version of (4.2) in the case when Δ is a single algebraic (S, D)-conjugacy class.

Theorem 4.10. *Let $p(t) \in R$ be any nonconstant cv-polynomial with respect to (S', D'). Let $\Delta := \Delta^{S,D}(a)$ be an algebraic (S, D)-conjugacy class in K, and let $\Delta' := p(\Delta) = \Delta^{S',D'}(p(a))$. Then* $\operatorname{rank} p(\Delta)$ *divides* $\operatorname{rank}\Delta$, *and the following statements are equivalent:*

(1) $\operatorname{rank}\Delta = \deg p(t) \cdot \operatorname{rank} p(\Delta)$;

(2) *The polynomial $p - p(a)$ is full at a;*

(3) *The minimal polynomial f_Δ of Δ belongs to $K[p(t)]$;*

(4) *$p - p(a)$ is a right divisor of f_Δ in R;*

(5) *$p - p(a)$ is, up to a left K-multiple, the minimal polynomial of some subset Δ_0 of Δ.*

Proof. Let $C := C^{S,D}(a)$ and $C' := C^{S',D'}(p(a))$. Then, by [L$_2$, (5.10)], $[K : C]_r = \operatorname{rank}\Delta$, and $[K : C']_r = \operatorname{rank}\Delta'$. But by (3.21)(1), we have $C \subseteq C'$, so the transitivity formula for vector space dimensions gives $[K : C]_r = [K : C']_r \cdot [C' : C]_r$. This implies that $\operatorname{rank}\Delta' | \operatorname{rank}\Delta$. Furthermore, by (3.21)(2),

$$(4.11)\quad \frac{\operatorname{rank}\Delta}{\operatorname{rank}\Delta'} = [C' : C]_r = [E(p - p(a), a) : C]_r \leq \deg(p - p(a)) = \deg p(t).$$

This gives another proof for the second inequality in (4.8), and from this new argument, we see immediately that (1) $\Leftrightarrow$ (2). The equivalence of (1) and (3) follows from (4.2), and finally, the equivalences of (2), (4) and (5) follow by applying (3.19) to the polynomial $p - p(a)$ (independently of the fact that $p(t)$ is a cv-polynomial). Q.E.D.

Example 4.12. We give here a simple example in the classical case $(S, D) = (I, 0)$ in which the conditions (1) through (5) in the above theorem are *not* satisfied. Let K be a central k-division algebra with a maximal subfield $L = k(a)$ of odd dimension n over k, and take $p(t)$ to be the central quadratic polynomial t^2. Here, $\Delta :=$ conjugacy class of a and $\Delta' :=$ conjugacy class of $p(a) = a^2$ both have rank n (since $L = k(a) = k(a^2)$), so the divisibility relation $\operatorname{rank} p(\Delta) | \operatorname{rank}\Delta$ holds, but (1) in the theorem does not. The exponential space $E(p - p(a), a)$ here is $C_K(a^2) = L$ which is 1-dimensional over $C := C_K(a) = L$, so $p - p(a)$ is not full at a. Lastly, f_Δ is the minimal polynomial of a over k; since this polynomial has odd degree n, it clearly cannot belong to $K[p(t)] = K[t^2]$.

We now finish this section by pointing out what is perhaps the most useful consequence of the condition that $f_\Delta \in K[p(t)]$. Recall from [L$_2$, §4] that an (S, D)-algebraic set Δ is said to be *full* if every root of its minimal polynomial f_Δ belongs to Δ.

Theorem 4.13. *Let Δ be a full (S, D)-algebraic set, and assume that $f_\Delta \in K[p(t)]$, where $p(t)$ is a nonconstant cv-polynomial as above. Then for any $b \in K$, we have $b \in \Delta \Leftrightarrow p(b) \in p(\Delta)$.*

Proof. ("$\Leftarrow$") Let $g(t')$ be the minimal polynomial for $p(\Delta)$. The given hypothesis implies that $g \circ p = d \cdot f_\Delta$ for some scalar $d \in K^*$ (cf. Step III in the proof of (4.2)). Suppose $p(b) \in p(\Delta)$. Then $(g \circ p)(b) = g(p(b)) = 0$ since g vanishes on $p(\Delta)$. But then we have $f_\Delta(b) = 0$, and the fullness of Δ implies that $b \in \Delta$. Q.E.D.

Since $p(\Delta^{S,D}(a)) = \Delta^{S',D'}(p(a))$, and $\Delta^{S,D}(a)$ is full if it is algebraic, we have in particular:

Corollary 4.14. *Let $\Delta = \Delta^{S,D}(a)$ be an algebraic class, and assume that its minimal polynomial f_Δ belongs to $K[p(t)]$, where $p(t)$ is a nonconstant cv-polynomial. Then for any $b \in K$, b is (S, D)-conjugate to a iff $p(b)$ is (S', D')-conjugate to $p(a)$.*

It is easy to see, by an example, that the hypothesis $f_\Delta \in K[p(t)]$ in this corollary cannot be omitted. For instance, let K be the division ring of the real quaternions with $(S, D) = (I, 0)$, and let $p(t)$ be the central polynomial t^2 in $K[t]$, so $p(t)$ is a cv-polynomial with respect to $(S', D') = (I, 0)$. For $a = i+1$ and $b = -(i+1)$, we have $p(a) = a^2 = b^2 = p(b)$, but the minimal polynomials of a and b over $Z(K) = \mathbf{R}$ are, respectively, $t^2 - 2t + 2$ and $t^2 + 2t + 2$, so a and b are *not* conjugate in K. Corollary (4.14) does not apply in this situation since the above minimal polynomials are not polynomials in t^2. In §6, an example will also be given (see (6.7)) to show that the hypothesis on the algebraicity of Δ is crucial for both (4.13) and (4.14).

5. Criterion for (S, D)-algebraicity and (S, D)-conjugacy

In this section, we shall apply the tools developed in the earlier sections to derive a general criterion for an (S, D)-conjugacy class $\Delta^{S,D}(a)$ to be algebraic; then we prove the promised Hilbert 90 Theorem for an element $b \in K$ to belong to such an algebraic class $\Delta^{S,D}(a)$. Basically, our technique is to translate properties involving (S, D) into analogous properties in the classical case when $(S, D) = (I, 0)$; the material in §2–§4 provides the necessary theoretical framework for such a transfer procedure. Once we are reduced to the case when $(S, D) = (I, 0)$, we can use freely the following classical results of Wedderburn and Dickson mentioned in the Introduction:

(5.1) *A conjugacy class $\Delta(a) = \{cac^{-1} : c \in K^*\}$ is algebraic iff a is algebraic over $Z(K)$ (the center of K);*

(5.2) *An element $b \in K$ belongs to an algebraic conjugacy class $\Delta(a)$ iff a and b have the same minimal polynomial over $Z(K)$.*

To begin our discussion, we first observe that a necessary condition for $R = K[t, S, D]$ to have an algebraic conjugacy class is that R not be a simple ring. In fact, if $\Delta^{S,D}(a)$ is an algebraic class, then the minimal polynomial of $\Delta^{S,D}(a)$ is a nonconstant invariant polynomial which generates a nonzero proper ideal in R. Since we are interested only in *algebraic* conjugacy classes in this section, *we shall henceforth assume that R is a nonsimple ring.* In particular, R has a monic nonconstant semi-invariant polynomial of minimal degree. We shall fix such a polynomial $p(t)$ in this section, and denote its degree by $n \geq 1$.

Our first step is to dispose of the case when S has infinite inner order. Recall from [L4] that the inner order of S, denoted by $o(S)$, is the smallest positive integer k such that S^k is an inner automorphism of K; if no such k exists, $o(S)$ is taken to be ∞. In particular, if S is not an automorphism, $o(S)$ is ∞ according to this definition.

Proposition 5.3. *Suppose $o(S) = \infty$.*

(1) *If $p(t)$ has no root in K, then K has no algebraic (S, D)-conjugacy classes.*

(2) *If $p(t)$ has a root in K, then the roots of $p(t)$ constitute the one and only algebraic (S, D)-conjugacy class in K, and $p(t)$ is its minimal polynomial. In particular, $p(t)$ is invariant. If, in addition, S is an automorphism, then in fact every semi-invariant polynomial in R is invariant.*

Proof. (1) Assume $p(t)$ has no root in K. Since $p(t)c = S^n(c)p(t)$ for every $c \in K$, $p(t)$ is a cv-polynomial in R with respect to $(S^n, 0)$. If there exists an algebraic class $\Delta^{S,D}(a)$, then by (4.7) $\Delta^{S^n}(p(a))$ is $(S^n, 0)$-algebraic. Since $p(a) \neq 0$, an argument involving the nonzero constant term of the minimal polynomial of $\Delta^{S^n}(p(a))$ shows that $o(S^n) < \infty$. (See [L$_2$, (5.17)] for the details.) But then we also have $o(S) < \infty$, a contradiction.

(2) Suppose now that $p(t)$ has a root $a \in K$. Applying the Conjugation Theorem (2.2) to $p(t)$ (or by [L$_2$, (5.1)]), we see that $p(\Delta^{S,D}(a)) = 0$. Therefore, $\Delta^{S,D}(a)$ is an algebraic class, and $p(t)$ is a left multiple of the minimal polynomial of $\Delta^{S,D}(a)$. Since $n = \deg p(t)$ is chosen minimal, $p(t)$ is exactly the minimal polynomial of $\Delta^{S,D}(a)$. In particular, $p(t)$ is invariant, and $\Delta^{S,D}(a)$ consists of all of its roots in K. The fact that $\Delta^{S,D}(a)$ must be the *unique* (S, D)-algebraic conjugacy class has been shown earlier in [L$_2$, (5.25)]. (Briefly, an algebraic conjugacy class must have minimal polynomial equal to $p(t)$ by an application of Cauchon's structure theory of invariant polynomials [Ca], since the assumption that $o(S) = \infty$ implies that R has no nonconstant central polynomials.) Finally, assume that S is an automorphism. Then, by [L$_2$, (2.11)(1)], every semi-invariant polynomial is a left scalar multiple of a power of $p(t)$, and is therefore an invariant polynomial. Q.E.D.

Since the result above settles all questions concerning algebraic conjugacy classes in the case when $o(S) = \infty$, we shall now work in the situation $o(S) < \infty$. This assumption implies in particular that S is an automorphism of K, and by [L$_2$, (2.11)(1)], all semi-invariant polynomials of R belong to $K[p(t)]$. Now we are ready to state and prove the main result of this paper.

(5.4) **Hilbert 90 Theorem for** (K, S, D). *Let $R = K[t, S, D]$ where $o(S) < \infty$, and let $p(t)$ be a monic semi-invariant polynomial of minimal degree $n \geq 1$ in R (we are assuming that such a polynomial exists). Let $k = o(S^n) = o(S)/(n, o(S))$, say $(S^n)^k = I_u$ (=inner automorphism sending c to ucu^{-1}). Then:*

(A) *A conjugacy class $\Delta^{S,D}(a)$ is (S, D)-algebraic iff $u^{-1}N_{k,S^n}(p(a))$ is algebraic over $Z(K)$, the center of K. Here, N_{k,S^n} denotes the kth power function with respect to $(S^n, 0)$, that is, $N_{k,S^n}(c) = S^{n(k-1)}(c)S^{n(k-2)}(c)\cdots S^n(c)c$ for every $c \in K$.*

(B) *If $\Delta^{S,D}(a)$ is an algebraic class, then for any $b \in K$ the following are equivalent:*

(1) *b is (S, D)-conjugate to a;*

(2) *$p(b)$ is S^n-conjugate to $p(a)$;*

(3) *$u^{-1}N_{k,S^n}(p(b))$ is conjugate (in the classical sense) to $u^{-1}N_{k,S^n}(p(a))$.*

(4) *$u^{-1}N_{k,S^n}(p(b))$ is algebraic over $Z(K)$ and has the same minimal polynomial over $Z(K)$ as $u^{-1}N_{k,S^n}(p(a))$.*

Proof. (A) Since $p(t)c = S^n(c)p(t)$ for every $c \in K$ and $S^{nk} = I_u$, we get $u^{-1}p(t)^k c = u^{-1}S^{nk}(c)p(t)^k = cu^{-1}p(t)^k$. Thus, $u^{-1}p(t)^k$ commutes with all scalars, i.e. it is a cv-polynomial with respect to $(I, 0)$. Applying Theorem 4.7, we see that $\Delta^{S,D}(a)$ is (S, D)-algebraic iff

$$(u^{-1}p^k)(\Delta^{S,D}(a)) = \Delta^{I,0}(u^{-1}(p^k)(a)) = \{bu^{-1}(p^k)(a)b^{-1} : b \in K^*\}$$

is $(I, 0)$-algebraic, i.e. iff $u^{-1}(p^k)(a)$ is algebraic over $Z(K)$ (by (5.1)). It now remains to calculate $(p^k)(a)$. Thinking of $p(t)^k$ as $g \circ p$ where $g(t') = t'^k \in$

$K[t', S^n]$, we see by the Composite Function Theorem 2.3 that $(p^k)(a)$ is the evaluation of $t'^k \in K[t', S^n]$ at $p(a)$, that is, $N_{k,S^n}(p(a))$. This proves (A).

To prove (B), let us now assume that $\Delta^{S,D}(a)$ is algebraic, and let $b \in K$. Noting that (3) $\Leftrightarrow$ (4) follows form (5.2), we need only prove the equivalence of (1), (2) and (3). Since the minimal polynomial of $\Delta^{S,D}(a)$ is invariant, it belongs to $K[p(t)]$ by [L$_2$, (2.9)], so we are in a position to apply Corollary 4.14. This gives immediately the equivalence (1) $\Leftrightarrow$ (2). The proof of (2) $\Leftrightarrow$ (3) is done similarly, by making a transfer from $R' = K[t', S^n]$ to $R'' = K[t'']$, using the cv-polynomial $u^{-1}t'^k$ in R' with respect to $(I, 0)$. The S^n-conjugacy class in question is now $\Delta^{S^n}(p(a))$. Depending on whether $p(a)$ is zero, it is necessary to go into two cases.

Case (i). $p(a) = 0$. In this case, $p(b)$ being S^n-conjugate to $p(a)$ simply means that $p(b) = 0$. But also $u^{-1}N_{k,S^n}(p(b))$ being conjugate to

$$u^{-1}N_{k,S^n}(p(a)) = 0$$

amounts to $p(b) = 0$, since S is injective. Therefore, (2) $\Leftrightarrow$ (3) is clear in this case.

Case (ii). $p(a) \neq 0$. Let $g(t') = \sum_{i=0}^r b_i t'^i \in R'$ be the minimal polynomial of $\Delta^{S^n}(p(a))$, where $r \geq 1$, and $b_r = 1$. We have a complete factorization $g(t') = (t' - c_1)\cdots(t' - c_r)$, where the c_i's are suitable elements in $\Delta^{S^n}(p(a))$ (see [La, Lemma 5]). Since $p(a) \neq 0$, we have $c_i \neq 0$ for all i, and therefore

$$b_0 = (-1)^r c_1 \cdots c_r \neq 0. \tag{5.5}$$

We now make the crucial claim that

$$g(t') \in K[u^{-1}t'^k] = K[t'^k]. \tag{5.6}$$

Once we have proved this claim, the transfer argument from $K[t', S^n]$ to $K[t'']$ indicated above will go through, and we will have (2) $\Leftrightarrow$ (3) by (4.14). To prove (5.6), we use the fact that $g(t')$ is (semi-)invariant in $K[t', S^n]$, which gives $g(t')c = (S^n)^r(c)g(t')$ for every $c \in K$. Comparing the left coefficients of t'^i, we get $b_i(S^n)^i(c) = (S^n)^r(c)b_i$. Upon replacing c by $S^{-ni}(c)$, this transforms into $b_i c = S^{n(r-i)}(c)b_i$, for every c. Therefore, whenever $b_i \neq 0$, we have $(S^n)^{(r-i)} = I_{b_i}$; since $o(S^n) = k$, this implies that $k|(r-i)$. In particular, by (5.5), we see that $k|r$, and consequently, whenever $b_i \neq 0$, we must have $k|i$ also. This shows that $g(t')$ has the form $b_0 + b_k t'^k + b_{2k}t'^{2k} + \cdots$; in other words, $g(t') \in K[t'^k]$;. This proves our claim (5.6). Q.E.D.

Remark 5.7. Conceptually, the equivalence (1) $\Leftrightarrow$ (3) amounts essentially to a direct transfer from $K[t, S, D]$ to $K[t'']$ by using the cv-polynomial $u^{-1}p(t)^k$ with respect to $(I, 0)$. However, to justify this transfer procedure, we would need to know that the minimal polynomial of $\Delta^{S,D}(a)$ belongs to $K[u^{-1}p(t)^k] = K[p(t)^k]$, which is not always true. In the proof given above, we have shown basically that this is true if $p(a) \neq 0$ (and we provided an easy argument to deal separately with the case $p(a) = 0$). But, instead of working with the minimal polynomial of $\Delta^{S,D}(a)$ in $K[t, S, D]$, it is easier and more natural to work with the minimal polynomial of $p(a)$ in $K[t', S^n]$. Therefore, we have chosen to "break up" the transfer (first from $K[t, S, D]$ to $K[t', S^n]$ and then from $K[t', S^n]$ to $K[t'']$), and prove (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) instead of proving directly (1) $\Leftrightarrow$ (3).

Remark 5.8. To properly understand (5.4)(B), it is important to say something about the role of the hypothesis that $\Delta^{S,D}(a)$ be an *algebraic* class. An analysis of the proof of (5.4) shows that, without assuming the algebraicity of $\Delta^{S,D}(a)$, we can still show that (1) in (5.4)(B) implies any of the other conditions. However, the *equivalence* of all these conditions is, in general, not true without the assumption on the algebraicity of $\Delta^{S,D}(a)$. In the next section, we shall give examples of triples (K, S, D) as in (5.4) for which (3) $\Leftrightarrow$ (1) fails to hold for a (necessarily nonalgebraic) (S, D)-conjugacy class $\Delta^{S,D}(a)$. In fact, there exist such counterexamples both of the automorphism type (with $D = 0$) and of the derivation type (with $S = I$), as we shall see in §6.

In §6, we shall also examine in detail the various special forms of the Hilbert 90 Theorem obtained above. Here we close this section by applying the Hilbert 90 Theorem to prove the following refinement of some theorems in [Le$_1$] and [L$_2$]. The point of this result is that it gives many examples of (K, S, D) for which *all* (S, D)-conjugacy classes are algebraic.

Theorem 5.9. *Let $R = K[t, S, D]$ be such that $o(S) < \infty$ and k is algebraic over its center. Then the following statements are equivalent:*

(1) *R is nonsimple;*

(2) *R has a nonconstant central polynomial;*

(3) *D is an algebraic derivation;*

(4) *There exists an algebraic (S, D)-conjugacy class;*

(5) *Every (S, D)-conjugacy class is algebraic;*

(6) *$[K : C^{S,D}(a)]_r < \infty$ for every $a \in K$.*

Proof. The equivalence of (1), (2) and (3) was proved in [Le$_1$, (2.4)], and (5) $\Leftrightarrow$ (6) was proved in [L$_2$, (5.10)]. (5) $\Rightarrow$ (3) and (3) $\Rightarrow$ (4) are both clear by noting that D is algebraic iff the class $\Delta^{S,D}(0)$ is algebraic [L$_2$, (5.10)]. Thus, the crucial implication we need to prove is (4) $\Rightarrow$ (5). Assume (4). Then R certainly has a nonconstant monic semi-invariant polynomial, and we can fix one, say $p(t)$, with minimal degree n. Letting $k := o(S^n) = o(S)/(n, o(S)) < \infty$, we can apply the Hilbert 90 Theorem (5.4). Since K is algebraic over its center, it follows from part (A) of this theorem that *all* (S, D)-conjugacy classes in K are algebraic. Q.E.D.

Remark 5.10. *If all (S, D)-conjugacy classes are algebraic, it can be shown that we must have $o(S) < \infty$.* In the case when there are at least two (S, D)-conjugacy classes, this follows from [L$_2$, (5.25)]. In the case when K itself constitutes a single (S, D)-conjugacy class, we would have a nonzero (S, D)-polynomial vanishing on K; in this situation, K. H. Leung has shown that K must be a finite field, so of course we will have $o(S) < \infty$. However, Leung's result is by no means easy to prove!

Corollary 5.11. *Suppose K is algebraic over $Z(K)$, and S is an automorphism of K such that $o(S) < \infty$. If D is an algebraic S-derivation, then so is $D - D_{a,S}$ for every $a \in K$. In particular (as already noted in* [Le$_2$, *p.* 23, *Corollary* 7]), *every inner S-derivation $D_{a,S}$ is algebraic.*

Proof. This follows from the theorem, in view of (1) $\Leftrightarrow$ (2) in (4.7). Q.E.D.

6. "Hilbert 90" in special cases, and counterexamples

In this section, we shall interpret our general Hilbert 90 Theorem (5.4) in various special cases, and explain why it covers the different known forms of "Hilbert 90" in the literature. First, to see why the expression $u^{-1}N_{k,S^n}(p(a))$ comes up in (5.4), it is best to begin with the special case when S and D are both inner.

Example 6.1. Suppose $S = I_u$ and $D = D_{d,S}$. Then $t-d$ is easily seen to be an invariant polynomial [L₂, (2.6)]. Using the notation of (5.4), we can choose $p(t) = t-d$ so we have $n = k = 1$ here. The expression $u^{-1}N_{k,S^n}(p(a))$ is now simply $u^{-1}(a-d)$. Theorem 5.4(A) says in this case that $\Delta^{S,D}(a)$ is algebraic iff $u^{-1}(a-d)$ is algebraic over $Z(K)$. (For instance, using (4.7), it follows that $D_{d,S}$ is algebraic iff $u^{-1}d$ is algebraic over $Z(K)$.) If $\Delta^{S,D}(a)$ is algebraic, (5.4)(B) says that $b \in K$ is (S, D)-conjugate to a iff $u^{-1}(b-d)$ is conjugate (in the classical sense) to $u^{-1}(a-d)$. The latter statement can be checked directly as follows. For b to be in $\Delta^{S,D}(a)$, we need the existence of $c \in K^*$ such that

$$\begin{aligned} b &= S(c)ac^{-1} + D(c)c^{-1} \\ &= ucu^{-1}ac^{-1} + [dc - S(c)d]c^{-1} \\ &= ucu^{-1}ac^{-1} + d - ucu^{-1}dc^{-1}, \end{aligned}$$

or equivalently, $u^{-1}(b-d) = c[u^{-1}(a-d)]c^{-1}$. So b is (S, D)-conjugate to a iff $u^{-1}(b-d)$ is conjugate (in the classical sense) to $u^{-1}(a-d)$, as predicted by (5.4)(B).

Example 6.2. Here we look at the case when $D = 0$ and $o(S) = k < \infty$. Since the polynomial t is obviously invariant, we can choose $p(t) = t$, so $n = 1$, and $(S^n)^k = S^k = I_u$ for some $u \in K^*$. The expression $u^{-1}N_{k,S^n}(p(a))$ is now $u^{-1}S^{k-1}(a)\cdots S(a)a$. So we get from (5.4):

(6.2)(A) *$\Delta^S(a)$ is algebraic iff $u^{-1}S^{k-1}(a)\cdots S(a)a$ is algebraic over $Z(K)$. In particular, letting $a = 1$ and using* [L₂, (5.17)], *we see that S is algebraic (as an endomorphism of K) iff $\Delta^S(1)$ is algebraic, iff u is algebraic over $Z(K)$.*

(6.2)(B) *Assume $\Delta^S(a)$ is algebraic. Then $b \in K$ can be written in the form $S(c)ac^{-1}$ for some $c \in K^*$ if and only if $u^{-1}S^{k-1}(b)\cdots S(b)b$ is conjugate (in the classical sense) to $u^{-1}S^{k-1}(a)\cdots S(a)a$. In particular, if u is algebraic over $Z(K)$, then $b \in K$ has the form $S(c)c^{-1}$ for some $c \in K^*$ iff $S^{k-1}(b)\cdots S(b)b$ is a commutator of the form $udu^{-1}d^{-1}$ for some $d \in K^*$.*

If $u = 1$ and K is a field, (6.2)(B) gives back the original form of the Hilbert 90 Theorem. If $u = 1$, K is a division ring, and $S^{k-1}(a)\cdots S(a)a$ is assumed to be in $Z(K) \cap K^S$, the first statement of (6.2)(B) was obtained by Jacobson in [J₃, Theorem 27] (see also [Co, p. 68] for the special case $a = 1$). Thus, (6.2)(B) improves Jacobson's Theorem 27 in two ways. First, since $u = 1$ in Jacobson's Theorem, the S there has finite order k in the group of automorphisms of K, and it generates the Galois group of the outer cyclic extension K/K^S. But in (6.2)(B), S is only assumed to have finite *inner* order, and it may not have finite order. Secondly, instead of assuming

$S^{k-1}(a)\cdots S(a)a \in Z(K)\cap K^S$, we need only assume that $S^{k-1}(a)\cdots S(a)a$ is algebraic over $Z(K)$.

Note that the "necessity' part of the main statement in (6.2)(B) can be easily checked directly, *without any condition on u.* In fact, if b has the form $S(c)ac^{-1}$ for some $c\in K^*$, then

$$\begin{aligned}
&u^{-1}S^{k-1}(b)\cdots S(b)b\\
&\qquad = u^{-1}S^{k-1}(S(c)ac^{-1})S^{k-2}(S(c)ac^{-1})\cdots S(S(c)ac^{-1})S(c)ac^{-1}\\
&\qquad = u^{-1}S^{k}(c)S^{k-1}(a)S^{k-2}(a)\cdots S(a)ac^{-1}\\
&\qquad = u^{-1}ucu^{-1}S^{k-1}(a)\cdots S(a)ac^{-1}\\
&\qquad = c[u^{-1}S^{k-1}(a)\cdots S(a)a]c^{-1}.
\end{aligned}$$

However, for the converses of the two statements in (6.2)(B) to be true, the assumption that $\Delta^s(a)$ is an *algebraic* class turns out to be essential. To see this, let us first record the following consequence of (6.2)(B) which is a familiar result in the field case.

Corollary 6.3. *Let S be an algebraic automorphism of a division ring K with inner order $k := o(S) < \infty$. then, for any kth root of unity $\omega \in K$ fixed by S, there exists $c\in K^*$ such that $S(c) = \omega c$. In particular, if k is even, there exists $c_0 \in K^*$ such that $S(c_0) = -c_0$.*

Proof. As we have already pointed out, the algebraicity of S means that $\Delta^S(1)$ is an algebraic class. Since $S^{k-1}(\omega)\cdots S(\omega)\omega = \omega^k = 1$, (6.2)(B) applied to $a = 1$ implies the existence of $c \in K^*$ such that $\omega = S(c)c^{-1}$. In the case when k is even, the last statement of the corollary follows by applying the above to $\omega = -1$. Q.E.D.

The assumption that S is an *algebraic* automorphism is essential in (6.3). To see this, let us construct a pair (K, S) where S has inner order $k = 2$ (but is not algebraic), and $S(c) \neq -c$ for every $c\in K^*$. For such a pair (K, S), the element $\omega = -1$ satisfies $S(\omega)\omega = 1$, but ω cannot be written in the form $S(c)c^{-1}$ for any $c \in K^*$, so $\omega \notin \Delta^S(1)$. This will then provide a counterexample to (6.2)(B) in the case where $a = 1$ and $\Delta^S(1)$ is not an algebraic class. The following construction of (K, S) is adapted from the last example given in §5 of [L4]. Let L be any field of characteristic not two, and let $F = L(\{x_i : i \in \mathbf{Z}\})$. Let σ be the L-automorphism of F defined by $\sigma(x_i) = x_{i+1}$ for any $i\in \mathbf{Z}$. Then let K be the division ring of twisted Laurent series $F((u, \sigma^2))$ (in which $ux_i = \sigma^2(x_i)u = x_{i+2}u$). We can extend σ to an automorphism S of K by defining $S(u) = u$. Then $S^2(x_i) = x_{i+2} = ux_iu^{-1}$, and $S^2(u) = u = uuu^{-1}$. This gives $S^2 = I_u$, and we have shown in [L4, end of §6] that S is not inner, so $k = o(S) = 2$. To show that $S(c) \neq -c$ for every $c \in K^*$ is reduced easily to showing that $\sigma(f) \neq -f$ for every $f\in F^*$. Since σ shifts the subscripts of all the variables $\{x_i : i \in \mathbf{Z}\}$ by one, clearly $S(f) = -f$ is possible only when f is a constant in L. However, σ is the identity on L and $\operatorname{char} L \neq 2$, so indeed $S(f) = f \neq -f$ for every $f \in L^*$. This shows that $\omega = -1$ *cannot* be expressed in the form $S(c)c^{-1}$ for any $c\in K^*$. Here, the element $u \in K^*$ is (necessarily) transcendental over $Z(K) = L$, and so S is not an algebraic automorphism of K by (6.2)(A).

Example 6.4. Let us now look at the case when $S = I$. Here we have $k = 1$ and $u = 1$. We still need to assume that R is nonsimple so that the polynomial $p(t)$ in (5.4) exists. The expression $u^{-1}N_{k,S^n}(p(a))$ now simplifies to $p(a)$, so we have:

(6.4)(A) $\Delta^D(a)$ *is algebraic iff* $p(a)$ *is algebraic over* $Z(K)$; *and*

(6.4)(B) *If* $\Delta^D(a)$ *is algebraic, then* $b \in K$ *can be written in the form* $cac^{-1} + D(c)c^{-1}$ *for some* $c \in K^*$ *iff* $p(b)$ *is conjugate* (*in the classical sense*) *to* $p(a)$.

Recalling that D is algebraic iff $\Delta^D(0)$ is algebraic, we have in particular the following special case of (6.4)(A):

(6.4)(A′) D *is algebraic iff the constant term of* $p(t)$ *is algebraic over* $Z(K)$.

This may seem a little surprising at first sight, but we can "explain" it as follows. Let $p(t) = \sum c_i t^i$. The semi-invariance of $p(t)$ means here that $p(t)c = cp(t)$ for every $c \in K$, so we have an operator equation $p(D)\lambda_c = \lambda_c p(D)$, where λ_c means left multiplication by c on K. Applying this to the element 1, we get $\sum_{i\geq 1} c_i D^i(c) + c_0 c = cc_0$, so $\sum_{i\geq 1} c_i D^i = D_{-c_0,I}$. This shows that D is a quasi-algebraic derivation (see [Le], [L$_2$, §3]), and, from this equation, it is no longer surprising that D is algebraic iff c_0 is algebraic over $Z(K)$.

Of course, the particular form of the polynomial $p(t)$ used above will depend on the specific pair (K, D) we are working with. In the case when $\operatorname{char} K = 0$, we know that $p(t)$ must have the form $t - d$ (if it exists), since R can be nonsimple only if D is inner [A$_2$]. This takes us back to the situation of Example (6.1), so we need not consider this case further. Let us now consider the case when $\operatorname{char} K = p > 0$. In this case, we know that, up to an additive constant, $p(t)$ is a so-called p-polynomial, i.e. $p(t)$ has the form $\sum_{i=0}^m d_i t^{p^i} - d$, with $d_m = 1$ (see [L$_2$, (3.11)(2)]). Writing N_j for the jth power function with respect to (I, D), (6.4)(B) is then valid with $p(a) = \sum d_i N_{p^i}(a) - d$ and $p(b) = \sum d_i N_{p^i}(b) - d$. In particular, for $a = 0$, we have the following characterization for the class $\Delta^D(0)$ consisting of the so-called logarithmic derivatives $\{D(c)c^{-1} : c \in K^*\}$:

(6.4)(B′) *For an algebraic derivation* D, *an element* $b \in K$ *is a logarithmic derivative iff* $\sum d_i N_{p^i}(b) - d$ *is conjugate* (*in the classical sense*) *to* $-d$.

Note that here the semi-invariant polynomial $p(t)$ may have degree less than that of the minimal polynomial of D, so the criterion for the logarithmic derivatives obtained in (6.4)(B′) is *not* the same as that in [Le$_3$, Proposition 1] (or in [L$_2$, (5.11)]). To compare (6.4)(B′) with the known results, it is best to assume now that K *is a field.* In this case, $\sum_{i=0}^m d_i D^{p^i} = D_{d,I} = 0$, so D is automatically an algebraic derivation. In fact, the minimal polynomial $g(t)$ of D is exactly $\sum_{i=0}^m d_i t^{p^i}$ (see, e.g. [L$_4$, (3.13)]). so (6.4)(B′) gives back the characterization in the references cited above:

(6.4)(B″) $b \in K$ *is a logarithmic derivative iff* $g(b) := \sum_{i=0}^m d_i N_{p^i}(b) = 0$.

This turns out to be just the same as Jacobson's characterization of logarithmic derivatives quoted in (1.3), since Jacobson has shown in [J$_1$] that $N_{p^i}(b)$ in this case is just $b^{[p^i]}$ as defined in (1.3). However, this fact does not seem to be well-known, so it behooves us to give a direct explanation here. In [J$_2$,

p. 190], it is shown that, in $K[t, D]$, one has the following noncommutative analogue of the Frobenius formula:

$$(t+b)^p = t^p + b^p + D^{p-1}(b) \quad (\forall b \in K).$$

By a suitable induction (using, for instance, the fact that $t^p \in K[t, D]$ is a cv-polynomial with respect to (I, D^p)), one can further show that

$$(6.5) \qquad \begin{gathered} (t+b)^{p^i} = t^{p^i} + b^{[p^i]}, \quad \text{where} \\ b^{[p^i]} := b^{p^i} + (D^{p-1}(b))^{p^{i-1}} + (D^{p^2-1}(b))^{p^{i-2}} + \cdots + D^{p^i-1}(b). \end{gathered}$$

From this definition and the usual Frobenius formula, it follows that

$$(6.6) \qquad (b+c)^{[p^i]} = b^{[p^i]} + c^{[p^i]} \quad (\forall b, c \in K);$$

in particular, one has $(-b)^{[p^i]} = -b^{[p^i]}$. Replacing b by $-b$ in (6.5), we obtain then

$$(6.5)' \qquad (t-b)^{p^i} = t^{p^i} + (-b)^{[p^i]} = t^{p^i} - b^{[p^i]}.$$

Evaluating this polynomial at b and transposing, we arrive at the desired explicit computation of the p^ith power functions in this case: $N_{p^i}(b) = b^{[p^i]}$. Therefore, (6.4)(B″) boils down to Jacobson's classical criterion for logarithmic derivatives given in (1.3). Also, since $b \in \Delta^D(a) \Leftrightarrow (b-a) \in \Delta^D(0)$, and $g(b-a) = g(b) - g(a)$, (6.4)(B) gives nothing more beyond (6.4)(B″).

We close this example by computing the minimal polynomial of *any* class $\Delta^D(a)$ $(a \in K)$. By [L$_2$, (5.10)], this minimal polynomial is seen to be

$$g(t-a) = \sum d_i(t-a)^{p^i} = \sum d_i(t^{p^i} - a^{[p^i]}) = g(t) - g(a).$$

In particular, all D-conjugacy classes have the same rank p^m. For instance, if D is nilpotent with minimal polynomial $g(t) = t^{p^m}$, then the minimal polynomial of $\Delta^D(a)$ for any a is just $t^{p^m} - a^{[p^m]} = (t-a)^m$. In this case, b is D-conjugate to a iff $b^{[p^m]} = a^{[p^m]}$. If $m = 1$, for example, this boils down to $(b-a)^p + D^{p-1}(b-a) = 0$.

Example 6.7. Still assuming $S = I$, we shall construct here a concrete example of a division ring K with an algebraic derivation D such that the (B) part of the Hilbert 90 Theorem (as well as the result (4.14)) fails for a nonalgebraic D-conjugacy class. Let L be a field of characteristic p, and let σ be the L-endomorphism of $L(x)$ defined by $\sigma(x) = x^p$. Then let $K = L(x)((u, \sigma))$ be the division ring of twisted Laurent series in u over $L(x)$. It is easy to check that there is a unique (usual) derivation D on K such that $D(L(x)) = 0$ and $D(u) = u$. Since $D(u^m) = mu^{m-1}D(u) = mu^m$ (for all m), we have $D^p(u^m) = m^p u^m = mu^m = D(u^m)$. From this, it is easy to see that D has minimal equation $D^p - D = 0$. Using [L$_4$, (3.11)], we further see that $p(t) := t^p - t$ is a (nonconstant) semi-invariant polynomial of the least degree in $K[t, D]$. Since D is algebraic, (6.4)(B″) implies that $b \in K$ is a logarithmic derivative iff $N_p(b) = b$. (For instance, any $m \in \mathbf{F}_p$ satisfies this equation, so m is a logarithmic derivative; in fact, as we saw above, $m = D(u^m)(u^m)^{-1}$.) While the class $\Delta^D(0)$ is algebraic, the classes $\Delta^D(x+m)$ $(m \in \mathbf{F}_p)$ are not, since

$$p(x+m) = N_p(x+m) - (x+m) = (x+m)^p - (x+m) = x^p - x$$

is obviously not algebraic over $Z(K) = L$ for any $m \in \mathbf{F}_p$. While the equation above shows that $p(x) = p(x+1) = \cdots = p(x+(p-1))$, we claim that $x, x+1, \ldots, x+(p-1)$ determine p *distinct* D-conjugacy classes. Indeed, if $\Delta^D(x+m) = \Delta^D(x+m')$, there would exist an equation $(x+m)c = c(x+m') + D(c)$, where $c = \sum_{i=n}^{\infty} f_i u^i$, with $f_i \in L(x)$, $f_n \neq 0$. Comparing the left coefficients of u^n yields the equation $(x+m)f_n = f_n(x^{p^n} + m' + n)$, which can hold only when $n = 0$ and $m = m' \in \mathbf{F}_p$.

Some other interesting remarks may be made about the D-conjugacy classes $\{\Delta^D(x+m) \colon m \in \mathbf{F}_p\}$. Since $q(t) := t^p$ is a cv-polynomial with respect to $(I, D^p) = (I, D)$ (see [L₄, (2.20)]), the Conjugation Theorem (2.2) implies that $a \mapsto q(a) = N_p(a)$ induces a map from D-conjugacy classes to D-conjugacy classes. As it turns out, this map permutes the p classes $\{\Delta^D(x+m) \colon m \in \mathbf{F}_p\}$ cyclically. In fact, since

$$q(x+m)u = (x+m)^p u = x^p u + mu = u(x+(m-1)) + Du,$$

we see that $q(x+m)$ is D-conjugate to $x+(m-1)$, so $q(\Delta^D(x+m)) = \Delta^D(x+(m-1))$ for all m. The fact that $x+(m-1)$ and x^p+m are D-conjugate should imply that $p(x+(m-1))$ and $p(x^p+m)$ are conjugate in the classical sense, since we know that $(1) \Rightarrow (2)$ in (5.4)(B) is true without any condition on the algebraicity of the classes. Indeed, we have here $p(x+(m-1)) = x^p - x$, $p(x^p+m) = (x^p+m)^p - (x^p+m) = x^{p^2} - x^p$, and these two elements are conjugate in K since $u(x^p - x) = (x^{p^2} - x^p)u$.

References

[A₁] S. A. Amitsur, *A generalization of a theorem on linear differential equations*, Bull. Amer. Math. Soc. **54** (1948), 937–941.

[A₂] ——, *Derivations in simple rings*, Proc. London Math. Soc. 7 (1957), 87–112.

[Ba] H. Bass, *Algebraic K-theory*, Benjamin, 1968.

[Ca] G. Cauchon, *Les T-anneaux et les anneaux à identités polynomiales noethériens*, Thèse, Orsay, 1977.

[Co] P. M. Cohn, *Skew field constructions*, London Math. Soc. Lecture Notes Ser., 27, Cambridge Univ. Press, 1977.

[H] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresber. Deutsch. Math.-Verein. **4** (1987), 175–546 (See also Gesammelte Abhandlungen, Vol. 1, Chelsea, New York, 1965, pp. 63–361.

[J₁] N. Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc. 42 (1937), 206–224.

[J₂] ——, *Lectures in abstract algebra*, Vol. 3, Van Nostrand, 1964. (Reprinted as Graduate Texts in Math., Vol. 32, Springer-Verlag, Berlin, Heidelberg and New York.).

[J₃] ——, *The theory of rings* (4th printing), Math. Surveys, vol. II, Amer. Math. Soc., Providence, R.I., 1968.

[L₁] T. Y. Lam and A. Leroy, *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119** (1988), 308–336.

[L₂] ——, *Algebraic conjugacy classes and skew polynomial rings*, Perspectives in Ring Theory, (F. van Oystaeyen and L. Le Bruyn. eds.), Proc. Antwerp Conf. in Ring Theory, Kluwer Academic, Dordrecht, Boston and London, 1988, pp. 153–203.

[L₃] T. Y. Lam, K. H. Leung, A. Leroy, and J. Matczuk, *Invariant and semi-invariant polynomials in skew polynomial rings*, Ring Theory 1989 (in honor of S. A. Amitsur), (L. Rowen, ed.), Israel Math. Conf. Proc., Vol. 1, Weizmann Science Press of Israel, 1989, pp. 247–261.

[L4] T. Y. Lam and A. Leroy, *Homomorphisms between Ore extensions*, Azumaya Algebras, Actions, and Modules (D. Haile and J. Osterburg, eds.), Contemp. Math., vol. 124, Amer. Math. Soc., Providence, RI., 1992, pp. 83–110.

[La] T. Y. Lam, *A general theory of Vandermonde matrices*, Exposition. Math. **4** (1986), 193–215.

[Le] B. Lemonnier, *Dimensions de Krull et codéviations, quelques applications en théorie des modules*, Thèse, Poitiers (1984).

[Le2] A. Leroy, J.-P. Tignol, and P. van Praag, *Sur les anneaux simples différentiels*, Comm. Algebra **10** (1982), 1307–1314.

[Le2] A. Leroy, *Dérivations algébriques*, Thèse, Université de l'Etat à Mons, 1985.

[Le3] ——, *Dérivées logarithmiques pour une S-dérivation algébrique*, Comm. Algebra **13** (1985), 85–99.

[Mc] J. McConnell and J.C. Robson, *Noetherian rings*, Wiley, London and New York, 1988.

[O] O. Ore, *Theory of noncommutative polynomials*, Ann. of Math. **34** (1933), 480–508.

[Re] C. Reid, *Hilbert*, Springer-Verlag, Berlin, Heidelberg, and New York, 1970.

[Ro] L. Rowen, *Ring theory*, Vol. I, Academic Press, New York, 1988.

Department of Mathematics, University of California, Berkeley, California 94720

Département de Mathematiques, Université de Valenciennes, 59,326 Valenciennes, France