Homomorphisms Between Ore Extensions

T. Y. Lam[1], University of California, Berkeley, Ca 94720
A. Leroy[1], Univ. de Valenciennes, 59.326 Valenciennes, France

Contents

§1. Introduction

The principal object of study in this paper is the Ore extension (*a.k.a.* skew polynomial ring) $K[t, S, D]$ over a division ring K. Here S is an endomorphism of K, and D is an S-derivation on K, that is, $D : K \longrightarrow K$ 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 $a \in K$. Since the introduction of the ring $K[t, S, D]$ by Ore [O_1] in 1933, there has been an extensive literature on its structure and applications (often for more general coefficient rings K). Modern introductions to the basic facts on Ore extensions can be found in the books [Co], [Mc], [Ro] and [JS], among others.

So far, the theory of Ore extensions has been focused on the study of one extension at a time. However, a careful look at some basic examples suggests that it is also important to study "transformations" from one Ore extension to another. In this paper, we shall formalize this idea and make the first systematic attempt to study homomorphisms between Ore extensions. As is easily seen, a K-homomorphism ϕ from one Ore extension $K[t', S', D']$ to another $K[t, S, D]$ is determined by $p(t) := \phi(t') \in K[t, S, D]$, which must

[1]Both authors supported in part by NSF

satisfy: $p(t)a = S'(a)p(t) + D'(a)$ in $K[t,S,D]$, for every $a \in K$. Such a polynomial $p(t)$ enables us to make a "change of variables" (from t' to t), so we shall call $p(t)$ a *change-of-variable polynomial* (or cv-polynomial for short). More precisely, we call $p(t) \in K[t,S,D]$ a cv-polynomial with respect to (S',D'). Whenever such a polynomial is given, we get a unique K-homomorphism $\phi: K[t',S',D'] \longrightarrow K[t,S,D]$ sending t' to $p(t)$, namely, for $g(t') = \sum b_i t'^i \in K[t',S',D']$, we have $\phi(g) = \sum b_i p(t)^i$. If the cv-polynomial $p(t)$ is not a constant, the associated K-homomorphism ϕ is easily seen to be an injection. In this case, we can identify $K[t',S',D']$ with $im\ \phi = K[p(t)]$, the subring of $K[t,S,D]$ generated by $p(t)$ over K. We shall speak of $K[p(t)]$ as an *Ore subextension* of $K[t,S,D]$.

Some precursors for the notion of cv-polynomials are those of invariant and semi-invariant polynomials. A polynomial $f(t) \in K[t,S.D]$ is said to be *right invariant* [2] if $f(t)K[t,S,D] \subseteq K[t,S,D]f(t)$, and *right semi-invariant*[2] if $f(t)K \subseteq K\,f(t)$. These polynomials arise naturally in the study of the ideals of $K[t,S,D]$, the minimal polynomials of algebraic (S,D)-conjugacy classes of K, and the algebraicity (and quasi-algebraicity) of the derivation D (see [Am], [Ca], [Le], [L_2] and [L_3]). Clearly, invariant polynomials are semi-invariant, and semi-invariant polynomials are exactly the cv-polynomials with respect to $(S',0)$ for some S'. Therefore, the theory of semi-invariant polynomials developed in [L_2], [L_3] can be used as a model for the new theory of cv-polynomials.

Let us now give a summary of the results in this paper. In §2, after giving examples of cv-polynomials, we study their general properties and characterizations. It is shown that *a polynomial $p(t) \in K[t,S,D]$ is a cv-polynomial iff* $p(t)K \subseteq K\,p(t) + K$; moreover, if $p(t)$ is not a constant, then $p(t)$ is a cv-polynomial with respect to a *uniquely determined* pair (S',D'). Another criterion for $p(t) = b_n t^n + \cdots + b_0$ to be a cv-polynomial in $K[t,S,D]$ is that the coefficient vector $(b_1,\cdots,b_n)$ of $p(t)$ (without b_0) be a common "left eigenvector" for a certain family of $n \times n$ matrices canonically associated with (K,S,D).

In §3, we study the relationship between cv- and semi-invariant polynomials by using the division process. It is shown that, *if we divide a cv-polynomial by a semi-invariant polynomial, then the remainder is a cv-polynomial, and if S is an automorphism, then the quotient is a semi-invariant polynomial.* This essentially reduces the consideration of cv-polynomials to that of semi-invariant polynomials together with cv-polynomials with degree less than that of a "minimal" non-constant semi-invariant polynomial (if it exists). In this section, we also obtain sharp quantitative information on the possible degrees of cv-polynomials in $K[t,S,D]$, in the case when S and D commute.

Using earlier results from [L_3] and [Le_1], existence and uniqueness theorems on cv-polynomials are obtained in §4. For instance, if $K[t,S,D]$ is a simple ring, then the cv-polynomials attached to any fixed (S',D') are determined up to an additive constant. In the existence direction, we show that $K[t,S,D]$ *has a non-linear cv-polynomial iff*

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

the S-derivation D is "cv-algebraic", in the sense that there exist constants $b_1, \cdots, b_n$ with $n \geq 2$, $b_n \neq 0$, such that $\sum_{i=1}^{n} b_i D^i$ is an S'-derivation for some endomorphism S' of K. This notion of cv-algebraicity for S-derivations is in direct generalization of Lemonnier's notion of quasi-algebraicity [Le], which in turn generalized the classical notion of algebraic derivations.

In the last section (§5), we study a comparison relationship among all Ore extensions over a fixed division ring K. For two such extensions R' and R, we define $R' \leq R$ if there exists an injective K-homomorphism from R' into R. (With respect to this relation, an Ore extension $K[t, S, D]$ is "minimal" exactly when D is *not* cv-algebraic.) If we have the relation $R' = K[t', S', D'] \leq R = K[t, S, D]$, it turns out that the two Ore extensions share many ring-theoretic properties. For instance, we show that *R is simple iff R' is simple, R has a non-constant central polynomial iff R' has a non-constant central polynomial, and also, (under a certain mild assumption on the inclusion map $R' \longrightarrow R$), D is algebraic iff D' is algebraic.* If $R' \leq R \leq R'$, it does not follow in general that $R' \cong R$. But if S is an automorphism of infinite inner order (see below), or if D is not a quasi-algebraic derivation, we show that $R' \leq R \leq R'$ does imply $R' \cong R$. Toward the end of §5, we investigate circumstances under which we can conclude that, if $p(t)$ is a non-linear cv-polynomial of minimal degree in $K[t, S, D]$, then any non-linear cv-polynomial $P(t)$ is expressible as a polynomial in $p(t)$ (i.e. $P(t) \in K[p(t)]$). It turns out that, under certain fairly general sufficient conditions, this can be guaranteed to happen. If this is the case, $K[p(t)]$ will, in fact, be the (unique) largest Ore subextension of $K[t, S, D]$.

In a sequel [L_4] to this paper, we shall present further aspects of the theory of cv-polynomials, prove a Composite Function Theorem for the evaluation of skew polynomials at constants, and apply the notion of cv-polynomials to derive new versions of Hilbert 90 Theorems for division rings with S-derivations.

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 to be used in the main text. If $D = 0$, we write $K[t, S]$ for $K[t, S, 0]$, and if $S = I$, we write $K[t, D]$ for $K[t, I, D]$. For $u \in K^*$, I_u denotes the inner automorphism of K associated with u, defined by $I_u(x) = uxu^{-1}$. If S is an endomorphism of K, the *inner order* of S, denoted by $o(S)$, is defined to be the smallest positive integer k such that S^k is an inner automorphism; if no such integer k exists, we take $o(S)$ to be ∞. In particular, if S is an endomorphism which is not an automorphism, we have by definition $o(S) = \infty$. 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 $x \in K$. Other standard ring-theoretic notations and terminology follow the books cited earlier in this Introduction.

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. CV-Polynomials and Their Characterizations

In the classical work on $K[t,S,D]$, it is well-recognized that in some special cases a change of variables can be used to express one Ore extension in terms of a simpler one. Two cases which immediately come to mind are the following:

(2.1) If D is S-inner, say $D = D_{c,S}$, then $K[t,S,D] = K[t-c,S]$.
(2.2) If S is an inner automorphism of K, say $S = I_u$ $(u \in K^*)$, then $K[t,S,D] = K[u^{-1}t, u^{-1}D]$.

We can look at these identifications from a slightly different point of view; namely, in both cases, we have an associated homomorphism between Ore extensions which turns out to be an isomorphism. In the case (2.1), we have $\phi : K[t',S] \longrightarrow K[t,S,D]$ defined by $\phi(\sum a_i t'^i) = \sum a_i(t-c)^i$, and in the case (2.2), we have $\psi : K[t', u^{-1}D] \longrightarrow K[t,S,D]$ defined by $\psi(\sum a_i t'^i) = \sum a_i(u^{-1}t)^i$. In each case, the change of variables is determined by an (S,D)-polynomial (respectively, $t-c$ and $u^{-1}t$) which is the image of the new variable t' from the other Ore extension.

These two basic examples suggest how we can deal with a change of variables from one Ore extension to another in general. For $R = K[t,S,D]$ and $R' = K[t',S',D']$, consider any K-homomorphism $\phi : R' \longrightarrow R$. Writing $p(t) := \phi(t') \in R$, we have $\phi(t'a) = \phi(t')\phi(a) = p(t)a$ for any $a \in K$. On the other hand, $\phi(t'a) = \phi(S'(a)t' + D'(a)) = S'(a)p(t) + D'(a)$. Therefore, we have the necessary condition:

$$p(t)a = S'(a)p(t) + D'(a) \quad \textit{for any } a \in K. \tag{2.3}$$

Conversely, if a polynomial $p(t) \in R$ is given satisfying (2.3), where S' is an endomorphism of K and D' is an S'-derivation, then we can define $\phi : R' \longrightarrow R$ by $\phi(\sum a_i t'^i) = \sum a_i p(t)^i$, and check easily that ϕ is the unique K-homomorphism from R' to R sending t' to $p(t)$. This motivates the following crucial definition:

Definition 2.4. A polynomial $p(t) \in R = K[t,S,D]$ satisfying (2.3) is called a *change-of-variable polynomial (or cv-polynomial)* with respect to (S', D'). 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').

By an easy degree argument, we see that a K-homomorphism $\phi : R' \longrightarrow R$ is *injective* iff the associated cv-polynomial $p(t) = \phi(t')$ has degree ≥ 1, and ϕ is *surjective* (respectively, *bijective*) iff $p(t)$ has degree $= 1$. These facts will be used freely in the rest of the paper.

At this time, we should remark that our requirement that $\phi : R' \longrightarrow R$ be a homomorphism over K is not strictly necessary. In general, we can deal with homomorphisms $\phi : R' \longrightarrow R$ with the property that $\theta := \phi|K$ is an automorphism of K. In this case, one can check as above that $p(t) := \phi(t')$ is a cv-polynomial with respect to (σ, δ), where $\sigma = \theta S' \theta^{-1}$ and $\delta = \theta D' \theta^{-1}$. In fact, ϕ can be factored as $\phi_1 \circ \Theta$ where $\Theta : R' \longrightarrow K[x,\sigma,\delta]$ is defined by $\Theta(\sum a_i t'^i) = \sum \theta(a_i)x^i$, and $\phi_1 : K[x,\sigma,\delta] \longrightarrow R$ is defined by $\phi_1(\sum b_i x^i) = \sum b_i p(t)^i$. The latter map ϕ_1 here is a K-homomorphism. Since the homomorphism Θ can be handled separately, it is sufficient to work with the

K-homomorphism ϕ_1. Therefore, we shall focus our attention on K-homomorphisms in this paper. *All homomorphisms between Ore extensions considered below will be assumed to be K-homomorphisms.*

Let us now give a few more examples of changing variables beyond the classical ones in (2.1) and (2.2).

(2.5) For $R = K[t]$ and $R' = K[t']$, the cv-polynomials in R with respect to $(I, 0)$ are exactly the polynomials in the center of R.

(2.6) The constant polynomial $p(t) = c \in K \subset R$ is a cv-polynomial with respect to (S', D') iff $ca = S'(a)c + D'(a)$ for all $a \in K$, that is, iff $D' = D_{c,S'}$. In particular, any constant polynomial in R is a cv-polynomial. Notice that here S' is completely arbitrary, while D' is uniquely determined by S' and c.

(2.7) For any linear polynomial $p(t) = ut + c$ $(u \in K^*)$, a routine calculation shows that $(ut+c)a = S'(a)(ut+c) + D'(a)$ where $S' = I_u \circ S$ and $D' = uD + D_{c,S'}$. Therefore, $p(t)$ is a cv-polynomial with respect to (S', D').

(2.8) Let $p(t) = \sum b_i t^i$ be a semi-invariant polynomial of degree n. Then for any $a \in K$, $p(t)a = cp(t)$ for some c, and a comparison of the (left) coefficient of t^n gives $c = b_n S^n(a) b_n^{-1}$, so $p(t)$ is a cv-polynomial with respect to $(I_{b_n} \circ S^n, 0)$. Conversely, any cv-polynomial with respect to any $(S', 0)$ is clearly a semi-invariant polynomial.

(2.9) Let $p(t)$, $q(t) \in R$ be cv-polynomials with respect to (S', D') and (S', D''). Then $p(t) + q(t)$ is also a cv-polynomial, with respect to $(S', D' + D'')$. From this, it follows easily that, over a field K, the sum of any two cv-polynomials in $K[t, D]$ of the same degree is another cv-polynomial.

(2.10) For $p(t) = t^2 + c \in R = K[t, S, D]$, an easy computation gives

$$p(t)a = S^2(t)p(t) + [DS(a) + SD(a)]t + (D^2 + D_{c,S^2})(a),$$

for any $a \in K$. Therefore, if $p(t)$ is a cv-polynomial, we must have $SD = -DS$; and conversely, if $SD = -DS$, then $p(t)$ is a cv-polynomial with respect to $(S^2, D^2 + D_{c,S^2})$.

(2.11) If K is a field of characteristic $p > 0$, and $R = K[t, D]$, then any "p-polynomial"[3] $\sum b_i t^{p^i}$ in R is a cv-polynomial, with respect to $(I, \sum b_i D^{p^i})$. A fuller discussion of this type of examples can be found at the end of this section.

Recall that an S-derivation D is said to be *algebraic* if there exists a nonzero polynomial $g(t) \in R$ such that $g(D) = 0$. Here, the evaluation of a polynomial $g(t) = \sum a_i t^i \in R$ at D is defined to be the operator $g(D) = \sum a_i D^i$ on K. Our next few results deal with the characterizations of cv-polynomials. The first result says in particular that, if $p(t) \in R$ is a non-constant cv-polynomial with respect to (S', D'), then S' and D' are uniquely determined by $p(t)$.[4]

[3]This terminology is due to Ore; see [O_2].

[4]If $p(t)$ is a *constant* polynomial instead, then, by (2.6), D' is uniquely determined, but S' is completely arbitrary.

Theorem 2.12. *Let $p(t) = \sum b_i t^i \in R$ be of degree $n \geq 0$, and let D' be any S'-derivation.*
(1) If $p(t)$ is a cv-polynomial with respect to (S', D'), then $D' = (p - b_0)(D) + D_{b_0,S'}$, and if $n \geq 1$, then $S' = I_{b_n} \circ S^n$.
(2) If D is not an algebraic derivation, then $p(t)$ is a cv-polynomial with respect to (S', D') iff $D' = (p - b_0)(D) + D_{b_0,S'}$.

Proof. Consider the homomorphism $\lambda : R \longrightarrow End(K, +)$ defined by $\lambda(t) = D$, and for $a \in K$, $\lambda(a) =$left multiplication by a on K. If $p(t)$ is a cv-polynomial with respect to (S', D'), the equation $p(t)a = S'(a)p(t) + D'(a)$ in R leads to an operator equation $p(D)\lambda(a) = \lambda(S'(a))p(D) + \lambda(D'(a))$. Evaluating at the element 1, we get $p(D)(a) = S'(a)p(D)(1) + D'(a) = S'(a)b_0 + D'(a)$, since $D^i(1) = 0$ for $i \geq 1$. Therefore, $D'(a) = (p - b_0)(D)(a) + D_{b_0,S'}(a)$, as desired. If $n \geq 1$, a comparison of the left coefficients of t^n in the equation $p(t)a = S'(a)p(t) + D'(a)$ gives $b_n S^n(a) = S'(a)b_n$ for every $a \in K$, so we get $S' = I_{b_n} \circ S^n$. For (2), we need only prove the "if" part, assuming that D is not algebraic. Let $q(t) = p(t) - b_0$. If $D' = q(D) + D_{b_0,S'}$, then $q(D) = D' - D_{b_0,S'}$ is an S'-derivation, so for any $a, b \in K$, we have $q(D)(ab) = S'(a)q(D)(b) + q(D)(a) \cdot b$. Therefore, we have an operator equation

$$q(D)\lambda(a) = \lambda(S'(a))q(D) + \lambda(q(D)(a)) \quad (\forall\, a \in K), \tag{2.13}$$

which holds in the image of λ. Since D is not algebraic, λ is injective, so (2.13) pulls back to a polynomial equation $q(t)a = S'(a)q(t) + q(D)(a)$. Therefore,

$$(p(t) - b_0)a = S'(a)(p(t) - b_0) + (D' - D_{b_0,S'})(a) = S'(a)p(t) + D'(a) - b_0 a,$$

and cancellation of the term $b_0 a$ shows that $p(t)$ is a cv-polynomial with respect to (S', D'). **Q.E.D.**

Part (1) of the above Theorem allows us to speak about non-constant cv-polynomials without reference to (S', D'). It also justifies the second part of Def. (2.4). We should note, however, that if D *is* algebraic, the sufficiency part in (2.12)(2) fails in general. For instance, if *char* $K = 2$, $S = S' = I$, $D' = 0$, and $D \neq 0 = D^2$, the polynomial $p(t) = t^3$ satisfies the equation in (2.12)(2), but it is not a cv-polynomial with respect to $(I, 0)$. In fact, if a is any element such that $D(a) \neq 0$, we have $t^3 a = at^3 + D(a)t^2 \neq at^3$.

Corollary 2.14. *We say that an injective homomorphism $\phi : K[t', S', D'] \longrightarrow K[t, S, D]$ is homogeneous if the associated cv-polynomial $p(t) := \phi(t')$ has zero constant term. In this case, D' and D are related by the equation $D' = p(D)$. Moreover, if λ is as above, and λ' is the corresponding map for the ring $K[t', S', D']$, then we have a commutative diagram:*

$$\begin{tikzcd} K[t', S', D'] \arrow[rr, "\phi"] \arrow[dr, "\lambda'"'] & & K[t, S, D] \arrow[dl, "\lambda"] \\ & End(K, +) & \end{tikzcd}$$

Proof. Setting $b_0 = 0$ in (2.12)(1), we get $D' = p(D)$. From this, we get $\lambda'(t') = D' = p(D) = \lambda(p(t)) = \lambda(\phi(t'))$. Since $K[t', S', D']$ is generated by K and t', the commutativity relation $\lambda' = \lambda \circ \phi$ follows. **Q.E.D.**

Generally speaking, the consideration of (injective) homomorphisms between Ore extensions can be reduced to the consideration of homogeneous ones. This is shown in the corollary below.

Corollary 2.15. *If there is an injection ϕ from $R' = K[t', S', D']$ to $R = K[t, S, D]$ (defined by a cv-polynomial $p(t) = \phi(t')$), then there is an Ore extension $R'' = K[t'', S', D'']$ with an isomorphism $\sigma : R' \longrightarrow R'$ such that R'' admits a homogeneous injection ϕ_1 into R satisfying $\phi = \phi_1 \circ \sigma^{-1}$. If $p(t)$ happens to have a root $c \in K$,[5] then there is also an Ore extension $\overline{R} = K[\overline{t}, S, \overline{D}]$ with an isomorphism $\tau : \overline{R} \longrightarrow R$ such that R' has a homogeneous injection ϕ_2 into $\overline{R}$ satisfying $\phi = \tau \circ \phi_2$.*

Proof. Let b_0 be the constant term of $p(t)$. Since $(t' - b_0)a = S'(a)(t' - b_0) + (D' - D_{b_0,S'})(a)$, we can take $D'' = D' - D_{b_0,S'}$ and define the isomorphism σ in the Corollary by $\sigma(t'') = t' - b_0$. We then define ϕ_1 by $\phi_1(t'') = p(t) - b_0$, and get the desired commutativity relation $\phi = \phi_1 \circ \sigma^{-1}$. For the second part of the Corollary, suppose that $p(c) = 0$. Then we can express $p(t)$ in the form $a_n(t-c)^n + \cdots + a_1(t-c)$, for suitable constants a_i's (see Footnote (5)). Now let $\overline{D}$ be $D - D_{c,S}$ and define τ by $\tau(\overline{t}) = t - c$, and ϕ_2 by $\phi_2(t') = a_n\overline{t}^n + \cdots + a_1\overline{t}$. **Q.E.D.**

To introduce the next result, recall that, for any $a \in K$, $t^i a = \sum_{j=0}^{i} f_j^i(a)t^j$ where $f_j^i \in End(K, +)$ is the sum of all possible products with j factors of S and $i - j$ factors of D (see [L$_1$: §2]). Let $M_n(a)$ denote the $n \times n$ matrix whose (i, j)-entry is $f_j^i(a)$ $(1 \leq i, j \leq n)$, where, of course, $f_j^i(a)$ is taken to be zero if $i < j$, i.e. $M_n(a)$ is a lower triangular matrix. The next result gives, among other information, an eigenvector interpretation for the coefficient vector $(b_1, \cdots, b_n)$ of a cv-polynomial $p(t)$.

Theorem 2.16. *Let $p(t) = \sum b_i t^i \in R$ be a polynomial of degree $n \geq 0$. Then the following are equivalent:*
(1) $p(t)$ is a cv-polynomial.
(2) For any $a \in K$, and $j = 1, 2, ..., n$, we have $\sum_{i=j}^{n} b_i f_j^i(a) = b_n S^n(a) b_n^{-1} b_j$.
(3) $(b_1, \cdots, b_n)$ is a left eigenvector for each matrix $M_n(a)$ $(a \in K)$.
(4) $p(t)K \subseteq K\,p(t) + K$.
If these conditions hold, then $u\,p(t) + c$ is also a cv-polynomial, for any $u, c \in K$.

Proof. If $p(t)$ is a constant polynomial $(n = 0)$, (1), (4) always hold, and (2), (3) hold vacuously. In this case, the last statement of the Proposition is trivial, in view of (2.6). Therefore, in the following, we may assume that $n \geq 1$.

(1)$\Longrightarrow$(2) Let $p(t)$ be a cv-polynomial, say with respect to (S', D'). For any $a \in K$, we have

$$p(t)a = \sum_{i=0}^{n} b_i t^i a = \sum_{i=0}^{n} b_i \sum_{j=0}^{i} f_j^i(a)t^j = \sum_{j=0}^{n} (\sum_{i=j}^{n} b_i f_j^i(a))t^j. \tag{2.17}$$

[5]This means that $p(c) = 0$, where the evaluation of skew polynomials at constants is as defined in [L$_1$]. However, the general theory of evaluation developed in [L$_1$] is not needed here, as one can simply interpret $p(c) = 0$ as saying that $p(t)$ has a right factor $(t - c)$ in R. This is how the condition $p(c) = 0$ is used in the proof of this Corollary.

On the other hand,

$$p(t)a = S'(a)p(t) + D'(a) = b_n S^n(a) b_n^{-1} \sum_{j=0}^{n} b_j t^j + D'(a), \tag{2.18}$$

by (2.12)(1). Comparing the coefficients of t^j $(1 \le j \le n)$, we get the identities in (2). (We observe in passing that, if we compare the constant coefficients instead, we get once more the equation $D' = (p - b_0)(D) + D_{b_0,S'}$ in (2.12)(1).)

(2)$\Longrightarrow$(3) In matrix notation, the equations in (2) can be expressed in the form

$$(b_1, \cdots, b_n) M_n(a) = b_n S^n(a) b_n^{-1} (b_1, \cdots, b_n),$$

so for each $a \in K$, $(b_1, \cdots, b_n)$ is a left eigenvector for $M_n(a)$ with eigenvalue $b_n S^n(a) b_n^{-1}$.

(3)$\Longrightarrow$(4) For each $a \in K$, we have $(b_1, \cdots, b_n) M_n(a) = \beta(a)(b_1, \cdots, b_n)$ for some "eigenvalue" $\beta(a) \in K$. Therefore, for $1 \le j \le n$, we have $\sum_{i=j}^{n} b_i f_j^i(a) = \beta(a) b_j$. Applying this to the equation (2.17) (after isolating the constant term), we have

$$p(t)a \in \sum_{j=1}^{n} \beta(a) b_j t^j + K \subseteq K\,p(t) + K, \quad \textit{for any } a \in K.$$

(4)$\Longrightarrow$(1) For any $a \in K$, we have uniquely determined constants $a_1, a_2 \in K$ such that $p(t)a = a_1 p(t) + a_2$. (Here we need to use the assumption that $n \ge 1$.) Define $S'(a) = a_1$ and $D'(a) = a_2$. Using the associativity of R, it is easy to check that S' is an endomorphism of K, and D' is an S'-derivation of K. Therefore, $p(t)$ is a cv-polynomial, with respect to (S', D').

The last part of the Theorem follows now by an application of the criterion (4), since we have $(u\,p(t) + c)K \subseteq u(K\,p(t) + K) + cK \subseteq K(u\,p(t) + c) + K$. **Q.E.D.**

Because of the last part of (2.16), it is usually sufficient to work with *monic* cv-polynomials. The characterization (4) for cv-polynomials is perhaps simplest and the most handy. It suggests, in fact, that we can define a notion of "cv-elements" in K-rings. Here, following P. M. Cohn, we say that a ring A is a *K-ring* if A is given with a subring isomorphic to (and identified with) K. For an element g in such a K-ring A, let us say that g is a *(right) cv-element of A* if $gK \subseteq Kg + K$. From this general definition, it follows readily that, if $A' \subseteq A$ are K-rings, then an element $g \in A'$ is a cv-element of A' iff it is a cv-element of A. Coming back to the setting of skew polynomial rings, this observation translates into the following useful (and otherwise non-trivial) statement on cv-polynomials under a change of variables:

Corollary 2.19. *Let $\phi : K[t', S', D'] \longrightarrow K[t, S, D]$ be an injective homomorphism, with $\phi(t') = p(t)$. Then $g(t') = \sum b_i t'^i$ is a cv-polynomial in $K[t', S', D']$ iff its image $\phi(g) = \sum b_i p(t)^i$ is a cv-polynomial in $K[t, S, D]$.*

To conclude this section, let us point out some nice applications of the formulas $t^n a = \sum_{j=0}^{n} f_j^n(a) t^j$. In the special case when $SD = DS$, we have $f_j^n = \binom{n}{j} S^j D^{n-j}$. If K has characteristic $p > 0$, then $f_j^{p^i} = 0$ whenever $0 < j < p^i$, and therefore, we have $t^{p^i} a = S^{p^i}(a) t^{p^i} + D^{p^i}(a)$ for all $a \in K$. This shows that:

Example 2.20. *If $SD = DS$ and char $K = p$, then, for each $i \geq 0$, $t^{p^i} \in K[t, S, D]$ is a cv-polynomial with respect to (S^{p^i}, D^{p^i}).*

To generate more examples of this nature, let K be a field of characteristic p, and $S = I$. For any (usual) derivation D we get from the above $(\sum b_i t^{p^i})a = a(\sum b_i t^{p^i}) + (\sum b_i D^{p^i})a$ for any $a \in K$. Therefore, any "p-polynomial" $\sum b_i t^{p^i}$ is a cv-polynomial with respect to $(I, \sum b_i D^{p^i})$. More generally, the same argument shows that:

Example 2.21. *For any field K of characteristic $p > 0$, if $p(t) \in K[t, S, D]$ is any cv-polynomial with respect to (I, D'), then $\sum b_i p(t)^{p^i}$ is a cv-polynomial with respect to $(I, \sum b_i D'^{p^i})$.*

§3. Relations Between CV- and Semi-invariant Polynomials

Since cv-polynomials are generalizations of semi-invariant polynomials, it is of interest to investigate the relationship between these two classes. In the theory of semi-invariant polynomials, it is important to fix a (monic) semi-invariant polynomial of the smallest degree ≥ 1, and study the other semi-invariant polynomials via this fixed polynomial. As it turns out, this polynomial is also useful in studying the class of cv-polynomials. On the other hand, a cv-polynomial of the least degree ≥ 2 (if it exists) plays an important role too, though in general this polynomial may have lower degree than the semi-invariant polynomial of the least degree mentioned above. In this section, we shall give quantitative information on the degrees of these key polynomials, and describe some methods for the determination of cv-polynomials in general. In the case when S is an automorphism and $SD = DS$, we shall obtain rather explicit information on the structure of all cv-polynomials.

Throughout this section, we shall work inside a fixed Ore extension $R = K[t, S, D]$. Our basic tool is the following result concerning the division of a cv-polynomial by a semi-invariant polynomial in R.

Proposition 3.1. *Let $f(t) \in R$ be a monic semi-invariant polynomial of degree $m \geq 1$. Let $p(t) \in R$ with $p(t) = q(t)f(t) + r(t)$ where deg $r(t) < m$. Then:*

(1) *$p(t)$ is a cv-polynomial with respect to (S', D') iff $r(t)$ is a cv-polynomial with respect to (S', D') and $q(t)S^m(a) = S'(a)q(t)$ for all $a \in K$.*
(2) *If $p(t)$ is a left multiple of $f(t)$, then $p(t)$ is a cv-polynomial iff it is semi-invariant.*

Now assume that $p(t)$ is a cv-polynomial and that S is an automorphism. Then

(3) *$q(t)$ is semi-invariant.*
(4) *If* deg $p(t) \geq m$ *and* $r(t) \notin K$, *then* $o(S) < \infty$ *and* deg $p(t) \equiv$ deg $r(t)$ (mod $o(S)$).

Proof. (1) Assume that $p(t)$ is a cv-polynomial with respect to (S', D'). Then, for any $a \in K$, we have $p(t)a = S'(a)p(t) + D'(a) = S'(a)q(t)f(t) + [S'(a)r(t) + D'(a)]$. On the other hand, $p(t)a = q(t)f(t)a + r(t)a = q(t)S^m(a)f(t) + r(t)a$. By the uniqueness of the division algorithm, we have

$$r(t)a = S'(a)r(t) + D'(a), \quad \textit{and} \tag{3.2}$$

(3.3) $$q(t)S^m(a) = S'(a)q(t).$$

Conversely, if these equations hold for all $a \in K$, then, from the above, it also follows that $p(t)a = S'(a)p(t) + D'(a)$, so $p(t)$ is a cv-polynomial with respect to (S', D').

(2) It suffices to prove the "only if" part. If $p(t)$ is a cv-polynomial with respect to (S', D'), say, and it is a left multiple of $f(t)$, then $r(t) = 0$ in the above, and (3.2) shows that $D' = 0$. Therefore, $p(t)$ is semi-invariant.

Now assume that $p(t)$ is a cv-polynomial and that S is an automorphism.

(3) Any element of K can be expressed in the form $S^m(a)$ for some $a \in K$. From (3.3), we can then conclude that $q(t)$ is a semi-invariant polynomial.

(4) Here we assume that $n = \deg p(t) \geq m$, and that $k = \deg r(t) \geq 1$. Let b, c be respectively the leading coefficients of $p(t)$ and $r(t)$. Applying (2.12)(1) to $p(t)$ and $r(t)$, we have $S' = I_b \circ S^n = I_c \circ S^k$, and therefore $S^{n-k} = I_{b^{-1}c}$. Since $n \geq m > k$, it follows that $o(S) < \infty$ and that $n \equiv k \pmod{o(S)}$. **Q.E.D.**

Theorem 3.4. *Assume that S is an automorphism. Let $f(t)$ be a monic semi-invariant polynomial of minimal degree $m \geq 1$, and let $p(t)$ be any cv-polynomial , say of degree $n \geq 1$. Then:*
(1) $p(t)$ can be represented in the form $\sum_{i\geq 1} c_i f(t)^i + r(t)$, where $c_i \in K$ and $r(t)$ is a cv-polynomial of degree $< m$. In particular, if $n \geq m$, then $m|n$.
(2) If $o(S) = \infty$ and $n \geq m$, then $p(t)$ is the sum of a semi-invariant polynomial and a constant.
(3) If $n \leq m$, then $n|\deg P(t)$ for any cv-polynomial $P(t)$ of degree $\geq n$. In particular, if $n \leq m$, then $n|m$.

Proof. (1) We may assume that $n \geq m$, for otherwise (1) is obvious. Write $p(t) = q(t)f(t) + r(t)$, where $\deg r(t) < m$. By (3.1)(3), $q(t)$ is sem-invariant, and by [L_2:(2.9)] $q(t)$ has the form $\sum_{i\geq 1} c_i f(t)^{i-1}$. Hence $p(t) = \sum_{i\geq 1} c_i f(t)^i + r(t)$, so $n = \deg p(t) = mi_0$ for the largest i_0 with $c_{i_0} \neq 0$.

(2) If $o(S) = \infty$, then (3.1)(4) guarantees that $r(t) \in K$, so $p(t)$ is the sum of the semi-invariant polynomial $q(t)f(t)$ with the constant $r(t)$.

(3) The proof of this part will be postponed to §5 (see (5.14)). We just observe at this point that the conclusion that $n|\deg P(t)$ may not be true if we do not assume that $n \leq m$. This may be seen from the examples given near the end of this section. **Q.E.D.**

Corollary 3.5. *Assume that S is an automorphism and that D is not S-inner. Let $f(t)$ be a (monic) semi-invariant polynomial of minimal degree $m \geq 1$, and let $p(t)$ be a (monic) cv-polynomial of minimal degree $n \geq 2$ (if both exist). Then $n|deg\ P(t)$ for any non-linear cv-polynomial $P(t)$. In particular, we have $n|m$ (so, for instance, if m is a prime, then we can conclude that $n = m$.)*

Proof. In view of (2.12)(1), the fact that D is not S-inner implies that $m \geq 2$. Since $f(t)$ is a cv-polynomial (of degree ≥ 2), we have by definition $n \leq m$. Part (3) of the Theorem now gives the desired conclusions. **Q.E.D.**

Remark 3.6. If D is an S-inner derivation, say $D = D_{b,S}$, we can choose $f(t) = t - b$ and $p(t) = (t-b)^2$. Here we have $m = 1$ and $n = 2$; the Corollary obviously fails in this case since $P(t) = (t-b)^m$ is semi-invariant for any m.

Remark 3.7. Keep the notations in (3.6) (but let D be arbitrary). If n happens to be equal to m, then any cv-polynomial $P(t)$ will be the sum of a semi-invariant polynomial with a linear polynomial (and by [L_2: (2.9)], the former lies in $K[f(t)]$). This follows from (3.1) by dividing $P(t)$ by $f(t)$, and noting that the remainder is a cv-polynomial with degree $< m = n$.

Later in this section, examples will be given to show that the quantitative results on deg $f(t)$ and deg $p(t)$ obtained above are the best possible. Before we give such examples, let us point out another connection between cv-polynomials and semi-invariant polynomials given by the process of formal differentiation. This result, however, requires some mild hypotheses on S and D.

Theorem 3.8. *Assume that S is an automorphism, and that $SD = DS$. Let $p(t) = \sum_{i=0}^{n} b_i t^i$ be any cv-polynomial in R. Then the formal derivative $p_1(t) := \sum_{i=1}^{n} i b_i t^{i-1}$ is semi-invariant. More generally, $p_j(t) := \sum_{i=0}^{n-j} \binom{i+j}{j} b_{i+j} t^i$ $(1 \le j \le n)$ are all semi-invariant polynomials.*

Proof. In view of $SD = DS$, the equations in (2.16)(2) simplify to

$$\sum_{i=j}^{n} \binom{i}{j} b_i S^j D^{i-j}(a) = b_n S^n(a) b_n^{-1} b_j\,, \tag{3.9}$$

for $j = 1, \cdots, n$. Therefore

$$\begin{aligned} p_1(t)a &= \sum_{i=1}^{n} i b_i \left(\sum_{j=0}^{i-1} \binom{i-1}{j} S^j D^{i-1-j}(a) t^j \right) \\ &= \sum_{j=0}^{n-1} \left(\sum_{i=j+1}^{n} i \binom{i-1}{j} b_i S^j D^{i-1-j}(a) \right) t^j \\ &= \sum_{j=1}^{n} \left(\sum_{i=j}^{n} i \binom{i-1}{j-1} b_i S^{j-1} D^{i-j}(a) \right) t^{j-1} \\ &= \sum_{j=1}^{n} j \left(\sum_{i=j}^{n} \binom{i}{j} b_i D^{i-j} S^{j-1}(a) \right) t^{j-1}. \end{aligned}$$

Replacing a by $S(a)$, we get

$$p_1(t)S(a) = \sum_{j=1}^{n} j \left(\sum_{i=j}^{n} \binom{i}{j} b_i D^{i-j} S^j(a) \right) t^{j-1} = \sum_{j=1}^{n} j b_n S^n(a) b_n^{-1} b_j t^{j-1} = b_n S^n(a) b_n^{-1} p_1(t),$$

by (3.9). Since S is an automorphism, this shows that $p_1(t)K \subseteq K\,p_1(t)$, so $p_1(t)$ is semi-invariant, as claimed. The more general fact that $p_j(t)$ $(1 \le j \le n)$ are semi-invariant can be proved in the same way by making use of the identity $\binom{i}{j}\binom{i-1}{k-j} = \binom{k}{j}\binom{i}{i-k}$ (see [Le_3] for a similar proof). **Q.E.D.**

Remarks 3.10. (a) Formally, $p_j(t)$ is just $p^{(j)}(t)$ "divided by $j!$", where $p^{(j)}(t)$ denotes the jth classical derivative of $p(t)$. (b) The Theorem is not true in general if $SD \neq DS$, as the example in (2.10) shows.

Corollary 3.11. *Assume that S is an automorphism, and $SD = DS$. Let $p(t) \in R$ be a cv-polynomial of degree $n \geq 2$, and assume that R has no non-constant semi-invariant polynomial of degree $< n$. Then char $K = p > 0$ and $p(t)$ has the form $\sum c_i t^{p^i} + c$.*

Proof. If *char* $K = 0$, then the derivative $p_1(t)$ of $p(t)$ has degree $n-1 \geq 1$ and is semi-invariant by (3.8), contradicting the hypothesis. Therefore, we must have *char* $K = p > 0$. Since the polynomials $p_j(t)$ are all semi-invariant, they must all have degree zero. Looking at the definition of the $p_j(t)$'s, we obtain $\binom{k}{j} b_k = 0$ for every k, j such that $1 \leq j < k \leq n$. This means that $b_k \neq 0$ $(k \geq 1)$ can occur only when k is a power of p. Therefore, $p(t)$ has the form $\sum c_i t^{p^i} + c$. **Q.E.D.**

Corollary 3.12. *Let S and D be as in* (3.11).
(1) *If R is simple and $p(t)$ is any cv-polynomial of degree $n \geq 2$, then char $K = p > 0$ and $p(t)$ has the form $\sum c_i t^{p^i} + c$.*
(2) *If D is not S-inner, and R has a non-constant semi-invariant polynomial $f(t)$ of minimal degree m, then char $K = p > 0$, and $f(t)$ has the form $\sum c_i t^{p^i} + c$.*
(3) *If D is not S-inner and R has a non-linear cv-polynomial $p(t)$ of minimal degree n, then char $K = p > 0$, $n = p$, and we could have chosen $p(t)$ to be t^p. If the polynomial $f(t)$ in* (2) *exists, say of degree $m = p^s$, then the possible degrees of cv-polynomials in R are exactly: $\{0, 1, p, p^2, \cdots, p^{s-1}, p^s, 2p^s, 3p^s, \cdots\}$. If $f(t)$ does not exist, then the possible degrees of cv-polynomials in R are exactly: $\{0, 1, p, p^2, \cdots\}$.*

Proof. In Case (1), there will be no non-constant semi-invariant polynomials of any degree (see (4.5) below). Therefore, we can apply (3.11) to any cv-polynomial of degree ≥ 2. In Case (2), we must have $m \geq 2$ (as in the proof of (3.5)). Then we can apply (3.11) to $f(t)$. In Case (3), if there was a non-constant semi-invariant polynomial of degree $< n$, it is also a cv-polynomial so it must be of the form $u(t-b)$, but then $D = D_{b,S}$, which is not the case. Therefore, (3.11) again applies to give *char* $K = p > 0$. By (2.20) and (3.4)(3), we see that t^p is a non-linear cv-polynomial of minimal degree. If R has no non-constant semi-invariant polynomial, then by (3.11), any non-linear cv-polynomial has degree p^i, and conversely, by (2.20), each t^{p^i} is a cv-polynomial. Finally, suppose R has a non-constant semi-invariant polynomial $f(t)$ of minimal degree m. By (2), $m = p^s$ for some $s \geq 1$. Then the powers $f(t)^j$ are certainly cv-polynomials (since they are semi-invariant), so we have cv-polynomials of all degrees from the set $\{0, 1, p, p^2, \cdots, p^{s-1}, p^s, 2p^s, 3p^s, \cdots\}$. Conversely, by (3.4)(1) and (3.11), these are the only possible degrees of cv-polynomials. **Q.E.D.**

We shall conclude this section by showing that the quantitative information given in (3.4), (3.6), (3.11) and (3.12) is the best possible. In particular, we shall give a class of nontrivial examples of Ore extensions in which all cv-polynomials can be explicitly determined. As before, $f(t)$ denotes a monic semi-invariant polynomial of minimal

degree $m \geq 1$. Let us first make an easy observation which is more or less folklore in the subject (see, *e.g.* [Am]); a proof is included for the convenience of the reader.

Lemma 3.13. *Let K be a field of characteristic $p > 0$ and let $S = I$. Let D be a (usual) derivation on K with monic minimal polynomial $g(t)$. Then $g(t) = f(t) - c$ for some $c \in K$, and it has the form $\sum c_i t^{p^i}$.*

Proof. From (3.12)(2) (or [L_2: (3.11)]) we know that $f(t)$ has the form $\sum c_i t^{p^i} + c$. Since $S = I$ here, the semi-invariance of $f(t)$ means that $(\sum c_i t^{p^i} + c)a = a(\sum c_i t^{p^i} + c)$ for all $a \in K$. Equating the constant terms of the two sides, we get $\sum c_i D^{p^i}(a) = 0$. Therefore, $\deg g(t) \leq \deg f(t)$. Since $g(t)$ is also semi-invariant, we have equality here. But then $f(t) - g(t)$ must be a constant, namely c. **Q.E.D.**

Examples 3.14. Keeping the notations in (3.13), it is known that there are examples of derivations D with minimal polynomial $g(t) = f(t)$ of any prescribed degree $m = p^s$ ($s \geq 1$). On the other hand, by (3.12)(3), $p(t) = t^p$ is a non-linear cv-polynomial of minimal degree. By (3.4)(1) and (3.11), any cv-polynomial has the form $c + \sum_{i=0}^{s-1} c_i t^{p^i} + \sum_{j \geq 1} e_j f(t)^j$. Conversely, by (2.9) and (2.11), any such polynomial is a cv-polynomial. This conforms with all the theoretic results obtained earlier in this section.

§4. Existence and Uniqueness of CV-Polynomials

For the rest of the paper, we'll fix the notation $R = K[t, S, D]$, $R' = K[t', S', D']$, and use freely the fact that homomorphisms from R' to R correspond to cv-polynomials in R with respect to (S', D').

Although a non-constant cv-polynomial $p(t)$ determines (S', D') (as in (2.12)(1)), we cannot expect (S', D') to determine $p(t)$. For instance, if $(S', D') = (I, 0)$, any polynomial in the center of R is a cv-polynomial with respect to (S', D'). However, some uniqueness results are possible, as we shall see in the results (4.3), (4.4) and (4.6) below. We begin by proving a certain commutation rule between S^n and D which results from the existence of a cv-polynomial of degree $n \geq 2$.

Proposition 4.1. *Let $p(t) = \sum b_i t^i \in R$ be a monic cv-polynomial of degree $n \geq 2$. Then we have $S^n D - D S^n = D_{c,S} S^n$, where $c := b_{n-1} - S(b_{n-1})$.*

Proof. The cv-polynomial $p(t)$ is with respect to (S^n, D') for some D'. If $D' = 0$, then $p(t)$ is semi-invariant, and the Proposition was proved in [L_3:(2.3)], under the assumption that $n \geq 1$. If D' is not necessarily zero, one can check that the calculation involving $q(t) := p(t)t - tp(t) = ct^n + \cdots$ in the proof of [L_3:(2.3)] is still correct modulo $Kt + K$. Thus, as long as $n \geq 2$, the method of comparing coefficients of t^n used in [L_3:(2.3)] suffices to give the conclusion in the Proposition. **Q.E.D.**

For the sake of completeness, we record below the exact equation relating $q(t) = p(t)t - tp(t)$ and $p(t)$, in generalization of [L_3: (2.3)]:

$$(4.2)\quad q(t)a = S^{n+1}(a)q(t) + (S^n D - D S^n)(a)p(t) + (D'S - SD')(a)t + (D'D - DD')(a).$$

Theorem 4.3. *Suppose S is an automorphism and $p(t) = \sum b_i t^i \in R$ is a monic cv-polynomial of degree $n \leq o(S)$. Then $p(t)t = (t+c)p(t) + e't + e$ where c is as in (4.1), and $e', e \in K$. If $p'(t) \in R$ is another monic cv-polynomial of degree n, then $p'(t) = p(t) + d$ for some $d \in K$.*

Proof. By (4.1) and (4.2), we have for any $a \in K$:

$$\begin{aligned} q(t)a &= S^{n+1}(a)q(t) + (cS^n(a) - S^{n+1}(a)c)p(t) + \textit{linear terms} \\ &= S^{n+1}(a)q(t) + cp(t)a - S^{n+1}(a)cp(t) + \textit{linear terms}. \end{aligned}$$

Therefore, $[q(t) - cp(t)]a = S^{n+1}(a)[q(t) - cp(t)] + \textit{linear terms}$. Now $q(t) - cp(t) = bt^m + \cdots$ where $0 \leq m < n$. We may assume that $b \neq 0$ for otherwise we have in fact $p(t)t = (t+c)p(t)$. Combining the last two equations, we get

$$(bt^m + \cdots)a = S^{n+1}(a)(bt^m + \cdots) + \textit{linear terms}.$$

If $m \geq 2$, comparison of the coefficients of t^m gives $bS^m(a) = S^{n+1}(a)b$ for all a, so $S^{n+1} = I_b \circ S^m$. This implies that $o(S) \leq n+1-m \leq n-1$, contradicting our assumption on n. Therefore, $q(t) - cp(t) = e't + e$ for some $e', e \in K$, and as a result, we have $p(t)t = (t+c)p(t) + e't + e$. Now suppose $p'(t)$ is another monic cv-polynomial of degree n. We have $p(t)a = S^n(a)p(t) + D'(a)$ and $p'(t)a = S^n(a)p'(t) + D''(a)$, where D', D'' are two S^n-derivations. Subtracting these, we get $[p'(t) - p(t)]a = S^n(a)[p'(t) - p(t)] + D''(a) - D'(a)$. If $p'(t) - p(t)$ is not a scalar, we'll have $p'(t) - p(t) = rt^k + \cdots$ for some $r \neq 0$ and $1 \leq k < n$. But then $[p'(t) - p(t)]a = (rt^k + \cdots)a = rS^k(a)t^k + \cdots$. Comparing terms of degree k, we get $S^n(a)r = rS^k(a)$, and hence $S^n = I_r \circ S^k$. Since S is an automorphism, this gives $S^{n-k} = I_r$, so $o(S) \leq n-k < n$, a contradiction. Therefore, $p'(t) - p(t) = d$ for some $d \in K$. **Q.E.D.**

Corollary 4.4. *Suppose K is a field and S is an endomorphism of K which is not an automorphism. Then the two conclusions of (4.3) hold for any monic cv-polynomials $p(t)$, $p'(t)$ of the same degree.*

Proof. In the notation of the proof above, I_b and I_r are both the identity since K is a field. Since S is injective, the equation $S^{n+1} = S^m$ would have implied that $S^{n+1-m} = I$, and similarly, $S^n = S^k$ would have implied that $S^{n-k} = I$, both of which are impossible since S is not an automorphism. Therefore, the argument above gives the desired conclusions about $p(t)$ and $p'(t)$ in this case. **Q.E.D.**

If R is a simple ring, then (without any assumptions on S) the cv-polynomials attached to any fixed (S', D') are determined up to an additive constant, as we shall see in Proposition 4.6 below. This result, however, depends on the main theorem of our earlier work [L_3:(3.6)] with Leung and Matczuk, which we recall here for later reference:

Theorem 4.5. *The Ore extension $R = K[t, S, D]$ is non-simple iff it contains a non-constant invariant polynomial, iff it contains a non-constant semi-invariant polynomial.*

Proposition 4.6. *Suppose $p(t)$ and $p'(t)$ in R are two distinct non-constant cv-polynomials with respect to (S', D'). Then either R is non-simple, or $o(S) \leq \deg p(t) = \deg p'(t)$ and $p'(t) = p(t) + c$ where $c \in K^*$ is such that $S' = I_c$.*

Proof. For any $a \in K$, we have $p(t)a = S'(a)p(t) + D'(a)$ and a similar equation for $p'(t)$. Subtracting, we see that $(p'(t) - p(t))a = S'(a)(p'(t) - p(t))$. So $p'(t) - p(t)$ is a semi-invariant polynomial. If deg $(p'(t) - p(t)) \geq 1$, then by (4.5) R is non-simple. Now assume deg $(p'(t) - p(t)) = 0$, i.e. $p'(t) - p(t) = c \in K^*$. Then $ca = S'(a)c$, so $S' = I_c$. In this case, if bt^n is the leading term of $p(t)$, we have $S' = I_b \circ S^n$ by (2.12). Therefore, $S^n = I_b^{-1} \circ S' = I_{b^{-1}c}$, so $o(S) \leq n = \deg p(t) = \deg p'(t)$. **Q.E.D.**

Having considered the uniqueness problem for cv-polynomials, let us now consider the existence problem. Since linear polynomials in R are always cv-polynomials, we are interested only in the existence of cv-polynomials of degree ≥ 2. To motivate our results in this direction, let us first recall a criterion of Lemonnier [Le] for the existence of a non-constant semi-invariant polynomial in R.

Lemonnier's Theorem 4.7. *R has a non-constant semi-invariant polynomial iff the S-derivation D is quasi-algebraic, which means that D satisfies one of the following equivalent conditions:*
(1) *There exist constants $b_i \in K$ with $b_n = 1$, such that $\sum_{i=1}^n b_i D^i$ is an S^n-inner derivation.*
(2) *There exist constants $b_1, \cdots, b_n$, not all zero, such that $\sum_{i=1}^n b_i D^i$ is an S'-inner derivation for some endomorphism S' of K.*

Modifying Lemonnier's notion of a quasi-algebraic derivation, we define an S-derivation D to be *cv-algebraic* if there exist constants $b_1, \cdots, b_n$ with $n \geq 2$, $b_n \neq 0$, such that $\sum_{i=1}^n b_i D^i$ is an S'-derivation for some endomorphism S' of K. For S-derivations, we have clearly "algebraic"$\Longrightarrow$"quasi-algebraic"$\Longrightarrow$"cv-algebraic". The following theorem and its corollary may be viewed as analogues of (4.7) above and our earlier result [L_2:(3.2)].

Theorem 4.8. *The following are equivalent for $R = K[t, S, D]$:*
(1) *R has a cv-polynomial of degree ≥ 2.*
(2) *There exists a polynomial $p(t) = \sum_{i=0}^n b_i t^i \in R$ with degree $n \geq 2$ and a pair (S', D') such that, for any $a \in K$, $p(t)a \equiv S'(a)p(t) + D'(a)$ (mod $R \cdot t$).*
(3) *The S-derivation D is cv-algebraic.*

Proof. (1)$\Longrightarrow$(2) is obvious. Now assume (2). Note that the given congruence in (2) means that $p(t)a$ and $S'(a)p(t) + D'(a)$ have the same constant terms when written out as (left) polynomials. Therefore, going through the first part of the proof of (2.16), we can still compare the constant terms, and get the equation $S'(a)b_0 + D'(a) = \sum_{i=0}^n b_i D^i(a)$ for any $a \in K$. By transposition, $\sum_{i=1}^n b_i D^i(a) = (D' - D_{b_0,S'})(a)$, so $\sum_{i=1}^n b_i D^i$ is an S'-derivation (namely $D' - D_{b_0,S'}$). By definition, D is cv-algebraic. Finally, for (3)$\Longrightarrow$(1), suppose D is cv-algebraic, say some $D' := \sum_{i=1}^n b_i D^i$ is an S'-derivation, where $b_n \neq 0$, $n \geq 2$, and S' is an endomorphism of K. Let $p(t) := \sum_{i=1}^n b_i t^i \in R$, so that $D' = p(D)$. If D is not algebraic, (2.12)(2) (applied with $b_0 = 0$) implies that $p(t)$ is a cv-polynomial with respect to (S', D') so we are done. If D is algebraic, the homomorphism $\lambda : R \longrightarrow End(K, +)$ in the proof of (2.12) has kernel $R \cdot q(t)$, where $q(t)$ is a suitable monic invariant polynomial (the "minimal polynomial"

of D). In this case, $p(t) := q(t)^2$ is clearly a cv- (in fact semi-invariant) polynomial of degree ≥ 2, again proving (1). **Q.E.D.**

Corollary 4.9. *D is cv-algebraic iff there exist constants $b_1, \cdots, b_n$ with $n \geq 2$ and $b_n = 1$ such that $\sum_{i=1}^{n} b_i D^i$ is an S^n-derivation.*

Proof. We need only prove the "only if" part. Assume D is cv-algebraic. Then R has a cv-polynomial $p(t)$ of degree $n \geq 2$. Scaling $p(t)$ and dropping its constant term, we may assume that $p(t) = t^n + b_{n-1}t^{n-1} + \cdots + b_1 t$. Then $p(t)$ is a cv-polynomial with respect to (S^n, D') for some S^n-derivation D'. By (2.12)(1), $D^n + b_{n-1}D^{n-1} + \cdots + b_1 D$ is an S^n-derivation (namely, D'). **Q.E.D.**

Example 4.10. We construct here an example of a usual derivation D which is cv-algebraic but not quasi-algebraic. We take $K = k(x_1, \cdots, x_n, \cdots)$, where k is a field of characteristic 2, and define a (usual) derivation D on K by $D(k) = 0$ and $D(x_i) = x_{i+1}$ for all $i \geq 1$. Then $t^2 \in R$ is a cv-polynomial with respect to (I, D^2) and D^2 is a usual derivation, so D is cv-algebraic. However, D is not quasi-algebraic. In fact, if it were, then according to (4.7)(1) there would exist $b, b_1, \cdots, b_n \in K$ with $b_n = 1$ such that $b_n D^n + \cdots + b_1 D = D_{b,I} = 0$ (since K is a field). This is easily seen to be impossible.

Example 4.11. There are many examples of S-derivations D which are not cv-algebraic. For instance, *if char $K = 0$, S is an automorphism, $SD = DS$, and D is not S-inner, then by* (3.12)(3) *D is not cv-algebraic.* For a more explicit construction, take $K = k(x)$ where k is a field of characteristic zero. The usual derivation $\frac{d}{dx}$ on K is clearly not inner, so by what we said above, D is not cv-algebraic. It is also easy to see by a direct argument that, for $n \geq 2$, $D^n + b_{n-1}D^{n-1} + \cdots + b_1 D$ can never be a (usual) derivation, for any $b_1, \cdots, b_{n-1} \in k(x)$.

A natural way to interpret the result in Theorem 4.8 is by using the notion of a minimal Ore extension. Let us say that $R = K[t, S, D]$ is a *minimal (resp. maximal) Ore extension of K* if there is no proper subring (resp. over-ring) of R which is also an Ore extension of K. From (4.8), it follows that *R is minimal in this sense iff D is not cv-algebraic.* (This is to be compared with (4.5) which says that R is simple iff D is not quasi-algebraic.) Using this notion of minimality, it is particularly easy to derive the following consequence of (4.8):

Corollary 4.12. *Let $c \in K$. Then an S-derivation D is cv-algebraic iff $D - D_{c,S}$ is cv-algebraic.*

Proof. We have an isomorphism $\phi : K[t', S, D - D_{c,S}] \longrightarrow K[t, S, D]$ defined by $\phi(t') = t - c$. From this isomorphism, it follows that $K[t, S, D]$ is minimal iff $K[t', S, D - D_{c,S}]$ is minimal. **Q.E.D.**

In the case when K is a field, it is possible to give more precise descriptions of the maximal as well as the minimal Ore extensions of K, and as it turns out, in this case

minimal Ore extensions are always maximal (though not conversely). To prove these results, we need the following well-known observation on (K, S, D) in case K is a field:

(4.13) *If $S \neq I$, then $D = D_{b,S}$ for some $b \in K$.*

In fact, if $S(a) \neq a$ for some $a \in K$, the equation $D(ac) = D(ca)$ (for any $c \in K$) leads to $(a - S(a))D(c) = D(a)c - S(c)D(a)$, so we have $D = D_{b,S}$ for $b = (a - S(a))^{-1}D(a)$.

Theorem 4.14. *For $R = K[t, S, D]$ where K is a field, the following are equivalent:*
(1) *R is a minimal Ore extension (i.e. D is not cv-algebraic);*
(2) *char $K = 0$, $S = I$, and $D \neq 0$.*

Proof. (2)$\Longrightarrow$(1) follows from (4.11). Conversely, assume (1). Then clearly $D \neq 0$ for otherwise $R = K[t, S] \supset K[t', S^2]$ with $t' = t^2$. We must also have $S = I$, for otherwise (4.13) gives $D = D_{b,S}$ for some $b \in K$, and (2.1) gives $R = K[t, S, D_{b,S}] = K[t - b, S]$, again contradicting the minimality of R. Finally, K must have zero characteristic, for if *char* $K = p > 0$, then, since $S = I$, R would have (by (2.20)) a non-linear cv-polynomial t^p. **Q.E.D.**

We finish this section by giving the analogue of (4.14) for *maximal* Ore extensions. The proof for this is, however, quite a bit more tricky.

Theorem 4.15. *For $R = K[t, S, D]$ where K is a field, the following are equivalent:*
(1) *R is a maximal Ore extension;*
(2) *One of the following holds:*
(2a) *S cannot be written as $\overline{S}^n$ where $\overline{S}$ is an endomorphism of K and $n \geq 2$;*
(2b) *char $K = 0$, $S = I$, and $D \neq 0$;*
(2c) *char $K = p$, $S = I$, D is not algebraic, and D cannot be written as $q(\overline{D})$ where q is a non-linear p-polynomial and $\overline{D}$ is a (usual) derivation.*

Proof. Let us first prove (2)$\Longrightarrow$(1). Suppose $R \subseteq \overline{R} = K[\overline{t}, \overline{S}, \overline{D}]$, with $t = p(\overline{t}) = b_n\overline{t}^n + \cdots + b_0$, $b_n \neq 0$. Then by (2.12)(1), $S = I_{b_n} \circ \overline{S}^n = \overline{S}^n$. If (2a) holds, then we must have $n = 1$ and so $R = \overline{R}$. Now suppose (2b) holds. If $\overline{S} \neq I$, then by (4.13) $\overline{D}$ is $\overline{S}$-inner, so after a change of variable in $\overline{R}$, we may assume that $\overline{D} = 0$. But then by (2.12)(1), $D = b_n\overline{D}^n + \cdots + b_1\overline{D} + D_{b_0,I} = 0$, a contradiction. Therefore, we must have $\overline{S} = I$, and, as we have just seen, $\overline{D} \neq 0$. But then by (4.14), $\overline{R} = K[\overline{t}, \overline{D}]$ is minimal, so we can conclude that $R = \overline{R}$. Finally, suppose (2c) holds. Since D is not algebraic, $S = I$, and K is a field, it follows that D is not quasi-algebraic and hence R is a simple ring by (4.5) and (4.7).[6] Referring ahead to (5.8)(2), we see that $\overline{R}$ is also simple. If deg $p(\overline{t}) \geq 2$, then by (3.12)(1), $q(\overline{t}) := p(\overline{t}) - b_0$ is a (non-linear) p-polynomial, and by (2.12)(1), $D = q(\overline{D}) + D_{b_0,I} = q(\overline{D})$, a contradiction. Therefore, $p(\overline{t})$ must be linear, and we have $R = \overline{R}$. This proves the maximality of R in all cases.

Next we shall assume (1) (that is, R is maximal), and try to prove (2). We may assume $S = \overline{S}^n$ for some $n \geq 2$ and some endomorphism $\overline{S}$ of K (for otherwise we have already (2a)). If $S \neq I$, then by (4.13), $D = D_{b,S}$ for some $b \in K$, so after

[6] Of course, it would have been more straightforward to use here the classical results of Amitsur [Am] on the simplicity of $K[t, D]$.

replacing t by $t-b$, we may assume that $D=0$. But then we can embed R into $K[\overline{t},\overline{S}]$ by sending t to $\overline{t}^n$, and this would contradict the maximality of R. Therefore, we must have $S=I$, and, as we have just seen, $D\neq 0$. If *char* $K=0$, we'll be in the situation (2b). Therefore, we may assume that *char* $K=p$. We claim that D cannot be an algebraic derivation. For, if it is, and $f(t)\in R=K[t,D]$ is its minimal polynomial, then $f(t)$ is an invariant polynomial of degree ≥ 2 (since $D\neq 0$), and we can embed R (properly) into itself by sending t to $t+f(t)$, in contradiction to the maximality of R. Finally, suppose we can write D in the form $q(\overline{D})$, where $\overline{D}$ is a usual derivation, $q(\overline{t})=c_m\overline{t}^{p^m}+\cdots+c_1\overline{t}^{p}+c_0\overline{t}$, with $m\geq 1$, and $c_m\neq 0$. Then, by (2.21), $q(\overline{t})$ is a cv-polynomial in $\overline{R}:=K[\overline{t},\overline{D}]$ with respect to $(I,q(\overline{D}))=(I,D)$, and we can embed R properly into $\overline{R}$ by sending t to $q(\overline{t})$, again in contradiction to the maximality of R. Therefore, we must now be in the situation (2c). **Q.E.D.**

From the last two results, we have the following somewhat surprising consequence:

Corollary 4.16. *For any field K, the minimality of $R=K[t,S,D]$ implies its maximality (but not conversely).*

If K is not a field, this Corollary does not hold. An example of a division ring K with $K[t,S,D]$ minimal but not maximal will be given toward the end of this paper.

§5. Comparison Between Ore Extensions

The study of homomorphisms between Ore extensions leads naturally to the following comparison relationship among *all* Ore extensions over a given division ring. For two such extensions R and R', let us define $R'\leq R$ if there exists an injective homomorphism $\phi: R'\longrightarrow R$; in other words, $R'\leq R$ iff R has a non-constant cv-polynomial with respect (S',D'). Clearly, "$\leq$" is a transitive (as well as reflexive) relation.

Some of the basic features of the relation "$\leq$" can be seen from the list of examples and results below.

(5.1) If $R'\leq R=K[t,S]$ (i.e. $D=0$), then $R'\cong K[t'',S']$. In fact, since $D=0$, an application of (2.12)(1) shows that $D'=D_{b,S'}$ for some $b\in K$. But then $R'=K[t',S',D_{b,S'}]=K[t'-b,S']$ by (2.1).

(5.2) If $R'\leq R=K[t,D]$ (i.e. $S=I$), then $R'\cong K[t'',D'']$ for some (usual) derivation D''. In fact, since $S=I$, (2.12)(1) shows that $S'=I_b$ for some $b\in K^*$, so $R'=K[t',I_b,D']=K[b^{-1}t',b^{-1}D']$.

(5.3) If $R'\leq R=K[t]$, then $R'\cong K[t'']$. This follows easily from the arguments used in the last two examples.

(5.4) We may have $R'\leq R$ and $R\leq R'$ without having $R'\cong R$. For instance, let S be an automorphism with $o(S)=3$, and let $R=K[t,S]$, $R'=K[t',S^2]$. Then, $t'\longmapsto t^2$ defines an injection $R'\longrightarrow R$. On the other hand, if $S^3=I_b$, $t\longmapsto b^{-1}t'^2$ defines an injection $R\longrightarrow R'$, since $(b^{-1}t'^2)a=b^{-1}S^4(a)t'^2=b^{-1}(bS(a)b^{-1})t'^2=S(a)(b^{-1}t'^2)$.

However, we *do not* have $R' \cong R$. Indeed, if there is such an isomorphism, (2.12)(1) would imply that $S^2 = I_c \circ S$ for some $c \in K^*$, contradicting the fact that $o(S) = 3$.

(5.5) A similar example of $R' \leq R \leq R'$ with non-isomorphic R, R' can be constructed for Ore extensions of the "derivation type" (i.e. with $S' = S = I$). Let K be a field of characteristic 2, and let D be a (usual) derivation with minimal equation $D^4 - D = 0$. Let $R = K[t, D]$ and $R' = K[t', D^2]$. Then $t' \longmapsto t^2$ and $t \longmapsto t'^2$ define embeddings $R' \longrightarrow R$ and $R \longrightarrow R'$. (So far we do not need K to be a field.) If there exists an isomorphism $R' \longrightarrow R$, (2.12)(1) would imply that $D^2 = bD + D_{c,I}$ for some $b, c \in K$. Since K is a field, this gives $D^2 = bD$, a contradiction. (An example of a derivation D in a field of characteristic 2 with minimal equation $D^4 - D = 0$ can be found in [Le$_2$: Prop.7, p.14]).

The last two examples are to be contrasted with our next result which says that, in a "sufficiently general" situation, $R' \leq R \leq R'$ will indeed imply that $R' \cong R$.

Theorem 5.6. *Let $R = K[t, S.D]$, $R' = K[t', S', D']$. Assume that either (1) S is an automorphism with $o(S) = \infty$, or (2) D is not quasi-algebraic. If $\phi : R' \longrightarrow R$ and $\psi : R \longrightarrow R'$ are injective ring homomorphisms, then both are isomorphisms. In particular, we always have $R' \leq R \leq R' \Longrightarrow R' \cong R$.*

Proof. Assume that one of ϕ and ψ is *not* an isomorphism. Then $\phi \circ \psi : R \longrightarrow R$ is injective but not surjective, so it corresponds to a cv-polynomial $p(t)$ of degree $n \geq 2$ with respect to (S, D). Suppose we are under the hypothesis (1). By (2.12)(1), we have $S = I_b \circ S^n$ for some $b \in K^*$. Since S is an automorphism, this implies that $S^{n-1} = I_{b^{-1}}$, so $o(S) \leq n - 1 < \infty$, a contradiction. Next suppose we are under the hypothesis (2). Then $D = (p - b_0)(D) + D_{b_0,S}$ where b_0 is the constant term of $p(t)$. Since $p(t)$ has degree $n \geq 2$, this implies that D is quasi-algebraic, again a contradiction. **Q.E.D.**

Remark 5.7. One might wonder if the Theorem still holds if we relax the hypothesis (2) above to (2'): *D is not algebraic.* The answer is that it does not. For instance, take the Ore extensions R, R' in (5.4). For suitable choices of (K, S), we can arrange to have an element $b \in K$ such that $D_{b,S}$ is not an algebraic derivation (though, of course, D is quasi-algebraic). The ring $R'' = K[t, S, D_{b,S}]$ is isomorphic to R by (2.1), and hence we have $R' \leq R'' \leq R'$; but $R'' \cong R$ is not isomorphic to R'.

Theorem 5.8. *Let $R = K[t, S, D]$ and $R' = K[t', S', D']$, as usual. Then*
(1) R is non-simple iff we have some $K[t'', S''] \leq R$.
(2) If $R' \leq R$, then R is simple iff R' is simple.

Proof. (1) Suppose R is non-simple. Then there exists a monic invariant polynomial $p(t) \in R$ of degree $n \geq 1$. Then $p(t)$ is a cv-polynomial with respect to $(S^n, 0)$ and we have an injective homomorphism $K[t'', S^n] \longrightarrow R$. Conversely, if we have some injection $K[t'', S''] \longrightarrow R$, then the associated cv-polynomial is a non-constant semi-invariant polynomial in R. By (4.5), R must be non-simple. To prove (2), let us view R' as a subring of R. If R' is non-simple, then by (1) we have some $K[t'', S''] \leq R'$. Since "$\leq$" is transitive, we have $K[t'', S''] \leq R$ and so by (1) again R is non-simple. Conversely, assume R is non-simple. Then R has a nonzero ideal $J = R \cdot f$ where f

is an invariant polynomial of degree $n \geq 1$. If $R' \cap J = 0$, then we have an injection $R' \longrightarrow R/J$. This is impossible since R/J has left K-dimension n, and R has infinite left dimension over K. **Q.E.D.**

The next result concerns the centers of Ore extensions. Following Cauchon [Ca], we say that $R = K[t, S, D]$ *has non-trivial center* if the center of R contains a non-constant polynomial. The following effective criterion for R to have non-trivial center has been given in [Le$_1$:(2.3)]:

(5.9) *$R = K[t, S, D]$ has non-trivial center iff R is non-simple and $o(S) < \infty$.*

Theorem 5.10. *Let R and R' be as above. Then*
(1) *R has non-trivial center iff we have some $K[t''] \leq R$.*
(2) *If $R' \leq R$, then R has non-trivial center iff R' has non-trivial center.*

Proof. (1) Suppose R has a central polynomial $p(t)$ of degree ≥ 1. Then $p(t)$ is a cv-polynomial with respect to $(I, 0)$ and $t'' \longmapsto p(t)$ defines an injection $K[t''] \longrightarrow R$. Conversely, suppose there is such an injection ϕ. Then, for $p(t) := \phi(t'') = bt^n + \cdots$ ($b \neq 0$, $n \geq 1$), we have $I = I_b \circ S^n$ by (2.12)(1), so $o(S) \leq n < \infty$. Since, by (5.8)(2), R is also non-simple, we conclude from (5.9) that R has non-trivial center. To prove (2), assume that $R' \subseteq R$. The "if" part of (2) follows from (1) as in the previous proof. For the "only if" part, assume R has non-trivial center, so $o(S) < \infty$ and R is non-simple. From (2.12)(1) again we deduce that $o(S') < \infty$, and (5.8)(2) implies that R' is non-simple. Another application of (5.9) shows that R' has non-trivial center. **Q.E.D.**

In parallel to (5.8)(1) and (5.10)(1), we have also the following criterion for $R = K[t, S, D]$ to contain an Ore extension of the derivation type.

Theorem 5.11. *We have some $K[t', D'] \leq R$ iff $o(S) < \infty$ and some $\sum_{i=1}^{n} b_i D^i$ is a usual derivation, where $b_1, \cdots, b_n \in K$ are not all zero.*

Proof. The "only if" part follows easily from (2.12)(1). Conversely, assume that $o(S) < \infty$, and that for $p(t) = \sum b_i t^i$, $D' := p(D)$ is a usual derivation. If D is not algebraic, (2.12)(2) implies that $p(t)$ is a cv-polynomial with respect to (I, D'), so we have $K[t', D'] \leq R$. Now assume D is algebraic; in particular, R has a monic invariant polynomial $q(t)$ of degree $k \geq 1$. Say $S^m = I_b$. Then, for any $a \in K$:

$$b^{-k} q(t)^m a = b^{-k} S^{km}(a) q(t)^m = b^{-k}(b^k a b^{-k}) q(t)^m = a b^{-k} q(t)^m,$$

so $t'' \longmapsto b^{-k} q(t)^m$ defines a homomorphism from $K[t'']$ to R, giving a stronger conclusion $K[t''] \leq R$ in this case. **Q.E.D.**

To complete our results in this direction, we shall also prove the following Proposition and Theorem concerning the behavior of the algebraicity of derivations under a change of Ore extensions.

Proposition 5.12. *Let $\phi : R' \longrightarrow R$ be a homogeneous injection, i.e. it is defined by a cv-polynomial $p(t)$ without constant term. Then D is algebraic iff D' is algebraic.*

Proof. For the maps λ and λ' defined in (2.14), we have by (2.14) the commutativity relation $\lambda' = \lambda \circ \phi$ (under the assumption that ϕ is homogeneous). If we think of ϕ as an inclusion map, this relation clearly implies that $ker\,\lambda' = R' \cap ker\,\lambda$. If D' is algebraic, then $ker\,\lambda' \neq 0$, so $ker\,\lambda$ is also nonzero, and D is algebraic. Conversely, if D is algebraic, then $ker\,\lambda \neq 0$, and the dimension argument in the proof of (5.8)(2) shows that $ker\,\lambda' = R' \cap ker\,\lambda \neq 0$, and therefore D' is algebraic. **Q.E.D.**

It is easy to see that, in the above Proposition, the homogeneity assumption on ϕ cannot be waived. For instance, we have an isomorphism $\phi : K[t', S, D'] \longrightarrow K[t, S, D_{c,S}]$ defined by $\phi(t') = t - c$, where $D' = 0$ is algebraic, but the S-inner derivation $D_{c,S}$ certainly need not be algebraic. Note that the isomorphism ϕ here is *not* homogeneous (unless $c = 0$). This "counter-example" shows that, in dealing with the hereditary properties of the algebraicity of D and D', we have to be careful about the inner derivations. The following result allows us to extend (5.12) to the case of a general injection $\phi : R' \longrightarrow R$, once we have taken the inner derivations into account.

Theorem 5.13. *Let $\phi : R' \longrightarrow R$ be an injection defined by a cv-polynomial $p(t)$. Then, for any $a \in K$, $D - D_{a,S}$ is algebraic iff $D' - D_{p(a),S'}$ is algebraic. (Here, the evaluation of the (S, D)-polynomial $p(t)$ at a is as defined in* [L_1: §2].)

Proof. We can think of R as $K[t - a, S, D - D_{a,S}]$, and R' as $K[t' - p(a), S', D' - D_{p(a),S'}]$. Using these new representations of R' and R, the map ϕ is determined by the cv-polynomial $\phi(t' - p(a)) = p(t) - p(a)$. Since $p(t) - p(a)$ is right-divisible by $t - a$ ([L_1: (2.4)]), the map ϕ is now homogeneous with respect to the new representations of R' and R. Applying the Proposition, it follows that $D - D_{a,S}$ is algebraic iff $D' - D_{p(a),S'}$ is algebraic. **Q.E.D.**

The Theorem above has also a very natural interpretation in terms of the notion of algebraic conjugacy classes developed in [L_2]. Recall that, for $a \in K$, the (S, D)-conjugacy class of a is defined to be $\triangle^{S,D}(a) = \{S(c)ac^{-1} + D(c)c^{-1} : c \in K^*\}$. Such a class is said to be *algebraic* (with respect to (S, D)) if some nonzero (S, D)-polynomial vanishes on it. In [L_2: (5.10)], we have shown that $\triangle^{S,D}(a)$ is algebraic iff $D - D_{a,S}$ is an algebraic S-derivation. Therefore, (5.13) has the following nice interpretation in terms of the preservation of algebraic conjugacy classes:

Theorem 5.14. *Let $p(t) \in R$ be any non-constant cv-polynomial with respect to (S', D'). Then, for any $a \in K$, the class $\triangle^{S,D}(a)$ is algebraic iff the class $\triangle^{S',D'}(p(a))$ is algebraic.*

Note that Proposition 5.12 is also true if we replace both occurrences of "algebraic" by "quasi-algebraic", and, for this, no assumption on the homogeneity of the map ϕ is required. In fact, for the quasi-algebraic case, Proposition 5.12 is just a combination of (4.5), (4.7) and (5.8)(2). The last case to consider is the case of cv-algebraic derivations. If $\phi : R' \longrightarrow R$ is any injection, clearly D' is cv-algebraic $\Longrightarrow D$ is cv-algebraic. The reverse implication holds if K is a field, by (4.16), but does not hold in general in view of the last remark in §4.

Next we shall bring into play the non-linear cv-polynomials of minimal degree. If $p(t)$ is such a polynomial, an interesting question to ask is: *under what conditions can we say that all non-linear cv-polynomials in R can be expressed as a polynomial in $p(t)$?* To facilitate the study of this problem, it is convenient to introduce the following terminology.

Definition 5.15. We say that R *has a largest Ore subextension* R' if R' is an Ore extension properly contained in R, and any Ore extension properly contained in R sits inside R'. (The idea is that any injection from any $R'' = K[t'', S'', D'']$ into R which is not an isomorphism should factor through an injection of R'' into R'.) If such an R' exists, it is clearly unique. Moreover, if $p(t)$ is a cv-polynomial such that $R' = K[p(t)]$, then $p(t)$ is a non-linear cv-polynomial of minimal degree. Conversely, if $p(t)$ is a non-linear cv-polynomial of minimal degree, then $K[p(t)]$ is the largest Ore subextension of R iff every non-linear cv-polynomial in R is contained in $K[p(t)]$.

Certainly, not every Ore extension R has a largest Ore subextension. For instance, in the usual polynomial ring $R = K[t]$, an Ore subextension $R' \subseteq R$ containing both $K[t^2]$ and $K[t^2+t]$ would have to contain t and hence equal to R. Therefore, $K[t]$ has no largest Ore subextension. However, it turns out that there are many examples of Ore extensions which do contain a largest Ore subextension. We shall now try to develop a general result which guarantees the existence of large classes of such examples. As a preparation, we need to go back to a result which was left unproved in §3, namely, part (3) of Theorem 3.4. For the reader's convenience, we restate this result, and then give its proof.

Proposition 5.16. *Assume that S is an automorphism. Let $p(t) \in R$ be a (monic) cv-polynomial of degree n and assume that R has no non-constant semi-invariant polynomial of degree $< n$. Then $n | \deg P(t)$ for any (monic) cv-polynomial $P(t)$ of degree $N \geq n$.*

Proof. By successive division, we can write

$$P(t) = \sum_{i=0}^{d} h_i(t) p(t)^i \,, \tag{5.17}$$

where $\deg h_i(t) < n$, $h_d(t) \neq 0$. We claim that $h_d(t) \in K$, which will give the desired conclusion since then $\deg P(t) = dn$. Say $p(t)$ is a cv-polynomial with respect to (S^n, D'). Then $p(t)^i a = \sum_{j=0}^{i} f_j'^i(a) p(t)^j$ where $f_j'^i$ is the sum of all products with j factors of $S' = S^n$ and $i-j$ factors of D' (see the paragraph before (2.16)). Therefore, for any $a \in K$:

$$P(t)a = \sum_{i=0}^{d} h_i(t) \sum_{j=0}^{i} f_j'^i(a) p(t)^j = \sum_{j=0}^{d} \left(\sum_{i=j}^{d} h_i(t) f_j'^i(a) \right) p(t)^j. \tag{5.18}$$

On the other hand, if the cv-polynomial $P(t)$ is with respect to (S^N, D''), we also have

$$P(t)a = S^N(a)P(t) + D''(a) = \sum_{j=0}^{d} S^N(a) h_j(t) p(t)^j + D''(a). \tag{5.19}$$

Since there is only one way to write $P(t)a$ as a sum of powers of $p(t)$ left-multiplied with polynomials of degree $< n$, we deduce that

$$S^N(a)h_j(t) + \delta_{j,0}D''(a) = \sum_{i=j}^{d} h_i(t)f_j'^i(a) \quad (0 \le j \le d), \tag{5.20}$$

where $\delta_{j,0}$ means the Kronecker deltas. For $j = d > 0$, this simplifies to $S^N(a)h_d(t) = h_d(t)S^{dn}(a)$. Since $S^{dn}(a)$ can be any element of K (S being an automorphism), this implies that $h_d(t)$ is semi-invariant, and therefore the hypothesis in the Proposition implies that $h_d(t) \in K$, as desired. **Q.E.D.**

Corollary 5.21. *Assume that S is an automorphism, and that R is simple. If $p_1(t)$ and $p_2(t)$ are two non-constant cv-polynomials in R, then the degree of one of them divides the degree of the other one.*

Now we are ready to prove the following result which gives, as a corollary, a general sufficient condition for an Ore extension R to have a largest Ore subextension.

Theorem 5.22. *Assume S is an automorphism, and that D is not S-inner. Let $p(t) \in R$ be a monic non-linear cv-polynomial of minimal degree n, and let $P(t)$ be a (monic) non-linear cv-polynomial of degree N. If $kn \not\equiv 1 \,(mod\ o(S))$ for all positive $kn \le N$, then $P(t) \in K[p(t)]$.*

Proof. As in the proof of (3.6), the assumptions on $p(t)$ here imply that R has no non-constant semi-invariant polynomial of degree $< n$. Hence, (5.16) applies. Expressing $P(t)$ as in (5.17) (and noting that deg $P(t) \ge n$), we have therefore $h_d(t) \in K$. Our goal is to show that all $h_j(t) \in K$, so that we can conclude that $P(t) \in K[p(t)]$. Proceeding by induction, we may assume that $h_d(t), h_{d-1}(t), \cdots, h_{j+1}(t) \in K$, and try to show that $h_j(t) \in K$. Now, by (5.20), we have for any $a \in K$:

$$S^N(a)h_j(t) + \delta_{j,0}D''(a) = h_j(t)S^{jn}(a) + \sum_{i>j}^{d} h_i(t)f_j'^i(a).$$

Therefore,

$$h_j(t)S^{jn}(a) = S^N(a)h_j(t) + constant. \tag{5.23}$$

Since $S^{jn}(a)$ can be any element of K, this implies that $h_j(t)$ is a cv-polynomial (by (2.16)(4)), and since deg $h_j(t) < n$, we must have $h_j(t) = a_jt + b_j$ for suitable constants a_j, b_j. Plugging this into (5.23) and comparing (left) coefficients of t, we get $a_jS^{jn+1}(a) = S^N(a)a_j$. If $a_j \ne 0$, this would give $I_{a_j} \circ S^{jn+1} = S^N = S^{dn}$, and hence $(d-j)n \equiv 1 \,(mod\ o(S))$, a contradiction. Therefore, $a_j = 0$ and we have $h_j(t) = b_j \in K$, as desired. **Q.E.D.**

Corollary 5.24. *Let (S, D) and $p(t)$ be as in Theorem 5.22, with $n = deg\ p(t)$. If $(n, o(S)) \ne 1$ (in particular, if $o(S) = \infty$), then $K[p(t)]$ is the largest Ore subextension in R.*

Proof. We need to show that any non-linear cv-polynomial $P(t)$ belongs to $K[p(t)]$. If it does not, the theorem implies that $kn \equiv 1\,(mod\ o(S))$ for some k. This means that $o(S) < \infty$ and that $(n, o(S)) = 1$, a contradiction. **Q.E.D.**

Remark 5.25. If we do not impose the hypothesis that $(n, o(S)) \neq 1$, the Corollary will not hold in general. For instance, let (K, S, D) be such that $char\ K = p > 0$, $SD = DS$, $S^{p-1} = I$, $D^p = D$, and D is not S-inner. Then $p(t) = t^p$ is a non-linear cv-polynomial of minimal degree. On the other hand, $P(t) = t^p - t$ is an invariant polynomial, for it obviously commutes with t, and also, for any $a \in K$:

$$P(t)a = t^p a - ta = (S^p(a)t^p + D^p(a)) - (S(a)t + D(a)) = S(a)P(t).$$

However, we have clearly $P(t) \notin K[t^p]$. Here, $o(S)|(p-1)$ so $(p, o(S)) = 1$. (Of course, we could have chosen $S = I$ and K to be a field in the above. In this case, we need only choose D to be a nonzero derivation with $D^p = D$.)

Remark 5.26. If we do not assume that D is not S-inner, the Corollary also fails to hold in general. For instance, let S be an automorphism of a division ring K with $o(S)$ equal to an even integer, and let $D = 0$. We can take $p(t) = t^2$ to be a non-linear cv-polynomial of minimal degree ($n = 2$). Then $(n, o(S)) = 2 \neq 1$, but clearly the invariant polynomial $P(t) = t^3$ is not in $K[t^2] \cong K[t', S^2]$. The Ore extension $R = K[t, S]$ has no largest Ore subextension in this case.

As it turns out, the sufficient condition $(n, o(S)) \neq 1$ for $K[p(t)]$ to be the largest Ore subextension of R is also not far from being necessary. To see this, we need the following simple observation:

Lemma 5.27. *Let $p(t) \in R$ be any monic cv-polynomial of degree $n \geq 2$, and let $u \in K^*$. Then $p(t) + ut$ is a cv-polynomial iff $S^n = I_u \circ S$. In particular, if S is an automorphism and $p(t)$ is a monic non-linear cv-polynomial of minimal degree n, then $p(t)$ is unique up to an additive constant iff $n \not\equiv 1\ (mod\ o(S))$.*

Proof. Suppose the cv-polynomial $p(t)$ is with respect to (S^n, D'). For any $a \in K$, we have

$$\begin{aligned}(p(t) + ut)a &= S^n(a)p(t) + D'(a) + u(S(a)t + D(a)) \\ &= S^n(a)(p(t) + ut) + (uS(a) - S^n(a)u)t + D'(a) + uD(a).\end{aligned}$$

Therefore, $p(t) + ut$ is a cv-polynomial iff $uS(a) = S^n(a)u$ for all $a \in K$; that is, iff $S^n = I_u \circ S$. If S is an automorphism, and n is assumed to be minimal, then, for any other monic cv-polynomial $p'(t)$ of degree n, the difference $p'(t) - p(t)$ is also a cv-polynomial (by (2.9)), of degree $< n$, so it has the form $ut + c$. The last conclusion in the Lemma now follows easily from this representation. **Q.E.D.**

Proposition 5.28. *Keeping the notations in* (5.22), *if $K[p(t)]$ is the largest Ore subextension of R, then we have $kn \not\equiv 1\ (mod\ o(S))$ whenever kn is the degree of a cv-polynomial $P(t)$. In particular, if for every $k \geq 1$ there exists a cv-polynomial of degree*

kn, then $(n, o(S)) \neq 1$ is a necessary as well as sufficient condition for $K[p(t)]$ to be the largest Ore subextension of R.

Proof. If $kn \equiv 1 \ (mod\ o(S))$ where kn is the degree of a cv-polynomial $P(t)$, then $S^{kn-1} = I_u$ for some $u \in K^*$, so $P(t) + ut$ is also a cv-polynomial by (5.27). Hence we have $P(t) + ut \in K[p(t)]$ as well as $P(t) \in K[p(t)]$. This gives $t \in K[p(t)]$, which contradicts $n = \deg p(t) \geq 2$. **Q.E.D.**

Since the phenomenon of an Ore extension containing a largest Ore subextension has not been observed before, we would like to conclude this paper by constructing some explicit examples. Note that for any such example $K[t, S, D]$, (5.28) implies that S cannot be an inner automorphism, and we can also see easily that D cannot be an S-inner derivation. To produce an actual example to which (5.24) applies, let k be any field, and let $F = k(\{x_i : i \in \mathbf{Z}\})$. Let σ be the k-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 $F((y, \sigma^p))$ (in which $yx_i = \sigma^p(x_i)y = x_{i+p}y$), where p is a fixed prime. We can extend σ to an automorphism S of K by defining $S(y) = y$. Further, it is easy to check that there is a unique S-derivation D on K specified by $D(k) = 0$, $D(x_i) = x_i$ ($\forall\ i \in \mathbf{Z}$), and $D(y) = 0$. We claim that: (1) $o(S) = p$, and (2) *D is not S-inner.* First, note that $S^p(x_i) = x_{i+p} = yx_iy^{-1}$, and $S^p(y) = y = yyy^{-1}$; hence we have $S^p = I_y$. To prove that $o(S) = p$, we need to show that S is not an inner automorphism. But if $S = I_u$ for some nonzero $u = \sum_{i=i_0}^{\infty} f_iy^i$ ($f_i \in F$, $f_{i_0} \neq 0$), then $ux_j = x_{j+1}u$ leads to $\sum_{i=i_0}^{\infty} f_ix_{j+ip}y^i = \sum_{i=i_0}^{\infty} x_{j+1}f_iy^i$. Comparing the coefficients of y^{i_0}, we get $f_{i_0}x_{j+i_0p} = x_{j+1}f_{i_0}$, which is impossible. To prove the second claim, assume that $D = D_{u,S}$ where u is as above. Then $x_j = D(x_j) = D_{u,S}(x_j) = ux_j - x_{j+1}u$ ($\forall\ j \in \mathbf{Z}$) leads to $x_j = \sum_{i=i_0}^{\infty} (f_ix_{j+ip} - x_{j+1}f_i)y^i$. Comparing the constant coefficients gives $x_j = f_0x_j - x_{j+1}f_0$, or $f_0 = x_j/(x_j - x_{j+1})$ for all j. This is clearly impossible. In this example, it is easy to check that $SD = DS$. Now assume that k has characteristic p. Then, by (3.12)(3), $p(t) = t^p \in K[t, S, D]$ is a non-linear cv-polynomial (with respect to (S^p, D^p)) of minimal degree, and we have $(o(S), \deg p(t)) = p \neq 1$. Therefore, (5.24) applies, giving the conclusion that $R' = K[t^p, S^p, D^p]$ is the largest Ore subextension of $R = K[t, S, D]$. As a strengthening of the claim (2) above, we leave it to the reader to check that D is in fact not a quasi-algebraic derivation, so the Ore extension R in question is a simple ring here.

In the above example, the Ore subextension $R' \subset R$ is not minimal since it contains in turn $K[t^{p^2}, S^{p^2}, D^{p^2}]$. However, we can arrange to have R' minimal by making the following changes in the construction. First, in the definition of D, we replace the conditions $D(x_i) = x_i$ by $D(x_i) = (-1)^i x_i$ (for every i). Then, we'll have $SD = -DS$ (instead of $SD = DS$), so according to (2.10) $q(t) = t^2 \in R$ is a cv-polynomial with respect to (S^2, D^2). Secondly, we take k to be of characteristic zero (instead of characteristic p). By the same proof as before, we can check that D^2 is not an S^2-inner derivation. But since we have now *char* $K = 0$, and $SD = -DS \Longrightarrow S^2D^2 = D^2S^2$, (4.11) implies that $R' = K[q(t)] \cong K[t', S^2, D^2]$ is a minimal Ore extension. Thus we have an example (promised earlier) of an Ore extension which is *minimal*, but not *maximal* (in view of $R' \subset R$).

In the last paragraph, $q(t) = t^2 \in R$ is clearly a non-linear cv-polynomial of minimal degree $n = 2$, but p can still be any prime. If we take $p = 2$, then $(n, o(S)) = (2, p) = 2$, so (5.24) applies. This implies that all non-linear cv-polynomials of R lie in $R' = K[q(t)]$. Since R' is minimal, we conclude further from (2.19) that the cv-polynomials in R are exactly those of the form $at^2 + b$, or $ct + d$ $(a, b, c, d \in K)$. Thus, we have an example of an Ore extension which has only linear and quadratic cv-polynomials. Furthermore, the only Ore extensions contained in R are R' and R itself.

References

[Am] S. A. Amitsur: *Derivations in simple rings,* Proc. London Math. Soc. **7**(1957), 87-112.

[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 Series, Vol. **27**, Cambridge University Press, 1977.

[JS] N. Jacobson and D. Saltman: *Finite Dimensional Division Algebras,* Springer-Verlag, Berlin-Heidelberg-New York, to appear.

[L_1] T. Y. Lam and A. Leroy: *Vandermonde and Wronskian matrices over division rings,* Journal of Algebra **119**(1988), 308-336.

[L_2] T. Y. Lam and A. Leroy: *Algebraic conjugacy classes and skew polynomial rings,* In: "Perspectives in Ring Theory", (F. van Oystaeyen and L. Le Bruyn, eds.), Proceedings of the Antwerp Conference in Ring Theory, pp.153-203, Kluwer Academic Publishers, 1988, Dordrecht/Boston/London.

[L_3] T. Y. Lam, K. H. Leung, A. Leroy and J. Matczuk: *Invariant and semi-invariant polynomials in skew polynomial rings,* in "Ring Theory 1989" (in honor of S. A. Amitsur), ed. L. Rowen, Israel Mathematical Conference Proceedings, Vol. **1**, pp. 247-261, Weizmann Science Press of Israel, 1989.

[L_4] T. Y. Lam and A. Leroy: *Hilbert 90 Theorems over division rings,* in preparation.

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

[Le_1] A. Leroy, J.-P. Tignol and P. van Praag: *Sur les anneaux simples différentiels,* Communications in Algebra **10**(1982), 1307-1314.

[Le_2] A. Leroy: *Dérivations algébriques,* Thèse, Université de l'Etat à Mons, 1985.

[Le_3] A. Leroy and J. Matczuk: *The extended centroid and X-inner automorphisms of Ore extensions,* to appear in Journal of Algebra.

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

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

[O_1] O. Ore: *Theory of non-commutative polynomials,* Annals of Math. **34**(1933), 480-508.

[O_2] O. Ore: *On a special class of polynomials,* Trans. Amer. Math. Soc. **35**(1933), 559-584.