Algebraic Conjugacy Classes and Skew Polynomial Rings

T. Y. Lam(*)
University of California
Berkeley, California 94720
U. S. A.

André Leroy
Université de l'État à Mons
B-7000 Mons
Belgium

Abstract. The goal of this paper is to develop further the theory of skew polynomial rings over division rings, using as our main tools the notions of invariant and semi-invariant polynomials. These notions arise naturally when one tries to study the algebraic conjugacy classes (in a suitably generalized sense) of the underlying division ring. A substantial part of our effort will also be devoted to the investigation of the properties and the characterizations of algebraic derivations, algebraic endomorphisms, and their respective minimal polynomials. This investigation is made possible by the discovery of the relationship between polynomial equations and differential equations, and the relationship between polynomial dependence and linear dependence. Applications of these results to the study of non-commutative Hilbert 90-type theorems will be presented in a forthcoming work $[LL_2]$.

§1. Introduction

Let K be a division ring equipped with a given endomorphism $S: K \longrightarrow K$. By an S-derivation on K, we mean an additive map $D : K \longrightarrow K$ with the property that $D(ab) = S(a)D(b) + D(a)b$ for all $a, b \in K$. For a given indeterminate t, let $R = K[t,S,D]$ denote the skew polynomial ring with respect to the triple (K,S,D), consisting of all left polynomials $\sum a_i t^i$ $(a_i \in K)$ which are added in the

(*)Supported in part by N.S.F.

usual way and multiplied according to the rule $ta = S(a)t + D(a)$ for any $a \in K$. This definition of skew polynomial rings was first introduced by Ore [O], who combined earlier ideas of Hilbert (in the case $D = 0$) and Schlessinger (in the case $S = I$). Ore lay a firm foundation for the study of $R = K[t,S,D]$ by establishing the unique factorization property of R, and using this, he studied, among other things, the problem of finding the greatest common divisors and the least common multiples of pairs of skew polynomials. Ever since the appearance of Ore's fundamental paper [O], the skew polynomial rings $K[t,S,D]$ (and their generalizations) have played an important role in non-commutative ring theory. About 15 years after Ore's paper appeared, Amitsur [A] made a basic contribution to the study of $K[t,S,D]$ by proving a generalization of a theorem on linear differential equations in a purely algebraic setting. Through this paper of Amitsur, the interesting role played by the so-called algebraic derivations (D is called <u>algebraic</u> if it satisfies a monic equation $\sum_{i=1}^{n} a_i D^i = 0$ over K) came to light. In [A'], Amitsur also studied, in the special case when $S = I$, the structure of the 2-sided ideals in $K[t,S,D]$; this work has been recently extended to the general case by Cauchon [C] and Lemonnier [Lem] (see also [Ca]).

Our present work is, in many ways, a continuation of the work on skew polynomial rings cited above. The point of departure is the introduction of the notion of "evaluation" of skew polynomials $f \in R$ on the constants $a \in K$. Surprisingly, the discovery of the right

definition of $f(a)$ came rather late in the game: two pertinent references are [Sm] and [Le], but even in these references, the fact that $f(a)$ amounts to the "evaluation" of f at a was not explicitly pointed out. In [LL_1], we rectified this by initiating the notation $f(a)$ for evaluation, and proved the all-important Product Theorem [LL_1 : (2.7)] for the evaluation of a product of two polynomials at $a \in K$. This notion of the evaluations of polynomials at constants enabled us to generalize the theory of Vandermonde and Wronskian matrices to the non-commutative setting, as in [LL_1].

The main goal of the present paper is to study the algebraic conjugacy classes in a division ring K equipped with (S,D). (We shall often write (K,S,D) to refer to this setting.) Recall from [LL_1] that two elements $a, b \in K$ are said to be (S,D)-conjugate if there exists an element $c \in K^*$ such that $b = a^c := S(c)ac^{-1} + D(c)c^{-1}$. (S,D)-conjugacy being an equivalence relation, we shall write $\Delta^{S,D}(a) := \{a^c : c \in K^*\}$ for the (S,D)-conjugacy class determined by a. This class is said to be (S,D)-algebraic (or algebraic for short) if there is a nonzero $f \in R$ which vanishes on all of $\Delta^{S,D}(a)$. The (unique) monic f of the least degree with this property is said to be the minimal polynomial of $\Delta^{S,D}(a)$. Such a polynomial f is always right invariant, in the sense that $f \cdot R \subseteq R \cdot f$. Therefore, the study of algebraic conjugacy classes is closely tied to the study of right invariant polynomials, which is, in turn, tied to the study of the 2-sided ideal structure of R.

This paper is organized as follows. In §2, we first study right invariant polynomials in R, along with the right semi-invariant polynomials. (We say that $g \in R$ is right semi-invariant if $g \cdot K \subseteq K \cdot g$.) We recall Cauchon's result on the classification of right invariant polynomials, and obtain (in the special case when S is an automorphism) a parallel result on the classification of right semi-invariant polynomials. In §3, we study Lemonnier's notion of quasi-algebraic derivations, and characterize in different ways the least possible degree of the non-constant right semi-invariant polynomials (if they exist). In §4, we fix our attention on a single (S,D)-conjugacy class $\Delta^{S,D}(a)$ and study the "polynomial dependence" (or P-dependence) among elements of $\Delta^{S,D}(a)$. It turns out that the P-dependence among elements of $\Delta^{S,D}(a)$ is "controlled" by the linear dependence of elements of K viewed as a right vector space over the division subring $C^{S,D}(a) := \{0\} \cup \{c \in K^* : a^c = a\}$. This fact is most succintly expressed by saying that there is a one-one correspondence between the lattice of "full" (S,D)-algebraic subsets of $\Delta^{S,D}(a)$ and the lattice of finite dimensional right $C^{S,D}(a)$-subspaces of K (cf. Theorem 4.5). This one-one correspondence is essentially given by the process of "exponentiation".

In §5 (which is perhaps the heart of this paper), we take up in earnest the study of the (S,D)-algebraic conjugacy classes in K. These classes are characterized in various ways, and their minimal polynomials are linked to the minimal polynomials of certain algebraic

derivations. This tie between the two kinds of minimal polynomials is made possible by Proposition 5.8 which establishes the basic relationship between polynomial equations and differential equations. One easily stated result is Corollary (5.12) which says that K has at least one (S,D)-algebraic class iff D is the sum of an inner S-derivation and an algebraic S-derivation. Among the many ramifications of our results characterizing the (S,D)-algebraic classes, one finds an interesting relationship between such classes and the notion of primitive rings: by Corollary 5.23, R is a left primitive ring unless all (S,D)-conjugacy classes are algebraic. Toward the end of the paper, we analyze the algebraic classes of K according as S is an automorphism of finite inner order or otherwise. In the latter case, we show that there is at most one (S,D)-algebraic class (Theorem (5.25)), while in the former case, we show that, with possibly one exception, the minimal polynomials of the algebraic classes are scalar multiples of central polynomials, and their degrees are all divisible by the inner order of S (Theorem (5.28)). Further results on the criteria for an (S,D)-conjugacy class to be algebraic, and for two elements in K to be (S,D)-conjugate (proved by using a certain "Composite Function Theorem") will be presented in a forthcoming work [LL_2].

Since this paper is largely a continuation of our earlier work [L] and [LL_1], the notations and terminology in these two papers will be used rather freely. However, the crucial definitions are

recalled for the convenience of the reader whenever possible. The definition of the evaluation of a polynomial $f \in R$ at $a \in K$ is needed only to the extent that $f(a)$ is the unique constant c such that $f(t) \in R\cdot(t-a) + c$. Whereas this is no doubt the best conceptual way to understand $f(a)$, we would be remiss if we do not mention at least once the "computational" definition of $f(a)$: if $f(t) = \sum b_i t^i$, then $f(a) := \sum b_i N_i(a)$, where the N_i's are defined inductively by: $N_o(a) = 1$, $N_{i+1}(a) = S(N_i(a))a + D(N_i(a))$. Note, however, that these formulas apply only to the evaluation of f on constants. An expression such as $f(D)$ (resp. $f(S)$) shall still have its usual meaning, namely, it stands for the operator $\sum b_i D^i$ (resp. $\sum b_i S^i$). The minimal polynomial of D (in case D is algebraic) is the monic polynomial $f \in R$ of the least degree such that $f(D) = 0$ (and similarly for S).

Often, we shall have occasion to specialize to the case $S = I$ (resp. the case $D = 0$). When we do this, we shall drop S (resp. D) from our notations. Thus, we shall write $K[t,D]$ to mean $K[t,I,D]$, and write $K[t,S]$ to mean $K[t,S,0]$. The same conventions will also apply to $\Delta^{S,D}(a)$ and $C^{S,D}(a)$. In any case, the abbreviated notations shall always be clear from the context.

We wish to thank Professor S. Amitsur for pointing out to us that his theorem on linear differential equations in $[A]$ can be proved by using the Density Theorem. Our presentations in the second half of §5 have taken his insightful comments into account.

§2. Invariant and Semi-invariant Polynomials

In this beginning section, we shall introduce the notions of right invariant and right semi-invariant polynomials and discuss their basic properties and characterizations. The important roles played by these two kinds of polynomials will be clear in the later sections when we take up the study of algebraic conjugacy classes in division rings. Throughout this section (and in fact the whole paper), we assume that the data (K,S,D) are given and fixed, where K is a division ring, S is an endomorphism of K, and D is an S-derivation on K. We shall always write R for the associated skew polynomial ring $K[t,S,D]$, and write K^* for the multiplicative group $K\setminus\{0\}$ of K.

Definition 2.1. A polynomial $f(t) \in R$ is called right invariant if $f \cdot R \subseteq R \cdot f$. (This means that the left ideal $R \cdot f$ is a 2-sided ideal of R.) A polynomial $g(t) \in R$ is called right semi-invariant if $g \cdot K \subseteq K \cdot g$. Left invariant and left semi-invariant polynomials are defined analogously.

The term "right invariant" is fairly standard in ring theory. Our choice of the new term "right semi-invariant" is based on the following rationale: Since R is generated as a ring by K and t, it follows that $f \in R$ is right invariant iff f is right semi-invariant and in addition $f \cdot t \subseteq R \cdot f$. This says that right semi-invariance amounts to "half" of the condition for right invariance. Also, note that the nonzero right (semi-) invariant polynomials are closed under multiplication, so they form a semigroup. In particular, if $a \in K^*$,

then f is right (semi-) invariant iff a·f is right (semi-) invariant. Because of this, it is generally sufficient to focus our study of right (semi-) invariant polynomials on the monic ones.

Lemma 2.2. For a monic polynomial $g(t) = \sum_{i=0}^{n} a_i t^i \in R$ of degree n, the following are equivalent:

(1) g is right semi-invariant;

(2) $g(t)c = S^n(c)g(t)$ for every $c \in K$;

(3) $S^n(c)a_j = \sum_{i=j}^{n} a_i f_j^i(c)$ for every j and every $c \in K$, where the operators $\{f_j^i\}$ are defined as at the beginning of §2 of $[LL_1]$.

Proof. (1)$\Longleftrightarrow$(2) follows by observing that, as a left polynomial, the leading coefficient of $g(t)c$ is $S^n(c)$. (2)$\Longleftrightarrow$(3) follows by comparing the coefficients of $S^n(c)g(t)$ with those of

$$\begin{aligned} g(t)c &= \sum_{i=0}^{n} a_i t^i c \\ &= \sum_{i=0}^{n} a_i \sum_{j=0}^{i} f_j^i(c) t^j \\ &= \sum_{j=0}^{n} \left(\sum_{i=j}^{n} a_i f_j^i(c) \right) t^j . \end{aligned}$$

Q.E.D.

Note that if $\Delta_{n+1}(c)$ denotes the $(n+1)\times(n+1)$ lower triangular matrix whose (i,j)-entry is $f_{j-1}^{i-1}(c)$ (cf. $[LL_1: (6.8)]$), then the condition (3) above can be expressed succintly in the matrix form:

$$(a_o, a_1, \ldots, a_n)\Delta_{n+1}(c) = S^n(c)(a_o, a_1, \ldots, a_n).$$

This says that $(a_o, a_1, \ldots, a_n)$ is a left "eigenvector" for the matrix $\Delta_{n+1}(c)$ with "eigenvalue" $S^n(c)$.

In the classical case $(S, D) = (I, 0)$, we see immediately that the right invariant and right semi-invariant polynomials are just the polynomials of the form $a \cdot \sum a_i t^i$, where $a \in K$ and all a_i's belong to the center $Z(K)$ of K. In order to get a good perspective on the general case, we shall work out below the classes of right invariant and right semi-invariant polynomials in the cases when $D = 0$ and when $S = I$. Throughout this paper, we shall write I_a for the inner automorphism $x \longmapsto axa^{-1}$ on K associated with $a \in K^*$. Also, we shall write $K^S = \{y \in K : S(y) = y\}$ and $K_D = \{y \in K : D(y) = 0\}$.

Proposition 2.3. Assume that $D = 0$, and let $f(t) = \sum_{i=0}^{n} a_i t^i \in K[t,S]$ be monic of degree n. Then

(1) f is right semi-invariant iff, for any j such that $a_j \neq 0$, we have $S^n = I_{a_j} \circ S^j$.

(2) f is right invariant iff f satisfies the condition above and in addition $a_j \in K^S$ for all j.

Proof. (1) Since $D = 0$, we have $f_j^i = 0$ whenever $i > j$. Thus, the condition in (2.2)(2) simplifies to $S^n(c)a_j = a_j S^j(c)$ $(\forall c \in K)$. If $a_j \neq 0$, this amounts to

$$S^n(c) = a_j S^j(c) a_j^{-1} = \left(I_{a_j} \circ S^j\right)(c) \qquad (\forall c \in K),$$

i.e. $S^n = I_{a_j} \circ S^j$. (Note. We cannot rewrite this as $S^{n-j} = I_{a_j}$ in general, since S is not assumed to be an automorphism. In the case when S is an automorphism, we can prove a much more precise result: see (2.12) below.)

(2) We need to work out here the condition for $f(t)t \in R \cdot f(t)$, i.e. for $f(t)t$ to be equal to $(t+c)f(t)$ for some $c \in K$. Since

$$(t+c)f(t) = t^{n+1} + \sum_{i=1}^{n} (S(a_{i-1}) + ca_i)t^i + ca_o ,$$

the conditions on c are that $a_i = S(a_i) + ca_{i+1}$ $(0 \leq i < n)$, and $ca_o = 0$. If $c \neq 0$, it follows by induction on i that all a_i's are zero. This is not the case as $a_n = 1$. Therefore, we must have $c = 0$ and the conditions above boil down to $a_i \in K^S$ for all i. Q.E.D.

Proposition 2.4. Assume that $S = I$ and let $f(t) = \sum_{i=o}^{n} a_i t^i \in K[t,D]$ be monic of degree n. Then

(1) $f(t)$ is right semi-invariant iff $ca_j = \sum_{i=j}^{n} \binom{i}{j} a_i D^{i-j}(c)$ for all $c \in K$ and all $j \geq 0$;

(2) $f(t)$ is right invariant iff f satisfies the condition above and in addition $a_j \in K_D$ for all j. Such a polynomial in fact belongs to the center of $K[t,D]$.

Proof. (1) Since $S = I$, f_j^i boils down to $\binom{i}{j} D^{i-j}$ for $i \geq j$. Thus the condition in (2.2)(2) simplifies to the one in (1).

(2) Again, we need to work out here the condition for $f(t)t$ to be equal to $(t+c)f(t)$ for some $c \in K$. Since

$$(t+c)f(t) = t^{n+1} + \sum_{i=1}^{n} \left(a_{i-1} + ca_i + Da_i\right) t^i + (ca_o + Da_o),$$

the conditions on c are that $ca_i + Da_i = 0$ for $0 \leq i \leq n$. Since $a_n = 1$, this amounts to $c = 0$ and $Da_i = 0$ for all i. We have then $f(t)t = tf(t)$, and since $f(t)c = cf(t)$ also, $f(t)$ belongs to the center of $K[t,D]$. Q.E.D.

By the above, we expect that there exist many examples of right semi-invariant polynomials which are not right invariant. Let us now record some such examples below.

Examples 2.5.

(a) Let $D = 0$, and let S be an automorphism of order 2. Then by (2.3), t^2+a is right semi-invariant for any $a \in Z(K)$, but such a polynomial is right invariant only if our a is also fixed by S.

(b) Let $S = I$, D be a derivation with $D^2 = 0$, and assume that char $K = 2$. Then by (2.4) (or by an explicit calculation), t^2+a is right semi-invariant for any $a \in Z(K)$, but such a polynomial is right invariant only if our a is also a constant of D.

The fact that we have to work with quadratic polynomials above has a good reason. In fact, the result below shows that, in the linear case, "right invariance" and "right semi-invariance" become synonymous terms.

Example 2.6. Here, we determine, in the general (S,D)-setting, all the the (monic) linear right invariant and right semi-invariant polynomials. Let $f(t) = t - b$, where $b \in K$. Then the following are equivalent:

(1) $f(t)$ is right invariant;

(2) $f(t)$ is right semi-invariant;

(3) $b \in Z^{S,D}(K) := \{ a \in K : a^c = a \ \ \forall c \in K^* \}$.

We need only show (2) $\Longrightarrow$ (3) $\Longrightarrow$ (1). Assume f is right semi-invariant. Then, for any $c \in K^*$,

$$S(c)(t - b) = (t - b)c = S(c)t + D(c) - bc.$$

Thus, $-S(c)b = D(c) - bc$ and hence $b = S(c)bc^{-1} + D(c)c^{-1} = b^c$, i.e. $b \in Z^{S,D}(K)$. Now assume $b \in Z^{S,D}(K)$. By reversing the above argument, we see that $f(t)$ is right semi-invariant. We finish by showing that $(t - b)t \in R\cdot(t - b)$. Assume, for the moment, that $b \neq 0$. From the equation $b^b = b$, we have $S(b)bb^{-1} + D(b)b^{-1} = b$, and so $D(b) = b'b$ for $b' = b - S(b)$. Of course, $D(b) = b'b$ also holds for $b = 0$. Thus, in any case,

$$\begin{aligned}(t - b)t &= t^2 - (S(b) + b')t + b'b - D(b)\\ &= t^2 - (S(b)t + D(b)) - b'(t - b)\\ &= t(t - b) - b'(t - b)\\ &= (t - b')(t - b) \in R\cdot(t - b),\end{aligned}$$

so $t - b$ is, in fact, right invariant. Q.E.D.

We have observed earlier that, if $g(t)$ and $h(t)$ in R are both right (semi-) invariant, then so is $g(t)h(t)$. In the case when S is an automorphism of K, we can prove some variations of this fact, as in part (3) of the following result.

Proposition 2.7. Let $S \in \mathrm{Aut}(K)$. Then

(1) $f(t) \in R$ is right (semi-) invariant iff f is left (semi-) invariant (cf. [Co': pp.296-297]);

(2) If f is right invariant, then $R\cdot f = f\cdot R$; if f is right semi-invariant, then $K\cdot f = f\cdot K$.

(3) Let $f(t) = g(t)h(t) \neq 0$ in R be right (semi-) invariant. Then $g(t)$ is right (semi-) invariant iff $h(t)$ is.

Proof. (1) By symmetry, it is sufficient to prove the "only if" parts. Assume f is right invariant. For any $p(t) \in R$, we can write $p(t)f(t) = f(t)q(t) + r(t)$ for some $q(t), r(t) \in R$ such that $\deg r(t) < \deg f(t)$. (This is possible since S is assumed to be an automorphism.) Since f is right invariant, $f(t)q(t) = q'(t)f(t)$ for some $q' \in R$. Thus, $(p(t) - q'(t))f(t) = r(t)$. By degree consideration, this implies that $q'(t) = p(t)$ and $r(t) = 0$, and so $p(t)f(t) = f(t)q(t) \in f(t)\cdot R$, i.e. $f(t)$ is left invariant. If $f(t)$ is right semi-invariant, the same argument for $p(t)$ a scalar shows that f is also left semi-invariant.

(2) This is already covered by the argument above.

(3) Assume $f(t)$ and $h(t)$ are both right invariant. Then, for any $p(t) \in R$, $ph = hp'$ for some $p' \in R$ (since h is also left invariant). Thus, $gph = ghp' = fp' = p''f$ for some $p'' \in R$, since f is right invariant. Cancelling h on the right, we have $gp = p''g$. Since $p \in R$ is arbitrary, this shows that g is right invariant. Similarly, if $f(t)$ and $g(t)$ are both right invariant, we can show that $h(t)$ is also right invariant. The arguments for the case of semi-invariance are almost the same as those given above; we shall therefore leave them to the reader.

In [C], Cauchon has determined the structure of the right invariant polynomials in $R = K[t,S,D]$, generalizing earlier work of

Amitsur [A'] in the case $S = I$. For the convenience of the reader, we shall recall Cauchon's result, which will be exploited in §5. Cauchon's result holds more generally for any artinian simple ring K, but we shall only be concerned with the case when K is a division ring here. Another pertinent reference for the result below is [Ca].

Theorem 2.8. (Cauchon) Let $q(t)$ be a (monic) nonconstant right invariant polynomial of the least degree (if it exists). Then any right invariant polynomial in R has the form $\alpha \cdot h(t)q(t)^r$ where $\alpha \in K$, $r \geq 0$ and $h(t)$ is a polynomial in $Z(R)$, the center of R. Moreover, let $h_o(t)$ be a nonconstant polynomial in $Z(R)$ of the least degree (if it exists); then $h_o(t) = \lambda \cdot q(t)^s$ for some $\lambda \in K^*$ and $s \geq 1$, and $Z(R) = Z(K)_{S,D}[h_o(t)]$ where $Z(K)_{S,D} = Z(K) \cap K^S \cap K_D$.

Prompted by this result, we shall try to determine also the structure of all right semi-invariant polynomials in R. Our methods below will lead to such a complete determination in the case when S is an automorphism of K. (The case when S is not an automorphism seems to be much more difficult, and will not be attempted here.) The first step in this analysis is the following.

Proposition 2.9. Assume $S \in \mathrm{Aut}(K)$, and let $p(t)$ be a (monic) nonconstant right semi-invariant polynomial in R of the least degree (if it exists). Then any right semi-invariant polynomial $f(t)$ lies in $K[p(t)] = \left\{ \sum a_i p(t)^i : a_i \in K \right\}$ (the subring of R generated by K and $p(t)$). In particular, $\deg f$ must be a multiple of $\deg p$.

Proof. Let $\deg p(t) = m > 0$ and $\deg f(t) = n$. We shall prove the Proposition by induction on n, the case $n = 0$ being clear. For $n > 0$, write $f(t) = q(t)p(t) + r(t)$, where $\deg r(t) < m$ (or $r(t) = 0$). Let $c \in K$. Assuming without loss of generality that f is monic, we have $f(t)c = S^n(c)f(t)$ for any $c \in K$, and so

$$S^n(c)q(t)p(t) + S^n(c)r(t) = q(t)p(t)c + r(t)c$$
$$= q(t)S^m(c)p(t) + r(t)c.$$

Transposition yields

$$\left[S^n(c)q(t) - q(t)S^m(c)\right] p(t) = r(t)c - S^n(c)r(t).$$

By degree consideration, we must have

(*) $\quad r(t)c = S^n(c)r(t)$ and

(**) $\quad q(t)S^m(c) = S^n(c)q(t)$.

Replacing c by $S^{-m}(c)$ (the fact that $S \in \mathrm{Aut}(K)$ is needed here), (**) shows that $q(t)\cdot K \subseteq K\cdot q(t)$, i.e. $q(t)$ is right semi-invariant. Using the inductive hypothesis, we have then $q(t) \in K[p(t)]$. From (*), we see also that $r(t)$ is right semi-invariant. Since $\deg r(t) < m$, $r(t)$ must then be a constant. Thus, we have

$$f(t) = q(t)p(t) + r(t) \in K[p(t)]\cdot p(t) + K \subseteq K[p(t)]. \quad \text{Q.E.D.}$$

Proposition 2.10. Assume that the above $p(t)$ exists (but not assuming S to be an automorphism). Then $p(t)$ is unique up to an additive constant. Moreover, for $a \in K^*$, $p(t) + a$ is right semi-invariant

iff $S^m = I_a$ (where $m = \deg p$). In particular, $p(t)$ is unique iff S^m is not an inner automorphism.

Proof. Suppose $p'(t)$ is another candidate. Then $\deg p' = \deg p = m$, from which we see easily that $p'(t) - p(t)$ is right semi-invariant. Therefore, $p'(t) - p(t) = a \in K$. For $p(t) + a$ $(a \in K^*)$ to be actually right semi-invariant, we need

$$\begin{aligned} S^m(c)(p(t) + a) &= (p(t) + a)c \\ &= S^m(c)(p(t) + a) + (ac - S^m(c)a) \end{aligned}$$

for all $c \in K$, i.e. $S^m(c) = aca^{-1}$. Thus the necessary and sufficient condition is that $S^m = I_a$. The last statement of the Corollary now follows immediately from this. Q.E.D.

We are now in a position to determine the set of all right semi-invariant polynomials in R, in case S is an automorphism. Letting $\mathrm{Inn}(K)$ denote the group of inner automorphisms of K, the order of S in $\mathrm{Aut}(K)/\mathrm{Inn}(K)$ is called the inner order of S. It turns out that it is this inner order which holds the key to the structure of the set of right semi-invariant polynomials.

Theorem 2.11. Assume $S \in \mathrm{Aut}(K)$, and let $p(t)$ be a (monic) non-constant right semi-invariant polynomial in R of the least degree, say m.

(1) If S has infinite inner order, then the right semi-invariant polynomials in R are precisely those of the form $a \cdot p(t)^r$ where $a \in K$ and $r \geq 0$.

(2) Let S be of finite inner order k, say $S^k = I_u$ $(u \in K^*)$. Let $d = \gcd(k, m)$ and write $k = dk'$, $m = dm'$. Then the right semi-invariant polynomials in R are precisely those of the form

$$(*) \qquad a \cdot \sum_{\substack{0 \le i \le r \\ i \equiv r \,(\mathrm{mod}\ k')}} \varepsilon_i u^{(r-i)m'/k'} p(t)^i ,$$

where $a \in K$, $\varepsilon_r = 1$ and $\varepsilon_i \in Z(K)$.

Proof. Let $f(t) \in R$ be a monic right semi-invariant polynomial. By (2.9), $f(t)$ is expressible in the form $\sum_{i=0}^{r} a_i p(t)^i$, with $n = \deg f = mr$, and $a_n = 1$. The right semi-invariance condition $f(t)c = S^n(c)f(t)$ $(\forall\, c \in K)$ now becomes

$$\sum S^n(c) a_i p(t)^i = \sum a_i p(t)^i c = \sum a_i S^{mi}(c) p(t)^i ,$$

i.e. $S^n(c)a_i = a_i S^{mi}(c)$ for $0 \le i \le r$. Replacing c by $S^{-mi}(c)$, this amounts to $S^{n-mi}(c)a_i = a_i c$ (for all $c \in K$). Therefore, in Case (1), all a_i's must be zero for $i < r$, and we get $f(t) = p(t)^r$. Conversely, of course, all $a \cdot p(t)^r$ are right semi-invariant. Now assume we are in Case (2), and use the notations there. Then, whenever $a_i \neq 0$, we have $S^{n-mi} = I_{a_i}$ and therefore the inner order k of S divides $n-mi = m(r-i)$, and so k' divides $r-i$. Moreover,

$$I_{a_i} = S^{n-mi} = S^{k(r-i)m'/k'} = I_u^{(r-i)m'/k'}$$

implies that $a_i = \varepsilon_i u^{(r-i)m'/k'}$ for some $\varepsilon_i \in Z(K)$. Therefore, $f(t)$ has the form (*) (with $a = 1$). Conversely, consider any

summand $f_i(t) = \varepsilon_i u^{(r-i)m'/k'} p(t)^i$ of (*) where $0 \leq i \leq r$, $i \equiv r \pmod{k'}$ and $\varepsilon_i \in Z(K)$. Writing $r-i = k'j$, we have $mi = mr - kjm'$, so for any $c \in K$:

$$\begin{aligned} f_i(t)c &= \varepsilon_i u^{jm'} \cdot S^{mi}(c)\, p(t)^i \\ &= \varepsilon_i u^{jm'} \left(S^{-k}\right)^{jm'} \left(S^{mr}(c)\right) p(t)^i \\ &= \varepsilon_i u^{jm'} \cdot I_{u^{-i}}^{jm'}\left(S^{mr}(c)\right) p(t)^i \\ &= \varepsilon_i S^{mr}(c)\, u^{jm'}\, p(t)^i \\ &= S^{mr}(c)\, f_i(t) \ . \end{aligned}$$

It follows that any $a \cdot \sum f_i(t)$ as in (*) is right semi-invariant.

Q.E.D.

It is worthwhile to record the simplest manifestation of the theorem above, in the special case when $D = 0$. Note that in this case we can choose $p(t) = t$.

Corollary 2.12. Assume that $S \in \mathrm{Aut}(K)$ and $D = 0$.
(1) If S has infinite inner order, then $a \cdot t^r$ $(a \in K,\ r \geq 0)$ are all the right semi-invariant polynomials in $R = K[t,S]$.
(2) Let S be of finite inner order k, say $S^k = I_u$. Then the right semi-invariant polynomials in R are precisely those of the form $a \cdot \sum_{j \geq 0} c_j u^j t^{r-kj}$, where $a \in K$, $c_0 = 1$, and $c_j \in Z(K)$.

§3. Quasi-algebraic derivations

The material in the second half of §2 calls to attention the important question: When does there exist a (monic) non-constant right semi-invariant polynomial in $R = K[t,S,D]$? In order to give an answer to this question, we recall the following definition which was first introduced in the 1984 thesis of B. Lemonnier [Lem].

Definition 3.1. An S-derivation D is called quasi-algebraic if there exist $a_1, \dots, a_n \in K$ with $a_n = 1$ such that $\sum_{i=1}^{n} a_i D^i$ is an inner derivation with respect to the endomorphism S^n. (For instance, any S-inner derivation is quasi-algebraic, and so is any algebraic S-derivation.)

With this defintion, we have the following answer to the question raised at the beginning of this section, without any assumptions imposed on S. The equivalence (1)$\Longleftrightarrow$(3) herein is due to Lemonnier [Lem: Th. (9.21)].

Theorem 3.2. The following are equivalent for $R = K[t,S,D]$:

(1) There exists a (monic) non-constant right semi-invariant polynomial in R ;

(2) There exists a polynomial $g(t) = \sum_{i=0}^{n} a_i t^i \in R$ with $n \geqslant 1$ and $a_n = 1$ such that for any $c \in K$:

(*) $\quad g(t)c \equiv S^n(c)g(t) \pmod{R\cdot t}$;

(3) The S-derivation D is quasi-algebraic.

Because of the intrinsic interest of this result, and because of the fact that Lemonnier's proof of (1)$\Longleftrightarrow$(3) is not easily accessible, we shall offer a complete and direct proof of the Theorem below.

Proof of (3.2). (1)$\Longrightarrow$(2) is obvious (see (2.2)(2)).

(2)$\Longrightarrow$(3). (*) means that $g(t)c$ and $S^n(c)g(t)$ have the same constant term when both are written out as left polynomials. Therefore, going through the proof of (2)$\Longleftrightarrow$(3) for Lemma 2.2, we can still compare the constant terms, and thereby ascertain the conclusion (2.2)(3) for $j = 0$, i.e. we'll have for all $c \in K$:

$$S^n(c)a_o = \sum_{i=o}^{n} a_i f_o^i(c) = \sum_{i=o}^{n} a_i D^i(c).$$

Therefore,

$$\sum_{i=1}^{n} a_i D^i(c) = S^n(c)a_o - a_o c = D_{-a_o, S^n}(c) \quad (\forall\, c \in K), \tag{3.3}$$

which means, by defintion, that D is quasi-algebraic.

(3)$\Longrightarrow$(1). Suppose D is quasi-algebraic, say with (3.3) holding for suitable constants $a_o, \ldots, a_n$, with $n \geqslant 1$, $a_n = 1$. Let $g(t) := \sum_{i=o}^{n} a_i t^i \in R$. Then, for any $x \in K$, we have

$$g(D)(x) = \left(D_{-a_o, S^n} + a_o I\right)(x) = S^n(x)a_o \,. \tag{3.4}$$

Replacing x by cx (where $c \in K$), we then have

$$g(D)(cx) = S^n(c)S^n(x)a_o = S^n(c)g(D)(x).$$

Therefore, we have an operator equation

(3.5) $\qquad g(D)c = S^n(c)g(D) \qquad (\forall c \in K),$

where the constants are thought of as left multiplication operators on K. This equation holds in the image of the natural ring homomorphism

(3.6) $\qquad \varepsilon : K[t,S,D] \longrightarrow \mathrm{End}\ (K, +)$

which sends t to D and sends the constants in K to their left multiplication operators. We now go into the following two cases.

Case A. $\ker \varepsilon = 0$ (i.e. D is not algebraic). Here, ε is injective, so the equation (3.5) pulls back to a polynomial equation $g(t)c = S^n(c)g(t)$ in $K[t,S,D]$, and hence $g(t)$ is right semi-invariant.

Case B. $\ker \varepsilon \neq 0$ (i.e. D is algebraic). Let $\ker \varepsilon = R \cdot h$ (using the fact that R is a left PID). Then, since $\ker \varepsilon$ is a 2-sided ideal, $h \neq 0$ is right invariant, in particular right semi-invariant. Q.E.D.

We have also the following supplement to the theorem above.

Theorem 3.7. Assume that R has a (monic) non-constant right semi-invariant polynomial.

(1) Let $p(t)$ be such a monic polynomial of the least degree, say m.

(2) Let $p'(t)$ be a monic non-constant polynomial of the least degree, say m', such that $p'(t)c \equiv S^{m'}(c)p'(t) \pmod{R \cdot t}$ $(\forall c \in K)$.

(3) Let $a_0, \ldots, a_n \in K$ be such that $n \geq 1$, $a_n = 1$, and

$\sum_{i=1}^{n} a_i D^i = D_{-a_o, S^n}$, where n is chosen to be as small as possible; let $g(t) = \sum_{i=o}^{n} a_i t^i$.

Then we have $m = m' = n$, $p'(t)$, $g(t)$ are both right semi-invariant, and $p(t) \equiv p'(t) \equiv g(t) \pmod{K}$. Moreover, $p(t) = p'(t) = g(t)$ unless S^m is an inner automorphism. If D happens to be algebraic and S is an automorphism, then the degree of the minimal polynomial for D is always a multiple of m.

Proof. From the proof of (2) $\Longrightarrow$ (3) in the theorem, we have $n \leq m'$, and of course also $m' \leq m$. As before, we shall distinguish the following two cases depending on the behavior of the homomorphism ε in (3.6) :

Case A. $\ker \varepsilon = 0$. From the "pullback" argument used before, we see that $g(t)$ and $p'(t)$ are in fact right semi-invariant. Therefore $m \leq n$ and hence $n \leq m' \leq m$ now become equalities. By (2.10), we conclude further that $p(t) \equiv p'(t) \equiv g(t) \pmod{K}$.

Case B. $\ker \varepsilon \neq 0$. Write $\ker \varepsilon = R \cdot h$ where h is the minimal polynomial of the algebraic derivation D. For the polynomial $g(t)$, recall that we have the operator equation

$$g(D)c = S^n(c)g(D) \qquad \text{(cf. (3.5))}$$

holding for every $c \in K$. Lifting this equation back to R using the homomorphism ε, we have

$$g(t)c - S^n(c)g(t) = q_c(t)h(t), \tag{3.8}$$

where $q_c(t) \in R$ depends on c. Since $h(t)$ is right invariant, $\deg h \geq m$. If there exists a $c \in K$ such that the LHS above is not zero, then, for this c, we would have

$$n > \deg (\text{LHS}) \geq \deg h(t) \geq m,$$

a contradiction. Therefore, the LHS of (3.8) is zero for all $c \in K$, i.e. g is right semi-invariant. Replacing g by p', we see similarly that p' is right semi-invariant. Therefore, we can finish the argument exactly as in Case A.

The uniqueness statement in the Theorem now follows from Prop. (2.10). In fact, we are free to change any one of $p(t)$, $p'(t)$ and $g(t)$ by an additive constant $a \in K$ iff $S^m = I_a$. Finally, if D is algebraic (Case B above), its minimal polynomial $h(t)$, being right invariant, will be expressible as a (left) polynomial in $p(t)$, in case S is an automorphism (see (2.9)). It follows then that $\deg h$ is divisible by $\deg p = m$. Q.E.D.

Corollary 3.9. Assume S is an automorphism, and that D is algebraic with a minimal polynomial h of prime degree ℓ. If D is not an inner S-derivation, then no $D^r + b_{r-1}D^{r-1} + \ldots + b_1 D$ with $r < \ell$ can be an inner S^r-derivation, and $h(t)$ has the least degree among all non-constant right semi-invariant polynomials.

Proof. Keeping the notations in Th. (3.7), we have $\deg g \mid \deg h$. Since $\deg h = \ell$ is prime and $n = \deg g \neq 1$, we must have $m = n = \ell$, which gives the two desired conclusions. Q.E.D.

Having looked at conditions for the existence of non-constant right semi-invariant polynomials, it is natural to look for conditions for the existence of non-constant right invariant polynomials (i.e. for the non-simplicity of R). There seems to be some evidence for the following

(3.10) Conjecture. R has a non-constant right invariant polynomial iff it has a non-constant right semi-invariant polynomial. Or equivalently (in view of Th. (3.2)), R is non-simple iff D is quasi-algebraic.

(Needless to say, the weight of the Conjecture is in the "if" part.)

Most remarkably, Lemonnier has proved the truth of this Conjecture in the case when S is an automorphism [Lem]. This result has provided the strongest evidence for the Conjecture so far. Recall also (from (2.6)) that if there is a linear right semi-invariant polynomial f, then f must be automatically right invariant. Such a polynomial f exists iff D is an inner S-derivation (cf. [LL_1: (3.4)(1)]): in this case, the Conjecture is, therefore, trivially true.

In view of Theorem (3.7), it will be of interest to give as much information as possible on "the" polynomial p(t), if it exists. We shall content ourselves here by dealing with the two key cases (a) D = 0, and (b) S = I. In case (a), we can just take p(t) = t and (3.7) gives all the desired information. In case (b), we have

the following fairly precise description of $p(t)$, largely inspired by ideas in [A'] and in [LM].

Theorem 3.11. (S = I) Let $p(t) = \sum a_i t^i$ be a monic non-constant right semi-invariant polynomial of the least degree, say m. (We are assuming that $p(t)$ exists.) Then:

(1) $D(a_i) = 0$ for $i = 1,2,\ldots,m$, and $D(a_o) \in Z(K)$, the center of K.

(2) If char $K = p > 0$, then $p(t)$ has the form $\sum_{i=o}^{k} c_i t^{p^i} + a_o$, where $c_i \in Z(K) \cap K_D$ and $D(a_o) \in Z(K)$. Moreover, $\sum_{i=o}^{k} c_i D^{p^i} = D_{-a_o}$.

(3) If char $K = 0$, then $p(t) = t + a_o$ and $D = D_{-a_o}$.

Proof. Since $S = I$, to say that a polynomial is right semi-invariant simply means that it commutes with constants (see(2.2)(2)). To prove (1), the crucial observation is that $tp(t) - p(t)t$ commutes with constants. In fact, for any $c \in K$,

$$\begin{aligned} \left[tp(t) - p(t)t\right] c &= tcp(t) - p(t)(ct + D(c)) \\ &= ctp(t) + D(c)p(t) - p(t)ct - p(t)D(c) \\ &= c\left[tp(t) - p(t)t\right]. \end{aligned} \tag{3.12}$$

On the other hand,

$$\begin{aligned} tp(t) - p(t)t &= t^{m+1} + a_{m-1}t^m + (D(a_{m-1}) + a_{m-2})t^{m-1} + \ldots. \\ &\quad - t^{m+1} - a_{m-1}t^m - \ldots. \\ &= \sum_{i=o}^{m-1} D(a_i)t^i \end{aligned}$$

has degree $< m$. Thus, (by the minimal choice of m), $tp(t) - p(t)t$ must be a constant (namely, $D(a_o)$). This gives $D(a_i) = 0$ for $i \geq 1$,

and (3.12) gives $D(a_o) \in Z(K)$.

(2) By (2.4)(1), we have

$$ca_j = \sum_{i=j}^{m} \binom{i}{j} a_i D^{i-j}(c) \quad \text{for any } c \in K, \text{ and } j \geq 0. \tag{3.13}$$

For $j \geq 1$, define the polynomials

$$\begin{cases} p_j(t) := \sum_{i=j}^{m} \binom{i}{j} a_i t^{i-j} \in K[t,D] & \text{with} \\ \deg p_j(t) \leq m - j < m. \end{cases} \tag{3.14}$$

Calculating as in [LM: pp.1255-1256], we can check via (3.13) that each $p_j(t)$ $(1 \leq j \leq m)$ commutes with constants. By the minimal choice of m, we must have then $p_j(t) = a_j \in Z(K)$ (in addition to $a_j \in K_D$ which we proved in (1)), and from (3.14), we see that

$$\binom{i}{j} a_i = 0 \quad \forall\ i, j \text{ such that } 1 \leq j < i \leq m. \tag{3.15}$$

Exactly as in [LM], we conclude from this that, when char $K = p > 0$, $a_j \neq 0$ $(j \geq 1)$ can occur <u>only when</u> j is a power of p. Therefore, $p(t)$ has the form $\sum_{i=o}^{k} c_i t^{p^i} + a_o$, and it follows from (3.3) that $\sum_{i=o}^{k} c_i D^{p^i}$ is equal to the inner derivation D_{-a_o}. (Aside from the constant term a_o, $p(t)$ is a "p-polynomial" in the sense of Ore [O'].)

(3) Now assume char $K = 0$. In this case, setting $i = m$ in (3.15), we have $\binom{m}{j} a_m = 0$ whenever $1 \leq j < m$. Since $a_m = 1$, the only way for this to be possible is when $m = 1$. Thus, $p(t) = t + a_o$, and by (3.3) (for instance), we have $D = D_{-a_o}$. Q.E.D.

§4. P-dependence and linear dependence

We begin by recalling some basic notions from [L]. These notions were introduced in [L] in the case $D = 0$, but they are equally meaningful in the general case. A set $\Delta \subseteq K$ is called (S,D)-algebraic (or just algebraic if (S,D) is clear from the context) if there exists a nonzero polynomial $f(t) \in R = K[t,S,D]$ such that $f(\Delta) = 0$. In this case, the monic f of the least degree with $f(\Delta) = 0$ is called the minimal polynomial of Δ, and the rank of Δ is defined to be the degree of such an f. The basic properties developed in [L] for minimal polynomials carry over without change to the (S,D)-setting. In particular, the minimal polynomial f for an (S,D)-algebraic set Δ has always a complete factorization $(t-a_1)\ldots(t-a_n)$ in $K[t,S,D]$ where each a_i is (S,D)-conjugate to some element of Δ, and any zero of f is also (S,D)-conjugate to some element of Δ. If Δ is (S,D)-algebraic, an element $b \in K$ is said to be P-dependent (or polynomially dependent) on Δ if every polynomial vanishing on Δ also vanishes on b (or, equivalently, the minimal polynomial of Δ vanishes on b). By what we said above, such an element b must be (S,D)-conjugate to some element of Δ.

In this section, we shall focus our attention on subsets of a fixed (S,D)-conjugacy class $\Delta^{S,D}(a)$. Let C denote the (S,D)-centralizer $C^{S,D}(a) = \{0\} \cup \{c \in K^* : a^c = a\}$ of a. Then C is a division subring of K (see $[LL_1]$), and K may be viewed as a right vector space over C. In this section, we shall show

that there is a very close relationship between P-dependence for elements in $\Delta^{S,D}(a)$ and right C-linear dependence for elements of K. The basic tool needed to establish this relationship is the idea of an "exponential space" introduced (though without such a name) in $[LL_1]$: for any polynomial $f(t) \in K[t,S,D]$, let

$$E(f, a) = \{0\} \cup \{y \in K^* : f(a^y) = 0\}. \tag{4.1}$$

This is easily seen to be a right C-vector space, henceforth called the exponential space of f at a. In $[LL_1$: Th. (4.2)], we have proved the basic inequality $\dim_C E(f, a) \leq \deg f$ (which, in the special case $a = 0$, boils down to Amitsur's Theorem in [A]). We shall now explore some consequences of this important inequality.

Proposition 4.2. Let Y be any subset of K^*, and let a^Y denote $\{a^y : y \in Y\}$. Then a^Y is (S,D)-algebraic iff span(Y) is finite dimensional over $C := C^{S,D}(a)$. (Here, span(Y) denotes the right C-vector space of K spanned by Y.) Furthermore, in this case, $\text{rank}\,(a^Y) = \dim_C \text{span}(Y)$.

Proof. For the "only if" part, let $f \in R = K[t,S,D]$ be the minimal polynomial of a^Y. Then $Y \subseteq E(f, a)$ and so

$$\dim_C \text{span}(Y) \leq \deg f = \text{rank}\,(a^Y) < \infty .$$

Conversely, suppose span(Y) has right C-dimension $n < \infty$ and let $y_1,\ldots,y_n \in Y$ form a C-basis for span(Y). Fix a polynomial $g \in R \setminus \{0\}$ of degree $\leq n$ such that $g(a^{y_i}) = 0$ for $i = 1,2,\ldots,n$

(see [L : Prop. 6]). Then $y_i \in E(g, a)$ for all i implies that $Y \subseteq E(g, a)$ and so $g(a^Y) = 0$. This shows that a^Y is (S,D)-algebraic with rank $(a^Y) \leq \deg g \leq n = \dim_C \text{span}(Y)$. Q.E.D.

Proposition 4.3. Let $Y \subseteq K^*$ be such that $a^Y \subseteq \Delta^{S,D}(a)$ is (S,D)-algebraic. Then, for any $x \in K^*$, a^x is P-dependent on a^Y iff $x \in \text{span}(Y)$.

Proof. First assume $x \in \text{span}(Y)$. Consider any $f \in R$ such that $f(a^Y) = 0$. Then $Y \subseteq E(f, a)$ implies that $\text{span}(Y) \subseteq E(f, a)$. Therefore, $x \in E(f, a)$, i.e. $f(a^x) = 0$. This shows that a^x is P-dependent on a^Y. Conversely, assume a^x is P-dependent on a^Y. Then rank $\{a^Y, a^x\}$ = rank (a^Y) and so, by the Proposition above, we have $\dim_C \text{span}\{Y, x\} = \dim_C \text{span}(Y)$. This clearly implies that $x \in \text{span}(Y)$. Q.E.D.

Definition 4.4. An (S,D)-algebraic set Δ is said to be full if every $x \in K$ which is P-dependent on Δ actually belongs to Δ.

From what we said earlier about minimal polynomials, it follows readily that an (S,D)-algebraic set Δ is full iff Δ consists of all the zeros of its minimal polynomial in K.

Theorem 4.5. Let $a \in K$ be given and let $C = C^{S,D}(a)$. Then there is a one-one correspondence between the full (S,D)-algebraic subsets of $\Delta^{S,D}(a)$ and the finite dimensional right C-linear subspaces of K. Moreover, this one-one correspondence preserves inclusion and rank.

Proof. For a finite dimensional right C-subspace $Y \dot{\cup} \{0\} \subseteq K$,

we associate the (S,D)-algebraic subset a^Y of $\Delta^{S,D}(a)$. We claim that a^Y is full. Indeed, let z be an element of K which is P-dependent on a^Y. Then z is a zero of the minimal polynomial of a^Y, and so $z \in \Delta^{S,D}(a)$. Write $z = a^x$ where $x \in K^*$. By Proposition (4.3), we must have $x \in \text{span}(Y) = Y \dot{\cup} \{0\}$ and so $a^x \in a^Y$, as desired. Next, we have to show that $Y \dot{\cup} \{0\} \longmapsto a^Y$ gives the desired one-one correspondence. First, suppose $a^Y = a^{Y'}$, where $Y \dot{\cup} \{0\}$, $Y' \dot{\cup} \{0\}$ are both finite dimensional right C-subspaces of K. Then for any $y \in Y$, we have $a^y = a^{y'}$ for some $y' \in Y'$. But then, conjugating by y'^{-1}, we get $a = (a^y)^{y'^{-1}} = a^{y'^{-1}y}$ (see $[LL_1: (2.6)]$), so $y'^{-1}y \in C$, i.e. $y \in y'C \subseteq Y' \dot{\cup} \{0\}$. This shows that $Y \subseteq Y'$ and so by symmetry we must have $Y = Y'$. Finally, let Δ be any full (S,D)-algebraic subset of $\Delta^{S,D}(a)$, say with minimal polynomial f. Then Δ consists of all zeros of f. Let $Y := \{ y \in K^* : a^y \in \Delta \}$. To show that $Y \dot{\cup} \{0\}$ is a right C-subspace of K, let $y_1, y_2 \in Y$ and $c_1, c_2 \in C$. We have $f(a^{y_1}) = f(a^{y_2}) = 0$ so $y_1, y_2 \in E(f, a)$, which implies that $y_1c_1+y_2c_2 \in E(f, a)$. If $y_1c_1+y_2c_2 \neq 0$, we'll have $f(a^{y_1c_1+y_2c_2}) = 0$ and so $a^{y_1c_1+y_2c_2} \in \Delta$. By the definition of Y, we have then $y_1c_1+y_2c_2 \in Y$. We have clearly $a^Y = \Delta$ and by Proposition (4.2), $\dim_C Y \dot{\cup} \{0\} = \text{rank } \Delta < \infty$. The proof is now complete.

In $[L]$, it was shown that many of the key facts on linear dependence and bases in linear algebra have valid analogues for P-dependence and P-bases. (All arguments in $[L]$ extend without

change to the (S,D)-setting.) The above results giving the explicit relationship between P-dependence and linear dependence have now explained why such a close analogy should exist. Actually, this relationship has already been exploited in [LL_1: Th. (4.4)] in our computation of the rank of an (S,D)-Vandermonde matrix. The work we did in this section gives a fuller treatment of the ideas involved, and makes explicit the one-one correspondence in Theorem 4.5 above.

§5. Algebraic Conjugacy Classes

We begin with a few basic observations.

Lemma 5.1. Let $f \in R = K[t,S,D]$ be a right semi-invariant polynomial. If $a \in K$ is such that $f(a) = 0$, then $f(\Delta^{S,D}(a)) = 0$.

Proof. For any $c \in K^*$, we have $f(t)c = c'f(t)$ for some $c' \in K$ depending on c. Using the Product Theorem $[LL_1: (2.7)]$ to evaluate the two sides of this equation at a, we get $f(a^c)c = c'f(a) = 0$, and so $f(a^c) = 0$ for every $c \in K^*$. Q.E.D.

Lemma 5.2. Let Δ be an (S,D)-algebraic subset of K which is closed under (S,D)-conjugation. (This means that Δ is the union of a finite number of (S,D)-conjugacy classes of K.) Then the minimal polynomial $f(t) \in R$ of Δ is a right invariant polynomial.

Proof. Consider any $h(t) \in R$. If we can show that $f(t)h(t)$ vanishes on Δ, then we will have $f \cdot h \in R \cdot f$ as desired. Let b be any element of Δ. By the Product Theorem again, we have

$$(fh)(b) = \begin{cases} 0 & \text{if } h(b) = 0, \\ f(b^c)c & \text{if } c := h(b) \neq 0. \end{cases}$$

In the second case, since $b \in \Delta$ implies that $b^c \in \Delta$, $f(b^c)$ is also zero, and so fh vanishes on all of Δ. Q.E.D.

Proposition 5.3. Let Δ be a full (S,D)-algebraic set (in the sense of (4.4)) with minimal polynomial $f \in R$. Then the following are equivalent:

(1) Δ is closed under (S,D)-conjugation;

(2) f is right invariant;

(3) f is right semi-invariant.

Proof. (1) $\Longrightarrow$ (2) is given by the preceding lemma, and (2) $\Longrightarrow$ (3) is obvious. For (3) $\Longrightarrow$ (1), let $a \in \Delta$ and consider any conjugate a^c of a. Since we assume f is right semi-invariant, $f(a) = 0$ implies that $f(a^c) = 0$ by Lemma 5.1. The fact that Δ is full means that Δ consists of all the zeros of f. Therefore, we have $a^c \in \Delta$. Q.E.D.

Proposition 5.4. Let Δ be a finite disjoint union $\bigcup_{i=1}^{n} \Delta^{S,D}(a_i)$. Then the following are equivalent:

(1) Δ is (S,D)-algebraic;

(1') Each $\Delta^{S,D}(a_i)$ $(1 \leq i \leq n)$ is (S,D)-algebraic;

(2) There is a nonzero right invariant polynomial which is a common left multiple of all $t - a_i$ $(1 \leq i \leq n)$;

(3) There is a nonzero right semi-invariant polynomial which is a common left multiple of all $t - a_i$ $(1 \leq i \leq n)$.

If these conditions hold, the monic f(t) of the least degree as in (2) (or (3)) is exactly the minimal polynomial of Δ. Furthermore, the minimal polynomials f_i of $\Delta^{S,D}(a_i)$ pairwise commute, and we have $f(t) = f_1(t)....f_n(t)$.

[Note. In the standard terminology of [J: p.38], the condition on the a_i's in (2) is that the left ideal $\bigcap_{i=1}^{n} R\cdot(t-a_i)$ be bounded.

In this case, the Corollary asserts that the "bound" of $\bigcap R\cdot(t-a_i)$ is given by $R\cdot f$, and that this is also the product of the bounds of $R\cdot(t-a_i)$ $(1\leq i\leq n)$.]

Proof of (5.4). (1) $\Longleftrightarrow$ (1') follows from the fact that the union of a finite number of algebraic sets is algebraic. But we can also avoid using this fact by proving (1') $\Longrightarrow$ (2) and (3) $\Longrightarrow$ (1), for then we'll have a complete cycle of implications

$$(1)\Longrightarrow(1')\Longrightarrow(2)\Longrightarrow(3)\Longrightarrow(1).$$

(1') $\Longrightarrow$ (2) Let f_i be the minimal polynomial of $\Delta^{S,D}(a_i)$. By (5.3), each f_i is right invariant. It follows that $f_1\cdots f_n$ is right invariant and is a left multiple of each of f_i. Since f_i is a left multiple of $t-a_i$, $f_1\cdots f_n$ gives the candidate for (2).

(3) $\Longrightarrow$ (1) Let $g(t)$ be a right semi-invariant polynomial as in (3). Then $g(a_i) = 0$ $(i\leq 1\leq n)$ implies that $g(\Delta^{S,D}(a_i)) = 0$ by (5.1), and so $g(\Delta) = 0$.

The above arguments also suffice to show that the monic $f(t)$ of the least degree as in (3) (or (2)) is exactly the minimal polynomial of Δ, and that such an f is a right factor of $f_1\cdots f_n$. Since by the Union Theorem in [L] (which extends verbatim to the (S,D)-setting) $\operatorname{rank}\Delta = \sum_{i=1}^{n}\operatorname{rank}\Delta^{S,D}(a_i) = \sum_{i=1}^{n}\deg f_i$, it follows that $f = f_1\cdots f_n$. Applying this in the case $n = 2$, we conclude further that $f_if_j = f_jf_i$ whenever $i \neq j$, since both sides of the equation give the minimal polynomial of $\Delta^{S,D}(a_i)\cup\Delta^{S,D}(a_j)$. Q.E.D.

Before we proceed further with our treatment of algebraic conjugacy classes, let us recall some facts from $[LL_1]$ in a form most suitable for applications in this section.

Lemma 5.5 Let $p(t) \in K[t,S,D]$ and $y \in K^*$. Then

(1) $p(D)(y) = p(0^y)y$;

(2) If $D = 0$, then $p(S)(y) = p(1^y)y$. (Here, $1^y = S(y)y^{-1}$.)

Proof. (1) has been shown in the proof of Cor. 4.3 of $[LL_1]$. For (2), first note that $N_i(1) = 1$ for all $i \geq 0$. (The N_i's are the generalized "power functions" with respect to (S,D): see $[LL_1: §2]$.) From $[LL_1$: Prop. (2.9)(1)] applied to the special case $D = 0$, we have then $N_i(1^y)y = S^i(y)$ for all $i \geq 0$. (This can also be checked by a direct calculation.) Thus, if $p(t) = \sum a_i t^i$, we have

$$p(S)(y) = \sum a_i S^i(y) = \sum a_i N_i(1^y)y = p(1^y)y. \quad \text{Q.E.D.}$$

Let $a \in K$ be a fixed element. Then, for any $c \in K$,

$$\begin{aligned}(t-a)c &= S(c)t + D(c) - ac \\ &= S(c)(t-a) + S(c)a - ac + D(c) \\ &= S(c)(t-a) + D'(c),\end{aligned}$$

where $D' := D - D_{a,S}$. ($D_{a,S}$ denotes the S-inner derivation of K sending y to $ay - S(y)a$.) Therefore, we have a well-defined ring homomorphism

$$\Lambda : K[t',S,D'] \longrightarrow K[t,S,D] \tag{5.6}$$

which is the identity on K and sends t' to $t-a$. Clearly Λ is an isomorphism of rings (with the inverse isomorphism sending t to $t'+a$). Let $g(t')$ be any polynomial in $K[t',S,D']$, and let $f(t) = \Lambda(g(t')) \in K[t,S,D]$. Then

$$(5.7) \qquad \begin{cases} f(t) = \Lambda(g(t')) = g(\Lambda(t')) = g(t-a), \text{ and} \\ g(t') = \Lambda^{-1}(f(t)) = f(\Lambda^{-1}(t)) = f(t'+a). \end{cases}$$

As we have observed in $[LL_1: \S 2]$, the division ring of constants of D' is just $C := C^{S,D}(a)$. The following lemma provides the basic link between the solutions of polynomial equations and the solutions of differential equations in K.

Proposition 5.8. For $f \in K[t,S,D]$ as above, and any $y \in K^*$, we have $g(D')(y) = f(a^y)y$. In particular, the exponential space $E(f, a)$ is exactly the right C-vector space of solutions (in y) of the differential equation $g(D')(y) = 0$.

Proof. We first show that, for any $b \in K$, we have $f(b) = g(b-a)$. (This is a special case of a more general result called the "Composite Function Theorem" in $[LL_2]$.) In fact, write

$$f(t) = q(t)(t-b) + f(b) \qquad \text{where } q(t) \in K[t,S,D].$$

Applying the inverse isomorphism Λ^{-1}, we get

$$g(t') = q(t'+a)(t'-(b-a)) + f(b) \qquad \text{in } K[t',S,D'].$$

Therefore, by the Remainder Theorem (applied to $K[t',S,D']$),

$f(b) = g(b-a)$. Now, let $b = a^y$, where $y \in K^*$. Since

$$\begin{aligned} D'(y)y^{-1} &= \left[D(y) - (ay - S(y)a\right] y^{-1} \\ &= D(y)y^{-1} - a + S(y)ay^{-1} \\ &= a^y - a, \end{aligned}$$

we get $f(a^y) = g(a^y - a) = g(D'(y)y^{-1})$. Therefore, by (5.5)(1) (applied to $g(t') \in K[t', S, D']$), we have

$$f(a^y)y = g(D'(y)y^{-1})y = g(D')(y). \qquad \text{Q.E.D.}$$

Remark 5.9. S. Amitsur [A] has shown that the solutions of the differential equation $g(D')(y) = 0$ form a right C-vector space of dimension $\leq \deg g$. (Amitsur's original arguments worked only in the case when S is an automorphism. A more general argument establishing the result for any endomorphism S can be found in [Co: p.65].) Assuming this result, the above Proposition leads to another proof of the fact that, as a right C-vector space, $E(f, a)$ has C-dimension $\leq \deg f$ (=deg g). This proof is somewhat different in spirit from the proof we gave earlier in [LL_1: Th. (4.2)].

Combining the preceding results with those of §4, we can now give some additional criteria (to (5.4)) for a given (S,D)-conjugacy class $\Delta^{S,D}(a)$ to be algebraic. Since $C^{S,D}(a)$ is just the division ring of the constants of the S-derivation $D' := D - D_{a,S}$, the equivalence of (2) and (3) below is well-known (dating from the work of Amitsur [A]). However, we'll prove this afresh as our arguments will

also yield the exact information relating the minimal polynomials of algebraic conjugacy classes and those of algebraic derivations.

Theorem 5.10. For $a \in K$, the following are equivalent:

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

(2) $\left[K : C^{S,D}(a)\right]_{rt} < \infty$;

(3) $D' := D - D_{a,S}$ is an algebraic S-derivation.

If these conditions hold, then

$$\text{rank } \Delta^{S,D}(a) = \left[K : C^{S,D}(a)\right]_{rt} = \deg (\text{min. poly. of } D').$$

Moreover, if $f(t) \in K[t,S,D]$ is the minimal polynomial of $\Delta^{S,D}(a)$, then the minimal polynomial of D' in $K[t',S,D']$ is given by $f(t' + a)$.

Proof. Let $Y = K^*$. Then $\Delta^{S,D}(a)$ is just a^Y. Since $\text{span}(Y) = K$ as a right $C^{S,D}(a)$-vector space, (1)$\Longleftrightarrow$(2) follows from Prop. (4.2). The last part of this Proposition also gives the equality $\text{rank } \Delta^{S,D}(a) = \left[K : C^{S,D}(a)\right]_{rt}$.

(1)$\Longrightarrow$(3) For the minimal polynomial $f(t)$ of $\Delta^{S,D}(a)$, we have $E(f, a) = K$. Let $g(t') = f(t'+a) \in K[t',S,D']$ so f and g are related as in (5.7). Then Proposition (5.8) gives $g(D') = 0$, so D' is algebraic.

(3)$\Longrightarrow$(1) Let $g_o(t') \in K[t',S,D']$ be the minimal polynomial of D'. Then by (5.8) again, we have $E(f_o, a) = K$ where $f_o(t) := g_o(t-a) \in K[t,S,D]$. This means that $f_o(a^y) = 0$ for all $y \in K^*$, so $\Delta^{S,D}(a)$ is (S,D)-algebraic.

Combining the arguments in the last two paragraphs, it is now clear that $g_o = g \in K[t',S,D']$. Q.E.D.

Let us now record a few consequences of the Theorem. As we have already pointed out, the following consequence (corresponding to the case $a = 0$) is largely classical: cf. [A] and [Le].

Corollary 5.11. D is algebraic iff $[K : K_D] < \infty$ iff the logarithmic derivatives with respect to D form an (S,D)-algebraic class $\Delta^{S,D}(0)$. In this case, the minimal polynomial $g(t) \in K[t,S,D]$ of D is equal to the minimal polynomial of $\Delta^{S,D}(0)$. In particular, g splits completely in $K[t,S,D]$, and an element $b \in K$ is a logarithmic derivative with respect to D iff $g(b) = 0$.

Next, note that the Theorem yields a criterion for the existence of an (S,D)-algebraic class:

Corollary 5.12. K has an (S,D)-algebraic conjugacy class iff D is the sum of an inner S-derivation and an algebraic S-derivation.

[Remark. If D is inner, say $D = D_{a,S}$, then $\Delta^{S,D}(a) = \{a\}$ is obviously an algebraic class. On the other hand, if D is algebraic, then $\Delta^{S,D}(0)$ is an algebraic class (see (5.11)). In general, if $D = D_{a,S} + D'$ where D' is an algebraic S-derivation, then (by the Theorem) $\Delta^{S,D}(a)$ is an algebraic class; moreover, an easy calculation shows that $\Delta^{S,D}(a) = a + \Delta^{S,D'}(0)$.]

If K is a field and $S = I$, then $D_{a,S} = 0$ for every $a \in K$. In this case, the Theorem gives the following:

Corollary 5.13. Let K be a field, and S = I. Then a derivation D on K is algebraic iff one (or all) of the (I,D)-conjugacy classes is (are) algebraic.

To put Theorem (5.10) in perspective, note that, in the classical case when (S,D) = (I,0), the condition that $\Delta^{S,D}(a)$ be algebraic means simply that a is algebraic over the center F of K, and rank $\Delta^{S,D}(a)$ is then given by the field extension degree $[F(a): F]$ (see [L: p.207]). In this case, the equality $[K : C(a)] = [F(a): F]$ is well-known, and is usually stated as a part of the Double Centralizer Theorem. Thus, the Theorem we proved above may be viewed as an extension of some of the consequences of the Double Centralizer Theorem to the (S,D)-setting.

Example. Let K be the division ring of the real quaternions and let S = I, D = 0, and a = -i. Then $\Delta^{S,D}(a)$ is (S,D)-algebraic (by the above) with minimal polynomial $f(t) = t^2+1 \in K[t]$. From (5.10), it follows that the minimal polynomial for the inner derivation $D' = 0 - D_{-i,I} = D_{i,I}$ is

$$\begin{aligned} g(t') = f(t'-i) &= (t'-i)^2 + 1 = t'^2 - it' - t'i \\ &= t'^2 - it' - (it' + D'i) \\ &= t'^2 - 2it' \in K[t',D']. \end{aligned}$$

Next, we shall obtain an analogue (and supplement) to Th. (5.10), in the case when D = 0. Let $a \in K$ be given, and assume $a \neq 0$. Since we now assume D = 0, we have

$$(a^{-1}t)c = a^{-1}S(c)t = a^{-1}S(c)a\cdot a^{-1}t \quad \text{(for any } c \in K^*\text{)}.$$

Writing $I_{a^{-1}}$ for the inner automorphism which sends x to $a^{-1}xa$, we have then $(a^{-1}t)c = \tilde{S}(c)t$ where $\tilde{S} = I_{a^{-1}} \circ S$. Therefore, we have a well-defined ring homomorphism

$$(5.14) \qquad \Gamma : K[\tilde{t},\tilde{S}] \longrightarrow K[t,S]$$

which is the identity on K, and sends $\tilde{t}$ to $a^{-1}t$. As was the case for Λ in (5.6), Γ is an isomorphism, with its inverse sending t to $a\tilde{t}$. For any $h(\tilde{t}) \in K[\tilde{t},\tilde{S}]$, define

$$(5.15) \qquad \begin{cases} f(t) := \Gamma(h(\tilde{t})) = h(a^{-1}t), & \text{so that} \\ h(\tilde{t}) = \Gamma^{-1}(f(t)) = f(a\tilde{t}). \end{cases}$$

We have now the following analogue of Prop. (5.8).

Proposition 5.16. ($D = 0$) With the above notations, we have $f(a^y)y = h(\tilde{S})(y)$ for any $y \in K^*$. In particular, the exponential space $E(f, a)$ is exactly the right $C^S(a)$-vector space of the solutions (in y) of the equation $h(\tilde{S})(y) = 0$. [Note. By (5.8), $E(f, a)$ is also the solution space of the differential equation $g(-D_{a,S})(y) = 0$, where $g(t') = f(t'+a)$.]

Proof. Proceeding as in the proof of (5.8), we can show that $f(t) = h(a^{-1}t) \Longrightarrow f(b) = h(a^{-1}b)$ for every $b \in K$. (Again, this is a special case of the Composite Function Theorem in $[LL_2]$.) Now applying Lemma (5.5)(2) to $h(\tilde{t}) \in K[\tilde{t},\tilde{S}]$, we have, for every $y \in K^*$:

$$h(\tilde{S})(y) = h(\tilde{S}(y)y^{-1})y$$
$$= f(a\tilde{S}(y)y^{-1})y$$
$$= f(a\cdot a^{-1}S(y)ay^{-1})y$$
$$= f(a^{y})y,$$

as desired. Q.E.D.

We have now the following refinement of Th. (5.10) in the case $D = 0$ (and S any endomorphism of K).

Theorem 5.17. ($D = 0$) For $a \in K^*$, the following are equivalent:

(1) $\Delta^S(a) = \{S(c)ac^{-1} : c \in K^*\}$ is S-algebraic;

(2) $[K : C^S(a)]_{rt} < \infty$ (where $C^S(a) = \{c \in K : S(c)a = ac)\}$);

(3) $D_{-a,S}$ is an algebraic S-derivation;

(4) The endomorphism $\tilde{S} = I_{a^{-1}} \circ S$ is algebraic.

If these conditions hold, and $f(t) \in K[t,S]$ is the minimal polynomial of $\Delta^S(a)$, then the minimal polynomial of $D_{-a,S}$ in $K[t',S,D_{-a,S}]$ is $f(t'+a)$, and the minimal polynomial of $\tilde{S}$ in $K[\tilde{t},\tilde{S}]$ is $f(a\tilde{t})$; moreover, S and $\tilde{S}$ must be automorphisms of finite inner order.

Proof. The equivalence of (1), (2), (3) and the relation between the minimal polynomials of $\Delta^S(a)$ and $D_{-a,S}$ follow by specializing (5.10) to the case $D = 0$. The equivalence of (1) with (4) and the relation between the minimal polynomials of $\Delta^S(a)$ and $\tilde{S}$ now follow similarly by applying Proposition (5.16). By [L: Lemma 5], $f(t)$ has the form $(t-a_1)\ldots(t-a_n) \in K[t,S]$ for suitable $a_i \in \Delta^S(a)$.

Therefore, $f(t)$ has constant term $b = a_1 \ldots a_n \neq 0$. By (2.3)(1), it follows that $S^n = I_b$, so S is an automorphism of finite inner order dividing n. Since $\tilde{S}$ has the same inner class as S, the same holds for $\tilde{S}$. Q.E.D.

Remark 5.18. It follows easily from the above that the S-inner derivation $D_{-a,S}$ satisfies a polynomial $g(t') \in K[t', S, D_{-a,S}]$ iff the endomorphism $\tilde{S} = I_{a^{-1}} \circ S$ satisfies the polynomial $h(\tilde{t}) = g(a(\tilde{t}-1)) \in K[\tilde{t}, \tilde{S}]$.

Letting $a = 1$ in Theorem (5.17), we get:

Corollary 5.19. ($D = 0$) The set $\{S(c)c^{-1} : c \in K^*\}$ is S-algebraic iff $[K : K^S]_{rt} < \infty$, iff $S - I$ is an algebraic S-derivation, iff S is an algebraic endomorphism. For any of these conditions to hold, S must be an automorphism of finite inner order.

(If S is assumed to be an automorphism of K to begin with, the implication that $[K : K^S]_{rt} < \infty \Longrightarrow S$ has finite inner order is, of course, a well-known fact in the Galois theory of division rings (see, e.g. [Co: p.47]).

Going back to the general (S,D)-setting, let us now give some simple characterizations for the minimal polynomials of the (S,D)-algebraic conjugacy classes in K.

Theorem 5.20. For a monic non-constant polynomial $f(t) \in R$, the following are equivalent:

(1) $f(t)$ *is the minimal polynomial of an* (S,D)*-algebraic conjugacy class* $\Delta^{S,D}(a)$;

(2) $f(t)$ *is right invariant, has a zero in* K, *and has no proper left or right factor which is right invariant;*

(3) $f(t)$ *is right semi-invariant, has a zero in* K, *and has no proper right factor which is right invariant.*

Proof. (2) $\Longrightarrow$ (3) is a tautology.

(3) $\Longrightarrow$ (1) Let $a \in K$ be a root of f. Then by (5.1), $f(\Delta^{S,D}(a)) = 0$ and so f is right divisible by f_o, the minimal polynomial of $\Delta^{S,D}(a)$. Since f_o is right invariant, (3) implies that $f = f_o$.

(1) $\Longrightarrow$ (2) We already know that f is right invariant, and that f has a root (namely, a). Consider the simple left R-module $V = R/R\cdot(t-a)$. We shall identify V with K via the correspondence $\overline{g(t)} \longmapsto g(a)$. Viewing K as a left R-module through this identification, the action of a polynomial $g(t) \in R$ on an element $c \in K^*$ is given by

$$g(t) * c = g(t)c \Big]_{t=a} = g(a^c)c, \tag{5.21}$$

by the Product Theorem in $\left[LL_1: (2.7)\right]$. In particular,

$$\begin{aligned} \operatorname{ann}_R V &= \left\{ g(t) \in R : \; g(a^c) = 0 \quad \forall\, c \in K^* \right\} \\ &= \left\{ g(t) \in R : \; g(\Delta^{S,D}(a)) = 0 \right\} \\ &= R\cdot f \,. \end{aligned} \tag{5.22}$$

Therefore, V is a *faithful* simple left $R/R\cdot f$-module. Since $R/R\cdot f$ is artinian, it follows that $R/R\cdot f$ is a simple ring. This means

that $R \cdot f$ is maximal as a 2-sided ideal in R, and so f has no proper right factor which is right invariant. It follows from this that f has also no proper left factor which is right invariant. Q.E.D.

The observation we made in the proof above about the simple left R-module $R/R \cdot (t-a)$ (for any a) have also some other consequences which are worth recording. If a is such that $\Delta^{S,D}(a)$ is not (S,D)-algebraic, the first two equalities in (5.22) would show that $R/R \cdot (t-a)$ is a faithful simple left R-module. Therefore, we have:

Corollary 5.23. $R = K[t,S,D]$ is a left primitive ring unless all (S,D)-conjugacy classes are algebraic. (In particular, $K[t]$ is a left primitive ring unless K is algebraic over its center.)

Also, whether $\Delta^{S,D}(a)$ is algebraic or not, for any polynomial $g(t) \in R$, the annihilator of g on K identified with $V = R/R \cdot (t-a)$ as a left R-module is (by (5.21)) exactly

$$\{0\} \cup \{c \in K^* : g(a^c) = 0\} = E(g, a).$$

This gives a very interesting new interpretation for the exponential space $E(g, a)$, which was pointed out to us by Professor S. Amitsur during the Conference. In fact, as Professor Amitsur further pointed out, the fact that $\dim_C E(g, a) \leq \deg g$ for $C = C^{S,D}(a)$ can be deduced from the Jacobson-Chevalley Density Theorem, upon noting that C is isomorphic to $\mathrm{End}_R V$ as a ring of right operators on V. This deduction is a rather illuminating exercise which we shall leave to the reader. Let us now make two additional remarks. First, in the

case when $\Delta^{S,D}(a)$ is algebraic with minimal polynomial f, the Artin-Wedderburn Theorem implies that

$$R/R\cdot f \cong \mathrm{End}_C\,(R/R\cdot(t-a)) \cong \mathbb{M}_n(C),$$

where $n = [K : C]_{rt} = \deg f$. Secondly, whether $\Delta^{S,D}(a)$ is algebraic or not, it is also possible to derive from the Density Theorem some of the key facts in §4 relating the P-dependence of elements in $\Delta^{S,D}(a)$ to the right C-linear dependence of the elements of K. However, we do not feel justified to include the details of these alternative proofs here.

To conclude this section, we shall now combine Theorem (5.20) with Cauchon's result (Theorem 2.8) to derive some more interesting information on the minimal polynomials of (S,D)-algebraic classes. We first make the following easy observation on $Z(R)$ (the center of $R = K[t,S,D]$) which is essentially well-known:

Lemma 5.24. If $Z(R)$ contains a polynomial $h(t) = \alpha^{-1}t^n + \ldots.$ of degree $n \geq 1$, then $S^n = I_\alpha$ and $S(\alpha) = \alpha$.

Proof. For any $c \in K$, we have $(\alpha^{-1}t^n + \ldots.)c = c(\alpha^{-1}t^n + \ldots.)$. Comparing leading coefficients, we get $\alpha^{-1}S^n(c) = c\alpha^{-1}$, so $S^n = I_\alpha$. Similarly, $(\alpha^{-1}t^n + \ldots.)t = t(\alpha^{-1}t^n + \ldots.)$ leads to $S(\alpha^{-1}) = \alpha^{-1}$. Q.E.D.

In case $D = 0$ and S is not an automorphism of finite inner order, we have shown in Theorem (5.17) that K has only one S-algebraic

conjugacy class, namely, $\Delta^S(0) = \{0\}$, with minimal polynomial t. Using Cauchon's Theorem (2.8) and Theorem (5.20), we can now generalize this fact to the case where D need not be zero.

Theorem 5.25. Assume that S is not an automorphism of finite inner order. (This includes the case when S is not onto.) Then there is at most one (S,D)-algebraic class $\Delta^{S,D}(a)$, and if such a class exists, its minimal polynomial $f(t)$ is a non-constant right invariant polynomial of the least degree.

Proof. Look at an algebraic class $\Delta^{S,D}(a)$ with minimal polynomial $f(t)$, and let $q(t)$ be a monic non-constant right invariant polynomial of the least degree, as in (2.8). Since by (5.24) there is no non-constant central polynomial, (2.8) and (5.20) imply that $f(t) = q(t)$; in particular, $\Delta^{S,D}(a)$ is unique (if it exists). Q.E.D.

Remark 5.26. It can be shown that the $f(t)$ above has, in fact, minimal degree among all non-constant right semi-invariant polynomials. We shall not prove this fact here since it does not follow directly from the techniques developed in this paper.

Finally, we treat the case when S is an automorphism of finite inner order.

Theorem 5.27. Let S be an automorphism of finite inner order k. Then, for all (S,D)-algebraic classes $\Delta^{S,D}(a)$ with possibly one exception, the following holds:

(1) The minimal polynomial $f(t)$ of $\Delta^{S,D}(a)$ lies in $K \cdot Z(R)$;

(2) $f(t)$ commutes with all monic right semi-invariant polynomial; and

(3) The rank of $\Delta^{S,D}(a)$ is divisible by k.

Finally, the rank of any (S,D)-algebraic class is divisible by $\deg q(t)$, where $q(t)$ is a monic non-constant right invariant polynomial of the least degree.

Proof. By (2.8), the minimal polynomial $f(t)$ of any algebraic class $\Delta^{S,D}(a)$ has the form $\alpha \cdot h(t)q(t)^r$, where $\alpha \in K^*$, $h(t) \in Z(R)$ and $r \geq 0$. Bringing (5.20) to bear, we see that $f(t)$ is either equal to $q(t)$ or $\alpha \cdot h(t)$. Thus, with the possible exception of one class, $\Delta^{S,D}(a)$ has minimal polynomial $f(t) = \alpha \cdot h(t) = \alpha(\alpha^{-1}t^n + \ldots)$, where $n = \deg h$. By (5.24), we must have $S^n = I_\alpha$ and $S(\alpha) = \alpha$. The former implies that $n = \text{rank } \Delta^{S,D}(a)$ is a multiple of the inner order k of S. To prove the property (2), let $g(t)$ be any monic right semi-invariant polynomial, say of degree m. Then we have

$$g(t)f(t) = g(t)\alpha h(t) = S^m(\alpha)g(t)h(t)$$
$$= \alpha h(t)g(t) = f(t)g(t),$$

as claimed. Finally, since in any case $f(t)$ is either $\alpha \cdot h(t)$ or $q(t)$, the last part of Cauchon's Theorem (2.8) implies that $n = \deg f$ is always divisible by $\deg q$. Q.E.D.

Note that part (2) above strengthens the fact, first proved in Proposition (5.4), that the minimal polynomials of two distinct (S,D)-

algebraic classes always commute. This fact is now an obvious consequence of (5.27)(2) when S is an automorphism of finite inner order, and, in view of (5.25), is vacuous when S is not an automorphism of finite inner order.

Of course, in Theorem (5.27), an "exceptional" (S,D)-algebraic class may indeed exist, and it would behave somewhat differently from the other algebraic classes. For instance, let K be a field with an automorphism S of order k, and let $F = K^S$. Then, in the notation of (2.8) (with $D = 0$), we have $q(t) = t$, $h_o(t) = t^k$ in $R = K[t,S]$, and $Z(R) = F[t^k]$. Any class $\Delta^S(a)$ with $a \in K^*$ has rank k and minimal polynomial $t^k - N_{K/F}(a)$ (see [L: p.208]), but the "exceptional" class $\Delta^S(0) = \{0\}$ has rank 1 and minimal polynomial $q(t) = t$. The former kind of minimal polynomials clearly all belong to $Z(R)$, but $q(t) = t$ does not. In fact, t fails to commute with all monic right semi-invariant polynomials: for instance, $t^k + a$ $(a \in K)$ is always right semi-invariant, but t does not commute with it unless $a \in F$.

References

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

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

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

[Ca] J. Carcanague, Idéaux bilatères d'un anneau de polynômes non commutatifs sur un corps, J. Algebra 18(1971), 1-18.

[Co] P. M. Cohn, Skew Field Constructions, London Math. Soc. Lecture Notes Series, Vol. 27, Cambridge University Press, 1977.

[Co'] P. M. Cohn, Free Rings and Their Relations, Academic Press, New York, 1971.

[J] N. Jacobson, The Theory of Rings, Mathematical Surveys, No.2, Amer. Math. Soc., Providence, R.I., 1943.

[L] T. Y. Lam, A general theory of Vandermonde matrices, Expositiones Mathematicae 4(1986), 193-215.

[Le] A. Leroy, Dérivées logarithmiques pour une S-dérivation algébrique, Communications in Algebra 13(1985), 85-99.

[Lem] B. Lemonnier, Dimension de Krull et codéviations, quelques applications en théorie des modules, Thèse, Poitiers, 1984.

[LL_1] T. Y. Lam and A. Leroy, Vandermonde and Wronskian matrices over division rings, to appear in Journal of Algebra.

[LL_2] T. Y. Lam and A. Leroy, Hilbert 90-type theorems for division rings, in preparation.

[LM] A. Leroy and J. Matczuk, Dérivations et automorphismes algébriques d'anneaux premiers, Communications in Algebra 13(1986), 1245-1266.