PRINCIPAL ONE-SIDED IDEALS IN ORE POLYNOMIAL RINGS

T. Y. LAM AND ANDRÉ LEROY

Abstract. For an endomorphism S of a division ring K and an S-derivation D on K, the Ore extension $R = K[t, S, D]$ consisting of left polynomials $\sum_i a_i t^i$ $(a_i \in K)$ is well known to be a principal left ideal domain, although, in the case when $S(K) \neq K$, R is not a principal right ideal domain (or even a right Ore domain). Using the theory of evaluation of left polynomials on scalars developed in our earlier papers, we define $f \in R$ to be a *Wedderburn polynomial* if f is the minimal polynomial of some (S, D)-algebraic subset of K. We note that Wedderburn polynomials are special cases of "fully reducible" elements in 2-firs. In this paper, we prove a general theorem on 2-firs which implies (in a very explicit way) that the class of Wedderburn polynomials in $R = K[t, S, D]$ is "symmetric" with respect to the left and right ideal structures of R. This 2-fir approach to R also enables us to develop a theory of *left* roots of the polynomials in R. This theory bears some resemblance to the theory of right roots studied in our earlier papers, but has a number of surprising new features.

§1. Introduction

The study of the (so-called) skew polynomial rings $K[t, S, D]$ goes back to the seminal paper of Ore [Or] in 1933. For the purposes of this paper, K is a division ring, S is an endomorphism of K, and D is an S-derivation of K; that is, an additive map from K to itself such that $D(ab) = S(a)D(b) + D(a)b$ for all a, $b \in K$. The Ore extension $R := K[t, S, D]$ consists of (left) polynomials $\sum_i a_i t^i$ $(a_i \in K)$, which are added in the usual way, and multiplied via the distributive law and Ore's commutation rule $ta = S(a)t + D(a)$ (for any $a \in K$). The important role played by Ore extensions in the study of division rings can perhaps be gauged from the fact that Jacobson's authoritative treatment of finite-dimensional division algebras [Ja$_2$] begins with a

Date: July 9, 1999.

1991 *Mathematics Subject Classification.* Primary 16D40, 16E20, 16L30; Secondary 16D70, 16E10, 16G30.

The research reported in this paper was partially supported by a grant from NSA (T.Y.L.) and a faculty grant from the Université d'Artois at Lens (A.L.).

long chapter on the basic theory of $K[t,S,D]$, which Jacobson used freely in his text.

It is well known that in the Ore extension R, one can "right-divide" a polynomial f by another polynomial $h \neq 0$ via an euclidean algorithm: $f = qh + r$, where either $r = 0$ or $\deg(r) < \deg(h)$. From this, it follows easily that R is a PLID (principal left ideal domain). However, it is also widely known that, if $S(K) \neq K$ (i.e. when S fails to be an automorphism of K), then left division does not work, and R is not a PRID (principal right ideal domain). To see the latter, we simply note that if a_i $(i \in I)$ are elements of K that are right linearly independent over $S(K)$, then the linear polynomials $a_i t \in R$ $(i \in I)$ are right linearly independent over R [La$_3$: p. 295].[1] Thus, in the case $S(K) \neq K$, R provides an example (possibly the most often quoted one) of a PLID that is not a right Ore domain. Along the same lines, many authors have constructed counterexamples in ring theory using one way or another Ore extensions $R = K[t,S,D]$ in the case $S(K) \neq K$. One realistic consequence of the failure of R to be a PRID in general is that the many pleasant arithmetic results on two-sided principal ideal domains (as developed, for instance, in [Ja$_1$, Ja$_2$] and [Co$_2$]) cannot be directly applied to R.

In this paper, we introduce a class $\mathcal{W}$ of polynomials, called *Wedderburn polynomials*, in the Ore polynomial ring R. These are polynomials in R which arise as minimal polynomials of (right) (S,D)-algebraic subsets of K. (For more details, see the beginning of §2.) In terms of the left ideal structure of R, $\mathcal{W}$ can be described as follows. Let $\mathcal{W}^\ell$ be the family of monic polynomials $f \in R$ such that Rf is an (arbitrary) intersection of principal left ideals of the form $R(t-a)$ $(a \in K)$, and let $\mathcal{W}_0^\ell$ be the family of monic polynomials $f \in R$ such that $Rf = R(t-a_1) \cap \cdots \cap R(t-a_n)$, where $a_i \in K$ and $n = \deg(f)$. It is not difficult to see that $\mathcal{W} = \mathcal{W}^\ell = \mathcal{W}_0^\ell$ (Proposition 2.6). Now, by using right (instead of left) principal ideals, we can similarly define two families of monic polynomials $\mathcal{W}^r$ and $\mathcal{W}_0^r$. In §4, we'll show that $\mathcal{W} = \mathcal{W}^r = \mathcal{W}_0^r$. This "symmetry" result serves to show that the family $\mathcal{W}$ of Wedderburn polynomials is sufficiently intrinsic to the ring R to be characterizable in terms of either its left structure or its right structure. This is possibly a bit surprising in view of the disparity that seems to exist between these two structures.

[1] In [La$_3$], the proof of this is given in the case $D = 0$. However, an easy modification of the proof taking the derivation into account will show that the conclusion holds good in general.

The proof for $\mathcal{W} = \mathcal{W}^r = \mathcal{W}_0^r$ is based on a general result on 2-firs proved in §3 (Theorem 3.6). (The definitions for 2-firs and semifirs are recalled in §3; for more details, we refer the reader to P. M. Cohn's book [Co$_1$].) A special feature of this result is that it gives us a *direct* way to go from an "irredundant" representation of fR ($f \in \mathcal{W}_0^r$) as an intersection of principal right ideals $(t-b)R$ to an irredundant representation of Rf as an intersection of principal left ideals $R(t-a)$, and vice versa if $f \in \mathcal{W}_0^\ell$. An interesting byproduct of these considerations is a theory of *left* roots of polynomials. Some aspects of this theory are similar to those in the theory of right roots developed in our earlier papers, but a number of surprising new features do emerge. This theory of left roots is presented in detail in the last two sections, §§5-6.

We stress again that the value of the results in this paper lies in the fact that they hold true in general *without any assumptions on* S. In the special case when S is an automorphism, R can be converted into an Ore ring of *right* polynomials $\sum_i t^i a_i$, with the new commutation rule $bt = t\,S^{-1}(b) - DS^{-1}(b)$ (for any $b \in K$). This implies (as in the case of left polynomials) that R is also a PRID. In this case, the desired results are usually much easier to obtain, and the 2-fir approach would not be really necessary.

The notations $\mathcal{W}^\ell$, $\mathcal{W}_0^\ell$, $\mathcal{W}^r$, $\mathcal{W}_0^r$ and $\mathcal{W}$ introduced above will be fixed throughout the paper. Also, R will always denote the Ore polynomial ring $K[t, S, D]$, except in §3. For any ring A, $\mathrm{U}(A)$ denotes the group of units of A. If A is a domain and x, y are elements of A, it is known that $A/Ax \cong A/Ay$ (as left A-modules) iff $A/xA \cong A/yA$ (as right A-modules) [Co$_1$: p. 28]. In this case, we say that the elements x, y are *similar* (in A). Other standard terminology and notations in ring theory can be found in [Co$_1$], [La$_2$] and [La$_3$].

§2. Algebraic Sets and the Family $\mathcal{W}$

We begin this section by studying the family of minimal polynomials of the left (S, D)-algebraic subsets of K. To define these terms, let us first recall the theory of "evaluation" of left polynomials at scalars, developed in our earlier paper [LL$_1$]. In this work, a uniquely determined scalar $f(a)$ is associated to any polynomial $f \in R = K[t, S, D]$ and any $a \in K$. Instead of reviewing the entire theory of evaluation, however, it will suffice for us to recall some of its main properties. The first is the Remainder Theorem [LL$_1$: (2.4)]:

$$f(t) = q(t)(t-a) + f(a), \tag{2.1}$$

where $q(t) \in R$ is uniquely determined by f and by a. ¿From this, it follows that f is right divisible by $t-a$ iff $f(a)=0$. (In this case, we say that a is a (right) root of f.) The second fact we need is the powerful Product Formula [LL$_1$: (2.7)] for evaluating $f=gh$ at any $a \in K$:

$$(2.2) \qquad (gh)(a) = \begin{cases} 0 & \text{if} \quad h(a)=0, \\ g(a^{h(a)})h(a) & \text{if} \quad h(a) \neq 0. \end{cases}$$

Here, for any $c \in K^*$, a^c denotes $S(c)ac^{-1}+D(c)c^{-1}$, which is called the (S,D)-*conjugate* of a (by c). With this general conjugation notation, it is easy to verify by a direct calculation that

$$(2.3) \qquad (a^c)^d = a^{dc} \quad \text{for any } c,\ d \in K^*.$$

¿From this, it follows readily that (S,D)-conjugacy is an equivalence relation. Another elementary formula involving (S,D)-conjugation is the following, which will turn out to be quite useful for the rest of the paper.

Lemma 2.4. *For any $b \in K$ and $d \in K^*$, $S(d)(t-b) = (t-b^d)\,d$ in R.*

Proof. Since $td = S(d)t + D(d)$ and $b^d\,d = S(d)b + D(d)$, we have

$$S(d)(t-b) = td - D(d) - S(d)b = (t-b^d)\,d,$$

as claimed. □

An immediate nice consequence of (2.4) is the following proposition on the relationship between (S,D)-conjugacy in K and the notion of similarity in R.

Proposition 2.5. *Let $b \in K$. A polynomial $p \in R$ is similar to $t-b \in R$ iff $p = a(t-b^c)$ for some $a,\ c \in K^*$.*

Proof. First assume p has the form $a(t-b^c)$, where $a,\ c \in K^*$. By (2.4),

$$R(t-b^c)c = R{\cdot}S(c)(t-b) = R(t-b).$$

Therefore, right multiplication by c defines a left R-module isomorphism from $R/Rp = R/(t-b^c)$ to $R/R(t-b)$, so p is similar to $t-b$. Conversely, suppose p is similar to $t-b$. Then $R/Rp \cong R/R(t-b)$ has left K-dimension 1, so p is linear. Write $p = a(t-b')$ ($a \in K^*$, $b' \in K$), and let φ be an R-isomorphism from $R/Rp = R/R(t-b')$ to $R/R(t-b)$. If we set $\overline{c} = \varphi(\overline{1})$, then

$$0 = \varphi\big((t-b')\,\overline{1}\big) = (t-b')\overline{c} \in R/R(t-b)$$

implies that $(t-b')c \in R(t-b)$. Evaluating $(t-b')c$ at b using (2.2), we get $0=(b^c-b')c$. Thus, $b'=b^c$, and $p=a(t-b^c)$, as desired. $\square$

Next, we review the notion of *right* (S,D)*-algebraic* (or simply "algebraic") subsets. A subset $\Delta \subseteq K$ is said to be algebraic if there exists a nonzero polynomial $f \in R$ such that $f(\Delta)=0$ (that is, $f(a)=0$ for every $a \in \Delta$). In this case, the *minimal polynomial* of Δ is defined to be the unique monic polynomial f_Δ of the least degree vanishing on Δ. By the euclidean algorithm for right division, f_Δ generates the left ideal of all polynomials vanishing on Δ. It is known that f_Δ always factors into $(t-a_1)\cdots(t-a_n)$, where each $a_i \in K$ is (S,D)-conjugate to some element of Δ [LL$_2$: §4]. The number $n=\deg(f_\Delta)$ here is called the *rank* of the algebraic set Δ, and will be abbreviated by $\mathrm{rk}(\Delta)$.

Polynomials of the form f_Δ (for algebraic subsets $\Delta \subseteq K$) are called *Wedderburn polynomials* (or W-polynomials for short) with respect to the triple (K,S,D). The family of such polynomials is denoted by $\mathcal{W}$; our nomenclature is in honor of Wedderburn's classical work [We]. For further motivation and various examples of W-polynomials, we refer the reader to our more detailed work [LL$_3$]. In this paper, we are primarily interested in issues surrounding the left-right symmetry of W-polynomials. We begin with the following easy proposition which relates $\mathcal{W}$ to the two families $\mathcal{W}^\ell$ and $\mathcal{W}_0^\ell$ defined in the Introduction (via principal left ideals of the form $R(t-a)$).

Proposition 2.6. $\mathcal{W}=\mathcal{W}^\ell=\mathcal{W}_0^\ell$.

Proof. If Δ is algebraic, then, by the right-division algorithm (and in particular (2.1)),

$$Rf_\Delta = \bigcap_{a\in\Delta} R(t-a).$$

Thus, $f_\Delta \in \mathcal{W}^\ell$. Conversely, if $f \in \mathcal{W}^\ell$, say $Rf=\bigcap_{i\in I} R(t-a_i)$, we conclude similarly that the set $\{a_i:\ i \in I\}$ is algebraic, and that f is its minimal polynomial. This shows that $\mathcal{W}=\mathcal{W}^\ell$. To show that these are also equal to $\mathcal{W}_0^\ell$, we proceed as follows.

In [LL$_2$] (and [La$_1$]), we have developed, in the general (S,D)-setting, a full theory of *polynomial independence* (or P-independence) for elements in K. Here, we shall only need the notion of a "P-basis". For any algebraic set Δ of rank n, there always exists a subset $\{a_1,\ldots,a_n\} \subseteq \Delta$ that has the same minimal polynomial as Δ; any such subset is called a *P-basis* of Δ (see [LL$_2$: §4]). The existence of such P-bases implies immediately that $\mathcal{W}^\ell = \mathcal{W}_0^\ell$. □

At this point, it is not clear how to deduce the similar equation for $\mathcal{W}^r$ and $\mathcal{W}_0^r$, since the theory of algebraic sets and their minimal polynomials is so far developed on one side only and not on the other. The left structure of R is easy to work with since R is a PLID, but in general R is not a PRID. We can think of the polynomials $f \in \mathcal{W}^r$ as monic least *right* common multiples of a set $\mathcal{F}$ of polynomials of the form $t - a$ $(a \in K)$ (just as we have done for $\mathcal{W}^\ell$ using least left common multiples), but there is not yet a theory of algebraic sets and P-bases *on the left* to enable us to readily replace $\mathcal{F}$ by a finite set of cardinality equal to $\deg(f)$. Also, there is no obvious way to relate $\mathcal{W}^r$ directly to the more easily understood $\mathcal{W}^\ell$. Thus, the remaining equalities $\mathcal{W} = \mathcal{W}^r = \mathcal{W}_0^r$ stated in the Introduction will have to await further analysis (in the next two sections).

Let us now give a few more facts about right (S, D)-algebraic sets (which will eventually be extended to left ones). For any polynomial $f \in R$, we'll write $V(f)$ for the set of its (right) zeros in K. To begin with, it is easy to see that *f is a W-polynomial iff $f = f_{V(f)}$*. The other characterizations for W-polynomials offered in the Proposition below are almost as straightforward.

Proposition 2.7. *For a monic polynomial $f \in R$ of degree n, the following are equivalent*:

(1) *f is a W-polynomial*;

(2) $\mathrm{rk}(V(f)) = n$;

(3) *For any $q \in R$, $V(f) \subseteq V(q) \Longrightarrow q \in R \cdot f$.*

Proof. (1) $\Longrightarrow$ (3). Assume f is a W-polynomial. If $V(f) \subseteq V(q)$, q vanishes on $V(f)$, so $f = f_{V(f)}$ is a right factor of q.

(3) $\Longrightarrow$ (2). By (3), any (nonzero) polynomial vanishing on $V(f)$ has degree $\geq n$. Thus, $\mathrm{rk}(V(f)) \geq n$, and (2) follows.

(2) $\Longrightarrow$ (1). In general, $f \in R \cdot f_{V(f)}$. By (2), $f_{V(f)}$ has degree n, so we must have $f = f_{V(f)}$; that is, f is a W-polynomial. □

One nice fact about Wedderburn polynomials is the "Factor Theorem", which states that, *if $f = f_1 g f_2 \in R$ where g is monic, then $f \in \mathcal{W}$ implies $g \in \mathcal{W}$.* This theorem can be deduced from the work of Ore [Or: Ch. 2, Theorem 4] (see also [Co$_1$: p. 189]). In the following, we give first a simple proof for the "left factor" version of this result, using properties of right zeros of polynomials. (We'll return to the general case later in (5.9).)

Left factor Theorem 2.8. *If f is a W-polynomial, then so is any monic left factor g of f.*

The main ingredient of the proof is the following general observation on the right zeros of polynomials.

Lemma 2.9. *For any polynomials g, h, $q \in R$, we have*

$$V(g) \subseteq V(q) \Longrightarrow V(gh) \subseteq V(qh).$$

Proof. Assuming $V(g) \subseteq V(q)$, consider any $a \in V(gh)$. If $h(a) = 0$, then clearly $a \in V(qh)$. Therefore, we may assume that $h(a) \neq 0$. By the Product Formula (2.2) (applied to gh), we must have $g\big(a^{h(a)}\big) = 0$. But then $q\big(a^{h(a)}\big) = 0$, and so the Product Formula (applied now to qh) shows that $a \in V(qh)$. □

Proof of (2.8). Suppose $f = gh \in \mathcal{W}^\ell$. To see that $g \in \mathcal{W}^\ell$, it suffices to show, in view of (2.7), that

$$\forall\, q \in R: \quad V(g) \subseteq V(q) \Longrightarrow q \in R \cdot g.$$

Assume that $V(g) \subseteq V(q)$. By (2.9), we have $V(gh) \subseteq V(qh)$. Since $gh = f \in \mathcal{W}^\ell$, (2.7)(3) shows that $qh \in R \cdot gh$. Right cancelling h, we get $q \in R \cdot g$, as desired. □

Based on (2.9), one might wonder if perhaps $V(g) \subseteq V(q)$ *also* implies $V(hg) \subseteq V(hq)$. But this implication is easily seen to be false by examples. Take, for instance, $g(t) = t - i$ and $q(t) = (t - j)(t - i)$ over the quaternions (with $(S, D) = (I, 0)$). Clearly, $V(g) \subseteq V(q)$. Choosing $h(t) = t + i$, we have $j \in V(hg) = V(t^2 + 1)$, but $j \notin V(hq)$ since an explicit calculation shows that $(hq)(j) = 2(i + j) \neq 0$. This "counterexample", however, should not cause any alarm. As it turns out, the analogue for Lemma 2.9, with the multiplier h on the *left*, will be correct as soon as we turn our attention from right zeros to *left* zeros (assuming that g is a monic polynomial). With such an analogue, one can then prove the *right* factor version of (2.8) in the same way as above (and thereby deduce the general factor theorem: see (5.9)). Situations such as this suggest strongly the desirability of a theory of left roots for the polynomials in R, applicable to the case where S is any endomorphism of K. Such a theory will be presented in §§5-6 below.

§3. Results on 2-Firs

In order to prove the left-right symmetry of Wedderburn polynomials (and to get a broader perspective on these polynomials in general), we shall exploit the notion of an n-fir due to P. M. Cohn. A ring R is said to be an *n-fir* if any left ideal of R generated by (at most) n elements is R-free of a unique rank. According to Cohn [Co$_1$: p. 65], n-fir is a left-right symmetric notion [and an n-fir (for $n \geq 1$) is always a domain]. If R is an n-fir for every integer n, we say that R is a *semifir.* The case of particular interest to us is that of a PLID (principal left ideal domain). Such a ring is clearly an n-fir for every n, and so it is a semifir. This observation applies, in particular, to the Ore polynomial ring $K[t, S, D]$.

For all intents and purposes, the consideration of 2-firs (instead of a semifir) will suffice for this section. In a 2-fir R, it is well known that, whenever $aR \cap bR \neq 0$, then $aR \cap bR$ and $aR + bR$ are both *principal* right ideals (see [Co$_1$: p. 80]). This crucial property of 2-firs will be used freely below without further mention. We shall now derive some other properties of 2-firs which will be useful to our study of Wedderburn polynomials. *Through the rest of this section, R will denote a 2-fir.*

Lemma 3.1. *Let $p \in R$ be an atom*[2]*, and let $q \in R$ be such that $q \notin pR$ and $pR \cap qR \neq 0$. Then $pR + qR = R$.*

Proof. Write $pR + qR = dR$ and $p = dr$, where $d, r \in R$. If $r \in \mathrm{U}(R)$, then $pR = drR = dR = pR + qR$, which contradicts $q \notin pR$. Thus, $r \notin \mathrm{U}(R)$, and we must have $d \in \mathrm{U}(R)$ (since p is an atom). From this, it follows that $pR + qR = dR = R$. □

Lemma 3.2. *If $p \in R$ is an atom, and $y \in R$ is similar to p (that is, $R/pR \cong R/yR$), then y is also an atom.*

Proof. First note that $y \notin \mathrm{U}(R)$, and also $y \neq 0$. (If $y = 0$, then R/pR is free of rank 1. This is not the case, as $\overline{1} \cdot p = 0 \in R/pR$.) Fix an R-isomorphism $\varphi : R/yR \longrightarrow R/pR$, say with $\varphi(\overline{1}) = \overline{q} \in R/pR$. Then

$$0 = \varphi(\overline{y}) = \overline{q}y \in R/pR \implies (0 \neq)\, qy = px \quad \text{(for some } x \in R\text{)}.$$

Consider *any* factorization $y = ab$, where $b \notin \mathrm{U}(R)$. Then, since $px = qy = qab$ is not zero, $pR \cap qaR \neq 0$. Also, $b \notin \mathrm{U}(R)$ shows that

[2] An *atom* in a domain R is an element which is nonzero and not a unit, and which is not a product of two nonunits in R.

$a \notin yR$, so $\overline{0} \neq \varphi(\overline{a}) = \overline{qa} \in R/pR$; that is, $qa \notin pR$. Thus, by Lemma 3.1, we have $pR + qaR = R$. Since φ is an isomorphism, this implies that $R = yR + aR = aR$, and hence $a \in \mathrm{U}(R)$. This shows that y is an atom. □

Remark 3.3. We included the statement (and a proof) of Lemma 3.2 above since we did not find this result in [Co$_1$]. The fact that we made rather heavy use of the 2-fir property in the proof of (3.2) suggests that this result is not true in general for 1-firs (i.e. domains). Indeed, in the Weyl algebra $\mathbb{R}\langle u, v\rangle$ with the relation $uv - vu = 1$, the elements $p = 1 + uv$ and $y = uv$ are similar. Here, p is an atom, but y is not (see [Co$_1$: p. 169]).

Proposition 3.4. *Let $p \in R$ be an atom, and let $q \in R$ be such that $q \notin pR$ and $pR \cap qR \neq 0$. Write $pR \cap qR = fR$, and $f = px = qy$ $(x, y \in R)$. Then* (1) *y is an atom similar to p, and* (2) *$Rf = Rx \cap Ry$.*

Proof. (1) The rule $\overline{1} \mapsto \overline{q}$ gives a well-defined R-homomorphism $\varphi : R/yR \longrightarrow R/pR$ (since $qy = px$). By Lemma 3.1, $pR + qR = R$, so φ is surjective. Also

$$\begin{aligned} \varphi(\overline{c}) = 0 &\implies qc \in pR \cap qR = fR \\ &\implies qc = fr = qyr \quad (\text{for some } r \in R) \\ &\implies c = yr \in yR \\ &\implies \overline{c} = 0 \in R/yR, \end{aligned}$$

so φ is also injective. Thus, φ is an isomorphism, and Lemma 3.2 shows that y is an atom (similar to p).

(2) Write $Rx \cap Ry = Rgx$ for some $g \in R$, and write $gx = hy$. Then

$$Rpx = Rf \subseteq Rx \cap Ry = Rgx \implies Rp \subseteq Rg.$$

Say $p = sg$ where $s \in R$. If $g \in \mathrm{U}(R)$, then $x = g^{-1}hy$ and hence $qy = px = pg^{-1}hy$. This leads to $q = pg^{-1}h \in pR$, which is not the case. Since p is an atom, we must have then $s \in \mathrm{U}(R)$. Thus, $Rf = Rpx = Rsgx = Rgx = Rx \cap Ry$. □

For any right ideal $A \subseteq R$ and any element $q \in R$, we'll use the standard notation $q^{-1}A$ for the set $\{r \in R : \ qr \in A\}$. It is easy to check that $q^{-1}A$ is a right ideal in R. The fact that q^{-1} may not exist in R should cause no serious problem for this notation. In case

q^{-1} does exist in R, the two possible interpretations for $q^{-1}A$ will be totally consistent.[3]

Corollary 3.5. *Let p be an atom, and $q \notin pR$. Then either $q^{-1}(pR) = 0$ or $q^{-1}(pR) = yR$ for some atom y similar to p.*

Proof. It is easy to see that (in any ring R and for every p, q):

$$(*) \qquad pR \cap qR = q\big(q^{-1}(pR)\big).$$

If $q^{-1}(pR) \neq 0$, then $pR \cap qR = fR$ for some $f \neq 0$. Write $f = px = qy$ as before. Then, by the Proposition, y is an atom similar to p, and $q\big(q^{-1}(pR)\big) = fR = qyR$ implies that $q^{-1}(pR) = yR$. □

We now come to the main result of this section, which deals with the class of fully reducible elements in R. By definition, a nonzero nonunit element $f \in R$ is (left) *fully reducible* if the principal left ideal Rf can be written as an (arbitrary) intersection $\bigcap_i Rp_i$, where the p_i's are atoms in R. This notion is of interest to us since, in the case when $p_i = t - a_i$ in $R = K[t, S, D]$, we retrieve, up to left scalar factors, the W-polynomials of the Ore polynomial ring (by (2.6)). The notion of fully reducible elements in $K[t, S, D]$ goes back to the work of Ore [Or].[4] In the case when S is an *automorphism* of K, Ore showed that "fully reducible" is a left-right symmetric notion for the ring $K[t, S, D]$. More generally, Cohn showed in [Co$_1$: p. 189] that the same is true for any atomic 2-fir (that is, a 2-fir in which any nonzero nonunit element is a finite product of atoms). Using this result of Cohn, one can check easily that the two families $\mathcal{W}^\ell$ and $\mathcal{W}^r$ are equal in $K[t, S, D]$, for *any* endomorphism S of K. However, for a fuller understanding of Wedderburn polynomials and their left-right symmetry, it will be desirable to prove a more *constructive* version of Cohn's result. This is done in the theorem below, where we'll consider only *finite* intersections of one-sided ideals generated by atoms. Recall that such an intersection is called *irredundant* if the intersection becomes bigger upon the omission of any of the intervening one-sided ideals.

Theorem 3.6. *Suppose $0 \neq fR = p_1R \cap \cdots \cap p_nR$ is an irredundant intersection, where the p_i's are atoms in R. If we write $\bigcap_{j \neq i} p_jR = g_iR$ and $f = g_ik_i$ $(1 \leq i \leq n)$, then*

[3] Also, the case $q = 0$ need not be excluded, as $0^{-1}A$ is simply R according to the definition given.

[4] In [Or], Ore called these elements "completely reducible". The somewhat shorter name "fully reducible" comes from [Co$_1$].

(1) *for each* i, k_i *is an atom similar to* p_i ;
(2) $Rf = \bigcap_{i=1}^{n} Rk_i$; *and*
(3) *the intersection representation for* Rf *in* (2) *is irredundant.*

Proof. We induct on n, the case $n = 1$ being clear. In the following, let $n \geq 2$. We have $g_n k_n = f = p_n h$ for some $h \in R$. We have $g_n \notin p_n R$ (for otherwise $fR = g_n R = p_1 R \cap \cdots \cap p_{n-1} R$, contradicting the irredundancy assumption). Since p_n is an atom and $p_n R \cap g_n R = fR \neq 0$, Prop. 3.4 implies that $Rf = Rk_n \cap Rh$ and that k_n is an atom similar to p_n. By symmetry, it follows that each k_i is an atom similar to p_i.

For any $j < n$, write $0 \neq p_j R \cap p_n R = p_n d_j R$. By Prop. 3.4 again, each d_j is an atom, and we have

$$\begin{aligned} p_n h R = fR &= \big(\textstyle\bigcap_{j<n} p_j R\big) \cap p_n R \\ &= \textstyle\bigcap_{j<n} (p_j R \cap p_n R) \\ &= \textstyle\bigcap_{j<n} (p_n d_j R) \\ &= p_n \big(\textstyle\bigcap_{j<n} d_j R\big). \end{aligned}$$

This implies that $(0\neq) hR = \bigcap_{j<n} d_j R$. By the same calculation, done with one index $i < n$ omitted, we also see that $\bigcap_{i\neq j<n} d_j R \supsetneqq hR$. Thus, the representation $hR = \bigcap_{j<n} d_j R$ is irredundant. For each $i < n$, let us write $\bigcap_{i\neq j<n} d_j R = q_i R$. Then

$$p_n q_i R = p_n \big(\bigcap_{i\neq j<n} d_j R\big) = \bigcap_{i\neq j<n} (p_j R \cap p_n R) = \big(\bigcap_{i\neq j<n} p_j R\big) \cap p_n R = g_i R,$$

so we can write $g_i = p_n q_i u_i$ for some units $u_i \in \mathrm{U}(R)$. Now for any $i < n$,

$$p_n h = f = g_i k_i = p_n q_i u_i k_i \implies h = q_i (u_i k_i).$$

Therefore, applying the inductive hypothesis to $hR = \bigcap_{j<n} d_j R$, we get

$$Rh = \bigcap_{i<n} R\, u_i k_i = \bigcap_{i<n} Rk_i\,, \tag{3.7}$$

and that this is an irredundant representation for Rh. Therefore,

$$Rf = Rh \cap Rk_n = \bigcap_{i=1}^{n} Rk_i\,,$$

as claimed. Finally, $\bigcap_{i\neq n} Rk_i = Rh \supsetneqq Rf$, and so by symmetry $\bigcap_{i\neq j} Rk_i \supsetneqq Rf$ for each j; that is, $Rf = \bigcap_{i=1}^{n} Rk_i$ is an irredundant representation for Rf. □

Remarks 3.8.

(1) Since the notion of a 2-fir is left-right symmetric, it follows that the analogue of (3.6) going from an irredundant representation of Rf to one for fR is also valid. This observation will be used freely in the following.

(2) In the case of an *atomic* 2-fir, it is easy to see that, if an intersection $A = \bigcap_i p_i R$ is nonzero (where the p_i's are atoms), then $A = \bigcap_{i \in I} p_i R$ for some finite set of indices I (and similarly for left ideals). Also, by picking I to be minimal, we may assume that this representation is irredundant. In this case, Theorem 3.6 yields directly the left-right symmetry of fully reducible elements in R.

§4. Applications to Wedderburn Polynomials

To apply the results of §3 to Wedderburn polynomials, we return now to the notation $R = K[t, S, D]$ used in the earlier sections. Since R is a PLID, it is clearly an atomic semifir, so Theorem (3.6) and Remark (3.8)(2) both apply. The latter implies, in particular, that we can replace any *nonzero* intersection $\bigcap_i p_i(t)R$ in R by a finite subintersection. This fact (which is actually clear from the presence of the degree function on $R \setminus \{0\}$) will be used freely below. To apply (3.6) more efficiently, we'll need the following observation on monic polynomials.

Lemma 4.1. *A principal right ideal $A \subseteq R$ is generated by a monic generator iff A contains a monic polynomial.*

Proof. We need only prove the "if" part. Assume that $A = hR$ contains a monic polynomial, say $f = h\big(a_m t^m + a_{m-1} t^{m-1} + \cdots\big)$, where $a_m \neq 0$. Since

$$f = (ha_m)\big(t^m + a_m^{-1} a_{m-1} t^{m-1} + \cdots\big),$$

ha_m must be a monic polynomial. We have $A = hR = (ha_m)R$, so ha_m is a monic generator for A. □

We shall use Theorem (3.6) only in the case when f is a monic polynomial, and the atoms $p_i \in R$ are of the form $t - b_i$ ($b_i \in K$, $1 \leq i \leq n$). Under the assumptions of (3.6), let us write $f = p_i h_i = (t - b_i)h_i$ for each i; then, h_i is also monic. (The "h" used in the proof of (3.6) is just h_n.) For each i, the g_i in (3.6) was picked to be a generator for $\bigcap_{j \neq i} p_j R$. Since this intersection contains the monic polynomial f, g_i can be chosen to be *monic* by (4.1). If indeed g_i

is so chosen, then the k_i's defined by the equations $f = g_i k_i$ in (3.6) are also monic. Now by (3.6)(1), k_i is similar to $p_i = t - b_i$; this implies that $R/Rk_i \cong R/Rp_i$. Computing (left) K-dimensions of both sides, we see that $\deg(k_i) = \deg(p_i) = 1$, and thus $k_i = t - a_i$ for some $a_i \in K$.[5] Taking all of these simplifications into account, we can state the following more specific version of (3.6) in the case when $p_i = t - b_i \in R = K[t, S, D]$.

Theorem 4.2. *Suppose $f \in R$ is a monic polynomial such that fR has an irredundant representation as $\bigcap_{i=1}^n (t - b_i)R$. Write*

$$f = (t - b_i)h_i = g_i(t - a_i) \quad (1 \le i \le n),$$

where g_i is a monic generator for $\bigcap_{j \ne i}(t - b_j)R$, for every i. Then Rf has an irredundant representation as $\bigcap_{i=1}^n R(t - a_i)$. Furthermore, we must have:

(1) $n = \deg(f)$;
(2) h_i *is the minimal polynomial of* $\{a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}$; *and*
(3) $b_i = a_i^{h_i(a_i)}$ *for every* i.

Proof. Everything follows from (3.6), except the additional conclusions (1), (2) and (3). For (1), we use the *irredundant* representation $Rf = \bigcap_{i=1}^n R(t - a_i)$. This representation of Rf shows that $\{a_1, \ldots, a_n\}$ is a P-independent set with minimal polynomial f. Therefore, $\deg(f) = n$. For (2), note that in the proof of (3.6), we have shown that $Rh_i = \bigcap_{j \ne i} R(t - a_j)$ for $i = n$, and therefore for every $i \in \{1, \ldots, n\}$. Moreover, we know that this is an irredundant representation. We can thus conclude, as above, that h_i is the minimal polynomial of $\{a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}$. In particular, $h_i(a_i) \ne 0$. Evaluating $f = (t - b_i)h_i$ at a_i, we get (by (2.2)):

$$0 = f(a_i) = \left(a_i^{h_i(a_i)} - b_i\right) h_i(a_i),$$

and therefore $b_i = a_i^{h_i(a_i)}$, as asserted in (3). □

A byproduct of the above considerations is the following.

Corollary 4.3. *If $0 \ne fR = c_1(t - b_1)R \cap \cdots \cap c_m(t - b_m)R$ (where $f \in R$ and c_i, $b_i \in K$), then $m \ge \deg(f)$.*

[5] If we invoke the full version of (2.5) here, we can say further that a_i is (S, D)-conjugate to b_i. This appeal to (2.5) is, however, not necessary since we'll actually be able to get a more precise formula relating a_i and b_i in (4.2)(3) below.

Proof. After a scaling from the left, we may assume that f is monic. Taking an irredundant representation

$$fR = c_{i_1}\big(t-b_{i_1}\big)R \cap \cdots \cap c_{i_n}\big(t-b_{i_n}\big)R$$

where $\{i_1, \ldots, i_n\} \subseteq \{1, \ldots, m\}$, we have (by (4.2)(1)) $\deg(f) = n \leq m$. □

Of course, we can also apply the analogue of (3.6) to $R = K[t, S, D]$ for the passage from left ideals to right ideals (in the case of monic linear atoms). The situation is basically symmetrical, but we can state the conclusions a little more succinctly in terms of minimal polynomials, as follows.

Theorem 4.4. *Suppose $f \in R$ is monic and Rf has an irredundant representation as $R(t-a_1) \cap \cdots \cap R(t-a_n)$. (In other words, f is the minimal polynomial of the P-independent set $\{a_1, \ldots, a_n\}$; in particular, $n = \deg(f)$.) If h_i is the minimal polynomial of $\{a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}$, then, for $b_i := a_i^{h_i(a_i)}$ $(1 \leq i \leq n)$, we have an irredundant representation $fR = \bigcap_{i=1}^{n}(t-b_i)R$.*

Needless to say, the statements of (4.2) and (4.4) were designed to explain the exact relationship between $\mathcal{W}_0^r$ and $\mathcal{W}_0^\ell$. In fact, by combining (2.6), (3.8)(2) with (4.2) and (4.4), we obtain a rather "constructive" proof of the following main result stated in the Introduction:

Theorem 4.5. $\mathcal{W} = \mathcal{W}^\ell = \mathcal{W}_0^\ell = \mathcal{W}^r = \mathcal{W}_0^r$.

§5. Theory of Left Roots for Ore Polynomials

Having seen that the Wedderburn polynomials can be described in terms of either the left or the right structure of the ring $R = K[t, S, D]$, we are now in a position to extend the theory of right roots to a theory of left roots for the polynomials in $R = K[t, S, D]$. The evaluation $f(a)$ of a polynomial f at $a \in K$ discussed in §2 may be called "right evaluation"; but there is no corresponding theory of "left evaluation" (in the general case when S is an arbitrary endomorphism of K). Recalling, however, that $f(a) = 0$ iff $f \in R(t-a)$ (we said a is a right root of f in this case), we can introduce the following definition:

Definition 5.1. We say that $b \in K$ is a *left root* (or *left zero*) of $f \in R$ if $f \in (t-b)R$. (In this case, we'll also say that f *left-vanishes on* b.) The set of all left roots of f will be denoted by $V'(f)$.

In the case of right zeros, the following fact is of paramount importance: If $a \in K$ is a right zero of $f = gh$ but is not a right zero of h, then some (S, D)-conjugate of a is a right zero of g. This fact is an immediate consequence of the Product Formula (2.2). Now we do not have a theory of left evaluations of polynomials (and in particular no analogue of (2.2)), but it turns out that a suitable analogue of the fact stated above *does* hold for left roots. The proof of this will be preceded by the following Proposition, which is really a consequence of our eralier 2-fir result (3.5).

Proposition 5.2. *Let* $A := h^{-1}\big(a(t-b)R\big)$*, where* $h \notin a(t-b)R$*, and* $a, b \in K$*. Then there exist* $a' \in K$ *(possibly zero) such that* $A = a'(t-b)R$*. Moreover,* A *contains a monic polynomial iff* $A = (t-b^d)R$ *for some* $d \in K^*$*.*

Proof. If $h^{-1}\big(a(t-b)R\big) = 0$, we are done by choosing $a' = 0$. Now assume $h^{-1}\big(a(t-b)R\big) \neq 0$. Then, by (3.5), $h^{-1}\big(a(t-b)R\big) = kR$ for some atom k similar to $t-b$ in R. By (2.5), k has the form $a_1(t-b^c)$ for some a_1, $c \in K^*$. Now by (2.4),

$$a_1(t-b^c)R = a_1(t-b^c)cR = a_1S(c)(t-b)R,$$

so the first conclusion follows by choosing $a' = a_1S(c) \in K^*$. For the second conclusion, it suffices to prove the “if” part. Assume that $A = a'(t-b)R$ contains a monic polynomial. By considering such a polynomial, we see easily that a' must have the form $S(d)$ for some $d \in K^*$. Then by (2.4) again,

$$A = S(d)(t-b)R = \big(t-b^d\big)dR = (t-b^d)R,$$

as desired. □

If a nonzero polynomial g has leading coefficient s, we can write $g = sg_0$ for a unique monic polynomial $g_0 \in R$; we shall call g_0 the *monic part* of g. This terminology and notation will be used in the result below, as well as occasionally in the rest of the paper.

Theorem 5.3. *Let* $f = hg \in R$*, where* $g \neq 0$*. If* $b \in V'(f)$ *but* $b \notin V'(h)$*, then* $b^d \in V'(g_0)$ *for some* $d \in K^*$*.*

Proof. The hypotheses on b give $hsg_0 = f \in (t-b)R$, and $hs \notin (t-b)R$. Since $g_0 \in (hs)^{-1}\big((t-b)R\big)$ is monic, the second part of (5.2) implies that $(hs)^{-1}\big((t-b)R\big)$ has the form $(t-b^d)R$ for some $d \in K^*$. Therefore, $g_0 \in (t-b^d)R$, and we have $b^d \in V'(g_0)$, as desired. □

Corollary 5.4. *If* $f = (t - a_1) \cdots (t - a_n) \in R$, *then any* $a \in V'(f)$ *is* (S, D)*-conjugate to some* a_i.

Proof. This follows immediately from (5.3) by induction on n. □

With the aid of (5.3), we can now prove the following left-multiplier analogue of (2.9) (for left zero sets).

Proposition 5.5. *Let* g, $h, q \in R$. *If* g *is monic, then*

$$(\dagger) \qquad V'(g) \subseteq V'(q) \Longrightarrow V'(hg) \subseteq V'(hq).$$

Proof. We apply here (5.3) instead of (2.2). Suppose that $V'(g) \subseteq V'(q)$ and let $b \in V'(hg)$. We may assume that $b \notin V'(h)$ (for otherwise we have already $b \in V'(hq)$). As in the proof of (5.3), we have $h^{-1}\big((t-b)R\big) = (t - b^d)R$ (for some $d \in K^*$), and $g \in (t - b^d)R$. But then $b^d \in V'(g) \subseteq V'(q)$, that is,

$$q \in (t - b^d)R = h^{-1}\big((t-b)R\big).$$

This yields $hq \in (t - b)R$, as desired. □

Remark 5.6. The monicity assumption on g in (5.5) is reasonable. In fact, if g has leading coefficient *not* in $S(K)$, it is easy to see that $V'(g) = \emptyset$ (cf. (5.10)(2) below), so the condition $V'(g) \subseteq V'(q)$ becomes vacuous. In this case, of course, the implication statement (†) cannot be true.

Using the notion of left roots of polynomials, we can now proceed to define *left* algebraic sets with respect to the triple (K, S, D). As we'll see from the following definition, there are two kinds of such sets to be considered.

Definition 5.7. A set $\Delta \subseteq K$ is said to be *left quasi-algebraic* (resp. *left algebraic*) if some nonzero polynomial (resp. *monic* polynomial) left-vanishes on Δ. (Instead of "left quasi-algebraic", we'll just say "quasi-algebraic" below. Note that there is no confusion possible since there is no need to talk about the notion of "right quasi-algebraic.")

In view of Remark (3.8)(2), *any* intersection $\bigcap_{b \in \Delta} (t-b)R$ is principal (possibly zero). If Δ is quasi-algebraic, then $\bigcap_{b \in \Delta}(t - b)R = fR$ for a *nonzero* polynomial f. Here, f is determined up to a right scalar multiple; we shall write *any such* f as ${}_{\Delta}f$, and call it *a minimal polynomial* of the quasi-algebraic set Δ. (This terminology is justified since f is indeed of the smallest degree among all nonzero polynomials left-vanishing on Δ). In the case when Δ is left algebraic (and only in that case), ${}_{\Delta}f$ can be chosen to be a *monic* polynomial (see (4.1)). We shall *always* choose ${}_{\Delta}f$ to be monic in this case, and call it *the* minimal polynomial of Δ. By (4.5), $\{{}_{\Delta}f : \Delta \subseteq K \text{ left algebraic}\}$ is just the set $\mathcal{W}$ of Wedderburn polynomials defined earlier. It will be of interest also to describe the family $\mathcal{W}' := \{{}_{\Delta}f : \Delta \subseteq K \text{ quasi-algebraic}\}$. For instance, how is this family related to $\mathcal{W}$?

First, we have the following easy proposition characterizing the polynomials in $\mathcal{W}'$ and $\mathcal{W}$ in terms of left roots. Its proof can be omitted since it is completely similar to that of (2.7).

Proposition 5.8. *A nonzero polynomial f belongs to $\mathcal{W}'$ iff $f = {}_{V'(f)}f$, and iff, $\forall\, q \in R$, $V'(f) \subseteq V'(q) \Longrightarrow q \in fR$. Such a polynomial belongs to $\mathcal{W}$ iff it is monic.*

With (5.8) in place, we can now easily derive the following result, the second part of which is the general Factor Theorem.

Theorem 5.9. *Suppose f is a W-polynomial. Then* (1) *so is any monic right factor of f.* (2) *In fact, if $f = f_1 g f_2$ where g is monic, then g is a W-polynomial.*

Proof. The "Right Factor Theorem" (1) can be proved from (5.5) and (5.8), in exactly the same way as the Left Factor Theorem (2.8) was proved from (2.7) and (2.9). After this, the general Factor Theorem (2) can be deduced as follows. Say $f = f_1 g f_2$, where g is monic. Write $f_2 = c f_3$, where f_3 is monic and $c \in K^*$ (the leading coefficient of f_2). Since $f = (f_1 g c) f_3$, $f_1 g c$ is monic, and hence in $\mathcal{W}$ by (2.8). Write $gc = c'g'$ for some monic $g' \in R$, and some $c' \in K^*$. Then $f_1 g c = (f_1 c')g' \in \mathcal{W}$ implies that $g' \in \mathcal{W}$, by (1). Now from $gc = c'g'$, the Product Formula yields $V(g) = V(g')^c$. From this and the fact that $g' \in \mathcal{W}$, we see easily that $g \in \mathcal{W}$, as desired. □

There are at least a few other ways to prove the Factor Theorem; see, e.g. [Or], [Co$_1$: p. 189], or [LL$_3$]. The point of the above presentation is, however, not so much to prove Factor Theorem alone, but to show that we have actually achieved enough left-right symmetry in the study of the ring $K[t, S, D]$ to give a proof of the Factor Theorem that works equally well on both sides.

We now come back to the question of relating $\mathcal{W}'$ to $\mathcal{W}$. The full answer to this question will be given in (5.12) below as a corollary of the following proposition on scaling.

Proposition 5.10. (1) *If $g \in R$ and $a = S(d)$ where $d \in K^*$, then $V'(ag) = V'(g)^d$.* (2) *For $f \in R$ with leading coefficient $a \in K^*$, let us write $f = af_0$ (f_0 being the "monic part" of f). If a has the form $S(d)$ where $d \in K^*$, then $V'(f) = V'(f_0)^d$; otherwise, $V'(f) = \emptyset$.*

Proof. If $b \in V'(g)$, then by (2.4),

$$ag \in a(t-b)R = S(d)(t-b)R = (t-b^d)R,$$

so $b^d \in V'(ag)$. This shows that $V'(g)^d \subseteq V'(ag)$. Replacing g by ag and a by a^{-1}, we also get $V'(ag)^{d^{-1}} \subseteq V'(a^{-1}ag) = V'(g)$, and conjugation by d gives the other inclusion $V'(ag) \subseteq V'(g)^d$. This proves the equality in (1). The first part of (2) follows immediately from this, and the second part is clear, since any polynomial of the form $(t-b)h$ $(h \in R)$ has leading coefficient in $S(K)$. □

Corollary 5.11. *For $\Delta \subseteq K$ and $d \in K^*$, Δ is quasi-algebraic iff Δ^d is. In this case, we have $S(d)\big({}_{\Delta}f\big) = {}_{\Delta^d}f$.*

Proof. The first conclusion follows since, by (5.10)(1), $g \in R$ left-vanishes on Δ iff ag left-vanishes on Δ^d. The second conclusion follows from this by taking $g \neq 0$ in this statement to be of the smallest possible degree. □

Corollary 5.12. *Let $f = af_0$ be a nonconstant polynomial, where f_0 is the monic part of f. Then $f \in \mathcal{W}'$ iff $a \in S(K)$ and $f_0 \in \mathcal{W}$.*

Proof. If $f \in \mathcal{W}'$, say $f = {}_{\Delta}f$, then $\Delta \neq \emptyset$, and so by (5.10)(2), $a \in S(K)$. By (5.11), $f_0 = a^{-1}f$ is also in $\mathcal{W}'$; since f_0 is monic, this gives $f_0 \in \mathcal{W}$. Conversely, if $f_0 \in \mathcal{W}$ and $a \in S(K)$, then (5.11) implies that $f = af_0 \in \mathcal{W}'$. □

The next result accounts for the exact relationship between quasi-algebraic sets and left algebraic sets.

Proposition 5.13. *A set Δ is quasi-algebraic iff Δ^e is left algebraic for some $e \in K^*$.*

Proof. The "if" part follows from the first statement of (5.11). To prove the "only if" part, we may assume that $\Delta \neq \emptyset$. Let $f = {}_{\Delta}f$, and write $f = af_0$ where f_0 is the monic part of f. By (5.12), we have $a = S(d)$ for some $d \in K^*$, and $f_0 \in \mathcal{W}$. Then $\Delta \subseteq V'(f) = V'(af_0) = V'(f_0)^d$. Letting $e = d^{-1}$ and conjugating this by e, we get $\Delta^e \subseteq V'(f_0)$. Since $V'(f_0)$ is left algebraic, so is Δ^e. □

We conclude this section with the following result relating the left root and right root sets of a polynomial in $\mathcal{W}'$.

Proposition 5.14. *For any polynomial $f \in \mathcal{W}'$, we have the following:*

(1) *Any left root $x \in V'(f)$ is (S, D)-conjugate to a right root of f;*

(2) *Any right root $y \in V(f)$ is (S, D)-conjugate to a left root of f;*

(3) *If $z \in K$ is a "middle root" of f, in the sense that $f \in R(t-z)R$, then z is (S, D)-conjugate to a left root, and also to a right root, of f.*

Proof. Write $f = af_0$ as in (5.12), where $f_0 \in \mathcal{W}$, and $a = S(d)$ $(d \in K^*)$.

(1) Write $f = (t-x)g$. Then $V(g) \subsetneq V(f) = V(f_0)$ (for, if equality holds, then g right-vanishes on $V(f_0)$, which is impossible). Take any element $c \in V(f) \setminus V(g)$. Using the Product Formula (2.2), we see from $f(c) = 0$ that $x = c^{g(c)}$.

(2) Writing $f = h(t-y)$, we have $V'(h) \subsetneq V'(f)$ by an argument similar to that given in (1). Take an element $b \in V'(f) \setminus V'(h)$. Since $t - y$ is monic, we see from (5.3) that $y = b^r$ for some $r \in K^*$.

(3) (This part, of course, contains (1) and (2); but its proof depends on both of these.) Write $f = h(t-z)g$, and $g = e^{-1}g_0$, where g_0 is the monic part of g. Then by (2.4):

$$f_0 = a^{-1}h(t-z)e^{-1}g_0 = a^{-1}h\,S(e^{-1})\big(t - z^e\big)g_0$$

implies that $h_0 := a^{-1}h\,S(e^{-1})\big(t - z^e\big) \in \mathcal{W}$, by the Left Factor Theorem (2.8). Therefore, by (2) above (applied to h_0), some (S, D)-conjugate $\big(z^e\big)^s \in V'(h_0)$. But by (5.10) (noting that $a^{-1} = S(d^{-1})$):

$$V'(h_0) \subseteq V'(f_0) = V'(a^{-1}f) = V'(f)^{d^{-1}}.$$

Thus, by (2.3), we have $z^{se} \in V'(f)^{d^{-1}}$, and hence $z^{dse} \in V'(f)$. By (1), z^{dse} is also (S, D)-conjugate to a right root of f. □

Remark 5.15. The three statements in (5.14) are not true for *general* polynomials in R. On the other hand, they are true for various other classes of polynomials besides $\mathcal{W}'$. We'll return to this theme in a later paper.

§6. Criteria for Finite Left Algebraic and Quasi-Algebraic Sets

This section will be devoted to a detailed discussion of finite left algebraic (and quasi-algebraic) sets, and their minimal polynomials. Early in this discussion, we'll discover one major difference between the left theory and the right theory of polynomials in R. For the right side, we know previously that every finite set in K is right algebraic; it turns out that this is no longer the case on the left side. The question of *when* a set Δ is quasi-algebraic or left algebraic is, therefore, of interest already in the case when Δ is finite. In this section, we shall provide inductive answers to this question.

The crucial structure to look at here is the partition of K into $S(K)$-cosets. Since $S(K)$ is a division subring, and therefore an additive subgroup, of K, it makes sense to talk about the additive cosets of $S(K)$ in K. Throughout this section, $S(K)$-cosets of K will be in this sense. The theory of left roots becomes harder (and more subtle) in the case when $S(K) \neq K$. The consideration of the $S(K)$-cosets, in part, reflects the additional difficulties encountered in this theory.

The first half of this section deals with the case of left algebraic sets. Our goal here is to give an inductive description of the finite left algebraic sets (in (6.9) below). We begin by noting that any singleton set $\{a\}$ is clearly left algebraic (and quasi-algebraic), with minimal polynomial $t-a$. The next case is that of a doubleton.

Proposition 6.1. *For $\Delta = \{a,\, b\} \subseteq K$, we have:*

(1) $(t-a)^{-1}\,(t-b)R = (a-b)^{-1}\,(t-b)R \neq 0$;

(2) Δ *is quasi-algebraic, with* ${}_{\Delta}f = (t-a)(a-b)^{-1}(t-b)$ *if* $a \neq b$. (*Recall that* ${}_{\Delta}f$ *is only determined up to a right scalar multiple.*)

Proof. Observe that, for any right ideal $A \subseteq R$ and any $g,\, h \in R$:

$$g \equiv h \ (\mathrm{mod}\ A) \Longrightarrow g^{-1}A = h^{-1}A. \tag{6.2}$$

This gives (1) since $t-a \equiv b-a$ (mod $(t-b)R$). Using (1) in conjunction with the general equation $(*)$ in the proof of (3.5), we get

$$(t-a)R \cap (t-b)R = (t-a)(a-b)^{-1}(t-b)R \neq 0, \tag{6.3}$$

and hence Δ is quasi-algebraic. Note that so far, everything said is formally correct even in the case $a=b$. (In this case, the two sides of (1) are R, and the two sides of (6.3) are $(t-a)R$: see Footnote (3).) From (6.3), we see that f_{Δ} is $t-a$ in case $a=b$, and is $(t-a)(a-b)^{-1}(t-b)$ in case $a \neq b$. □

Remark 6.4. Of course, by symmetry, we could also have taken ${}_{\Delta}f$ to be $(t-b)(b-a)^{-1}(t-a)$ in case $a \neq b$. This means that

$$(t-a)(a-b)^{-1}(t-b) = (t-b)(b-a)^{-1}(t-a)\varepsilon$$

for some $\varepsilon \in K^*$. Comparing leading coefficients shows quickly that $\varepsilon = -1$. This leads to an interesting quadratic identity:

$$(6.5) \qquad (t-a)(a-b)^{-1}(t-b) = (t-b)(a-b)^{-1}(t-a) \in R.$$

To get a feeling for this identity, consider the case when $R = K[t]$ (ordinary polynomial ring). Equating the constant coefficients, we get the identity

$$(6.6) \qquad a(a-b)^{-1}b = b(a-b)^{-1}a.$$

This is indeed true (in any ring R in which $a-b \in \mathrm{U}(R)$), although not exactly trivial. (On the other hand, the equation (6.6) for all rings in which $a-b$ is a unit also implies (6.5), by replacing a by $t-b$, and b by $t-a$.)

Corollary 6.7. *A doubleton set $\Delta = \{a, b\} \subseteq K$ is left algebraic iff $a - b \in S(K)$. (This implies, in particular, that the left algebraicity of $\{a, b\}$ depends only on the endomorphism S, and not on the S-derivation D.)*

Proof. If $a-b = S(d^{-1})$, say, then by (6.3) and (2.4):

$$(t-a)R \cap (t-b)R = (t-a)S(d)(t-b)R = (t-a)(t-b^d)R.$$

Thus, Δ is left algebraic (with ${}_{\Delta}f = (t-a)(t-b^d)$). Conversely, if Δ is left algebraic, say with (monic) minimal polynomial f, then by (6.1)(2),

$$fd = (t-a)(a-b)^{-1}(t-b) \quad (\text{for some } d \in K^*).$$

Comparing leading coefficients, we get $S^2(d) = S((a-b)^{-1})$, and hence $a - b = S(d^{-1}) \in S(K)$. □

The Corollary above says that $\{a, b\}$ is left algebraic iff a and b lie in the same $S(K)$-coset. Since any subset of a left algebraic set is (clearly) left algebraic, we deduce immediately the following.

Corollary 6.8. *Any left algebraic set $\Delta \subseteq K$ lies in a single $S(K)$-coset. Equivalently, the left zeros of any monic polynomial in R always lie in a single $S(K)$-coset.*

With the aid of (6.8), we can now give the following inductive description of a finite left algebraic set.

Theorem 6.9. *Let $\Delta = \{b_1, \ldots, b_n\} \subseteq K$ where the b_i 's are distinct. Then Δ is left algebraic iff there exist $d_2, \ldots, d_n \in K^*$ such that $b_1 - b_i = S(d_i^{-1})$ $(i \geq 2)$ and $\Gamma := \{b_2^{d_2}, \ldots, b_n^{d_n}\}$ is left algebraic. In this case, we have ${}_{\Delta}f = (t - b_1)\big({}_{\Gamma}f\big)$.*

Proof. If Δ is to be left algebraic, it must lie in a single $S(K)$-coset of K (by (6.8)), so we must have $b_1 - b_i = S(d_i^{-1})$ for some (uniquely determined) $d_i \in K^*$ $(i \geq 2)$. With these d_i 's in place, the left algebraicity of Δ amounts to the existence of a monic polynomial $f \in R$ such that $(t - b_1)f \in \bigcap_{i=2}^{n} (t - b_i)R$, or equivalently,

$$\begin{aligned} f &\in \textstyle\bigcap_{i=2}^{n} (t - b_1)^{-1}(t - b_i)R \\ &= \textstyle\bigcap_{i=2}^{n} (b_1 - b_i)^{-1}(t - b_i)R \quad \text{(by (6.1)(1))} \\ &= \textstyle\bigcap_{i=2}^{n} S(d_i)(t - b_i)R \\ &= \textstyle\bigcap_{i=2}^{n} (t - b_i^{d_i})R \qquad\qquad \text{(by (2.4))}. \end{aligned}$$

This amounts precisely to the left algebraicity of $\Gamma := \{b_2^{d_2}, \ldots, b_n^{d_n}\}$. In this case, taking f above to be monic of the smallest degree, we see that the minimal polynomial ${}_{\Delta}f$ is given by $(t - b_1)\big({}_{\Gamma}f\big)$. □

As an illustration of (6.9), we record below the following explicit criterion for a 3-element set to be left algebraic.

Corollary 6.10. *For distinct $a, b, c \in K$, the set $\Delta = \{a, b, c\}$ is left algebraic iff there exist d, $e \in K^*$ such that $a - b = S(d^{-1})$, $a - c = S(e^{-1})$, and $b^d - c^e \in S(K)$.*

Proof. This follows from (6.9) and (6.7). □

Example 6.11. Using (6.10), it is easy to give an example of a set $\{a, b, c\}$ that lies in an $S(K)$-coset but is not left algebraic. Take, for instance, $K = \mathbb{Q}(x)$ with S defined by $S(x) = x^2$ and $D = 0$. Then, for $a = 0$, $b = 1$ and $c = x^2$, we have $\Delta = \{a, b, c\} \subseteq S(K)$ (the identity $S(K)$-coset). Here, $d = -1$, $e = -x^{-1}$, and an easy computation shows that $b^d - c^e = 1 - x \notin S(K)$. Therefore, Δ is *not* left algebraic.

Next, we consider the case of quasi-algebraic sets. Recalling (5.13), we do have the following useful information on quasi-algebraic sets as a consequence of (6.8).

Proposition 6.12. *Any quasi-algebraic set can be (S, D)-conjugated into some $S(K)$-coset of K. Equivalently, for any nonzero polynomial f, there exists $e \in K^*$ such that $V'(f)^e$ lies in some $S(K)$-coset.*

In order to give an inductive description of finite quasi-algebraic sets, we first make the following useful observation.

Lemma 6.13. *Let $b_i \in K$ and $a_i \in K^*$ for $i = 1, 2, \ldots, n$. If $\bigcap_{i=1}^n a_i(t-b_i)R \neq 0$, then $a_1^{-1}a_i \in S(K)$ for all i (that is, all a_i's lie in the same left $S(K^*)$-coset of K^*).*

Proof. Take any nonzero $a_1(t-b_1)f \in \bigcap_{i=2}^n a_i(t-b_i)R$. Then there exist nonzero $g_2, \ldots, g_n \in R$ such that $a_1(t-b_1)f = a_i(t-b_i)g_i$. Comparing leading coefficients of the two sides, we see that $a_1^{-1}a_i \in S(K)$ for all $i \geq 2$ (and of course also for $i = 1$). □

We can now prove the following analogue of Theorem 6.9 for quasi-algebraic sets.

Theorem 6.14. *Let $\Delta = \{b_1, \ldots, b_n\} \subseteq K$ where the b_i's are distinct. Then Δ is quasi-algebraic iff there exist $e_2, \ldots, e_n \in K^*$ such that*

$$(6.15) \qquad (b_1 - b_2)(b_1 - b_i)^{-1} = S(e_i) \quad (i \geq 2)$$

and $\Gamma := \{b_2^{e_2}, \ldots, b_n^{e_n}\}$ is quasi-algebraic. In this case, we have

$$_\Delta f = (t - b_1)(b_1 - b_2)^{-1} \left(_\Gamma f \right).$$

Proof. The quasi-algebraicity of Δ means the existence of a nonzero polynomial $(t-b_1)f$ which lies in $(t-b_i)R$ for all $i \geq 2$. Arguing as in the proof of (6.9), we see that this means $f \in \bigcap_{i=2}^n (b_1-b_i)^{-1}(t-b_i)R$. According to (6.13), a necessary condition for this is that $(b_1-b_2)(b_1-b_i)^{-1} = S(e_i)$ for some $e_i \in K^*$ for $i \geq 2$. (Note that, of course, $e_2 = 1$ here.) With these e_i's in place, we have

$$\begin{aligned} \textstyle\bigcap_{i=2}^n (b_1 - b_i)^{-1}(t - b_i)R &= (b_1 - b_2)^{-1} \textstyle\bigcap_{i=2}^n S(e_i)(t - b_i)R \\ &= (b_1 - b_2)^{-1} \textstyle\bigcap_{i=2}^n \left(t - b_i^{e_i}\right)R, \end{aligned}$$

by (2.4). Thus, Δ is quasi-algebraic iff there exist $e_2, \ldots, e_n$ as in (6.15) such that $\Gamma := \{b_2^{e_2}, \ldots, b_n^{e_n}\}$ is quasi-algebraic. In this case, we see also (as in the proof of (6.9)) that the minimal polynomial $_\Delta f$ is given by $(t - b_1)(b_1 - b_2)^{-1} \left(_\Gamma f \right)$. □

Since a doubleton set is always quasi-algebraic by (6.1)(2),[6] the theorem above simplifies to the following in the case $n = 3$.

Corollary 6.16. *For a, b, c distinct, $\Delta = \{a, b, c\} \subseteq K$ is quasi-algebraic iff $(a-b)(a-c)^{-1} \in S(K)$. (Again, as in (6.7), this implies*

[6] In fact, (6.1)(2) itself can be recovered from (6.14) with $n = 2$.

that the quasi-algebraicity of $\{a, b, c\}$ *depends only on* S*, and not on* D*.)*

Of course, the condition that Δ be quasi-algebraic is *symmetric* in a, b, c. At first sight, the condition $(a-b)(a-c)^{-1} \in S(K)$ above does not "look" symmetric. But by a small miracle, it is. In fact, if we write $\sigma_{a,b,c} = (a-b)(a-c)^{-1} \in K$, then an easy calculation shows that

$$\sigma_{a,b,c} = \sigma_{a,c,b}^{-1}, \quad \text{and} \quad \sigma_{a,b,c} + \sigma_{c,b,a} = 1.$$

These identities show that $\sigma_{a,b,c} \in S(K)$ iff $\sigma_{a',b',c'} \in S(K)$ for any permutation (a', b', c') of (a, b, c).

Corollary 6.17. (1) *If* a, b, c *lie in a single* $S(K)$*-coset of* K*, then* $\{a, b, c\}$ *is always quasi-algebraic.* (2) *If* $\Delta \subseteq K$ *is quasi-algebraic, then either* Δ *lies in a single* $S(K)$*-coset, or no two elements of* Δ *are in the same* $S(K)$*-coset.* (*Equivalently, for any nonzero polynomial* f*, either all left roots of* f *lie in a single* $S(K)$*-coset, or no two left roots lie in the same* $S(K)$*-coset.*)

Proof. (1) In view of (6.1)(2), we may assume that $a \neq c$. From $a - b \in S(K)$ and $a - c \in S(K)$, we have $(a-b)(a-c)^{-1} \in S(K)$, so (6.16) implies that $\{a, b, c\}$ is quasi-algebraic.

(2) Suppose two certain elements, say $a,\ b \in \Delta$, are in an $S(K)$-coset C. Consider a third element $c \in \Delta \setminus \{a, b\}$ (if any). Since $\{a, b, c\} \subseteq \Delta$ is quasi-algebraic, $(a-b)(a-c)^{-1} \in S(K)$ by (6.16). But $a-b \in S(K)$, since $a,\ b \in C$. Therefore, we must have $a - c \in S(K)$, which implies that $c \in C$. □

By (2) of the above Corollary, we see that quasi-algebraic sets Δ come in two flavors: let us say Δ is of type 1 when Δ lies in a single $S(K)$-coset, and of type 2 when no two elements of Δ are in the same $S(K)$-coset. Note that both types are indeed possible for Δ of any finite cardinality. For type 1 this is trivial. (Simply note that, in the case $S(K) = K$, any Δ under consideration is of type 1.) The following example shows the existence of arbitrarily large finite quasi-algebraic sets Δ of type 2.

Example 6.18. Using the same example as in (6.11), let $\Delta = \{a_i\}$ be any finite set of rational numbers. Then Δ is a left algebraic set in the identity coset $S(K)$ of K. By (5.11), the set Δ^x is quasi-algebraic. Here, $a_i^x = S(x)a_i x^{-1} = a_i x$, so $a_i^x - a_j^x = (a_i - a_j)x \notin S(K)$ for $i \neq j$. Thus, no two of the elements in Δ^x are in the same $S(K)$-coset of K, and so Δ^x is (quasi-algebraic) of type 2.

Remarks 6.19. (1) It is worth pointing out that the inductive criterion for quasi-algebraic sets in (6.14) is needed mainly in the type 2 case. If the set $\Delta = \{b_1, \dots, b_n\}$ is known to lie in a single $S(K)$-coset, we can write $b_1 - b_i = S(d_i^{-1})$ for suitable $d_i \in K^*$ $(i \geq 2)$. The same argument for the proof of (6.9) (applied to $f \neq 0$ instead of f monic) shows that Δ is quasi-algebraic iff $\{b_2^{d_2}, \dots, b_n^{d_n}\}$ is quasi-algebraic. This criterion is a little simpler than that given in (6.14).

(2) Using (1) above, it is very easy to produce a 4-element set $\Delta = \{b_1, b_2, b_3, b_4\}$ in some $S(K)$-coset that is not quasi-algebraic. (This will show that (6.17)(1) cannot be further improved.) In fact, taking again the same example (K, S, D) as in (6.11), we can choose $b_1 = 0$, $b_2 = 1$, $b_3 = -1$ and $b_4 = x^2$, which all lie in the identity $S(K)$-coset. In the notation of (1), we have here $d_2 = -1$, $d_3 = 1$, and $d_4 = -1/x$. A simple computation shows that

$$b_2^{d_2} = 1, \quad b_3^{d_3} = -1, \quad \text{and} \quad b_4^{d_4} = x.$$

Since the first two of these lie in the identity $S(K)$-coset and the third does not, (6.17)(2) implies that $\{b_2^{d_2}, b_3^{d_3}, b_4^{d_4}\}$ is *not* quasi-algebraic. It then follows from (1) above that $\{b_1, b_2, b_3, b_4\}$ is also not quasi-algebraic.

In summary, we know that a finite subset $\Delta \subseteq K$ need not be left algebraic or even quasi-algebraic. But if $|\Delta| \leq 1$, then Δ is left algebraic, and if $|\Delta| \leq 2$, then Δ is quasi-algebraic. In case Δ lies in a single $S(K)$-coset, if $|\Delta| \leq 2$, then Δ is left algebraic, and if $|\Delta| \leq 3$, then Δ is quasi-algebraic. The upper bounds used in these statements are the best possible.

References

[Co$_1$] P. M. Cohn: *Free Rings and Their Relations*, 2nd Edition, London Math. Soc. Monograph No. 19, Academic Press, London/New York, 1985.

[Co$_2$] P. M. Cohn: *Skew Fields. Theory of General Division Rings*, Encyclopedia in Math., Vol. 57, Cambridge Univ. Press, Cambridge, 1995.

[Ja$_1$] N. Jacobson: *The Theory of Rings*, Math. Surveys, No. 2, Amer. Math. Soc., Providence, R.I., 1943.

[Ja$_2$] N. Jacobson: *Finite-Dimensional Division Algebras over Fields,* Springer-Verlag, Berlin-Heidelberg-New York, 1996.

[La$_1$] T. Y. Lam: *A general theory of Vandermonde matrices*, Expositiones Mathematicae **4**(1986), 193-215.

[La$_2$] T. Y. Lam: *A First Course in Noncommutative Rings*, Graduate Texts in Math., Vol. **131**, Springer-Verlag, Berlin-Heidelberg-New York, 1991.

[La$_3$] T. Y. Lam: *Lectures on Modules and Rings*, Graduate Texts in Math., Vol. **189**, Springer-Verlag, Berlin-Heidelberg-New York, 1999.

[LL$_1$] T. Y. Lam and A. Leroy: *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119**(1988), 308-336.

[LL$_2$] 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.

[LL$_3$] T. Y. Lam and A. Leroy: *Wedderburn polynomials over division rings,* I, in preparation.

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

[We] J. H. M. Wedderburn: *On division algebras*, Trans. A.M.S. **22**(1921), 129-135.

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

E-mail address: `lam@math.berkeley.edu`

Department of Mathematics, Université d'Artois, 62307 Lens Cedex, France

E-mail address: `leroy@euler.univ-artois.fr`